aws

Guide d’administration

AWS Directory Service

Version 1.0

AWS Directory Service: Guide d’administration

Table of Contents

Qu'est-ce que c'est AWS Directory Service ?

AWS Directory Service propose plusieurs manières d'utiliser Microsoft Active Directory (AD) avec d'autres AWS services. Les annuaires stockent des informations sur les utilisateurs, les groupes et les appareils, et les administrateurs les utilisent pour gérer l'accès aux informations et aux ressources. AWS Directory Service propose plusieurs choix d'annuaires aux clients qui souhaitent utiliser des applications compatibles Microsoft AD ou LDAP (Lightweight Directory Access Protocol) existantes dans le cloud. Il offre également ces mêmes possibilités pour les développeurs qui ont besoin d'un annuaire pour gérer des utilisateurs, des groupes, des appareils et des accès.

Que choisir ?

Vous pouvez choisir des services d'annuaire qui offrent les fonctionnalités et la scalabilité correspondant le mieux à vos besoins. Utilisez le tableau suivant pour déterminer quelle option d' AWS Directory Service annuaire convient le mieux à votre organisation.

Que devez-vous faire ?	AWS Directory Service Options recommandées
J'ai besoin d'Active Directory ou de LDAP pour mes applications dans le cloud	Utilisez AWS Directory Service pour Microsoft Active Directory (Standard Edition ou Enterprise Edition) si vous avez besoin d'une solution Microsoft Active Directory dans le AWS cloud prenant en charge Active Directory les charges de travail compatibles, ou des AWS applicati ons et services tels qu'Amazon et WorkSpaces Amazon QuickSight, ou si vous avez besoin d'un support LDAP pour les applications Linux. Utilisez AD Connector uniquement si vous devez autoriser vos utilisateurs locaux à se connecter aux AWS appli cations et aux services avec leurs Active Directory informations d'identification. Vous pouvez également utiliser AD Connector pour associer des instances Amazon EC2 à votre domaine existantActive Directory. Utilisez Simple AD si vous avez besoin d'un annuaire à faible échelle et peu coûteux avec une Active Directory

Que devez-vous faire ?	AWS Directory Service Options recommandées
	compatibilité de base prenant en charge les applications compatibles avec Samba 4, ou si vous avez besoin d'une compatibilité LDAP pour les applications compatibles LDAP.
Je développe des applications SaaS	Utilisez Amazon Cognito si vous développez des applications SaaS à grande échelle et si vous avez besoin d'un annuaire évolutif pour gérer et authentifier vos abonnés qui soit également capable de gérer les identités de réseaux sociaux.

Pour plus d'informations sur les options d' AWS Directory Service annuaire, voir Comment choisir Active Directory des solutions sur AWS.

AWS Directory Service options

AWS Directory Service inclut plusieurs types de répertoires parmi lesquels choisir. Pour plus d'informations, sélectionnez l'un des onglets suivants :

AWS Directory Service for Microsoft Active Directory

Également connu sous le nom de AWS Managed Microsoft AD, AWS Directory Service for Microsoft Active Directory est alimenté par un véritable Microsoft Windows Server Active Directory (AD), géré AWS dans le AWS cloud. Il vous permet de migrer un large éventail d'applications compatibles avec Active Directory vers le cloud. AWS AWS Managed Microsoft AD fonctionne avec Microsoft SharePoint les groupes de disponibilité Microsoft SQL Server Always On et de nombreuses applications .NET. Il prend également en charge les applications et services AWS gérés WorkSpaces, notamment Amazon WorkDocs, Amazon, Amazon QuickSight, Amazon Chime, Amazon Connect et Amazon Relational Database Service pour (Amazon RDS pourSQL Server, Microsoft SQL Server Amazon RDS pour et Amazon RDS Oracle pour PostgreSQL).

AWS Managed Microsoft AD est approuvé pour les applications dans le AWS cloud soumises à la conformité à la loi américaine HIPAA (Health Insurance Portability and Accountability Act) ou à la norme de sécurité des données du secteur des cartes de paiement (PCI DSS) lorsque vous activez la conformité pour votre annuaire.

Toutes les applications compatibles fonctionnent avec les informations d'identification utilisateur que vous stockez dans AWS Managed Microsoft AD, ou vous pouvez vous connecter à votre infrastructure AD existante en toute confiance et utiliser les informations d'identification d'une application Active Directory exécutée sur site ou sur EC2 Windows. Si vous associez des instances EC2 à votre Microsoft AD AWS géré, vos utilisateurs peuvent accéder aux charges de travail Windows dans le AWS cloud avec la même expérience d'authentification unique (SSO) Windows que lorsqu'ils accèdent aux charges de travail de votre réseau sur site.

AWS Managed Microsoft AD prend également en charge les cas d'utilisation fédérés à l'aide Active Directory d'informations d'identification. Seul, AWS Managed Microsoft AD vous permet de vous connecter au AWS Management Console. Vous pouvez également obtenir des informations d'identification à court terme à utiliser avec le AWS SDK et la CLI, et utiliser des intégrations SAML préconfigurées pour vous connecter à de nombreuses applications cloud. AWS IAM Identity Center En ajoutant Microsoft Entra Connect (anciennement connu sous le nom deAzure Active Directory Connect) et éventuellement Active Directory Federation Service (AD FS), vous pouvez vous connecter à Microsoft Office 365 d'autres applications cloud avec des informations d'identification stockées dans AWS Managed Microsoft AD.

Le service inclut les fonctions clés qui vous permettent d'étendre votre schéma, de gérer des stratégies de mot de passe et d'activer des communications LDAP sécurisées via le protocole SSL (Secure Socket Layer) ou TLS (Transport Layer Security). Vous pouvez également activer l'authentification multifactorielle (MFA) pour AWS Managed Microsoft AD afin de fournir un niveau de sécurité supplémentaire lorsque les utilisateurs AWS accèdent à des applications depuis Internet. Comme il Active Directory s'agit d'un annuaire LDAP, vous pouvez également utiliser AWS Managed Microsoft AD pour l'authentification SSH (Linux Secure Shell) et pour d'autres applications compatibles LDAP.

AWS assure la surveillance, les instantanés quotidiens et la restauration dans le cadre du service : vous ajoutez des utilisateurs et des groupes à Managed AWS Microsoft AD, et vous administrez la stratégie de groupe à l'aide d'Active Directoryoutils courants exécutés sur un Windows ordinateur connecté au domaine Managed AWS Microsoft AD. Vous pouvez également mettre à l'échelle l'annuaire en déployant des contrôleurs de domaine supplémentaires et contribuer à améliorer les performances des applications en répartissant les demandes sur un plus grand nombre de contrôleurs de domaine.

AWS Managed Microsoft AD est disponible en deux éditions : Standard et Enterprise.

- Standard Edition : AWS Managed Microsoft AD (Standard Edition) est optimisé pour être utilisé comme annuaire principal dans les petites et moyennes entreprises comptant jusqu'à

5 000 employés. Il offre suffisamment de capacité de stockage pour prendre en charge jusqu'à 30 000* objets d'annuaire (par exemple, des utilisateurs, des groupes et des ordinateurs).

- Enterprise Edition : AWS Managed Microsoft AD (Enterprise Edition) s'adresse aux grandes entreprises qui ont à gérer jusqu'à 500 000* objets d'annuaire.

* Les plafonds indiqués sont fournis à titre indicatif. Votre annuaire peut prendre en charge plus ou moins d'objets d'annuaire, selon la taille de vos objets et le comportement et les besoins de performances de vos applications.

Quand l'utiliser

AWS Managed Microsoft AD est votre meilleur choix si vous avez besoin de Active Directory fonctionnalités réelles pour prendre en charge AWS des applications ou des Windows charges de travail, notamment Amazon Relational Database Service pour. Microsoft SQL Server C'est également la meilleure solution si vous recherchez une solution autonome Active Directory dans le AWS cloud compatible avec Office 365 ou si vous avez besoin d'un annuaire LDAP pour prendre en charge vos applications Linux. Pour plus d'informations, consultez AWS Microsoft AD géré.

AD Connector

AD Connector est un service proxy qui permet de connecter facilement des AWS applications compatibles, telles qu'Amazon WorkSpaces, Amazon et Amazon QuickSight EC2 pour les Windows Server instances, à votre environnement local existant. Microsoft Active Directory Avec AD Connector, vous pouvez simplement ajouter un compte de service à votreActive Directory. AD Connector vous évite aussi d'avoir à synchroniser vos annuaires et vous épargne le coût et la complexité associés à l'hébergement d'une infrastructure de fédération.

Lorsque vous ajoutez des utilisateurs à AWS des applications telles qu'Amazon QuickSight, AD Connector lit vos fichiers existants Active Directory pour créer des listes d'utilisateurs et de groupes parmi lesquels sélectionner. Lorsque les utilisateurs se connectent aux AWS applications, AD Connector transmet les demandes de connexion à vos contrôleurs de Active Directory domaine locaux à des fins d'authentification. AD Connector fonctionne avec de nombreuses AWS applications et services WorkSpaces, notamment Amazon WorkDocs, Amazon QuickSight, Amazon Chime, Amazon Connect et Amazon. WorkMail Vous pouvez également associer vos Windows instances EC2 à votre Active Directory domaine sur site via AD Connector en utilisant une jointure de domaine fluide. AD Connector permet également à vos utilisateurs

d'accéder aux AWS ressources AWS Management Console et de les gérer en se connectant avec leurs Active Directory informations d'identification existantes. AD Connector n'est pas compatible avec RDS SQL Server.

Vous pouvez également utiliser AD Connector pour activer l'authentification multifactorielle (MFA) pour les utilisateurs de AWS votre application en la connectant à votre infrastructure MFA existante basée sur Radius. Les utilisateurs bénéficient ainsi d'une couche de sécurité supplémentaire quand ils accèdent aux applications AWS .

Avec AD Connector, vous pouvez continuer à gérer votre compte Active Directory comme vous le faites actuellement. Par exemple, vous ajoutez de nouveaux utilisateurs et groupes et vous mettez à jour les mots de passe à l'aide des outils d'Active Directoryadministration standard de votre environnement localActive Directory. Cela vous permet d'appliquer de manière cohérente vos politiques de sécurité, telles que l'expiration des mots de passe, l'historique des mots de passe et le verrouillage des comptes, que les utilisateurs accèdent aux ressources sur site ou dans le AWS cloud.

Quand l'utiliser

AD Connector est votre meilleur choix lorsque vous souhaitez utiliser votre annuaire local existant avec des AWS services compatibles. Pour plus d'informations, consultez AD Connector.

Simple AD

Simple AD est un Microsoft Active Directory annuaire compatible alimenté par Samba 4. AWS Directory Service Simple AD prend en charge les Active Directory fonctionnalités de base telles que les comptes utilisateurs, les adhésions à des groupes, l'adhésion à un domaine Linux ou à des instances EC2 Windows basées sur le protocole, l'authentification unique basée sur Kerberos et les politiques de groupe. AWS assure la surveillance, les instantanés quotidiens et la restauration dans le cadre du service.

Simple AD est un annuaire autonome hébergé dans le cloud, qui vous permet non seulement de créer et gérer des identités d'utilisateurs, mais également de gérer l'accès aux applications. Vous pouvez utiliser de nombreuses applications et outils connus Active Directory qui nécessitent des Active Directory fonctionnalités de base. Simple AD est compatible avec les AWS applications suivantes : Amazon WorkSpaces, Amazon WorkDocs QuickSight, Amazon et Amazon WorkMail. Vous pouvez également vous connecter à l' AWS Management Console aide de comptes utilisateur Simple AD et pour gérer les AWS ressources.

Simple AD ne prend pas en charge l'authentification multifactorielle (MFA), les relations de confiance, la mise à jour dynamique du DNS, les extensions de schéma, la communication via LDAPS PowerShell , les applets de commande AD ou le transfert de rôles FSMO. Simple AD n'est pas compatible avec RDS SQL Server. Les clients qui ont besoin des fonctionnalités d'un annuaire actuel Microsoft Active Directory ou qui envisagent d'utiliser leur annuaire avec RDS SQL Server devraient plutôt utiliser Managed AWS Microsoft AD. Veuillez vous assurer que vos applications requises sont entièrement compatibles avec Samba 4 avant d'utiliser Simple AD. Pour plus d'informations, veuillez consulter https://www.samba.org.

Quand l'utiliser

Vous pouvez utiliser Simple AD comme annuaire autonome dans le cloud pour prendre en charge les Windows charges de travail nécessitant des Active Directory fonctionnalités de base, des AWS applications compatibles ou pour prendre en charge les charges de travail Linux nécessitant un service LDAP. Pour plus d'informations, consultez Simple AD.

Amazon Cognito

Amazon Cognito est un annuaire d'utilisateurs qui ajoute l'inscription et la connexion à votre application web ou mobile à l'aide de groupes d'utilisateurs Amazon Cognito.

Quand l'utiliser

Vous pouvez également utiliser Amazon Cognito pour créer des champs d'inscription personnalisés et stocker ces métadonnées dans l'annuaire d'utilisateurs. Ce service entièrement géré peut évoluer pour prendre en charge des centaines de millions d'utilisateurs. Pour plus d'informations sur les Groupes d'utilisateurs Amazon Cognito, veuillez consulter le Guide du développeur Amazon Cognito.

Consultez Disponibilité de la région pour AWS Directory Service pour obtenir la liste des types d'annuaires pris en charge par région.

Fonctionnement avec Amazon EC2

Une compréhension de base d'Amazon EC2 est essentielle pour l'utiliser AWS Directory Service. Nous vous recommandons de commencer par lire les rubriques suivantes :

- Qu'est-ce qu'Amazon EC2 dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.

- Lancement d'instances EC2 dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.
- Groupes de sécurité dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.
- Qu'est-ce qu'Amazon VPC ? dans le Guide de l'utilisateur Amazon VPC
- Ajout d'une passerelle privée virtuelle matérielle à votre VPC dans le Guide de l'utilisateur Amazon VPC.

Commencer avec AWS Directory Service

Si ce n'est pas déjà fait, vous devrez également créer un AWS compte et utiliser le AWS Identity and Access Management service pour contrôler l'accès.

Pour travailler avec AWS Directory Service, vous devez remplir les conditions requises pour le service d' AWS annuaire pour Microsoft Active Directory, AD Connector ou Simple AD. Pour plus d'informations, veuillez consulter AWS Conditions préalables à la gestion de Microsoft AD, Conditions préalables requises pour AD Connector ou Prérequis pour Simple AD.

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et utilisez uniquement l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.

2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, voir Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

En savoir plus

- Pour plus d'informations sur la procédure de connexion en AWS Management Console tant qu'utilisateur d'IAM Identity Center, voir Se connecter au portail d'accès IAM Identity Center.
- Pour plus d'informations sur la procédure de connexion en AWS Management Console tant qu'utilisateur IAM, voir Se connecter en AWS Management Console tant qu'utilisateur IAM.
- Pour plus d'informations sur l'utilisation des politiques IAM pour contrôler l'accès à vos AWS Directory Service ressources, consultezUtilisation de politiques basées sur l'identité (politiques IAM) pour AWS Directory Service.

AWS Microsoft AD géré

AWS Directory Service vous permet d'exécuter Microsoft Active Directory (AD) en tant que service géré. AWS Directory Service pour Microsoft Active Directory, également appelé AWS Managed Microsoft AD, est alimenté par Windows Server 2019. Lorsque vous sélectionnez et lancez ce type de répertoire, il est créé sous la forme d'une paire de contrôleurs de domaine hautement disponible connectés à votre cloud privé virtuel (Amazon VPC). Les contrôleurs de domaine s'exécutent dans différentes zones de disponibilité dans la région de votre choix. La supervision et la restauration de l'hôte, la réplication des données, les instantanés ainsi que les mises à jour logicielles sont automatiquement configurés et gérés pour vous.

Avec AWS Managed Microsoft AD, vous pouvez exécuter des charges de travail basées sur des annuaires dans le AWS cloud, notamment des applications .NET Microsoft SharePoint et SQL Server personnalisées. Vous pouvez également configurer une relation de confiance entre AWS Managed Microsoft AD in the AWS Cloud et votre environnement local existant MicrosoftActive Directory, en fournissant aux utilisateurs et aux groupes l'accès aux ressources de l'un ou l'autre domaine, en utilisant AWS IAM Identity Center.

AWS Directory Service permet de configurer et d'exécuter facilement des annuaires dans le AWS cloud, ou de connecter vos AWS ressources à un répertoire sur site Microsoft Active Directory existant. Lorsque votre annuaire est créé, vous pouvez l'utiliser pour plusieurs tâches :

- Gérer des utilisateurs et des groupes
- Fournir une authentification unique aux applications et services
- Créer et appliquer une stratégie de groupe
- Simplifier le déploiement et la gestion de Linux et des charges de Microsoft Windows travail basées sur le cloud
- Vous pouvez utiliser AWS Managed Microsoft AD pour activer l'authentification multifactorielle en l'intégrant à votre infrastructure MFA existante basée sur Radius afin de fournir un niveau de sécurité supplémentaire lorsque les utilisateurs accèdent aux applications AWS
- Connectez-vous en toute sécurité à Amazon EC2 Linux et aux instances Windows

> **Note**
>
> AWS gère les licences de vos instances de Windows serveur pour vous ; il vous suffit de payer pour les instances que vous utilisez. Il n'est pas non plus nécessaire d'acheter des

licences d'accès client (CAL) Windows Server supplémentaires, car l'accès est inclus dans le prix. Chaque instance est fournie avec deux connexions à distance à des fins administratives uniquement. Si vous avez besoin de plus de deux connexions, ou si vous avez besoin de ces connexions à des fins autres qu'administratives, vous devrez peut-être utiliser des CAL Remote Desktop Services supplémentaires pour les utiliser sur AWS.

Lisez les rubriques de cette section pour commencer à créer un annuaire Microsoft AD AWS géré, à créer une relation de confiance entre AWS Managed Microsoft AD et vos annuaires locaux et à étendre votre schéma Microsoft AD AWS géré.

Rubriques

- Commencer à utiliser AWS Managed Microsoft AD
- Concepts clés pour AWS Managed Microsoft AD
- Bonnes pratiques pour AWS Managed Microsoft AD
- Cas d'utilisation de AWS Managed Microsoft AD
- Comment administrer AWS Managed Microsoft AD
- AWS Quotas Managed Microsoft AD
- Compatibilité des applications pour AWS Managed Microsoft AD
- AWS Tutoriels de laboratoire de test Microsoft AD gérés
- Résolution des problèmes liés AWS à Managed Microsoft AD

Articles AWS de blog sur la sécurité connexes

- Comment déléguer l'administration de votre annuaire Microsoft AD AWS géré à vos utilisateurs Active Directory locaux
- Comment configurer des politiques de mot de passe encore plus strictes pour répondre à vos normes de sécurité à l'aide AWS Directory Service de AWS Managed Microsoft AD
- Comment augmenter la redondance et les performances de AWS Microsoft AD AWS Directory Service pour Managed en ajoutant des contrôleurs de domaine
- Comment activer l'utilisation de postes de travail distants en déployant le gestionnaire de licences Microsoft Remote Desktop sur AWS Managed Microsoft AD
- Comment y accéder à l' AWS Management Console aide de AWS Managed Microsoft AD et de vos informations d'identification locales

- Comment activer l'authentification multifactorielle pour les AWS services à l'aide de AWS Managed Microsoft AD et d'informations d'identification locales
- Comment se connecter facilement aux AWS services à l'aide de votre Active Directory local

Commencer à utiliser AWS Managed Microsoft AD

AWS Managed Microsoft AD crée un environnement entièrement géré, Microsoft Active Directory dans le AWS Cloud et est alimenté par Windows Server 2019 et fonctionne aux niveaux fonctionnels de la forêt et du domaine R2 R2 2012. Lorsque vous créez un annuaire avec AWS Managed Microsoft AD, vous AWS Directory Service créez deux contrôleurs de domaine et ajoutez le service DNS en votre nom. Les contrôleurs de domaine sont créés dans différents sous-réseaux d'un Amazon VPC. Cette redondance permet de garantir que votre répertoire reste accessible même en cas de panne. Si vous avez besoin de contrôleurs de domaine supplémentaires, vous pouvez les ajouter ultérieurement. Pour plus d'informations, consultez Déploiement de contrôleurs de domaine supplémentaires.

Rubriques

- AWS Conditions préalables à la gestion de Microsoft AD
- Créez votre Microsoft AD AWS géré
- Qu'est-ce qui est créé avec votre annuaire Microsoft AD Active Directory AWS géré
- Autorisations pour le compte administrateur

AWS Conditions préalables à la gestion de Microsoft AD

Pour créer un Microsoft AD AWS géréActive Directory, vous avez besoin d'un Amazon VPC avec les éléments suivants :

- Au moins deux sous-réseaux. Chaque sous-réseau doit disposer d'une zone de disponibilité différente.
- Le VPC doit avoir la location matérielle par défaut.
- Vous ne pouvez pas créer un Microsoft AD AWS géré dans un VPC à l'aide des adresses de l'espace d'adressage 198.18.0.0/15.

Si vous devez intégrer votre domaine Microsoft AD AWS géré à un Active Directory domaine local existant, les niveaux fonctionnels de forêt et de domaine de votre domaine local doivent être définis sur Windows Server 2003 ou version ultérieure.

AWS Directory Service utilise une structure à deux VPC. Les instances EC2 qui constituent votre répertoire s'exécutent en dehors de votre AWS compte et sont gérées par AWS. Elles ont deux cartes réseau, `ETH0` et `ETH1`. `ETH0` est la carte de gestion et existe en dehors de votre compte. `ETH1` est créé au sein de votre compte.

La plage IP de gestion du réseau ETH0 de votre annuaire est 198.18.0.0/15.

AWS IAM Identity Center prérequis

Si vous envisagez d'utiliser IAM Identity Center avec AWS Managed Microsoft AD, vous devez vous assurer que les conditions suivantes sont réunies :

- Votre répertoire Microsoft AD AWS géré est configuré dans le compte de gestion de votre AWS organisation.
- Votre instance d'IAM Identity Center se trouve dans la même région que celle dans laquelle votre répertoire Microsoft AD AWS géré est configuré.

Pour plus d'informations, consultez les conditions requises pour IAM Identity Center dans le guide de l' AWS IAM Identity Center utilisateur.

Prérequis pour l'authentification multifactorielle

Pour prendre en charge l'authentification multifactorielle avec votre annuaire Microsoft AD AWS géré, vous devez configurer votre serveur RADIUS (Remote Authentication Dial-In User Service) sur site ou basé sur le cloud de la manière suivante afin qu'il puisse accepter les demandes provenant de votre annuaire AWS Microsoft AD géré dans. AWS

1. Sur votre serveur RADIUS, créez deux clients RADIUS pour représenter les deux contrôleurs de domaine (DC) Microsoft AD AWS gérés dans AWS. Vous devez configurer les deux clients à l'aide des paramètres communs suivants (votre serveur RADIUS peut être différent) :
   - Adresse (DNS ou IP) : il s'agit de l'adresse DNS de l'un des AWS contrôleurs Microsoft AD gérés. Les deux adresses DNS se trouvent dans la console AWS Directory Service sur la page Détails de l'annuaire Microsoft AD AWS géré dans lequel vous prévoyez d'utiliser le MFA. Les adresses DNS affichées représentent les adresses IP des deux contrôleurs de domaine Microsoft AD AWS gérés utilisés par AWS.

> **Note**
>
> Si votre serveur RADIUS prend en charge les adresses DNS, vous ne devez créer qu'une seule configuration du client RADIUS. Sinon, vous devrez créer une configuration du client RADIUS par DC AWS Managed Microsoft AD.

- Port number : configurez le numéro de port sur lequel votre serveur RADIUS accepte les connexions client RADIUS. Le port RADIUS standard est 1812.
- Shared secret : entrez ou générez un secret partagé qui sera utilisé par le serveur RADIUS pour se connecter aux clients RADIUS.
- Protocole : vous devrez peut-être configurer le protocole d'authentification entre les contrôleurs de AWS domaine Microsoft AD gérés et le serveur RADIUS. Les protocoles pris en charge sont PAP, CHAP MS-CHAPv1 et MS-CHAPv2. Le protocole MS-CHAPv2 est recommandé, car il offre le meilleur niveau de sécurité des trois différentes options.
- Application name : ce paramètre facultatif sur certains serveurs RADIUS, identifie généralement l'application dans des messages ou des rapports.

2. Configurez votre réseau existant pour autoriser le trafic entrant depuis les clients RADIUS (adresses DNS Microsoft AD DC AWS gérées, voir étape 1) vers le port de votre serveur RADIUS.
3. Ajoutez une règle au groupe de sécurité Amazon EC2 dans votre domaine AWS Microsoft AD géré qui autorise le trafic entrant depuis l'adresse DNS et le numéro de port du serveur RADIUS définis précédemment. Pour plus d'informations, veuillez consulter la section Adding rules to a security group (français non garanti) dans le Guide de l'Utilisateur EC2.

Pour plus d'informations sur l'utilisation de AWS Managed Microsoft AD avec MFA, consultez. Activer l'authentification multifactorielle pour AWS Managed Microsoft AD

Créez votre Microsoft AD AWS géré

Pour créer un nouvel annuaire, exécutez les étapes suivantes. Avant de commencer cette procédure, assurez-vous que vous avez terminé les prérequis identifiés dans AWS Conditions préalables à la gestion de Microsoft AD.

Pour créer un annuaire Microsoft AD AWS géré

1. Dans le panneau de navigation de la console AWS Directory Service, choisissez Annuaires, puis Configurer un annuaire.

2. Sur la page Select directory type (Sélectionner un type d'annuaire), choisissez AWS Managed Microsoft AD, puis Next (Suivant).
3. Sur la page Enter directory information (Saisir les détails de l'annuaire), renseignez les informations suivantes :

   Edition

   Choisissez entre l'édition Standard ou l'édition Enterprise de AWS Managed Microsoft AD. Pour plus d'informations sur les éditions, veuillez consulter AWS Directory Service for Microsoft Active Directory (français non garanti).

   Nom de DNS de l'annuaire

   Nom complet de l'annuaire, par exemple `corp.example.com`.

   > **Note**
   >
   > Si vous prévoyez d'utiliser Amazon Route 53 pour le DNS, le nom de domaine de votre AWS Managed Microsoft AD doit être différent de votre nom de domaine Route 53. Des problèmes de résolution DNS peuvent survenir si Route 53 et AWS Managed Microsoft AD partagent le même nom de domaine.

   Nom NetBIOS de l'annuaire

   Nom court de l'annuaire, par exemple `CORP`.

   Description de l'annuaire

   Description facultative de l'annuaire.

   Mot de passe administrateur

   Mot de passe de l'administrateur de l'annuaire. Le processus de création d'un annuaire crée un compte d'administrateur avec le nom utilisateur `Admin` et ce mot de passe.

   Ce mot de passe ne peut pas contenir le terme « admin ».

   Le mot de passe de l'administrateur de l'annuaire est sensible à la casse et doit comporter entre 8 et 64 caractères (inclus). Il doit également contenir au moins un caractère de trois des quatre catégories suivantes :

- Lettres minuscules (a-z)
- Lettres majuscules (A-Z)
- Chiffres (0-9)
- Caractères non alphanumériques (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirmer le mot de passe

Saisissez à nouveau le mot de passe de l'administrateur.

4. Sur la page Choose VPC and subnets (Choisir un VPC et des sous-réseaux), indiquez les informations suivantes, puis choisissez Next (Suivant).

   VPC

   VPC de l'annuaire.

   Sous-réseaux

   Choisissez les sous-réseaux pour les contrôleurs de domaine. Les deux sous-réseaux doivent être dans des zones de disponibilité différentes.

5. Sur la page Review & create (Vérifier et créer), vérifiez les informations concernant l'annuaire et effectuez les modifications nécessaires. Lorsque les informations sont correctes, choisissez Create directory (Créer l'annuaire). La création de l'annuaire prend entre 20 et 40 minutes. Une fois l'annuaire créé, le champ Statut prend la valeur Actif.

Qu'est-ce qui est créé avec votre annuaire Microsoft AD Active Directory AWS géré

Lorsque vous créez un Active Directory avec AWS Managed Microsoft AD, AWS Directory Service vous effectuez les tâches suivantes en votre nom :

- Crée et associe automatiquement une interface réseau Elastic (ENI) à chacun de vos contrôleurs de domaine. Chacun de ces ENI est essentiel à la connectivité entre votre VPC AWS Directory Service et les contrôleurs de domaine et ne doit jamais être supprimé. Vous pouvez identifier toutes les interfaces réseau réservées à l'utilisation AWS Directory Service par la description : « interface réseau AWS créée pour le répertoire directory-id ». Pour plus d'informations, consultez Elastic Network Interfaces dans le guide de l'utilisateur Amazon EC2 pour les instances Windows. Le serveur DNS par défaut de AWS Managed Microsoft AD Active Directory est le serveur DNS

VPC avec Classless Inter-Domain Routing (CIDR) +2. Pour plus d'informations, consultez le serveur Amazon DNS dans le guide de l'utilisateur Amazon VPC.

> **Note**
>
> Les contrôleurs de domaine sont déployés par défaut dans deux zones de disponibilité d'une région et connectés à votre Amazon VPC (VPC). Les sauvegardes sont effectuées automatiquement une fois par jour, et les volumes Amazon EBS (EBS) sont chiffrés pour garantir la sécurité des données au repos. Les contrôleurs de domaine qui échouent sont automatiquement remplacés dans la même zone de disponibilité à l'aide de la même adresse IP, et une reprise après sinistre complète peut être effectuée avec la dernière sauvegarde.

- Met en service Active Directory dans votre VPC à l'aide de deux contrôleurs de domaine pour la tolérance aux pannes et la haute disponibilité. Des contrôleurs de domaine supplémentaires peuvent être mis en service pour une résilience et des performances supérieures une fois que l'annuaire a été créé avec succès et qu'il est actif. Pour plus d'informations, consultez Déploiement de contrôleurs de domaine supplémentaires.

> **Note**
>
> AWS n'autorise pas l'installation d'agents de surveillance sur les contrôleurs de domaine Microsoft AD AWS gérés.

- Crée un groupe de sécuritéAWS qui établit des règles réseau pour le trafic entrant et sortant de vos contrôleurs de domaine. La règle de trafic sortant par défaut autorise tous les ENI ou instances de trafic attachés au groupe de AWS sécurité créé. La règle entrante par défaut n'autorise que le trafic via les ports qui sont exigés par Active Directory quelle que soit la source (0.0.0.0/0). Les règles 0.0.0.0/0 n'introduisent pas de failles de sécurité car le trafic vers les contrôleurs de domaine est limité au trafic provenant de votre VPC, d'autres VPC homologues ou de réseaux que vous vous êtes connectés via AWS Transit AWS Direct Connect Gateway ou Virtual Private Network. Pour plus de sécurité, aucune adresse IP Elastic n'est attachée aux ENI créées et vous n'avez pas l'autorisation d'attacher une adresse IP Elastic à ces ENI. Par conséquent, le seul trafic entrant capable de communiquer avec votre Microsoft AD AWS géré est le VPC local et le trafic routé par VPC. Soyez extrêmement attentif si vous tentez de modifier ces règles, car vous risquez de ne plus pouvoir communiquer avec vos contrôleurs de domaine. Pour plus d'informations, consultez

Bonnes pratiques pour AWS Managed Microsoft AD. Les règles AWS de groupe de sécurité suivantes sont créées par défaut :

Règles entrantes

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
ICMP	N/A	0.0.0.0/0	Ping	LDAP Keep Alive, DFS
TCP et UDP	53	0.0.0.0/0	DNS	Authentification d'utilisateur et d'ordinateur, résolution de noms, approbations
TCP et UDP	88	0.0.0.0/0	Kerberos	Authentification d'utilisateur et d'ordinateur, approbations au niveau de la forêt
TCP et UDP	389	0.0.0.0/0	LDAP	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP et UDP	445	0.0.0.0/0	SMB / CIFS	Réplication, authentification d'utilisateur et d'ordinateur, stratégie de groupe, approbations
TCP et UDP	464	0.0.0.0/0	Mot de passe Kerberos (modification/définition)	Réplication, authentification d'utilisateur et d'ordinateur, approbations
TCP	135	0.0.0.0/0	Réplication	RPC, EPM
TCP	636	0.0.0.0/0	LDAP SSL	Directory, réplication, stratégie d'authentification d'utilisateur et d'ordinateur, approbations
TCP	1024-65535	0.0.0.0/0	RPC	Réplication, authentification d'utilisateur et d'ordinateur, stratégie de groupe, approbations

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP	3268 - 3269	0.0.0.0/0	LDAP GC et LDAP GC SSL	Directory , réplicati on, stratégie d'authentification d'utilisateur et d'ordinateur, approbations
UDP	123	0.0.0.0/0	Heure Windows	Heure Windows, approbations
UDP	138	0.0.0.0/0	DFSN et NetLogon	DFS, stratégie de groupe
Tous	Tous	sg-###### ############	Tout le trafic	

Règles sortantes

Protocole	Plage de ports	Destination	Type de trafic	Utilisation d'Active Directory
Tous	Tous	sg-###### ############	Tout le trafic	

- Pour plus d'informations sur les ports et les protocoles utilisés par Active Directory, veuillez consulter la section Service overview and network port requirements for Windows (français non garanti) dans la documentation Microsoft.
- Création d'un compte d'administrateur d'annuaire avec le nom d'utilisateur Admin et le mot de passe spécifié. Ce compte est situé sous l'unité d'organisation Users (Utilisateurs) (par exemple, Corp > Users). Vous utilisez ce compte pour gérer votre annuaire dans le AWS Cloud. Pour plus d'informations, consultez Autorisations pour le compte administrateur.

> **Important**
>
> N'oubliez pas de sauvegarder ce mot de passe. AWS Directory Service ne stocke pas ce mot de passe et il ne peut pas être récupéré. Vous pouvez toutefois réinitialiser un mot de passe depuis la AWS Directory Service console ou à l'aide de l'ResetUserPasswordAPI.

- Crée les trois unités d'organisation sous le domaine racine :

Nom de l'unité d'organisation	Description
AWS Groupes délégués	Stocke tous les groupes que vous pouvez utiliser pour déléguer AWS des autorisations spécifiques à vos utilisateurs.
AWS Réservé	Stocke tous les comptes spécifiques à la AWS gestion.

<votrenomdedomaine>	Le nom de cette unité d'organisation est basé sur le nom NetBIOS que vous avez saisi lors de la création de votre annuaire. Si vous n'avez pas spécifié de nom NetBIOS, il comprendra par défaut la première partie du nom DNS de votre annuaire (par exemple, dans le cas de soc.exemple.com, le nom NetBIOS serait soc). Cette unité d'organisation est détenue par AWS et contient tous vos AWS objets de répertoire associés, sur lesquels vous avez le contrôle total. Deux unités d'organisation enfants existent par défaut sous cette unité d'organisation : Computers (Ordinateurs) et Users (Utilisateurs). Par exemple :
	• Corp
	  • Computers (Ordinateurs)
	  • Users

- Crée les groupes suivants dans l'unité d' AWS organisation des groupes délégués :

Nom du groupe	Description
AWS Opérateurs de comptes délégués	Les membres de ce groupe de sécurité ont peu de capacités de gestion de compte comme les réinitialisations de mots de passe
AWS Administrateurs d'activation basés sur Active Directory délégués	Les membres de ce groupe de sécurité peuvent créer des objets d'activation de licences en volume Active Directory, ce qui permet aux entreprises d'activer des ordinateurs via une connexion à leur domaine.
AWS Ajout délégué de postes de travail aux utilisateurs du domaine	Les membres de ce groupe de sécurité peuvent joindre 10 ordinateurs à un domaine.
AWS Administrateurs délégués	Les membres de ce groupe de sécurité peuvent gérer AWS Managed Microsoft AD, avoir le contrôle total de tous les objets de votre unité d'organisation et peuvent gérer les groupes contenus dans l'unité d' AWS organisation des groupes délégués.
AWS Autorisation déléguée d'authentifier des objets	Les membres de ce groupe de sécurité ont la possibilité de s'authentifier auprès des ressources informatiques de l'unité d'organisation AWS réservée (uniquement nécessaire pour les objets locaux avec des approbations activées par l'authentification sélective).
AWS Délégué autorisé à s'authentifier auprès des contrôleurs de domaine	Les membres de ce groupe de sécurité ont la possibilité de s'authentifier auprès des ressources informatiques dans l'unité d'organisation des contrôleurs de domaine (uniquement nécessaire pour les objets sur site avec les approbations activées pour l'authentification sélective).

Nom du groupe	Description
AWS Administrateurs délégués de durée de vie des objets supprimés	Les membres de ce groupe de sécurité peuvent modifier l'DeletedObjectLifetimeobjet MSDs, qui définit la durée pendant laquelle un objet supprimé pourra être récupéré depuis la corbeille AD.
AWS Administrateurs de systèmes de fichiers distribués délégués	Les membres de ce groupe de sécurité peuvent ajouter et supprimer des espaces de noms FRS, DFS-R et DFS.
AWS Administrateurs de systèmes de noms de domaine délégués	Les membres de ce groupe de sécurité peuvent gérer les DNS intégré à Active Directory.
AWS Administrateurs délégués du protocole de configuration dynamique des hôtes	Les membres de ce groupe de sécurité peuvent autoriser des serveurs DHCP Windows dans l'entreprise.
AWS Administrateurs délégués des autorités de certification d'entreprise	Les membres de ce groupe de sécurité peuvent déployer et gérer une autorité de certification d'entreprise Microsoft.
AWS Administrateurs délégués de politiques de mots de passe détaillées	Les membres de ce groupe de sécurité peuvent modifier les stratégies de gestion de mots de passe granulaires prédéfinies.
AWS Administrateurs FSx délégués	Les membres de ce groupe de sécurité ont la possibilité de gérer les ressources Amazon FSx.
AWS Administrateurs de politiques de groupe délégués	Les membres de ce groupe de sécurité peuvent effectuer des tâches de gestion de stratégies de groupe (créer, modifier, supprimer un lien).

Nom du groupe	Description
AWS Administrateurs de délégation Kerberos délégués	Les membres de ce groupe de sécurité peuvent activer une délégation sur les ordinateurs et les comptes utilisateur.
AWS Administrateurs de comptes de services gérés délégués	Les membres de ce groupe de sécurité peuvent créer et supprimer des comptes de services gérés.
AWS Appareils non conformes à la norme MS-NPRC délégués	Les membres de ce groupe de sécurité seront exemptés de l'obligation d'exiger des communications par canal sécurisé avec les contrôleurs de domaine. Ce groupe est destiné aux comptes d'ordinateur.
AWS Administrateurs de services d'accès à distance délégués	Les membres de ce groupe de sécurité peuvent ajouter et supprimer des serveurs RAS du groupe de serveurs RAS et IAS.
AWS Administrateurs délégués des modifications de répertoire répliquées	Les membres de ce groupe de sécurité peuvent synchroniser les informations de profil dans Active Directory avec le SharePoint serveur.
AWS Administrateurs de serveurs délégués	Les membres de ce groupe de sécurité sont inclus dans le groupe d'administrateurs locaux sur tous les ordinateurs liés au domaine.
AWS Administrateurs de sites et de services délégués	Les membres de ce groupe de sécurité peuvent renommer l'objet « Default-First-Site-Name » dans les sites et services Active Directory.
AWS Administrateurs de gestion de système délégués	Les membres de ce groupe de sécurité peuvent créer et gérer des objets dans le conteneur System Management.

Nom du groupe	Description
AWS Administrateurs de licences Terminal Server délégués	Les membres de ce groupe de sécurité peuvent ajouter et supprimer des serveurs de licences Terminal Server dans le groupe de serveurs de licences Terminal Server.
AWS Administrateurs délégués des suffixes de nom d'utilisateur principal	Les membres de ce groupe de sécurité peuvent ajouter et supprimer des suffixes de noms principaux d'utilisateurs.

- Crée et applique les objets de stratégie de groupe (GPO) suivants :

> **Note**
>
> Vous n'êtes pas autorisé à supprimer, modifier ou dissocier ces GPO. Ceci est intentionnel car ils sont réservés à AWS l'usage. Vous pouvez les relier à des UO que vous contrôlez si nécessaire.

Nom de la stratégie de groupe	S'applique à	Description
Stratégie de domaine par défaut	Domaine	Inclut les stratégies de mot de passe de domaine et Kerberos.
ServerAdmins	Tous les comptes d'ordinateurs autres que contrôleurs de domaine	Ajoute les « administrateurs de serveur AWS délégués » en tant que membre du groupe BUILTIN \ Administrators.
AWS Politique de réserve : utilisateur	AWS Comptes utilisateurs réservés	Définit les paramètres de sécurité recommandés pour tous les comptes utilisateurs

Nom de la stratégie de groupe	S'applique à	Description
		de l'unité d'organisation AWS réservée.
AWS Politique Active Directory gérée	Tous les contrôleurs de domaine	Définit les paramètres de sécurité recommandés sur tous les contrôleurs de domaine.
TimePolicyNT5DS	Tous les contrôleurs de domaine non PDCE	Définit la stratégie d'heure de tous les contrôleurs de domaine non PDCE de manière à utiliser l'heure Windows (NT5DS).
TimePolicyPDC	Le contrôleur de domaine PDCe	Définit la stratégie d'heure du contrôleur de domaine PDCe de manière à utiliser le protocole NTP (Network Time Protocol).
Stratégie des contrôleurs de domaine par défaut	Non utilisé	Provisionnée lors de la création du domaine, la politique AWS Managed Active Directory est utilisée à sa place.

Si vous souhaitez voir les paramètres de chaque GPO, vous pouvez les afficher à partir d'une instance Windows jointe au domaine avec la console de gestion des stratégies de groupe (GPMC) activée.

Autorisations pour le compte administrateur

Lorsque vous créez un AWS annuaire Directory Service pour Microsoft Active Directory, vous AWS créez une unité organisationnelle (UO) pour stocker tous les groupes et comptes AWS associés.

Pour plus d'informations sur cette unité d'organisation, veuillez consulter Qu'est-ce qui est créé avec votre annuaire Microsoft AD Active Directory AWS géré. Cela inclut le compte Admin. Le compte Admin dispose des autorisations pour effectuer les activités administratives courantes suivantes pour votre unité d'organisation :

- Ajouter, mettre à jour ou supprimer des utilisateurs, des groupes et des ordinateurs. Pour plus d'informations, consultez Gérer des utilisateurs et des groupes dans AWS Managed Microsoft AD.
- Ajouter des ressources à votre domaine, comme des serveurs de fichiers ou d'impression, puis attribuer des autorisations pour ces ressources aux utilisateurs et groupes dans votre unité d'organisation.
- Créer des unités d'organisation et des conteneurs supplémentaires.
- Déléguez l'autorité des unités d'organisation et des conteneurs supplémentaires. Pour plus d'informations, consultez Délégation des privilèges de jonction d'annuaire pour AWS Managed Microsoft AD.
- Créer et associer des stratégies de groupes.
- Restaurer des objets supprimés de la corbeille Active Directory.
- Exécutez les Windows PowerShell modules Active Directory et DNS sur le service Web Active Directory.
- Créer et configurer des comptes de services gérés de groupe. Pour plus d'informations, consultez Comptes de service administrés de groupe.
- Configurer la délégation Kerberos contrainte. Pour plus d'informations, consultez Délégation Kerberos contrainte.

Le compte Admin dispose également de droits pour exécuter les activités suivantes au niveau du domaine :

- Gérer les configurations DNS (ajouter, supprimer ou mettre à jour des enregistrements, des zones et des redirecteurs)
- Afficher les journaux d'évènements DNS
- Afficher les journaux d'évènements de sécurité

Seules les actions répertoriées ici sont autorisées pour le compte Admin. De même, le compte Admin ne détient pas les autorisations liées à toutes les actions sur l'annuaire en dehors de votre unité d'organisation spécifique, comme sur l'unité d'organisation parent.

> **Important**
>
> AWS Les administrateurs de domaine ont un accès administratif complet à tous les domaines hébergés sur AWS. Consultez votre accord AWS et la FAQ sur la protection AWS des données pour plus d'informations sur la manière dont vous AWS gérez le contenu, y compris les informations d'annuaire, que vous stockez sur AWS les systèmes.

> **Note**
>
> Nous vous recommandons de ne pas supprimer ou renommer ce compte. Si vous ne souhaitez plus utiliser le compte, nous vous recommandons de définir un mot de passe long (64 caractères aléatoires maximum), puis de désactiver le compte.

Comptes disposant de droits d'administrateur d'entreprise et de domaine

AWS remplace automatiquement le mot de passe administrateur intégré par un mot de passe aléatoire tous les 90 jours. Chaque fois que le mot de passe administrateur intégré est demandé pour un usage humain, un AWS ticket est créé et enregistré auprès de l' AWS Directory Service équipe. Les informations d'identification du compte sont chiffrées et traitées via des canaux sécurisés. De plus, les informations d'identification du compte administrateur ne peuvent être demandées que par l'équipe AWS Directory Service de direction.

Pour effectuer la gestion opérationnelle de votre annuaire, AWS vous avez le contrôle exclusif des comptes dotés des privilèges d'administrateur d'entreprise et d'administrateur de domaine. Cela inclut le contrôle exclusif du compte administrateur Active Directory. AWS protège ce compte en automatisant la gestion des mots de passe grâce à l'utilisation d'un coffre-fort de mots de passe. Lors de la rotation automatique du mot de passe administrateur, AWS crée un compte utilisateur temporaire et lui accorde les privilèges d'administrateur de domaine. Ce compte temporaire est utilisé en tant que sauvegarde en cas de défaillance de la rotation du mot de passe du compte administrateur. Après avoir AWS réussi à faire pivoter le mot de passe administrateur, AWS supprime le compte administrateur temporaire.

Normalement AWS , le répertoire est entièrement géré par automatisation. Si un processus d'automatisation ne parvient pas à résoudre un problème opérationnel, vous devrez AWS peut-être demander à un ingénieur de support de se connecter à votre contrôleur de domaine (DC) pour effectuer un diagnostic. Dans ces rares cas, AWS implémente un système de demande/

notification pour accorder l'accès. Au cours de ce processus, AWS l'automatisation crée un compte utilisateur à durée limitée dans votre annuaire doté d'autorisations d'administrateur de domaine. AWS associe le compte utilisateur à l'ingénieur chargé de travailler sur votre annuaire. AWS enregistre cette association dans notre système de journalisation et fournit à l'ingénieur les informations d'identification à utiliser. Toutes les actions réalisées par l'ingénieur sont consignées dans les journaux d'événements Windows. Au terme du temps alloué, l'automatisation supprime le compte utilisateur.

Vous pouvez surveiller les actions du compte administrateur à l'aide de la fonction de transfert de journaux de votre annuaire. Cette fonctionnalité vous permet de transférer les événements de sécurité AD à votre CloudWatch système où vous pouvez mettre en œuvre des solutions de surveillance. Pour plus d'informations, consultez Activer le transfert de journaux.

Les ID d'événements de sécurité 4624, 4672 et 4648 sont tous consignés lorsqu'une personne se connecte à un DC de manière interactive. Vous pouvez consulter le journal des événements de sécurité Windows de chaque DC à l'aide de l'Observateur d'événements de Microsoft Management Console (MMC) à partir d'un ordinateur Windows joint au domaine. Vous pouvez également Activer le transfert de journaux envoyer tous les journaux des événements de sécurité aux CloudWatch journaux de votre compte.

Il est possible que des utilisateurs soient parfois créés et supprimés au sein de l'unité d'organisation AWS réservée. AWS est responsable de la gestion et de la sécurité de tous les objets de cette unité d'organisation et de toute autre unité d'organisation ou conteneur pour lesquels nous ne vous avons pas délégué les autorisations d'accès et de gestion. Vous pouvez voir des créations et des suppressions dans cette UO. Cela est dû au fait qu'il AWS Directory Service utilise l'automatisation pour alterner régulièrement le mot de passe de l'administrateur de domaine. Lorsque le mot de passe a effectué une rotation, une sauvegarde est créée en cas d'échec de la rotation. Une fois la rotation réussie, le compte de sauvegarde est automatiquement supprimé. De même, dans les rares cas où un accès interactif est nécessaire sur les contrôleurs de domaine à des fins de dépannage, un compte utilisateur temporaire est créé pour qu'un AWS Directory Service ingénieur puisse l'utiliser. Une fois qu'un ingénieur aura terminé son travail, le compte utilisateur temporaire sera supprimé. Notez que chaque fois que des informations d'identification interactives sont demandées pour un annuaire, l'équipe AWS Directory Service de direction en est informée.

Concepts clés pour AWS Managed Microsoft AD

Vous tirerez le meilleur parti d'AWS Managed Microsoft AD en vous familiarisant avec les concepts clés suivants.

Rubriques

Schéma Active Directory

Un schéma est la définition des attributs et classes qui font partie d'un annuaire distribué et sont similaires aux champs et tables d'une base de données. Les schémas incluent un ensemble de règles qui déterminent le type et le format des données qui peuvent être ajoutées ou incluses dans la base de données. La classe Utilisateur est l'exemple d'une classe qui est stockée dans la base de données. Quelques exemples d'attributs de classe Utilisateur peuvent inclure le prénom, le nom, le numéro de téléphone de l'utilisateur, etc.

Éléments du schéma

Les attributs, les classes et les objets sont les éléments de base qui sont utilisés pour créer des définitions d'objets dans le schéma. Voici les détails sur les éléments du schéma que vous devez connaître avant d'entamer le processus d'extension de votre schéma AWS Managed Microsoft AD.

Attributs

Chaque attribut de schéma, qui est similaire au champ d'une base de données, possède plusieurs propriétés qui définissent les caractéristiques de l'attribut. Par exemple, la propriété utilisée par les clients LDAP pour lire et écrire l'attribut est `LDAPDisplayName`. La propriété `LDAPDisplayName` doit être unique sur tous les attributs et classes. Pour obtenir une liste complète des caractéristiques de l'attribut, veuillez consulter Characteristics of Attributes (français non garanti) sur le site web MSDN. Pour plus d'informations sur la création d'un nouvel attribut, veuillez consulter Defining a New Attribute (français non garanti) sur le site web MSDN.

Classes

Les classes sont analogues aux tables dans une base de données et disposent également de plusieurs propriétés à définir. Par exemple, le code `objectClassCategory` définit la catégorie de la classe. Pour obtenir une liste complète des caractéristiques de la classe, veuillez consulter Characteristics of Object Classes (français non garanti) sur le site web MSDN. Pour

plus d'informations sur la création d'une nouvelle classe, veuillez consulter Defining a New Class (français non garanti) sur le site web MSDN.

Identificateur d'objet (OID)

Chaque classe et attribut doit posséder un OID unique pour tous vos objets. Les fournisseurs de logiciel doivent obtenir leurs propres OID pour garantir l'unicité. L'unicité permet d'éviter les conflits lorsque le même attribut est utilisé par plus d'une application à différentes fins. Pour garantir l'unicité, vous pouvez obtenir un OID racine auprès d'une autorité d'enregistrement de nom ISO. Sinon, vous pouvez obtenir un OID de base auprès de Microsoft. Pour plus d'informations sur les OID et leur obtention, veuillez consulter Object Identifiers (français non garanti) sur le site web MSDN.

Attributs liés à un schéma

Certains attributs sont liés entre deux classes par des liens suivants et précédents. Le meilleur exemple est les groupes. Lorsque vous observez un groupe, il vous montre les membres qui le composent ; si vous observez un utilisateur, vous pouvez voir les groupes auxquels il appartient. Lorsque vous ajoutez un utilisateur à un groupe, Active Directory crée un lien suivant vers le groupe. Ensuite, Active Directory ajoute un lien précédent à partir du groupe de l'utilisateur. Un ID de lien unique doit être généré lors de la création d'un attribut qui sera lié. Pour plus d'informations, veuillez consulter Linked Attributes (français non garanti) sur le site web MSDN.

Rubriques en relation

- Quand étendre votre schéma AWS Managed Microsoft AD
- Tutoriel : extension de votre schéma Microsoft AD AWS géré

Application de correctifs et maintenance pour AWS Managed Microsoft AD

Le AWS Directory Service for Microsoft Active Directory, également appelé AWS DS for AWS Managed Microsoft AD, correspond en fait aux services de domaine Active Directory (AD DS) Microsoft fournis en tant que service géré. Le système utilise Microsoft Windows Server 2019 pour les contrôleurs de domaine (DC), et AWS ajoute les logiciels aux contrôleurs de domaine à des fins de gestion du service. AWS met à jour (application de correctifs) les contrôleurs de domaine pour ajouter de nouvelles fonctionnalités et maintenir le logiciel Microsoft Windows Server à jour. Pendant le processus d'application des correctifs, votre annuaire reste disponible pour utilisation.

Garantie de la disponibilité

Par défaut, chaque annuaire se compose de deux contrôleurs de domaine, chacun d'entre eux étant installé dans une zone de disponibilité différente. À votre convenance, vous pouvez ajouter des contrôleurs de domaine pour augmenter encore la disponibilité. Pour les environnements critiques nécessitant une haute disponibilité et une tolérance aux pannes, nous recommandons de déployer des contrôleurs de domaine supplémentaires. AWSapplique des patchs à vos contrôleurs de domaine de manière séquentielle, période pendant laquelle le contrôleur de domaine qui applique activement les correctifs AWS n'est pas disponible. Si un ou plusieurs contrôleurs de domaine sont temporairement hors service, AWS diffère l'application des correctifs tant que votre annuaire ne dispose pas d'au moins deux contrôleurs de domaine opérationnels. Ceci vous permet d'utiliser les autres contrôleurs de domaine opérationnels pendant le processus d'application des correctifs, qui prend généralement de 30 à 45 minutes par contrôleur, même si cette durée peut varier. Pour garantir que vos applications puissent accéder à un contrôleur de domaine au cas où un ou plusieurs contrôleurs de domaine sont indisponibles pour une raison quelconque, notamment l'application des correctifs, vos applications doivent utiliser le localisateur de service de contrôleur de domaine Windows et ne pas utiliser des adresses de contrôleur de domaine statiques.

Présentation de la planification d'application des correctifs

Pour que le logiciel Microsoft Windows Server reste à jour sur vos contrôleurs de domaine, AWS utilise les mises à jour Microsoft. À mesure que Microsoft met à disposition des déploiements de correctifs mensuels pour Windows Server, AWS fait son possible pour tester et appliquer ces déploiements sur tous les contrôleurs de domaine des clients dans un délai de trois semaines calendaires. En outre, AWS vérifie les mises à jour que Microsoft publie en dehors du déploiement mensuel en fonction de leur applicabilité aux contrôleurs de domaine et de leur urgence. Pour les correctifs de sécurité que Microsoft évalue comme étant critiques ou importants, et qui sont pertinents pour les contrôleurs de domaine, AWS fait son possible pour tester et déployer ces correctifs dans un délai de cinq jours.

Comptes de service administrés de groupe

Avec Windows Server 2012, Microsoft a introduit une nouvelle méthode que les administrateurs peuvent utiliser pour gérer les comptes de service : les comptes de service administrés de groupe (appelés gMSA). Grâce aux comptes gMSA, les administrateurs de service n'ont plus à gérer manuellement la synchronisation des mots de passe entre les instances de service. Un administrateur peut simplement créer un gMSA dans Active Directory, puis configurer plusieurs instances de service pour utiliser ce compte gMSA spécifique.

Pour accorder les autorisations nécessaires pour que des utilisateurs dans AWS Managed Microsoft AD puissent créer un gMSA, vous devez ajouter leurs comptes en tant que membre du groupe de sécurité Administrateurs délégués de comptes de services gérés AWS. Par défaut, le compte administrateur est membre de ce groupe. Pour plus d'informations sur les GMSA, consultez la section Présentation des comptes de services gérés par le groupe sur le site Web de Microsoft. TechNet

Post du blog sur la sécurité AWS

- Comment le service AWS Managed Microsoft AD simplifie le déploiement et améliore la sécurité des applications .NET intégrées à Active Directory

Délégation Kerberos contrainte

La délégation Kerberos contrainte est une fonctionnalité de Windows Server. Cette fonctionnalité permet aux administrateurs de services de spécifier et d'appliquer des limites d'approbation d'applications en limitant l'étendue d'intervention des services applicatifs qui agissent au nom d'un utilisateur. Cela peut être utile lorsque vous avez besoin de spécifier les comptes de service frontaux qui sont autorisés à déléguer des tâches à leurs services dorsaux. La délégation Kerberos contrainte empêche également votre gMSA de se connecter à n'importe quel service pour le compte de vos utilisateurs Active Directory, ce qui évite le risque d'abus par un développeur malveillant.

Par exemple, supposons que l'utilisateur jdupont se connecte à une application RH. Vous voulez que votre instance SQL Server applique les autorisations de base de données de jdupont. Cependant, par défaut, SQL Server ouvre la connexion à la base de données en utilisant les informations d'identification du compte hr-app-service de service qui s'applique, au lieu des autorisations configurées par jsmith. Vous devez permettre à l'application de paie RH d'accéder à la base de données SQL Server à l'aide des informations d'identification de jdupont. Pour ce faire, vous activez la délégation contrainte Kerberos pour le compte de hr-app-service service dans votre répertoire Managed AWS Microsoft AD dans. AWS Lorsque jdupont se connecte, Active Directory émet un ticket Kerberos que Windows utilise automatiquement lorsque jdupont tente d'accéder à d'autres services sur le réseau. La délégation Kerberos permet au hr-app-service compte de réutiliser le ticket Kerberos jsmith lors de l'accès à la base de données, appliquant ainsi des autorisations spécifiques à jsmith lors de l'ouverture de la connexion à la base de données.

Pour accorder les autorisations nécessaires pour que des utilisateurs dans AWS Managed Microsoft AD puissent configurer une délégation Kerberos contrainte, vous devez ajouter leurs comptes en tant que membre du groupe de sécurité Administrateurs délégués de délégation Kerberos AWS. Par défaut, le compte administrateur est membre de ce groupe. Pour plus d'informations sur la délégation

contrainte de Kerberos, consultez la section Présentation de la délégation contrainte de Kerberos sur le site Web de Microsoft. TechNet

La délégation contrainte basée sur les ressources a été introduite avec Windows Server 2012. Elle fournit à l'administrateur de service principal la possibilité de configurer la délégation contrainte pour le service.

Bonnes pratiques pour AWS Managed Microsoft AD

Voici quelques suggestions et directives à prendre en compte pour éviter les problèmes et tirer le meilleur parti de AWS Managed Microsoft AD.

Configuration : prérequis

Pensez à utiliser ces consignes avant de créer votre annuaire.

Vérifiez que vous avez le type d'annuaire approprié

AWS Directory Service propose plusieurs méthodes d'utilisation Microsoft Active Directory avec d'autres AWS services. Vous pouvez choisir le service d'annuaire doté des fonctionnalités dont vous avez besoin à un prix adapté à votre budget :

- AWS Directory Service pour Microsoft Active Directory est un service géré riche en fonctionnalités Microsoft Active Directory hébergé sur le AWS cloud. AWS Managed Microsoft AD est votre meilleur choix si vous avez plus de 5 000 utilisateurs et que vous avez besoin d'établir une relation de confiance entre un annuaire AWS hébergé et vos annuaires locaux.
- AD Connector connecte simplement votre site existant Active Directory à AWS. AD Connector est votre meilleur allié si vous souhaitez utiliser votre annuaire sur site existant avec les services AWS .
- Simple AD est un annuaire à petite échelle et à faible coût doté d'une Active Directory compatibilité de base. Il prend en charge jusqu'à 5 000 utilisateurs, des applications compatibles avec Samba 4 et une compatibilité LDAP pour les applications LDAP.

Pour une comparaison plus détaillée des AWS Directory Service options, voirQue choisir ?.

Assurez-vous que vos VPC et instances sont correctement configurés

Pour vous connecter à vos annuaires, les gérer et les utiliser, vous devez configurer correctement les VPC auxquels les annuaires sont associés. Consultez AWS Conditions préalables à la gestion de

Microsoft AD, Conditions préalables requises pour AD Connector ou Prérequis pour Simple AD pour obtenir plus d'informations sur les exigences de sécurité et de mise en réseau des VPC.

Si vous ajoutez une instance à votre domaine, assurez-vous de disposer d'une connectivité et d'un accès à distance à votre instance, comme décrit dans Joindre une instance Amazon EC2 à votre compte AWS Microsoft AD géré Active Directory.

Tenez compte des limites

Découvrez les différentes limites applicables à votre type d'annuaire spécifique. Le stockage disponible et la taille globale de vos objets sont les seules limites quant au nombre d'objets que vous pouvez stocker dans votre annuaire. Consultez AWS Quotas Managed Microsoft AD, Quotas AD Connector ou Quotas Simple AD pour plus d'informations sur l'annuaire que vous avez choisi.

Comprenez la configuration et l'utilisation AWS des groupes de sécurité de votre annuaire

AWS crée un groupe de sécurité et l'attache aux interfaces réseau élastiques du contrôleur de domaine de votre annuaire. Ce groupe de sécurité bloque le trafic inutile vers le contrôleur de domaine et autorise le trafic nécessaire aux communications Active Directory. AWS configure le groupe de sécurité pour ouvrir uniquement les ports nécessaires aux communications Active Directory. Dans la configuration par défaut, le groupe de sécurité accepte le trafic vers ces ports depuis n'importe quelle adresse IP. AWS attache le groupe de sécurité aux interfaces de vos contrôleurs de domaine accessibles depuis vos VPC pairs ou redimensionnés. Ces interfaces n'étant pas accessibles depuis Internet, même si vous modifiez les tables de routage, changez les connexions réseau vers votre VPC et configurez le service de passerelle NAT. Par conséquent, seules les instances et les ordinateurs qui disposent d'un chemin d'accès réseau dans le VPC peuvent accéder à l'annuaire. Cela simplifie la configuration et vous permet de ne plus avoir à configurer des plages d'adresses spécifiques. Au lieu de cela, vous configurez dans le VPC des routes et des groupes de sécurité qui autorisent uniquement le trafic provenant d'instances et d'ordinateurs approuvés.

Modification du groupe de sécurité de l'annuaire

Si vous souhaitez renforcer la sécurité des groupes de sécurité de vos annuaires, vous pouvez les modifier pour accepter le trafic d'une liste d'adresses IP plus restrictive. Par exemple, vous pouvez modifier les adresses acceptées de 0.0.0.0/0 à une plage CIDR spécifique à un seul sous-réseau ou ordinateur. De même, vous pouvez choisir de restreindre les adresses de destination vers lesquelles vos contrôleurs de domaine peuvent communiquer. Effectuez ces modifications uniquement si

vous avez entièrement compris le fonctionnement du filtrage des groupes de sécurité. Pour plus d'informations, veuillez consulter la section Amazon EC2 security groups for Linux instances (français non garanti) dans le Guide de l'utilisateur Amazon EC2. Des modifications inappropriées peuvent entraîner une perte de communication avec les ordinateurs et les instances concernés. AWS recommande de ne pas essayer d'ouvrir des ports supplémentaires vers le contrôleur de domaine car cela réduit la sécurité de votre répertoire. Lisez attentivement le Modèle de responsabilité partagée AWS.

> **Warning**
>
> Vous êtes techniquement en mesure d'associer les groupes de sécurité utilisés par votre annuaire avec d'autres instances EC2 que vous créez. Il AWS déconseille toutefois cette pratique. AWS peut avoir des raisons de modifier le groupe de sécurité sans préavis pour répondre aux besoins fonctionnels ou de sécurité du répertoire géré. Ces modifications affectent toutes les instances avec lesquelles vous associez le groupe de sécurité de l'annuaire. De plus, l'association du groupe de sécurité de l'annuaire avec vos instances EC2 entraîne un risque de sécurité potentiel pour vos instances EC2. Le groupe de sécurité de l'annuaire accepte le trafic sur les ports Active Directory requis depuis n'importe quelle adresse IP. Si vous associez ce groupe de sécurité avec une instance EC2 dont l'adresse IP publique est rattachée à Internet, n'importe quel ordinateur sur Internet peut communiquer avec votre instance EC2 sur les ports ouverts.

Configuration : création de votre annuaire

Voici quelques suggestions à prendre en compte lorsque vous créez votre annuaire.

Rétention de vos ID et mot de passe d'administrateur

Lorsque vous configurez votre annuaire, vous fournissez un mot de passe pour le compte d'administrateur. Cet identifiant de compte est Admin for AWS Managed Microsoft AD. Retenez le mot de passe créé pour ce compte, sinon vous ne serez pas en mesure d'ajouter des objets à votre annuaire.

Créer un jeu d'options DHCP

Nous vous recommandons de créer un ensemble d'options DHCP pour votre AWS Directory Service répertoire et d'attribuer le jeu d'options DHCP au VPC dans lequel se trouve votre répertoire. De cette

façon, toutes les instances de ce VPC peuvent pointer vers le domaine spécifié, et les serveurs DNS peuvent résoudre leurs noms de domaine.

Pour plus d'informations sur les jeux d'options DHCP, veuillez consulter Création ou modification d'un ensemble d'options DHCP.

Activer le paramètre du redirecteur conditionnel

Les paramètres de transfert conditionnel suivants Stockez ce redirecteur conditionnel dans Active Directory, répliquez-le comme suit : doit être activé. L'activation de ces paramètres empêchera le paramètre du redirecteur conditionnel de disparaître lorsqu'un nœud est remplacé en raison d'une défaillance de l'infrastructure ou d'une panne de surcharge.

Déploiement de contrôleurs de domaine supplémentaires

Par défaut, AWS crée deux contrôleurs de domaine qui existent dans des zones de disponibilité distinctes. Cela fournit une résilience aux pannes lors de l'application des correctifs logiciels et d'autres événements qui peuvent rendre un contrôleur de domaine inaccessible ou indisponible. Nous vous recommandons de déployer des contrôleurs de domaine supplémentaires pour augmenter encore plus la résilience et garantir des performances d'augmentation en cas d'événement à long terme affectant l'accès à un contrôleur de domaine ou à une zone de disponibilité.

Pour plus d'informations, consultez Utilisez le service de localisation des contrôleurs de domaine de Windows.

Comprendre les restrictions sur le nom d'utilisateur pour les applications AWS

AWS Directory Service prend en charge la plupart des formats de caractères pouvant être utilisés dans la construction des noms d'utilisateur. Cependant, certaines restrictions de caractères sont appliquées aux noms d'utilisateur qui seront utilisés pour se connecter à AWS des applications, telles qu'Amazon WorkSpaces WorkDocs WorkMail, Amazon ou Amazon QuickSight. Ces restrictions empêchent l'utilisation des caractères suivants :

- Espaces
- Caractères multioctets
- !"#$%&'()*+,/:;<=>?@[\]^`{|}~

> **Note**
>
> Le symbole @ est autorisé s'il précède un suffixe UPN.

Utilisation de votre annuaire

Voici quelques suggestions à garder à l'esprit lorsque vous utilisez votre annuaire.

Ne pas modifier les utilisateurs, groupes et unités d'organisation prédéfinis

Lorsque vous lancez un annuaire, il AWS crée une unité organisationnelle (AWS Directory Service UO) qui contient tous les objets de votre répertoire. Cette unité d'organisation, qui porte le nom NetBIOS que vous avez saisi lorsque vous avez créé votre annuaire, est située dans la racine du domaine. La racine du domaine est détenue et gérée par AWS. Plusieurs groupes et un utilisateur administratif sont créés.

Ne déplacez pas, ne supprimez pas ou ne modifiez pas ces objets prédéfinis. Cela peut rendre votre répertoire inaccessible à la fois par vous-même et AWS. Pour plus d'informations, consultez Qu'est-ce qui est créé avec votre annuaire Microsoft AD Active Directory AWS géré.

Jonction automatique des domaines

Lors du lancement d'une instance Windows destinée à faire partie d'un AWS Directory Service domaine, il est souvent plus facile de rejoindre le domaine dans le cadre du processus de création de l'instance plutôt que de l'ajouter manuellement ultérieurement. Pour joindre automatiquement un domaine, il suffit de sélectionner l'annuaire approprié pour le paramètre Domain join directory lors du lancement d'une nouvelle instance. Pour plus de détails, veuillez consulter Associez facilement une instance Windows Amazon EC2 à votre compte AWS Microsoft AD géré Active Directory.

Configuration appropriée des relations d'approbation

Lorsque vous configurez une relation de confiance entre votre annuaire Microsoft AD AWS géré et un autre annuaire, gardez à l'esprit les consignes suivantes :

- Le type d'approbation doit correspondre des deux côtés (forêt ou externe)
- Assurez-vous que la direction d'approbation est correctement configurée si vous utilisez une approbation unidirectionnelle (sortante sur le domaine d'approbation, entrante sur le domaine approuvé)

- Les noms de domaine complets (FQDNS) et les noms NetBIOS doivent être uniques entre les forêts et les domaines

Pour plus de détails et des instructions spécifiques sur la configuration d'une relation d'approbation, veuillez consulter Création d'une relation d'approbation.

Gestion de votre annuaire

Pensez à utiliser ces suggestions pour la gestion de votre annuaire.

Suivez les performances de votre contrôleur de domaine

Pour optimiser les décisions de dimensionnement et améliorer la résilience et les performances des annuaires, nous vous recommandons d'utiliser CloudWatch des métriques. Pour plus d'informations, consultez Surveiller vos contrôleurs de domaine grâce à des métriques de performance.

Pour obtenir des instructions sur la façon de configurer les métriques du contrôleur de domaine à l'aide de la CloudWatch console, consultez Comment automatiser le dimensionnement de AWS Managed Microsoft AD en fonction des métriques d'utilisation dans le blog sur la AWS sécurité.

Planifiez soigneusement les extensions de schéma

Appliquez soigneusement les extensions de schéma de manière à indexer votre annuaire pour les requêtes importantes et fréquentes. Veillez à ne pas trop indexer l'annuaire, car les index consomment de l'espace d'annuaire, et la modification rapide des valeurs indexées risque d'entraîner des problèmes de performance. Pour ajouter des index, vous devez créer un fichier LDIF (Directory Interchange Format) de LDAP (Lightweight Directory Access Protocol) et étendre la modification de votre schéma. Pour plus d'informations, consultez Étendre votre schéma.

À propos des équilibreurs de charge

N'utilisez pas d'équilibreur de charge devant les points de terminaison Microsoft AD AWS gérés. Microsoft a conçu Active Directory (AD) pour une utilisation avec un algorithme de détection des contrôleurs de domaine (DC) qui permet de détecter le contrôleur de domaine opérationnel le plus réactif sans équilibrage de charge externe. Les équilibreurs de charge réseau externes ne détectent pas avec exactitude les contrôleurs de domaine actifs, ce qui peut entraîner l'envoi de votre application à un contrôleur de domaine qui sera prochainement disponible, mais qui n'est pas encore prêt à être utilisé. Pour plus d'informations, voir Équilibreurs de charge et Active Directory sur Microsoft, TechNet qui recommande de corriger les applications pour qu'elles utilisent correctement Active Directory plutôt que d'implémenter des équilibreurs de charge externes.

Réalisation d'une sauvegarde de votre instance

Si vous décidez d'ajouter manuellement une instance à un AWS Directory Service domaine existant, effectuez d'abord une sauvegarde ou prenez un instantané de cette instance. Cela est particulièrement important lors de la jonction d'une instance Linux. Certaines des procédures utilisées pour ajouter une instance, si elles ne sont pas effectuées correctement, peuvent rendre votre instance inaccessible ou non utilisable. Pour plus d'informations, consultez Création d'un instantané ou d'une restauration de votre annuaire.

Configuration de la messagerie SNS

Avec Amazon Simple Notification Service (Amazon SNS), vous pouvez recevoir des e-mails ou des messages texte (SMS) lorsque le statut de votre annuaire change. Vous êtes averti lorsque votre annuaire passe du statut Active au statut Impaired ou Inoperable. Vous recevez également une notification lorsque l'annuaire renvoie un statut Active (Actif).

N'oubliez pas non plus que si vous avez une rubrique SNS qui reçoit des messages AWS Directory Service, avant de supprimer cette rubrique de la console Amazon SNS, vous devez associer votre annuaire à une autre rubrique SNS. Sinon, vous risquez de manquer des messages importants sur le statut de l'annuaire. Pour savoir comment configurer Amazon SNS, veuillez consulter Configurer les notifications d'état de l'annuaire avec Amazon SNS.

Appliquer les paramètres du service d'annuaire

AWS Managed Microsoft AD vous permet d'adapter votre configuration de sécurité pour répondre à vos exigences de conformité et de sécurité. AWS Managed Microsoft AD déploie et gère la configuration sur tous les contrôleurs de domaine de votre annuaire, y compris lors de l'ajout de nouvelles régions ou de contrôleurs de domaine supplémentaires. Vous pouvez configurer et appliquer ces paramètres de sécurité à tous vos annuaires nouveaux et existants. Vous pouvez le faire dans la console en suivant les étapes indiquées dans Modifier les paramètres de sécurité de l'annuaire ou via l'UpdateSettings API.

Pour plus d'informations, consultez Configurer les paramètres de sécurité de l'annuaire.

Supprimez les applications d'entreprise Amazon avant de supprimer un annuaire

Avant de supprimer un répertoire associé à une ou plusieurs applications Amazon Enterprise telles qu'Amazon WorkSpaces Application Manager WorkSpaces, Amazon WorkDocs, Amazon ou Amazon WorkMail Relational Database Service (Amazon RDS), vous devez d'abord supprimer chaque

application. AWS Management Console Pour en savoir plus sur la suppression de ces applications, veuillez consulter Supprimer votre Microsoft AD AWS géré.

Utiliser les clients SMB 2.x lors de l'accès aux partages SYSVOL et NETLOGON

Les ordinateurs clients utilisent le module SMB (Server Message Block) pour accéder aux partages SYSVOL et NETLOGON sur les contrôleurs de domaine AWS Microsoft AD gérés pour la stratégie de groupe, les scripts de connexion et d'autres fichiers. AWS Managed Microsoft AD ne prend en charge que la version 2.0 (SMBv2) et les versions ultérieures de SMB.

Les protocoles SMBv2 et les versions plus récentes ajoutent un certain nombre de fonctionnalités qui améliorent les performances du client et augmentent la sécurité de vos contrôleurs de domaine et de vos clients. Cette modification fait suite aux recommandations de l'United States Computer Emergency Readiness Team et de Microsoft pour désactiver SMBv1.

> **Important**
>
> Si vous utilisez actuellement des clients SMBv1 pour accéder aux partages SYSVOL et NETLOGON de votre contrôleur de domaine, vous devez mettre à jour ces clients pour utiliser SMBv2 ou les versions plus récentes. Votre répertoire fonctionnera correctement, mais vos clients SMBv1 ne parviendront pas à se connecter aux partages SYSVOL et NETLOGON de vos contrôleurs de domaine AWS Microsoft AD gérés et ne pourront pas non plus traiter la politique de groupe.

Les clients SMBv1 fonctionneront avec tous les autres serveurs de fichiers compatibles SMBv1 que vous possédez. Toutefois, il est AWS recommandé de mettre à jour tous vos serveurs et clients SMB vers SMBv2 ou une version plus récente. Pour en savoir plus sur la désactivation de SMBv1 et sa mise à jour vers les nouvelles versions SMB sur vos systèmes, consultez ces publications sur Microsoft et le Support. TechNet

Suivi des connexions à distance SMBv1

Vous pouvez consulter le journal des événements Microsoft-Windows-SMBServer/Audit Windows en vous connectant à distance au contrôleur de domaine AWS Microsoft AD géré. Tous les événements de ce journal indiquent des connexions SMBv1. Voici un exemple des informations que vous pouvez voir dans l'un de ces journaux :

Accès SMB1

Adresse du client : ###.###.###.###

Conseils :

Cet événement indique qu'un client a tenté d'accéder au serveur à l'aide de SMB1. Pour arrêter d'auditer l'accès au SMB1, utilisez l'Windows PowerShellapplet de commande Set-. SmbServerConfiguration

Programmation de vos applications

Avant de programmer vos applications, prenez en compte les éléments suivants :

Utilisez le service de localisation des contrôleurs de domaine de Windows

Lorsque vous développez des applications, utilisez le service de localisation Windows DC ou le service DNS dynamique (DDNS) de votre Managed AWS Microsoft AD pour localiser les contrôleurs de domaine (DC). Ne codez pas en dur les applications avec l'adresse d'un contrôleur de domaine. Le service de localisation des contrôleurs de domaine permet de garantir que l'annuaire est distribué et vous permet de tirer parti de la mise à l'échelle horizontale en ajoutant des contrôleurs de domaine à votre déploiement. Si vous liez votre application à un contrôleur de domaine corrigé et que celui-ci subit une application de correctifs ou une récupération, votre application perdra l'accès au contrôleur de domaine au lieu d'utiliser l'un des contrôleurs de domaine restants. En outre, le codage en dur du contrôleur de domaine peut entraîner la création d'un point chaud sur un seul contrôleur de domaine. Dans des cas extrêmes, la création de ce point chaud peut entraîner une absence de réponse de votre contrôleur de domaine. Dans de tels cas, l'automatisation de l' AWS annuaire peut également signaler le répertoire comme étant altéré et peut déclencher des processus de restauration qui remplacent le contrôleur de domaine qui ne répond pas.

Testez la charge avant de lancer la production

Assurez-vous de procéder à des tests avec des objets et des requêtes représentatifs de votre charge de travail de production afin de confirmer que l'annuaire s'adapte à la charge de travail de votre application. Si vous avez besoin de capacité supplémentaire, procédez à des tests avec des contrôleurs de domaine supplémentaires tout en répartissant les requêtes entre les contrôleurs de domaine. Pour plus d'informations, consultez Déploiement de contrôleurs de domaine supplémentaires.

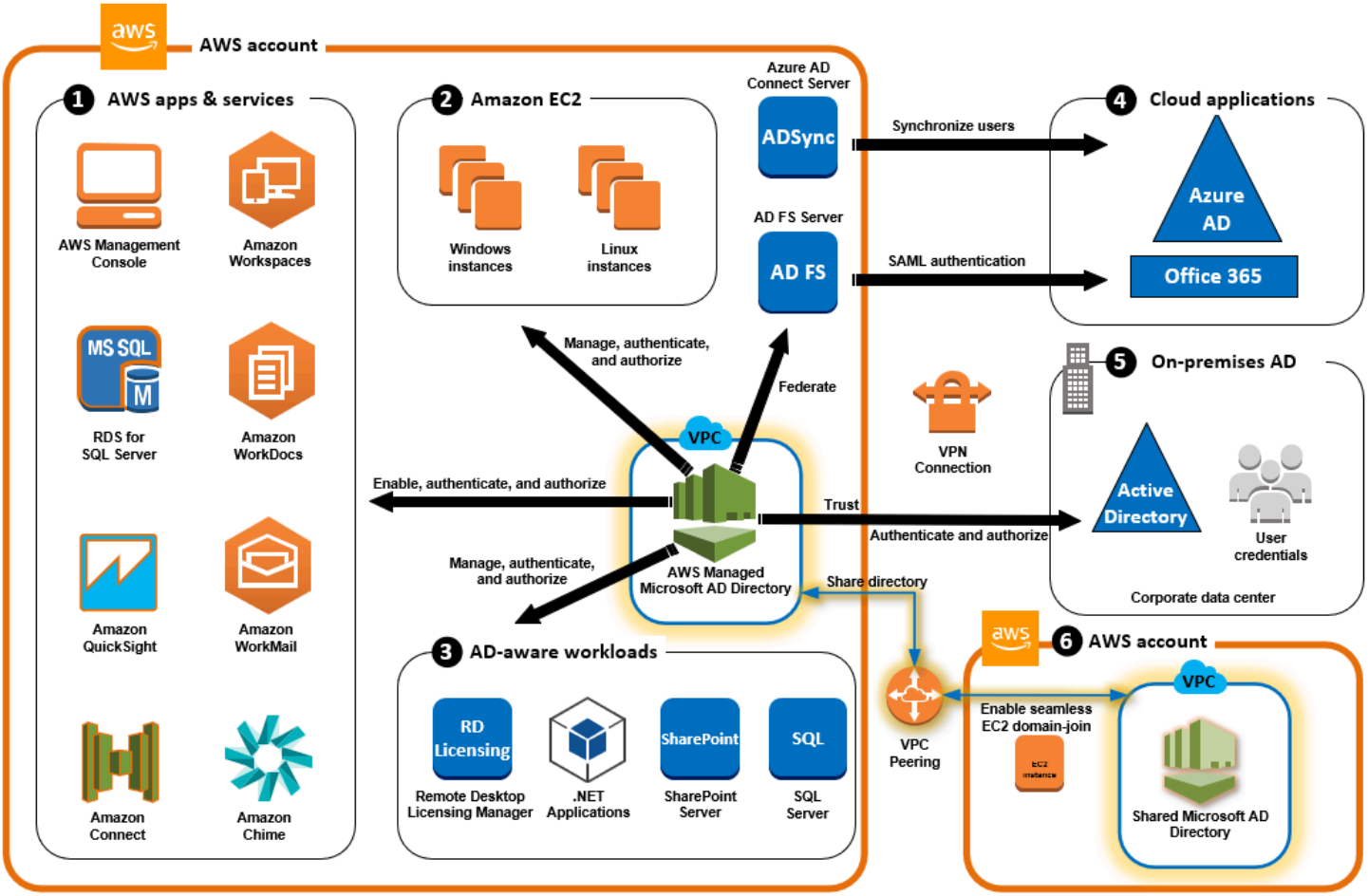
Utilisez des requêtes LDAP efficaces

De vastes requêtes LDAP effectuées dans un contrôleur de domaine sur des dizaines de milliers d'objets peuvent consommer des cycles de processeur considérables sur un seul contrôleur de domaine, ce qui se traduit par la création de points chauds. Ces points chauds peuvent affecter les applications qui partagent le même contrôleur de domaine lors de la requête.

Cas d'utilisation de AWS Managed Microsoft AD

Avec AWS Managed Microsoft AD, vous pouvez partager un répertoire unique pour plusieurs cas d'utilisation. Par exemple, vous pouvez partager un annuaire pour authentifier et autoriser l'accès aux applications .NET, Amazon RDS for SQL Server avec l'authentification Windows activée, et Amazon Chime pour la messagerie et la vidéoconférence.

Le schéma suivant montre certains des cas d'utilisation de votre annuaire Microsoft AD AWS géré. Il s'agit notamment de la possibilité d'accorder à vos utilisateurs l'accès à des applications cloud externes et de permettre à vos utilisateurs Active Directory locaux de gérer les ressources du AWS cloud et d'y avoir accès.



Utilisez AWS Managed Microsoft AD pour l'un des cas d'utilisation professionnels suivants.

Rubriques

- Cas d'utilisation 1 : connectez-vous aux AWS applications et aux services avec des informations d'identification Active Directory
- Cas d'utilisation 2 : gestion des instances Amazon EC2
- Cas d'utilisation 3 : fournir des services d'annuaire à vos charges de travail compatibles avec Active Directory
- Cas d'utilisation 4 : AWS IAM Identity Center vers Office 365 et d'autres applications cloud
- Cas d'utilisation 5 : étendre votre Active Directory sur site au cloud AWS
- Cas d'utilisation 6 : partagez votre annuaire pour associer facilement des instances Amazon EC2 à un domaine sur plusieurs comptes AWS

Cas d'utilisation 1 : connectez-vous aux AWS applications et aux services avec des informations d'identification Active Directory

Vous pouvez activer plusieurs AWS applications et services tels que Amazon Chime AWS Client VPNAWS Management ConsoleAWS IAM Identity Center, Amazon Connect, Amazon FSx, Amazon, Amazon RDS for SQL Server, QuickSightAmazon, Amazon, Amazon, WorkDocs WorkMail Amazon WorkSpaces, et utiliser AWS votre annuaire Microsoft AD géré. Lorsque vous activez une AWS application ou un service dans votre annuaire, vos utilisateurs peuvent accéder à l'application ou au service avec leurs informations d'identification Active Directory.

Par exemple, vous pouvez permettre à vos utilisateurs de se connecter à l' AWS Management Console aide de leurs informations d'identification Active Directory. Pour ce faire, vous l'activez en AWS Management Console tant qu'application dans votre annuaire, puis vous assignez vos utilisateurs et groupes Active Directory à des rôles IAM. Lorsque vos utilisateurs se connectent au AWS Management Console, ils assument un rôle IAM pour gérer les AWS ressources. Cela vous permet d'accorder plus facilement à vos utilisateurs un accès à AWS Management Console sans qu'il soit nécessaire de configurer et de gérer une infrastructure SAML distincte.

Pour améliorer encore l'expérience de l'utilisateur final, vous pouvez activer les fonctionnalités d'authentification unique pour Amazon WorkDocs, qui permettent à vos utilisateurs d'accéder à Amazon WorkDocs depuis un ordinateur connecté à l'annuaire sans avoir à saisir leurs informations d'identification séparément.

Vous pouvez accorder l'accès aux comptes utilisateurs de votre annuaire ou de votre Active Directory local, afin qu'ils puissent se connecter AWS Management Console ou AWS CLI utiliser leurs informations d'identification et autorisations existantes pour gérer les AWS ressources en attribuant des rôles IAM directement aux comptes utilisateurs existants.

Intégration AWS de FSx for Windows File Server à Managed Microsoft AD

L'intégration de FSx for Windows File Server AWS à Managed Microsoft AD fournit un système de fichiers de protocole SMB (Server Message Block) natif entièrement géré basé sur Microsoft Windows qui vous permet de déplacer facilement vos applications et clients Windows (qui utilisent le stockage de fichiers partagé) vers. AWS Bien que FSx for Windows File Server puisse être intégré à un Microsoft Active Directory autogéré, nous n'aborderons pas ce scénario ici.

Cas d'utilisation et ressources courants d'Amazon FSx

Cette section fournit une référence aux ressources sur les intégrations courantes de FSx for Windows File Server avec les cas d'utilisation de AWS Managed Microsoft AD. Chacun des cas d'utilisation présentés dans cette section commence par une configuration de base de AWS Managed Microsoft AD et de FSx for Windows File Server. Pour plus d'informations sur la création de ces configurations, veuillez consulter :

- Commencer à utiliser AWS Managed Microsoft AD
- Mise en route avec Amazon FSx

FSx for Windows File Server en tant que stockage permanent sur des conteneurs Windows

Amazon Elastic Container Service (ECS) prend désormais en charge les conteneurs Windows sur les instances de conteneur qui sont lancées avec l'AMI Windows optimisée pour Amazon ECS. Les instances de conteneur Windows utilisent leur propre version de l'agent de conteneur Amazon ECS. Sur l'AMI Windows optimisée pour Amazon ECS, l'agent de conteneur Amazon ECS s'exécute comme un service sur l'hôte.

Amazon ECS prend en charge l'authentification Active Directory pour les conteneurs Windows par l'intermédiaire d'un type de compte de service spécial appelé gMSA (group Managed Service Account). Étant donné que les conteneurs Windows ne peuvent pas être joints à un domaine, vous devez configurer un conteneur Windows pour qu'il s'exécute avec un compte gMSA.

Éléments connexes

- FSx for Windows File Server en tant que stockage permanent sur des conteneurs Windows
- Comptes de service administrés de groupe

Support pour Amazon AppStream 2.0

Amazon AppStream 2.0 est un service de streaming d'applications entièrement géré. Il fournit une gamme de solutions permettant aux utilisateurs de sauvegarder et d'accéder aux données par le biais de leurs applications. Amazon FSx avec AppStream 2.0 fournit un lecteur de stockage persistant personnel utilisant Amazon FSx et peut être configuré pour fournir un dossier partagé permettant d'accéder aux fichiers courants.

Éléments connexes

- Procédure pas à pas 4 : Utilisation d'Amazon FSx avec Amazon 2.0 AppStream
- Utilisation d'Amazon FSx avec Amazon 2.0 AppStream
- Utilisation d'Active Directory avec AppStream 2.0

Prise en charge de Microsoft SQL Server

FSx for Windows File Server peut être utilisé comme option de stockage pour Microsoft SQL Server 2012 (à partir de la version 11.x de 2012) et les bases de données système plus récentes (notamment Master, Model, MSDB et TempDB), ainsi que pour les bases de données utilisateur du moteur de base de données.

Éléments connexes

- Installez SQL Server avec un stockage en partage de fichiers SMB
- Simplifiez vos déploiements à haute disponibilité de Microsoft SQL Server à l'aide de FSx for Windows File Server
- Comptes de service administrés de groupe

Prise en charge des dossiers personnels et des profils d'utilisateurs itinérants

FSx for Windows File Server peut être utilisé pour stocker les données des dossiers personnels des utilisateurs Active Directory et de Mes documents dans un emplacement central. FSx for Windows File Server peut également être utilisé pour stocker des données provenant de profils d'utilisateurs itinérants.

Éléments connexes

- Les annuaires personnels de Windows simplifiés avec Amazon FSx
- Déploiement de profils d'utilisateurs itinérants
- Utilisation de FSx for Windows File Server avec WorkSpaces

Prise en charge du partage de fichiers en réseau

Les partages de fichiers en réseau sur un serveur FSx for Windows File Server constituent une solution de partage de fichiers gérée et capable d'être mise à l'échelle. L'un des cas d'utilisation est celui des lecteurs mappés pour les clients qui peuvent être créés manuellement ou via une politique de groupe.

Éléments connexes

- Démonstration 6 : mettre à l'échelle les performances avec Shards
- Mappage des lecteurs
- Utilisation de FSx for Windows File Server avec WorkSpaces

Prise en charge de l'installation du logiciel de politique de groupe

La taille et les performances du dossier SYSVOL étant limitées, il est recommandé d'éviter de stocker des données telles que des fichiers d'installation de logiciels dans ce dossier. Comme solution possible à ce problème, FSx for Windows File Server peut être configuré pour stocker tous les fichiers logiciels installés à l'aide de la politique de groupe.

Éléments connexes

- Comment utiliser la politique de groupe pour installer des logiciels à distance dans Windows Server 2008 et Windows Server 2003

Prise en charge des cibles Windows Server Backup

FSx for Windows File Server peut être configuré comme lecteur cible dans Windows Server Backup à l'aide du partage de fichiers UNC. Dans ce cas, vous devez spécifier le chemin d'accès UNC vers votre FSx for Windows File Server plutôt que vers le volume EBS attaché.

Éléments connexes

- Effectuez une récupération de l'état du système de votre serveur

Amazon FSx prend également en charge le partage d'annuaires AWS Microsoft AD géré. Pour plus d'informations, consultez :

- Partagez votre annuaire
- Utilisation d'Amazon FSx avec Managed AWS Microsoft AD dans un autre VPC ou un autre compte

Intégration d'Amazon RDS à AWS Managed Microsoft AD

Amazon RDS prend en charge l'authentification externe des utilisateurs de bases de données à l'aide de Kerberos avec Microsoft Active Directory. Kerberos est un protocole d'authentification réseau qui utilise les tickets et la cryptographie de clé symétrique pour vous éviter d'acheminer vos mots de passe via le réseau. La prise en charge de Kerberos et Active Directory par Amazon RDS procure les avantages d'une authentification unique et centralisée des utilisateurs de bases de données, afin que vous puissiez conserver vos informations d'identification dans Active Directory.

Pour commencer à utiliser ce cas d'utilisation, vous devez d'abord configurer une configuration de base de AWS Managed Microsoft AD et Amazon RDS.

- Commencer à utiliser AWS Managed Microsoft AD
- Mise en route avec Amazon RDS

Tous les cas d'utilisation mentionnés ci-dessous débuteront par une base AWS Managed Microsoft AD et Amazon RDS et expliqueront comment intégrer Amazon RDS à Managed AWS Microsoft AD.

- Utilisation de l'authentification Windows avec une instance de base de données Amazon RDS for SQL Server
- Utilisation de l'authentification Kerberos pour MySQL
- Utilisation de l'authentificationKerberos avec Amazon RDS for Oracle
- Utilisation de l'authentification Kerberos avec Amazon RDS for PostgreSQL

Amazon RDS prend également en charge le partage d'annuaires Microsoft AD AWS géré. Pour plus d'informations, veuillez consulter :

- Partagez votre annuaire
- Regrouper vos instances Amazon RDS DB des différents comptes dans un seul domaine partagé

Pour plus d'informations sur la jonction d'un Amazon RDS for SQL Server à votre Active Directory, veuillez consulter Join Amazon RDS for SQL Server to your self-managed Active Directory (français non garanti).

Application .NET utilisant Amazon RDS for SQL Server avec des comptes de service administrés de groupe

Vous pouvez intégrer Amazon RDS for SQL Server à une application .NET de base et à des comptes de services administrés de groupe (gMSA). Pour plus d'informations, consultez Comment AWS Managed Microsoft AD contribue à simplifier le déploiement et à améliorer la sécurité des applications .NET intégrées à Active Directory

Cas d'utilisation 2 : gestion des instances Amazon EC2

À l'aide des outils d'administration Active Directory habituels, vous pouvez appliquer des objets de politique de groupe (GPO) Active Directory pour gérer de manière centralisée vos instances Amazon EC2 pour Windows ou Linux en joignant vos instances à votre domaine Microsoft AWS AD géré.

En outre, vos utilisateurs peuvent se connecter à vos instances à l'aide de leurs informations d'identification Active Directory. Ainsi, vous n'avez plus besoin d'utiliser d'informations d'identification d'instance individuelle ou distribuer de fichiers de clé privée (PEM). Cela vous permet d'accorder ou de révoquer instantanément l'accès aux utilisateurs à l'aide des outils d'administration des utilisateurs Active Directory que vous utilisez déjà.

Cas d'utilisation 3 : fournir des services d'annuaire à vos charges de travail compatibles avec Active Directory

AWS Managed Microsoft AD est un véritable Microsoft Active Directory qui vous permet d'exécuter des charges de travail compatibles avec Active Directory traditionnelles, telles que Remote Desktop Licensing Manager et Microsoft et SharePoint Microsoft SQL Server Always On in the Cloud.
AWS AWS Managed Microsoft AD vous aide également à simplifier et à améliorer la sécurité des applications .NET intégrées à Active Directory en utilisant des comptes de service gérés de groupe (GMSA) et une délégation contrainte Kerberos (KCD).

Cas d'utilisation 4 : AWS IAM Identity Center vers Office 365 et d'autres applications cloud

Vous pouvez utiliser AWS Managed Microsoft AD AWS IAM Identity Center pour fournir des applications cloud. Vous pouvez utiliser Microsoft Entra Connect (anciennement connu sous le nomAzure Active Directory Connect) pour synchroniser vos utilisateurs dans Microsoft Entra (anciennement connu sous le nom de Azure Active Directory (AzureAD)), puis utiliser Active Directory

Federation Services (AD FS) afin que vos utilisateurs puissent accéder à Microsoft Office 365 et à d'autres applications cloud SAML 2.0 en utilisant leurs informations d'identification Active Directory.

L'intégration de AWS Managed Microsoft AD à IAM Identity Center ajoute des fonctionnalités SAML à votre AWS Microsoft AD géré et/ou à vos domaines fiables sur site. Une fois intégré, vos utilisateurs peuvent utiliser IAM Identity Center avec des services compatibles avec le AWS Management Console protocole SAML, notamment des applications cloud tierces telles qu'Office 365, Concur et Salesforce, sans avoir à configurer une infrastructure SAML. Pour une démonstration du processus permettant à vos utilisateurs locaux d'utiliser IAM Identity Center, visionnez la vidéo suivante YouTube .

> **Note**
>
> AWS Single Sign-On a été renommé IAM Identity Center.

Cas d'utilisation 5 : étendre votre Active Directory sur site au cloud AWS

Si vous disposez déjà d'une infrastructure Active Directory et que vous souhaitez l'utiliser lors de la migration de charges de travail compatibles avec Active Directory vers le cloud AWS , Managed AWS Microsoft AD peut vous aider. Vous pouvez utiliser les approbations Active Directory pour connecter AWS Managed Microsoft AD à votre Active Directory existant. Cela signifie que vos utilisateurs peuvent accéder aux AWS applications compatibles avec Active Directory avec leurs informations d'identification Active Directory locales, sans que vous ayez à synchroniser les utilisateurs, les groupes ou les mots de passe.

Par exemple, vos utilisateurs peuvent se connecter à Amazon AWS Management Console et à l'aide WorkSpaces de leurs noms d'utilisateur et mots de passe Active Directory existants. En outre, lorsque vous utilisez des applications compatibles SharePoint avec Active Directory, telles que Managed AWS Microsoft AD, les utilisateurs Windows connectés peuvent accéder à ces applications sans avoir à saisir à nouveau leurs informations d'identification.

Vous pouvez également migrer votre domaine Active Directory sur site AWS afin de vous libérer de la charge opérationnelle de votre infrastructure Active Directory à l'aide du kit de migration Active Directory (ADMT) et du service d'exportation de mots de passe (PES) pour effectuer la migration.

Cas d'utilisation 6 : partagez votre annuaire pour associer facilement des instances Amazon EC2 à un domaine sur plusieurs comptes AWS

Le partage de votre répertoire entre plusieurs AWS comptes vous permet de gérer facilement AWS des services tels qu'Amazon EC2 sans avoir à gérer un répertoire pour chaque compte et chaque VPC. Vous pouvez utiliser votre annuaire depuis n'importe quel compte AWS et n'importe quel VPC Amazon à l'intérieur d'une région AWS . Cette fonctionnalité permet de gérer, de façon plus simple et plus économique, les charges de travail prenant en charge les annuaires, avec un seul annuaire, entre différents comptes et VPC. Par exemple, vous pouvez maintenant gérer vos charges de travail Windows déployées dans les instances EC2 entre différents comptes et VPC, en toute simplicité, en utilisant un même annuaire AWS Managed Microsoft AD.

Lorsque vous partagez votre répertoire AWS Managed Microsoft AD avec un autre AWS compte, vous pouvez utiliser la console Amazon EC2 ou AWS Systems Managerjoindre facilement vos instances depuis n'importe quel Amazon VPC au sein du compte et de la région. AWS Vous pouvez déployer rapidement vos charges de travail prenant en charge les annuaires sur les instances EC2, en éliminant le besoin de joindre manuellement vos instances à un domaine ou de déployer des annuaires dans chaque compte et VPC. Pour plus d'informations, voir Partagez votre annuaire.

Comment administrer AWS Managed Microsoft AD

Cette section répertorie toutes les procédures d'exploitation et de maintenance d'un environnement Microsoft AD AWS géré.

Rubriques

- Sécuriser votre annuaire AWS Managed Microsoft AD
- Surveiller votre AWS Managed Microsoft AD
- Réplication multi-régions
- Partagez votre annuaire
- Joindre une instance Amazon EC2 à votre compte AWS Microsoft AD géré Active Directory
- Gérer des utilisateurs et des groupes dans AWS Managed Microsoft AD
- Connectez-vous à votre infrastructure Active Directory existante
- Connectez votre Microsoft AD AWS géré à Microsoft Entra Connect Sync
- Étendre votre schéma
- Gérez votre répertoire Microsoft AD AWS géré

- Accorder aux utilisateurs et aux groupes l'accès aux ressources AWS
- Permettre l'accès aux AWS applications et aux services
- Activation de l'accès à AWS Management Console avec les informations d'identification AD
- Déploiement de contrôleurs de domaine supplémentaires
- Migrer les utilisateurs d'Active Directory vers AWS Managed Microsoft AD

Sécuriser votre annuaire AWS Managed Microsoft AD

Cette section décrit les éléments à prendre en compte pour sécuriser votre environnement AWS Managed Microsoft AD.

Rubriques

- Gérer les politiques de mot de passe pour AWS Managed Microsoft AD
- Activer l'authentification multifactorielle pour AWS Managed Microsoft AD
- Activer le protocole LDAP ou LDAPS sécurisé
- Gérez la conformité pour AWS Managed Microsoft AD
- Améliorer la configuration de la sécurité réseau AWS Managed Microsoft AD
- Configurer les paramètres de sécurité de l'annuaire
- Configurer le AWS Private CA connecteur pour AD

Gérer les politiques de mot de passe pour AWS Managed Microsoft AD

AWS Managed Microsoft AD vous permet de définir et d'attribuer différentes politiques de verrouillage des mots de passe et des comptes (également appelées politiques de mot de passe détaillées) pour les groupes d'utilisateurs que vous gérez dans votre domaine AWS Microsoft AD géré. Lorsque vous créez un annuaire Microsoft AD AWS géré, une politique de domaine par défaut est créée et appliquée auActive Directory. Cette stratégie contient les paramètres suivants :

Politique	Paramètre
Appliquer l'historique des mots de passe	24 mots de passe mémorisés
Durée de vie maximale du mot de passe	42 jours *
Durée de vie minimale du mot de passe	1 jour

Politique	Paramètre
Longueur minimum du mot de passe	7 caractères
Le mot de passe doit respecter des exigences de complexité	Activées
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivées

* Remarque : la durée de vie maximale du mot de passe de 42 jours comprend le mot de passe administrateur.

Par exemple, vous pouvez attribuer un paramètre de stratégie moins strict pour les employés qui n'ont accès qu'à des informations de faible importance. Pour les cadres supérieurs qui accèdent régulièrement à des informations confidentielles, vous pouvez appliquer des paramètres plus stricts.

Les ressources suivantes Microsoft Active Directory permettent d'en savoir plus sur les politiques de mot de passe et les politiques de sécurité détaillées :

- Configuration des paramètres de politique de sécurité
- Exigences de complexité des mots de passe
- Complexité des mots de passe et considérations

AWS fournit un ensemble de politiques de mot de passe détaillées dans AWS Managed Microsoft AD que vous pouvez configurer et attribuer à vos groupes. Pour configurer les politiques, vous pouvez utiliser des outils de Microsoft stratégie standard tels que le centre d'Active Directoryadministration. Pour commencer à utiliser les outils Microsoft de politique, voirInstallation des outils d'administration Active Directory pour Microsoft AD AWS géré.

Comment les politiques relatives aux mots de passe sont appliquées

Il existe des différences dans la façon dont les politiques de mot de passe affinées sont appliquées selon que le mot de passe a été réinitialisé ou modifié. Les utilisateurs du domaine peuvent modifier leur propre mot de passe. Un Active Directory administrateur ou un utilisateur disposant des autorisations nécessaires peut réinitialiser les mots de passe des utilisateurs. Consultez le tableau suivant pour plus d'informations.

Politique	Réinitialisation du mot	Changement de mot de passe
Appliquer l'historique des mots de passe	 Non	 Oui
Durée de vie maximale du mot de passe	 Oui	 Oui
Durée de vie minimale du mot de passe	 Non	 Oui
Longueur minimum du mot de passe	 Oui	 Oui
Le mot de passe doit respecter des exigences de complexité	 Oui	 Oui

Ces différences ont des conséquences sur le plan de la sécurité. Par exemple, chaque fois que le mot de passe d'un utilisateur est réinitialisé, les politiques relatives à l'historique des mots de passe et à l'âge minimum des mots de passe ne sont pas appliquées. Pour plus d'informations, consultez la documentation Microsoft sur les considérations de sécurité liées à l'application de l'historique des mots de passe et des politiques relatives à l'âge minimum des mots de passe.

Rubriques

- Paramètres de stratégie pris en charge
- Déléguer des autorisations de gestion de vos stratégies de mot de passe

- Attribuer des stratégies de mot de passe à vos utilisateurs

Article AWS de blog sur la sécurité connexe

- Comment configurer des politiques de mot de passe encore plus strictes pour répondre à vos normes de sécurité à l'aide AWS Directory Service de AWS Managed Microsoft AD

Paramètres de stratégie pris en charge

AWS Managed Microsoft AD inclut cinq politiques détaillées avec une valeur de priorité non modifiable. Les stratégies possèdent un certain nombre de propriétés que vous pouvez configurer pour mettre en œuvre vos mots de passe et actions de verrouillage de compte en cas d'échecs de connexion. Vous pouvez attribuer des stratégies à zéro ou plusieurs groupes Active Directory. Si un utilisateur final est membre de plusieurs groupes et reçoit plus d'une stratégie de mot de passe, Active Directory applique la stratégie avec la valeur de priorité la plus faible.

AWS politiques de mots de passe prédéfinies

Le tableau suivant répertorie les cinq politiques incluses dans votre répertoire Microsoft AD AWS géré et la valeur de priorité qui leur est attribuée. Pour plus d'informations, consultez Priorité.

Nom de la politique	Priorité
CustomerPSO-01	10
CustomerPSO-02	20
CustomerPSO-03	30
CustomerPSO-04	40
CustomerPSO-05	50

Propriétés de stratégie de mot de passe

Vous pouvez modifier les propriétés suivantes dans vos stratégies de mot de passe pour respecter les normes de conformité qui répondent à vos besoins métier.

- Nom de la politique

- Appliquer l'historique des mots de passe
- Longueur minimum du mot de passe
- Durée de vie minimale du mot de passe
- Durée de vie maximale du mot de passe
- Enregistrer les mots de passe en utilisant un chiffrement réversible
- Le mot de passe doit respecter des exigences de complexité

Vous ne pouvez pas modifier les valeurs de priorité pour ces stratégies. Pour plus de détails sur la manière dont ces paramètres affectent l'application des mots de passe, voir AD DS : politiques de mot de passe précises sur le site Web de Microsoft TechNet. Pour obtenir des informations générales sur ces politiques, consultez la section Politique en matière de mots de passe sur le TechNet site Web de Microsoft.

Stratégies de verrouillage de compte

Vous pouvez également modifier les propriétés suivantes de vos stratégies de mot de passe pour indiquer si et comment Active Directory doit verrouiller un compte en cas d'échecs de connexion :

- Nombre d'échecs de connexion autorisés
- Durée de verrouillage du compte
- Réinitialiser les tentatives de connexion échouées après une période donnée

Pour obtenir des informations générales sur ces politiques, consultez la section Politique de verrouillage des comptes sur le TechNet site Web de Microsoft.

Priorité

Les stratégies avec une valeur de priorité inférieure ont une priorité plus élevée. Vous pouvez attribuer des stratégies de mot de passe à des groupes de sécurité Active Directory. Même si vous devez appliquer une seule stratégie à un groupe de sécurité, un même utilisateur peut recevoir plus d'une stratégie de mot de passe. Par exemple, si `jsmith` est membre du groupe RESSOURCES HUMAINES et également membre du groupe RESPONSABLES. Si vous attribuez CustomerPSO-05 (avec une priorité de 50) au groupe RESSOURCES HUMAINES, et CustomerPSO-04 (avec une priorité de 40) au groupe RESPONSABLES, CustomerPSO-04 a la priorité la plus élevée et Active Directory applique cette stratégie à `jsmith`.

Si vous attribuez plusieurs stratégies à un utilisateur ou un groupe, Active Directory détermine la stratégie résultante comme suit :

1. Une stratégie que vous attribuez directement à l'objet utilisateur s'applique.
2. Si aucune stratégie n'est attribuée directement à l'objet utilisateur, la stratégie avec la valeur de priorité la plus faible reçue par l'utilisateur suite à son adhésion à un groupe s'applique.

Pour plus de détails, voir AD DS : politiques de mot de passe détaillées sur le site Web de Microsoft TechNet.

Déléguer des autorisations de gestion de vos stratégies de mot de passe

Vous pouvez déléguer les autorisations de gestion des politiques de mot de passe à des comptes utilisateur spécifiques que vous avez créés dans votre AWS Managed Microsoft AD en ajoutant les comptes au groupe de sécurité AWS Delegated Fine Grained Password Policy Administrators. Lorsqu'un compte devient membre de ce groupe, il dispose des autorisations nécessaires pour modifier et configurer les stratégies de mot de passe précédemment mentionnées.

Pour déléguer des autorisations de gestion de vos stratégies de mot de passe

1. Lancez le centre d'administration Active Directory (ADAC) à partir de n'importe quelle instance EC2 gérée que vous avez jointe à votre domaine AWS Microsoft AD géré.
2. Basculez vers l'arborescence et accédez à l'unité d'organisation AWS Delegated Groups (Groupes délégués). Pour plus d'informations sur cette unité d'organisation, veuillez consulter Qu'est-ce qui est créé avec votre annuaire Microsoft AD Active Directory AWS géré.
3. Recherchez le groupe d'utilisateurs AWS Delegated Fine Grained Password Policy Administrators (Administrateurs délégués de stratégies de mot de passe affinées). Ajoutez des utilisateurs ou des groupes de votre domaine à ce groupe.

Attribuer des stratégies de mot de passe à vos utilisateurs

Les comptes utilisateurs membres du groupe de sécurité AWS Delegated Fine Grained Password Policy Administrators (Administrateurs délégués de stratégies de mot de passe affinées) peuvent recourir à la procédure suivante pour attribuer des stratégies à des utilisateurs et des groupes de sécurité.

Pour attribuer des stratégies de mot de passe à vos utilisateurs

1. Lancez le centre d'administration Active Directory (ADAC) à partir de n'importe quelle instance EC2 gérée que vous avez jointe à votre domaine AWS Microsoft AD géré.
2. Passez à l'arborescence et accédez à System\Password Settings Container.
3. Double-cliquez sur la stratégie affinée que vous souhaitez modifier. Cliquez sur Ajouter pour modifier les propriétés de la stratégie et ajouter des utilisateurs ou des groupes de sécurité à la stratégie. Pour plus d'informations sur les stratégies affinées fournies par défaut avec AWS Managed Microsoft AD, veuillez consulter AWS politiques de mots de passe prédéfinies.
4. Pour vérifier que la politique de mot de passe a été appliquée, exécutez la PowerShell commande suivante :

```
Get-ADUserResultantPasswordPolicy -Identity 'username'
```

> **Note**
>
> Évitez d'utiliser la commande `net user`, car ses résultats peuvent être inexacts.

Si vous ne configurez aucune des cinq politiques de mot de passe de votre annuaire Microsoft AD AWS géré, Active Directory utilise la stratégie de groupe de domaines par défaut. Pour plus d'informations sur l'utilisation du Conteneur de paramètres de mots de passe, veuillez consulter ce billet de blog Microsoft.

Activer l'authentification multifactorielle pour AWS Managed Microsoft AD

Vous pouvez activer l'authentification multifactorielle (MFA) pour votre annuaire Microsoft AD AWS géré afin de renforcer la sécurité lorsque vos utilisateurs spécifient leurs informations d'identification AD pour y accéder. Applications Amazon Enterprise prises en charge Lorsque vous activez la MFA, vos utilisateurs saisissent leur nom d'utilisateur et leur mot de passe (premier facteur), comme ils en ont l'habitude, mais ils doivent également saisir un code d'authentification (deuxième facteur) qui leur est fourni par votre solution MFA matérielle ou virtuelle. Ensemble, ces facteurs offrent une sécurité supplémentaire en empêchant l'accès à vos applications d'entreprise Amazon si les utilisateurs ne sont pas en mesure d'indiquer des informations d'identification utilisateur valides et un code MFA valide.

Pour activer l'authentification MFA, vous devez posséder une solution MFA qui est un serveur Remote authentication dial-in user service (RADIUS), ou disposer d'un plugin sur un serveur RADIUS déjà installé dans votre infrastructure sur site. Votre solution d'authentification MFA doit utiliser des codes secrets uniques que les utilisateurs obtiennent à partir d'un périphérique physique ou d'un logiciel exécuté sur un périphérique, par exemple un téléphone portable.

RADIUS est un protocole client/serveur standard qui assure l'authentification, l'autorisation et la gestion de la comptabilité afin de permettre aux utilisateurs de se connecter aux services réseau. AWS Managed Microsoft AD inclut un client RADIUS qui se connecte au serveur RADIUS sur lequel vous avez implémenté votre solution MFA. Votre serveur RADIUS valide le nom d'utilisateur et le code secret unique. Si votre serveur RADIUS valide correctement l'utilisateur, AWS Managed Microsoft AD authentifie ensuite l'utilisateur auprès d'Active Directory. Une fois l'authentification Active Directory réussie, les utilisateurs peuvent accéder à l' AWS application. La communication entre le client Microsoft AD RADIUS AWS géré et votre serveur RADIUS nécessite que vous configuriez des groupes AWS de sécurité qui permettent la communication via le port 1812.

Vous pouvez activer l'authentification multifactorielle pour votre annuaire Microsoft AD AWS géré en suivant la procédure suivante. Pour plus d'informations sur la configuration de votre serveur RADIUS pour être utilisé avec AWS Directory Service et MFA, veuillez consulter Prérequis pour l'authentification multifactorielle.

Considérations

Voici quelques considérations relatives à l'authentification multifactorielle pour votre Microsoft AD AWS géré :

- L'authentification multifactorielle n'est pas disponible pour Simple AD. Toutefois, l'authentification MFA peut être activée pour votre annuaire AD Connector. Pour plus d'informations, consultez Activer l'authentification multifactorielle pour AD Connector.
- Le MFA est une fonctionnalité régionale de Managed AWS Microsoft AD. Si vous utilisez Réplication multi-régions, les procédures suivantes doivent être appliquées séparément dans chaque région. Pour plus d'informations, consultez Caractéristiques mondiales et régionales.
- Si vous avez l'intention d'utiliser AWS Managed Microsoft AD pour les communications externes, nous vous recommandons de configurer une passerelle Internet ou une passerelle Internet de traduction d'adresses réseau (NAT) en dehors du AWS réseau pour ces communications.
  - Si vous souhaitez prendre en charge les communications externes entre votre Microsoft AD AWS géré et votre serveur RADIUS hébergé sur le AWS réseau, veuillez contacter AWS Support.

Activer l'authentification multifactorielle pour AWS Managed Microsoft AD

La procédure suivante explique comment activer l'authentification multifactorielle pour AWS Managed Microsoft AD.

1. Identifiez l'adresse IP de votre serveur MFA RADIUS et de votre répertoire AWS Managed Microsoft AD.
2. Modifiez vos groupes de sécurité Virtual Private Cloud (VPC) pour permettre les communications via le port 1812 entre vos points de terminaison IP AWS Microsoft AD gérés et votre serveur MFA RADIUS.
3. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).
4. Choisissez le lien d'ID de répertoire pour votre annuaire Microsoft AD AWS géré.
5. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :
   - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région dans laquelle vous souhaitez activer l'authentification MFA, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour plus d'informations, consultez Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Mise en réseau et sécurité.
6. Dans la section Authentification multifactorielle, choisissez Actions, puis sélectionnez Activer.
7. Dans la page Activer l'authentification multifactorielle (MFA), indiquez les valeurs suivantes :

   Afficher l'étiquette

   Indiquez un nom d'étiquette.

   Nom DNS ou adresses IP du serveur RADIUS

   Adresses IP des points de terminaison de votre serveur RADIUS ou adresse IP de l'équilibreur de charge de votre serveur RADIUS. Vous pouvez entrer plusieurs adresses IP en les séparant par une virgule (par exemple, `192.0.0.0,192.0.0.12`).

   > **Note**
   >
   > La MFA RADIUS s'applique uniquement pour authentifier l' AWS Management Console accès aux applications et services Amazon Enterprise tels qu'Amazon

ou WorkSpaces Amazon QuickSight Chime. Il ne fournit pas de MFA aux charges de travail Windows exécutées sur des instances EC2 ou pour la connexion à une instance EC2. AWS Directory Service ne prend pas en charge l'authentification RADIUS Challenge/Response.
Les utilisateurs doivent disposer de leur code MFA au moment d'entrer leurs noms d'utilisateur et leurs mots de passe. Vous devez également utiliser une solution qui effectue une MFA, out-of-band telle que la vérification du texte par SMS pour l'utilisateur. Dans les solutions out-of-band MFA, vous devez vous assurer de définir la valeur du délai d'expiration RADIUS de manière appropriée pour votre solution. Lorsque vous utilisez une solution out-of-band MFA, la page de connexion invite l'utilisateur à saisir un code MFA. Dans ce cas, les utilisateurs doivent entrer leurs mots de passe dans la zone de mot de passe et dans la zone MFA.

Port

Port que votre serveur RADIUS utilise pour les communications. Votre réseau local doit autoriser le trafic entrant via le port du serveur RADIUS par défaut (UDP:1812) en provenance des serveurs. AWS Directory Service

Shared secret code

Code secret partagé qui a été spécifié lorsque vos points de terminaison RADIUS ont été créés.

Confirmer le code secret partagé

Confirmez le code secret partagé pour vos points de terminaison RADIUS.

Protocole

Sélectionnez le protocole qui a été spécifié lorsque vos points de terminaison RADIUS ont été créés.

Délai d'attente du serveur (en secondes)

Durée, en secondes, d'attente de la réponse du serveur RADIUS. La valeur doit être comprise entre 1 et 50.

> **Note**
>
> Nous vous recommandons de configurer le délai d'attente de votre serveur RADIUS à 20 secondes ou moins. Si le délai d'attente est supérieur à 20 secondes, le système ne peut pas réessayer avec un autre serveur RADIUS, ce qui peut entraîner un échec lié au délai d'attente.

Nombre maximal de tentatives RADIUS

Nombre de tentatives de communication avec le serveur RADIUS. La valeur doit être comprise entre 0 et 10.

L'authentification multifactorielle est disponible lorsque le paramètre RADIUS Status passe à l'état Enabled.

8. Sélectionnez Activer.

Applications Amazon Enterprise prises en charge

Toutes les applications informatiques Amazon Enterprise WorkSpaces, y compris Amazon, Amazon, Amazon WorkDocs WorkMail QuickSight, ainsi que l'accès à AWS IAM Identity Center Managed Microsoft AD et AD Connector avec MFA, AWS Management Console sont prises en charge lors de l'utilisation de AWS Managed Microsoft AD et AD Connector.

Pour plus d'informations sur la configuration de l'accès utilisateur de base aux applications Amazon Enterprise, l'authentification AWS unique et l' AWS Management Console utilisation AWS Directory Service, consultez Permettre l'accès aux AWS applications et aux services etActivation de l'accès à AWS Management Console avec les informations d'identification AD.

Article AWS de blog sur la sécurité connexe

- Comment activer l'authentification multifactorielle pour les AWS services à l'aide de AWS Managed Microsoft AD et d'informations d'identification locales

Activer le protocole LDAP ou LDAPS sécurisé

LDAP (Lightweight Directory Access Protocol) est un protocole de communication standard utilisé pour lire et écrire des données vers et depuis Active Directory. Certaines applications utilisent LDAP pour ajouter, supprimer ou rechercher des utilisateurs et des groupes dans Active Directory ou pour transférer des informations d'identification afin d'authentifier des utilisateurs dans Active Directory. Chaque communication LDAP comprend un client (par exemple une application) et un serveur (comme Active Directory).

Par défaut, les communications via LDAP ne sont pas chiffrées. Cela permet à un utilisateur malveillant d'utiliser un logiciel de surveillance réseau pour afficher les paquets de données sur le réseau. C'est pourquoi de nombreuses stratégies de sécurité d'entreprise imposent généralement aux organisations de chiffrer toutes les communications LDAP.

Pour atténuer cette forme d'exposition des données, AWS Managed Microsoft AD propose une option : vous pouvez activer LDAP via Secure Sockets Layer (SSL) /Transport Layer Security (TLS), également connu sous le nom de LDAPS. Avec LDAPS, vous pouvez renforcer la sécurité de votre réseau. Vous pouvez également répondre aux exigences de conformité en chiffrant toutes les communications entre vos applications compatibles LDAP et Managed AWS Microsoft AD.

AWS Managed Microsoft AD prend en charge le protocole LDAPS dans les scénarios de déploiement suivants :

- Le protocole LDAPS côté serveur chiffre les communications LDAP entre vos applications commerciales ou locales compatibles LDAP (agissant en tant que clients LDAP) et Managed AWS Microsoft AD (agissant en tant que serveur LDAP). Pour plus d'informations, consultez Activer LDAPS côté serveur à l'aide de Managed Microsoft AD AWS.
- Le protocole LDAPS côté client chiffre les communications LDAP entre des AWS applications telles que WorkSpaces (agissant en tant que clients LDAP) et votre Active Directory autogéré (sur site) (agissant en tant que serveur LDAP). Pour plus d'informations, voir Activer LDAPS côté client à l'aide de Managed Microsoft AD AWS.

Rubriques

Activer LDAPS côté serveur à l'aide de Managed Microsoft AD AWS

La prise en charge du protocole SSL (Lightweight Directory Access Protocol) /Transport Layer Security (TLS) (LDAPS) côté serveur chiffre les communications LDAP entre vos applications commerciales ou locales compatibles LDAP et votre annuaire Microsoft AD géré. AWS Cela permet d'améliorer la sécurité de votre réseau et de répondre aux critères de conformité à l'aide du protocole de chiffrement SSL (Secure Sockets Layer).

Activer LDAPS côté serveur

Pour obtenir des instructions détaillées sur la façon de configurer et de configurer le protocole LDAPS côté serveur et votre serveur d'autorité de certification (CA), consultez la section Comment activer le protocole LDAPS côté serveur pour votre annuaire Microsoft AD AWS géré sur le blog de sécurité. AWS

Vous devez effectuer la plupart des tâches de configuration à partir de l'instance Amazon EC2 que vous utilisez pour gérer vos contrôleurs de domaine AWS Managed Microsoft AD. Les étapes suivantes vous indiquent comment activer LDAPS pour votre domaine dans le AWS cloud.

Si vous souhaitez utiliser l'automatisation pour configurer votre infrastructure PKI, vous pouvez utiliser l'infrastructure à clé publique Microsoft sur AWS QuickStart Guide. Plus précisément, vous devez suivre les instructions du guide pour charger le modèle de déploiement de Microsoft PKI dans un VPC existant sur AWS. Une fois que vous avez chargé le modèle, assurez-vous de choisir **`AWSManaged`** quand vous accédez à l'option Type de services de domaine Active Directory. Si vous avez utilisé le QuickStart guide, vous pouvez accéder directement àÉtape 3 : créer un modèle de certificat.

Rubriques

- Étape 1 : déléguer les rôles autorisés à activer LDAPS
- Étape 2 : configurer votre autorité de certification
- Étape 3 : créer un modèle de certificat
- Étape 4 : Ajouter des règles de groupe de sécurité

Étape 1 : déléguer les rôles autorisés à activer LDAPS

Pour activer le protocole LDAPS côté serveur, vous devez être membre du groupe Admins ou AWS Delegated Enterprise Certificate Authority Administrators de votre annuaire AWS Microsoft AD géré. Vous pouvez également être l'utilisateur administratif par défaut (compte Admin). Si vous préférez,

vous pouvez faire en sorte qu'un autre utilisateur que le compte Admin configure LDAPS. Dans ce cas, ajoutez cet utilisateur au groupe Admins ou AWS Delegated Enterprise Certificate Authority Administrators dans votre répertoire AWS Managed Microsoft AD.

Étape 2 : configurer votre autorité de certification

Avant de pouvoir activer LDAPS côté serveur, vous devez créer un certificat. Ce certificat doit être émis par un serveur Microsoft Enterprise CA joint à votre domaine Microsoft AD AWS géré. Une fois créé, le certificat doit être installé sur chacun des contrôleurs de domaine qui se trouvent dans ce domaine. Ce certificat permet au service LDAP se trouvant sur les contrôleurs de domaine d'écouter et d'accepter automatiquement les connexions SSL provenant de clients LDAP.

> **Note**
>
> Le protocole LDAPS côté serveur avec AWS Microsoft AD géré ne prend pas en charge les certificats émis par une autorité de certification autonome. Il ne prend pas non plus en charge les certificats émis par une autorité de certification tierce.

Selon vos besoins spécifiques, vous disposez de différentes options pour configurer une autorité de certification ou pour vous connecter à une autorité de certification dans votre domaine :

- Créer une autorité de certification Microsoft Enterprise subordonnée — (recommandé) Cette option vous permet de déployer un serveur Microsoft Enterprise CA subordonnée dans le AWS cloud. Le serveur peut utiliser Amazon EC2 pour fonctionner avec votre autorité de certification Microsoft racine existante. Pour plus d'informations sur la configuration d'une autorité de certification Microsoft Enterprise subordonnée, consultez Étape 4 : ajouter une autorité de certification Microsoft Enterprise à votre répertoire AWS Microsoft AD dans Comment activer le protocole LDAPS côté serveur pour votre répertoire AWS Microsoft AD géré.
- Créer une autorité de certification Microsoft d'entreprise racine : avec cette option, vous pouvez créer une autorité de certification Microsoft d'entreprise racine dans le AWS cloud à l'aide d'Amazon EC2 et la joindre à votre domaine AWS Microsoft AD géré. Cette autorité de certification racine peut émettre le certificat sur vos contrôleurs de domaine. Pour plus d'informations sur la configuration d'une nouvelle autorité de certification racine, voir Étape 3 : Installation et configuration d'une autorité de certification hors ligne dans Comment activer le protocole LDAPS côté serveur pour votre annuaire AWS Microsoft AD géré.

Pour en savoir plus sur la manière d'associer votre instance EC2 à votre domaine, veuillez consulter Joindre une instance Amazon EC2 à votre compte AWS Microsoft AD géré Active Directory.

Étape 3 : créer un modèle de certificat

Une fois votre autorité de certification d'entreprise configurée, vous pouvez configurer le modèle de certificat d'authentification Kerberos.

Pour créer un modèle de certificat

1. Lancez Microsoft Windows Server Manager. Sélectionnez Outils > Autorité de certification.
2. Dans la fenêtre Autorité de certification, développez l'arborescence Autorité de certification dans le volet de gauche. Cliquez avec le bouton droit sur Modèles de certificats, puis sélectionnezGérer.
3. Dans la fenêtre Console de modèles de certificats, cliquez avec le bouton droit sur Authentification Kerberos, puis sélectionnez Dupliquer le modèle.
4. La fenêtre Propriétés du nouveau modèle s'ouvre.
5. Dans la fenêtre Propriétés du nouveau modèle, accédez à l'onglet Compatibilité, puis procédez comme suit :

    a. Remplacez l'Autorité de certification par le système d'exploitation correspondant à votre autorité de certification.
    b. Si une fenêtre Modifications résultantes s'affiche, sélectionnez OK.
    c. Changez le destinataire de la certification en Windows 10/Windows Server 2016.

    > **Note**
    >
    > AWS Managed Microsoft AD est alimenté par Windows Server 2019.

    d. Si la fenêtre Modifications résultantes s'affiche, sélectionnez OK.
6. Cliquez sur l'onglet Général et redéfinissez le Nom d'affichage du modèle sur LDAPoverSSL ou tout autre nom que vous préférez.
7. Cliquez sur l'onglet Sécurité et sélectionnez Contrôleurs de domaine dans la section Noms de groupes ou d'utilisateurs. Dans la section Autorisations pour les contrôleurs de domaine, vérifiez que les cases Autoriser pour la lecture, l'inscription et l'inscription automatique sont cochées.
8. Cliquez sur OK pour créer le modèle de certificat LDAPoverSSL (ou le nom que vous avez spécifié ci-dessus). Fermez la fenêtre de la Console des modèles de certificats.

9. Dans la fenêtre Autorité de certificats, cliquez avec le bouton droit sur Modèles de certificats, puis sélectionnez Nouveau > Modèle de certificat à émettre.
10. Dans la fenêtre Activer les modèles de certificats, choisissez LDAPoverSSL (ou le nom que vous avez spécifié ci-dessus), puis cliquez sur OK.

Étape 4 : Ajouter des règles de groupe de sécurité

Dans la dernière étape, vous devez ouvrir la console Amazon EC2 et ajouter des règles de groupe de sécurité. Ces règles permettent à vos contrôleurs de domaine de se connecter à votre autorité de certification d'entreprise pour demander un certificat. Pour ce faire, vous devez ajouter des règles entrantes afin que votre autorité de certification d'entreprise puisse accepter le trafic entrant à partir de vos contrôleurs de domaine. Vous devez ensuite ajouter des règles de trafic sortant pour autoriser le trafic entre vos contrôleurs de domaine et l'autorité de certification d'entreprise.

Une fois les deux règles configurées, vos contrôleurs de domaine demandent automatiquement un certificat à votre autorité de certification d'entreprise et activent LDAPS pour votre annuaire. Le service LDAP sur vos contrôleurs de domaine est maintenant prêt à accepter les connexions LDAPS.

Pour configurer des règles de groupe de sécurité

1. Accédez à votre console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2 et connectez-vous avec vos informations d'identification d'administrateur.
2. Dans le volet de gauche, sélectionnez Security Groups sous l'onglet Network & Security.
3. Dans le volet principal, choisissez le groupe AWS de sécurité pour votre autorité de certification.
4. Sélectionnez l'onglet Inbound (Entrant), puis Edit (Modifier).
5. Dans la boîte de dialogue Edit inbound rules, exécutez l'une des actions suivantes :
   - Choisissez Add Rule (Ajouter une règle).
   - Choisissez l'option All traffic pour le champ Type et l'option Custom pour le champ Source.
   - Entrez le groupe de AWS sécurité de votre répertoire (par exemple, sg-123456789) dans la case à côté de Source.
   - Choisissez Enregistrer.
6. Choisissez maintenant le groupe de AWS sécurité de votre annuaire Microsoft AD AWS géré. Sélectionnez l'onglet Outbound, puis Edit.
7. Dans la boîte de dialogue Edit outbound rules, exécutez l'une des actions suivantes :

- Choisissez Add Rule (Ajouter une règle).
- Choisissez l'option All traffic pour le champ Type et l'option Custom pour le champ Destination.
- Tapez le groupe de AWS sécurité de votre autorité de certification dans le champ Destination.
- Choisissez Enregistrer.

Vous pouvez tester la connexion LDAPS au répertoire Microsoft AD AWS géré à l'aide de l'outil LDP. L'outil LDP est fourni avec les outils d'administration Active Directory. Pour plus d'informations, consultez Installation des outils d'administration Active Directory pour Microsoft AD AWS géré.

> **Note**
>
> Avant de tester la connexion LDAPS, vous devez attendre jusqu'à 30 minutes pour que l'autorité de certification secondaire transmette un certificat à vos contrôleurs de domaine.

Pour plus de détails sur le protocole LDAPS côté serveur et pour voir un exemple de cas d'utilisation expliquant comment le configurer, consultez la section Comment activer le protocole LDAPS côté serveur pour votre annuaire Microsoft AD AWS géré sur le blog de sécurité. AWS

Activer LDAPS côté client à l'aide de Managed Microsoft AD AWS

La prise en charge du protocole SSL (Lightweight Directory Access Protocol) /Transport Layer Security (TLS) (LDAPS) côté client dans Managed AWS Microsoft AD chiffre les communications entre Microsoft Active Directory (AD) autogéré (sur site) et les applications. AWS Des exemples de telles applications incluent WorkSpaces AWS IAM Identity Center QuickSight, Amazon et Amazon Chime. Ce chiffrement vous permet de protéger les données d'identité de votre organisation et de répondre à vos exigences de sécurité.

Prérequis

Avant d'activer LDAPS côté client, vous devez satisfaire les exigences suivantes.

Rubriques

- Créez une relation de confiance entre votre Microsoft AD AWS géré et votre solution autogérée Microsoft Active Directory
- Déployer des certificats de serveur dans Active Directory

- Exigences relatives aux certificats de l'autorité de certification
- Exigences liées à la mise en réseau

Créez une relation de confiance entre votre Microsoft AD AWS géré et votre solution autogérée Microsoft Active Directory

Tout d'abord, vous devez établir une relation de confiance entre votre Microsoft AD AWS géré et votre service autogéré Microsoft Active Directory pour activer le LDAPS côté client. Pour plus d'informations, consultez the section called “Création d'une relation d'approbation”.

Déployer des certificats de serveur dans Active Directory

Afin d'activer LDAPS côté client, vous devez obtenir et installer des certificats de serveur pour chaque contrôleur de domaine dans Active Directory. Ces certificats seront utilisés par le service LDAP pour écouter et accepter automatiquement les connexions SSL provenant de clients LDAP. Vous pouvez utiliser des certificats SSL émis par un déploiement ADCS (services de certificat Active Directory) interne ou achetés auprès d'un émetteur commercial. Pour plus d'informations sur les exigences relatives aux certificats de serveur Active Directory, veuillez consulter LDAP over SSL (LDAPS) Certificate (français non garanti) sur le site web de Microsoft.

Exigences relatives aux certificats de l'autorité de certification

Un certificat d'autorité de certification (CA), qui représente l'émetteur de vos certificats de serveur, est requis pour le fonctionnement de LDAPS côté client. Les certificats d'une autorité de certification sont mis en correspondance avec les certificats de serveur présentés par vos contrôleurs de domaine Active Directory pour chiffrer les communications LDAP. Notez les exigences suivantes relatives aux certificats d'autorité de certification :

- L'autorité de certification d'entreprise (CA) est requise pour activer le protocole LDAPS côté client. Vous pouvez utiliser le service de Active Directory certification, une autorité de certification commerciale tierce ou AWS Certificate Manager. Pour plus d'informations sur Microsoft l'autorité de certification d'entreprise, consultez Microsoftla documentation.
- Pour que vous puissiez enregistrer un certificat, celui-ci doit expirer dans plus de 90 jours.
- Les certificats doivent être au format PEM (Privacy-Enhanced Mail). Si vous exportez des certificats d'autorité de certification à partir d'Active Directory, choisissez X.509 codé en base64 (.CER) comme format de fichier d'exportation.
- Un maximum de cinq (5) certificats CA peuvent être stockés par répertoire Microsoft AD AWS géré.

- Les certificats utilisant l'algorithme de signature RSASSA-PSS ne sont pas pris en charge.
- Les certificats d'autorité de certification qui sont chaînés à chaque certificat de serveur dans chaque domaine approuvé doivent être enregistrés.

Exigences liées à la mise en réseau

AWS le trafic LDAP de l'application s'exécutera exclusivement sur le port TCP 636, sans retour sur le port LDAP 389. Toutefois, les communications LDAP Windows prenant en charge la réplication, les approbations, etc. continueront d'utiliser le port LDAP 389 avec une sécurité native Windows. Configurez les groupes de AWS sécurité et les pare-feux réseau pour autoriser les communications TCP sur le port 636 dans Managed AWS Microsoft AD (sortie) et Active Directory autogéré (entrée). Laissez le port LDAP 389 ouvert entre AWS Managed Microsoft AD et Active Directory autogéré.

Activer LDAPS côté client

Pour activer LDAPS côté client, vous importez votre certificat d'une autorité de certification (CA) dans AWS Managed Microsoft AD, puis vous activez LDAPS sur votre annuaire. Lors de l'activation, tout le trafic LDAP entre les applications AWS et votre Active Directory autogéré est transmis avec le chiffrement de canal Secure Sockets Layer (SSL).

Vous pouvez utiliser deux méthodes différentes pour activer LDAPS côté client pour votre annuaire. Vous pouvez utiliser la AWS Management Console méthode ou la AWS CLI méthode.

> **Note**
>
> Le LDAPS côté client est une fonctionnalité régionale de Managed AWS Microsoft AD. Si vous utilisez Réplication multi-régions, les procédures suivantes doivent être appliquées séparément dans chaque région. Pour plus d'informations, consultez Caractéristiques mondiales et régionales.

Rubriques

Étape 1 : enregistrer un certificat dans AWS Directory Service

Utilisez l'une des méthodes suivantes pour enregistrer un certificat dans AWS Directory Service.

Méthode 1 : Pour enregistrer votre certificat dans AWS Directory Service (AWS Management Console)

1. Dans le volet de navigation de la AWS Directory Service console, sélectionnez Annuaires.
2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Détails de l'annuaire, effectuez l'une des opérations suivantes :
   - Si plusieurs régions apparaissent sous Réplication multirégionale, sélectionnez la région dans laquelle vous souhaitez enregistrer votre certificat, puis cliquez sur l'onglet Réseau et sécurité. Pour plus d'informations, consultez Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication multirégionale, cliquez sur l'onglet Réseau et sécurité.
4. Dans la section LDAPS côté client sélectionnez le menu Actions, puis Enregistrer le certificat.
5. Dans la boîte de dialogue Enregistrer un certificat d'une autorité de certification, sélectionnez Parcourir, puis le certificat et choisissez Ouvrir.
6. Choisissez Register certificate (Enregistrer le certificat).

Méthode 2 : Pour enregistrer votre certificat dans AWS Directory Service (AWS CLI)

- Exécutez la commande suivante. Pour les données de certificat, pointez vers l'emplacement de votre fichier de certificat de CA. Un ID de certificat sera fourni dans la réponse.

```
aws ds register-certificate --directory-id your_directory_id --certificate-data
 file://your_file_path
```

Étape 2 : Vérifier l'état d'enregistrement

Pour afficher l'état d'un enregistrement de certificat ou d'une liste de certificats enregistrés, utilisez l'une des méthodes suivantes.

Méthode 1 : pour vérifier le statut d'enregistrement du certificat dans AWS Directory Service (AWS Management Console)

1. Accédez à la section LDAPS côté client sur la page Détails de l'annuaire.
2. Vérifiez l'état de l'enregistrement de certificat actuel qui s'affiche sous la colonne État de l'enregistrement. Lorsque la valeur de l'état de l'enregistrement passe à Enregistré, cela signifie que votre certificat a été enregistré avec succès.

Méthode 2 : pour vérifier le statut d'enregistrement du certificat dans AWS Directory Service (AWS CLI)

- Exécutez la commande suivante. Si la valeur de l'état renvoie `Registered`, cela signifie que votre certificat a été enregistré avec succès.

```
aws ds list-certificates --directory-id your_directory_id
```

Étape 3 : Activer LDAPS côté client

Utilisez l'une des méthodes suivantes pour activer le protocole LDAPS côté client dans. AWS Directory Service

> **Note**
>
> Avant de pouvoir activer LDAPS côté client, vous devez avoir enregistré avec succès au moins un certificat.

Méthode 1 : pour activer le protocole LDAPS côté client dans () AWS Directory ServiceAWS Management Console

1. Accédez à la section LDAPS côté client sur la page Détails de l'annuaire.
2. Sélectionnez Activer. Si cette option n'est pas disponible, vérifiez qu'un certificat valide a bien été enregistré, puis réessayez.
3. Dans la boîte de dialogue Activer LDAPS côté client choisissez Activer.

Méthode 2 : pour activer le protocole LDAPS côté client dans () AWS Directory ServiceAWS CLI

- Exécutez la commande suivante.

```
aws ds enable-ldaps --directory-id your_directory_id --type Client
```

Étape 4 : Vérifier l'état LDAPS

Utilisez l'une des méthodes suivantes pour vérifier l'état du LDAPS dans AWS Directory Service.

Méthode 1 : pour vérifier le statut LDAPS dans AWS Directory Service ()AWS Management Console

1. Accédez à la section LDAPS côté client sur la page Détails de l'annuaire.
2. Si la valeur d'état est affichée en tant que Activé, cela signifie que LDAPS a été configuré avec succès.

Méthode 2 : pour vérifier le statut LDAPS dans AWS Directory Service ()AWS CLI

- Exécutez la commande suivante. Si la valeur d'état renvoie `Enabled`, cela signifie que LDAPS a été configuré avec succès.

```
aws ds describe-ldaps-settings --directory-id your_directory_id
```

Gérer LDAPS côté client

Utilisez ces commandes pour gérer votre configuration LDAPS.

Vous pouvez utiliser deux méthodes différentes pour gérer les paramètres LDAPS côté client. Vous pouvez utiliser la AWS Management Console méthode ou la AWS CLI méthode.

Afficher les détails du certificat

Utilisez l'une des méthodes suivantes pour voir lorsqu'un certificat est défini pour expirer.

Méthode 1 : pour afficher les détails du certificat dans AWS Directory Service (AWS Management Console)

1. Dans le volet de navigation de la AWS Directory Service console, sélectionnez Annuaires.
2. Choisissez le lien de l'ID correspondant à votre annuaire.

3. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :

   - Si plusieurs régions apparaissent sous Réplication multirégionale, sélectionnez la région dans laquelle vous souhaitez afficher le certificat, puis cliquez sur l'onglet Réseau et sécurité. Pour plus d'informations, consultez Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication multirégionale, cliquez sur l'onglet Réseau et sécurité.

4. Les informations relatives au certificat sont affichées dans la section LDAPS côté client sous Certificats d'une autorité de certification.

Méthode 2 : pour afficher les détails du certificat dans AWS Directory Service (AWS CLI)

- Exécutez la commande suivante. Pour l'ID de certificat, utilisez l'identifiant renvoyé par `register-certificate` ou `list-certificates`.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Annuler l'enregistrement d'un certificat

Utilisez l'une des méthodes suivantes pour annuler l'enregistrement d'un certificat.

> **Note**
>
> Si un seul certificat est enregistré, vous devez d'abord désactiver LDAPS avant de pouvoir annuler l'enregistrement d'un certificat.

Méthode 1 : pour annuler l'enregistrement d'un certificat dans AWS Directory Service ()AWS Management Console

1. Dans le volet de navigation de la AWS Directory Service console, sélectionnez Annuaires.
2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :

   - Si plusieurs régions apparaissent sous Réplication multirégionale, sélectionnez la région dans laquelle vous souhaitez annuler l'enregistrement d'un certificat, puis cliquez sur l'onglet

Réseau et sécurité. Pour plus d'informations, consultez Régions principales et régions supplémentaires.

- Si aucune région n'apparaît sous Réplication multirégionale, cliquez sur l'onglet Réseau et sécurité.

4. Dans la section LDAPS côté client choisissez Actions, puis Annuler l'enregistrement du certificat.
5. Dans la boîte de dialogue Annuler l'enregistrement d'un certificat d'une autorité de certification, choisissez Annuler l'enregistrement.

Méthode 2 : pour annuler l'enregistrement d'un certificat dans AWS Directory Service ()AWS CLI

- Exécutez la commande suivante. Pour l'ID de certificat, utilisez l'identifiant renvoyé par `register-certificate` ou `list-certificates`.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Désactiver LDAPS côté client

Utilisez l'une des méthodes suivantes pour désactiver LDAPS côté client.

Méthode 1 : pour désactiver le protocole LDAPS côté client dans () AWS Directory ServiceAWS Management Console

1. Dans le volet de navigation de la AWS Directory Service console, sélectionnez Annuaires.
2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :

   - Si plusieurs régions apparaissent sous Réplication multirégionale, sélectionnez la région dans laquelle vous souhaitez désactiver LDAPS côté client, puis cliquez sur l'onglet Réseau et sécurité. Pour plus d'informations, consultez Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication multirégionale, cliquez sur l'onglet Réseau et sécurité.

4. Dans la section LDAPS côté client choisissez Désactiver.
5. Dans la boîte de dialogue Désactiver LDAPS côté client, choisissez Désactiver.

Méthode 2 : pour désactiver le protocole LDAPS côté client dans () AWS Directory ServiceAWS CLI

- Exécutez la commande suivante.

```
aws ds disable-ldaps --directory-id your_directory_id --type Client
```

Problèmes d'inscription aux certificats

Le processus d'inscription de vos contrôleurs de domaine Microsoft AD AWS gérés avec les certificats CA peut prendre jusqu'à 30 minutes. Si vous rencontrez des problèmes lors de l'inscription du certificat et souhaitez redémarrer vos contrôleurs de domaine Microsoft AD AWS gérés, vous pouvez contacter AWS Support. Pour créer un dossier d'assistance, consultez les sections Création de dossiers d'assistance et gestion des dossiers.

Gérez la conformité pour AWS Managed Microsoft AD

Vous pouvez utiliser AWS Managed Microsoft AD pour prendre en charge vos applications compatibles Active Directory, dans le AWS cloud, qui sont soumises aux exigences de conformité suivantes. Sachez toutefois que vos applications ne respecteront pas ces exigences de conformité si vous utilisez Simple AD.

Normes de conformité prises en charge

AWS Managed Microsoft AD a fait l'objet d'un audit selon les normes suivantes et peut être utilisé dans le cadre de solutions pour lesquelles vous devez obtenir une certification de conformité.

FedRAMP

AWS Managed Microsoft AD répond aux exigences de sécurité du Federal Risk and Authorization Management Program (FedRAMP) et a reçu l'autorisation provisoire d'exploitation (P-ATO) du FedRAMP Joint Authorization Board (JAB) sur la base de référence modérée et élevée du FedRAMP. Pour de plus amples informations sur FedRAMP, veuillez consulter FedRAMP compliance (français non garanti).

AWS Managed Microsoft AD possède une attestation de conformité à la norme de sécurité des données (DSS) de l'industrie des cartes de paiement (PCI) version 3.2 au niveau 1 du fournisseur de services. Les clients qui utilisent AWS des produits et services pour stocker, traiter ou transmettre les données des titulaires de cartes peuvent utiliser AWS Managed Microsoft AD pour gérer leur propre certification de conformité à la norme PCI DSS.

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. Il est important de noter que vous devez configurer des politiques de mot de passe précises dans AWS Managed Microsoft AD afin qu'elles soient conformes aux normes PCI DSS version 3.2. Pour plus de détails sur les politiques qui doivent être appliquées, consultez la section ci-dessous intitulée Activer la conformité PCI pour votre annuaire Microsoft AD AWS géré.

AWS a étendu son programme de conformité à la loi HIPAA (Health Insurance Portability and Accountability Act) pour inclure Managed AWS Microsoft AD en tant que service éligible à la loi HIPAA. Si vous avez signé un accord de partenariat commercial (BAA) avec AWS, vous pouvez utiliser AWS Managed Microsoft AD pour créer vos applications conformes à la loi HIPAA.

AWS propose un livre blanc axé sur la loi HIPAA aux clients qui souhaitent en savoir plus sur la manière dont ils peuvent tirer parti AWS pour le traitement et le stockage des informations de santé. Pour de plus amples informati ons, veuillez consulter HIPAA compliance (français non garanti).

Responsabilité partagée

La sécurité, et notamment la conformité aux réglementations FedRAMP, HIPAA et PCI, est une responsabilité partagée. Il est important de comprendre que le statut de conformité de AWS Managed Microsoft AD ne s'applique pas automatiquement aux applications que vous exécutez dans le AWS cloud. Vous devez vous assurer que votre utilisation des AWS services est conforme aux normes.

Pour obtenir la liste complète des différents programmes de AWS conformité pris en charge par AWS Managed Microsoft AD, consultez la section AWS Services concernés par programme de conformité.

Assurez la conformité à la norme PCI pour votre AWS annuaire Microsoft AD géré

Pour activer la conformité PCI pour votre annuaire Microsoft AD AWS géré, vous devez configurer des politiques de mot de passe détaillées, comme indiqué dans le document d'attestation de conformité (AOC) et de résumé des responsabilités PCI DSS fourni par. AWS Artifact

Pour plus d'informations sur l'utilisation de politiques de mots de passe détaillées, veuillez consulter Gérer les politiques de mot de passe pour AWS Managed Microsoft AD.

Améliorer la configuration de la sécurité réseau AWS Managed Microsoft AD

Le groupe de sécurité AWS mis en service pour l'annuaire AWS Managed Microsoft AD est configuré avec les ports réseau entrants minimum requis pour la prise en charge de tous les cas d'utilisation connus de votre annuaire AWS Managed Microsoft AD. Pour plus d'informations sur le groupe de sécurité AWS mis en service, veuillez consulterQu'est-ce qui est créé avec votre annuaire Microsoft AD Active Directory AWS géré.

Pour améliorer la sécurité réseau de votre annuaire AWS Managed Microsoft AD, vous pouvez modifier le groupe de sécurité AWS en fonction des scénarios courants présentés ci-dessous.

Rubriques

- Prise en charge des applications AWS seulement
- Applications AWS seulement avec prise en charge d'approbation
- Prise en charge de charges de travail Active Directory natives et d'applications AWS
- Prise en charge de charges de travail Active Directory natives et d'applications AWS avec prise en charge d'approbation

Prise en charge des applications AWS seulement

Tous les comptes d'utilisateur sont mis en service uniquement dans votre AWS Managed Microsoft AD pour être utilisés avec des applications AWS prises en charge, telles que les suivantes :

- Amazon Chime
- Amazon Connect
- Amazon QuickSight
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail
- AWS Client VPN
- AWS Management Console

Vous pouvez utiliser la configuration de groupe de sécurité AWS suivante pour bloquer tout le trafic non essentiel vers vos contrôleurs de domaine AWS Managed Microsoft AD.

> **Note**
>
> - Les éléments suivants ne sont pas compatibles avec cette configuration de groupe de sécurité AWS :
>   - instances Amazon EC2
>   - Amazon FSx
>   - Amazon RDS for MySQL
>   - Amazon RDS for Oracle
>   - Amazon RDS for PostgreSQL
>   - Amazon RDS for SQL Server
>   - WorkSpaces
>   - Active Directory approuve
>   - Clients ou serveurs joints au domaine

Règles entrantes

Aucun.

Règles sortantes

Aucun.

Applications AWS seulement avec prise en charge d'approbation

Tous les comptes d'utilisateur sont mis en service dans votre AWS Managed Microsoft AD ou Active Directory approuvé pour être utilisés avec des applications AWS prises en charge, telles que les suivantes :

- Amazon Chime
- Amazon Connect
- Amazon QuickSight
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS Client VPN
- AWS Management Console

Vous pouvez modifier la configuration du groupe de sécurité AWS mis en service pour bloquer tout le trafic non essentiel vers vos contrôleurs de domaine AWS Managed Microsoft AD.

> **Note**
>
> - Les éléments suivants ne sont pas compatibles avec cette configuration de groupe de sécurité AWS :
>   - instances Amazon EC2
>   - Amazon FSx
>   - Amazon RDS for MySQL
>   - Amazon RDS for Oracle
>   - Amazon RDS for PostgreSQL
>   - Amazon RDS for SQL Server

  - WorkSpaces
  - Active Directory approuve
  - Clients ou serveurs joints au domaine
- Pour cette configuration, vous devez vous assurer que le réseau « CIDR sur site » est sécurisé.
- TCP 445 est utilisé uniquement pour la création d'une approbation et peut être supprimé une fois que l'approbation a été établie.
- TCP 636 est requis uniquement lorsque LDAP sur SSL est en cours d'utilisation.

Règles entrantes

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP et UDP	53	CIDR sur site	DNS	Authentification d'utilisateur et d'ordinateur, résolution de noms, approbations
TCP et UDP	88	CIDR sur site	Kerberos	Authentification d'utilisateur et d'ordinateur, approbations au niveau de la forêt
TCP et UDP	389	CIDR sur site	LDAP	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP et UDP	464	CIDR sur site	Mot de passe Kerberos (modification/définition)	Réplication, authentification d'utilisateur et d'ordinateur, approbations
TCP	445	CIDR sur site	SMB / CIFS	Réplication, authentification d'utilisateur et d'ordinateur, approbations de stratégie de groupe
TCP	135	CIDR sur site	Réplication	RPC, EPM
TCP	636	CIDR sur site	LDAP SSL	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
TCP	49152 - 65535	CIDR sur site	RPC	Réplication, authentification d'utilisateur et d'ordinateur, stratégie de groupe, approbations

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP	3268 - 3269	CIDR sur site	LDAP GC et LDAP GC SSL	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
UDP	123	CIDR sur site	Heure Windows	Heure Windows, approbations

Règles sortantes

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
Tous	Tous	CIDR sur site	Tout le trafic	

Prise en charge de charges de travail Active Directory natives et d'applications AWS

Les comptes d'utilisateur sont mis en service uniquement dans votre AWS Managed Microsoft AD pour être utilisés avec des applications AWS prises en charge, telles que les suivantes :

- Amazon Chime
- Amazon Connect
- instances Amazon EC2
- Amazon FSx
- Amazon QuickSight
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL

- Amazon RDS for SQL Server
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- AWS Management Console

Vous pouvez modifier la configuration du groupe de sécurité AWS mis en service pour bloquer tout le trafic non essentiel vers vos contrôleurs de domaine AWS Managed Microsoft AD.

> **Note**
>
> - Les approbations Active Directory ne peuvent pas être créées et gérées entre votre annuaire AWS Managed Microsoft AD et le domaine sur site.
> - Vous devez vous assurer que le réseau « CIDR client » est sécurisé.
> - TCP 636 est requis uniquement lorsque LDAP sur SSL est en cours d'utilisation.
> - Si vous souhaitez utiliser une autorité de certification d'entreprise avec cette configuration, vous devrez créer une règle sortante « TCP, 443, CIDR d'autorité de certification ».

Règles entrantes

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP et UDP	53	CIDR client	DNS	Authentification d'utilisateur et d'ordinateur, résolution de noms, approbations
TCP et UDP	88	CIDR client	Kerberos	Authentification d'utilisateur et

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
				d'ordinateur, approbations au niveau de la forêt
TCP et UDP	389	CIDR client	LDAP	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
TCP et UDP	445	CIDR client	SMB / CIFS	Réplication, authentification d'utilisateur et d'ordinateur, approbations de stratégie de groupe
TCP et UDP	464	CIDR client	Mot de passe Kerberos (modification/définition)	Réplication, authentification d'utilisateur et d'ordinateur, approbations
TCP	135	CIDR client	Réplication	RPC, EPM

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP	636	CIDR client	LDAP SSL	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
TCP	49152 - 65535	CIDR client	RPC	Réplication, authentification d'utilisateur et d'ordinateur, stratégie de groupe, approbations
TCP	3268 - 3269	CIDR client	LDAP GC et LDAP GC SSL	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
TCP	9389	CIDR client	SOAP	Services Web AD DS
UDP	123	CIDR client	Heure Windows	Heure Windows, approbations
UDP	138	CIDR client	DFSN et NetLogon	DFS, stratégie de groupe

Règles sortantes

Aucun.

Prise en charge de charges de travail Active Directory natives et d'applications AWS avec prise en charge d'approbation

Tous les comptes d'utilisateur sont mis en service dans votre AWS Managed Microsoft AD ou Active Directory approuvé pour être utilisés avec des applications AWS prises en charge, telles que les suivantes :

- Amazon Chime
- Amazon Connect
- instances Amazon EC2
- Amazon FSx
- Amazon QuickSight
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- AWS Management Console

Vous pouvez modifier la configuration du groupe de sécurité AWS mis en service pour bloquer tout le trafic non essentiel vers vos contrôleurs de domaine AWS Managed Microsoft AD.

> **Note**
>
> - Vous devez vous assurer que les réseaux « CIDR sur site » et « CIDR client » sont sécurisés.

- TCP 445 avec le réseau « CIDR sur site » est utilisé uniquement pour la création d'une approbation et peut être supprimé une fois que l'approbation a été établie.
- TCP 445 avec le réseau « CIDR client » doit être conservé ouvert, car il est requis pour le traitement de la stratégie de groupe.
- TCP 636 est requis uniquement lorsque LDAP sur SSL est en cours d'utilisation.
- Si vous souhaitez utiliser une autorité de certification d'entreprise avec cette configuration, vous devrez créer une règle sortante « TCP, 443, CIDR d'autorité de certification ».

Règles entrantes

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP et UDP	53	CIDR sur site	DNS	Authentification d'utilisateur et d'ordinateur, résolution de noms, approbations
TCP et UDP	88	CIDR sur site	Kerberos	Authentification d'utilisateur et d'ordinateur, approbations au niveau de la forêt
TCP et UDP	389	CIDR sur site	LDAP	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP et UDP	464	CIDR sur site	Mot de passe Kerberos (modification/définition)	Réplication, authentification d'utilisateur et d'ordinateur, approbations
TCP	445	CIDR sur site	SMB / CIFS	Réplication, authentification d'utilisateur et d'ordinateur, approbations de stratégie de groupe
TCP	135	CIDR sur site	Réplication	RPC, EPM
TCP	636	CIDR sur site	LDAP SSL	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
TCP	49152 - 65535	CIDR sur site	RPC	Réplication, authentification d'utilisateur et d'ordinateur, stratégie de groupe, approbations

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP	3268 - 3269	CIDR sur site	LDAP GC et LDAP GC SSL	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
UDP	123	CIDR sur site	Heure Windows	Heure Windows, approbations
TCP et UDP	53	CIDR client	DNS	Authentification d'utilisateur et d'ordinateur, résolution de noms, approbations
TCP et UDP	88	CIDR client	Kerberos	Authentification d'utilisateur et d'ordinateur, approbations au niveau de la forêt
TCP et UDP	389	CIDR client	LDAP	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP et UDP	445	CIDR client	SMB / CIFS	Réplication, authentification d'utilisateur et d'ordinateur, approbations de stratégie de groupe
TCP et UDP	464	CIDR client	Mot de passe Kerberos (modification/définition)	Réplication, authentification d'utilisateur et d'ordinateur, approbations
TCP	135	CIDR client	Réplication	RPC, EPM
TCP	636	CIDR client	LDAP SSL	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
TCP	49152 - 65535	CIDR client	RPC	Réplication, authentification d'utilisateur et d'ordinateur, stratégie de groupe, approbations

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP	3268 - 3269	CIDR client	LDAP GC et LDAP GC SSL	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
TCP	9389	CIDR client	SOAP	Services Web AD DS
UDP	123	CIDR client	Heure Windows	Heure Windows, approbations
UDP	138	CIDR client	DFSN et NetLogon	DFS, stratégie de groupe

Règles sortantes

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
Tous	Tous	CIDR sur site	Tout le trafic	

Configurer les paramètres de sécurité de l'annuaire

Vous pouvez configurer des paramètres d'annuaire précis pour votre AWS Managed Microsoft AD afin de répondre à vos exigences en matière de conformité et de sécurité sans augmenter la charge de travail opérationnelle. Dans les paramètres de l'annuaire, vous pouvez mettre à jour la configuration des canaux sécurisés pour les protocoles et les chiffrements utilisés dans votre annuaire. Par exemple, vous avez la possibilité de désactiver les anciens chiffrements individuels, tels que RC4 ou DES, et les protocoles, tels que SSL 2.0/3.0 et TLS 1.0/1.1. AWS Managed

Microsoft AD déploie ensuite la configuration sur tous les contrôleurs de domaine de votre annuaire, gère les redémarrages des contrôleurs de domaine et maintient cette configuration à mesure que vous mettez à l'échelle ou que vous déployez d'autres Régions AWS. Pour plus d'informations sur tous les paramètres disponibles, consultez Liste des paramètres de sécurité de l'annuaire.

Modifier les paramètres de sécurité de l'annuaire

Vous pouvez configurer et modifier les paramètres de n'importe lequel de vos annuaires.

Pour modifier les paramètres de l'annuaire

1. Connectez-vous à la console de gestion AWS et ouvrez la console AWS Directory Service à l'adresse https://console.aws.amazon.com/directoryservicev2/.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sous Networking & security (Réseau et sécurité), recherchez Directory settings (Paramètres de l'annuaire), puis choisissez Edit settings (Modifier les paramètres).
4. Dans Edit settings (Modifier les paramètres), modifiez la valeur des paramètres que vous souhaitez modifier. Lorsque vous modifiez un paramètre, son statut passe de Default (Par défaut) à Ready to Update (Prêt pour la mise à jour). Si vous avez déjà modifié le paramètre, son statut passe de Updated (Mis à jour) à Ready to Update (Prêt pour la mise à jour). Choisissez ensuite Review (Examiner).
5. Dans Review and update setting (Examen et mise à jour des paramètres), consultez la section Directory settings (Paramètres de l'annuaire) et assurez-vous que les nouvelles valeurs sont toutes correctes. Si vous souhaitez apporter d'autres modifications à vos paramètres, choisissez Edit settings (Modifier les paramètres). Lorsque vous êtes satisfait de vos modifications et que vous êtes prêt à implémenter les nouvelles valeurs, choisissez Update settings (Mettre à jour les paramètres). Vous êtes ensuite renvoyé à la page d'ID de l'annuaire.

> **Note**
>
> Sous Directory settings (Paramètres de l'annuaire), vous pouvez consulter le statut de vos paramètres mis à jour. Lorsque les paramètres sont implémentés, le statut affiche Updating(Mise à jour). Vous ne pouvez pas modifier d'autres paramètres lorsqu'un paramètre affiche la mention Updating (Mise à jour) sous Status (Statut). Le statut affiche la mention Updated (Mis à jour) si le paramètre est correctement mis à jour avec votre modification. Le statut affiche la mention Failed (Échec) si le paramètre ne se met pas à jour avec votre modification.

Échec des paramètres de sécurité de l'annuaire

Si une erreur se produit lors d'une mise à jour des paramètres, le statut affiche la mention Failed (Échec). En cas d'échec, les paramètres ne sont pas mis à jour avec les nouvelles valeurs et les valeurs d'origine restent implémentées. Vous pouvez réessayer de mettre à jour ces paramètres ou rétablir leurs valeurs précédentes.

Pour résoudre l'échec de la mise à jour des paramètres

- Sous Directory settings (Paramètres de l'annuaire), choisissez Resolve failed settings (Résoudre l'échec de mise à jour des paramètres). Ensuite, effectuez l'une des actions suivantes :
  - Pour rétablir vos paramètres à leur valeur d'origine avant l'échec de mise à jour, choisissez Revert failed settings (Rétablir les paramètres qui n'ont pas pu être mis à jour). Choisissez ensuite Revert (Rétablir) dans la fenêtre contextuelle.
  - Pour réessayer de mettre à jour les paramètres de votre annuaire, choisissez Retry failed settings (Réessayer les paramètres qui n'ont pas pu être mis à jour). Si vous souhaitez apporter des modifications supplémentaires aux paramètres de votre annuaire avant de réessayer les mises à jour qui ont échoué, choisissez Continue editing (Continuer les modifications). Sous Review and retry failed updates (Examiner et réessayer les mises à jour qui ont échoué), choisissez Update settings (Mettre à jour les paramètres).

Liste des paramètres de sécurité de l'annuaire

La liste suivante indique le type, le nom du paramètre, le nom de l'API, les valeurs potentielles et la description du paramètre pour tous les paramètres de sécurité d'annuaire disponibles.

TLS 1.2 et AES 256/256 sont les paramètres de sécurité d'annuaire par défaut si tous les autres paramètres de sécurité sont désactivés. Ils ne peuvent pas être désactivés.

Type	Nom du paramè	Nom d'API	Valeurs potentielles	Description du paramètre
Authentification basée sur des certificats	Compen ion de l'antidat age	CERTIFICA TE_BACKDA TING_COMP ENSATION	Années : 0 à 50 Mois : 0 à 11 Jours : 0 à 30	Spécifiez une valeur indiquant la durée pendant

Type	Nom du paramè	Nom d'API	Valeurs potentielles	Description du paramètre
	des certifica ts		Heures : 0 à 23 Minutes : 0 à 59 Secondes : 0 à 59	laquelle un certificat peut être antérieur à un utilisate ur dans Active Directory et continuer à être utilisé pour l'authent ification dans Active Directory. La valeur par défaut est de 10 minutes. Vous pouvez définir cette valeur entre 1 seconde et 50 ans. Pour configure r ce paramètre , vous devez sélectionner le type de compatibilité pour Strong Certifica te Binding Enforce.

Type	Nom du paramè	Nom d'API	Valeurs potentielles	Description du paramètre
				Pour plus d'informations, consultez l'article KB5014754 : modifications apportées à l'authentification basée sur les certificats sur les contrôleurs de domaine Windows dans la documentation Microsoft Support.

Type	Nom du paramè	Nom d'API	Valeurs potentielles	Description du paramètre
	Applicat on stricte des certifica ts	CERTIFICA TE_STRONG _ENFORCEM ENT	Compatibilité, Application complète	Spécifiez l'un des types d'application suivants : • Compatibilité (par défaut) : l'authent ification est autorisée si un certifica t ne peut pas être clairement mappé à un utilisateur. Si le certificat est antérieur au compte utilisateur dans Active Directory, vous devez également définir la compensat ion de l'antidatage des certifica ts, sinon l'authent ification échouera.

Type	Nom du paramè	Nom d'API	Valeurs potentielles	Description du paramètre
				• Application complète : l'authentification n'est pas autorisée si un certificat ne peut pas être clairement mappé à un utilisateur. Si vous choisissez ce type d'application, la compensation de l'antidatage des certificats ne peut pas être configurée. Pour plus d'informations, consultez l'article KB5014754 : modifications apportées

Type	Nom du paramè	Nom d'API	Valeurs potentielles	Description du paramètre
				à l'authentification basée sur les certificats sur les contrôleurs de domaine Windows dans la documentation Microsoft Support.
Canal sécurisé : chiffrement	AES 12	AES_128_128	Activer, Désactiver	Activez ou désactivez le chiffrement AES 128/128 pour sécuriser les communications entre les contrôleurs de domaine de votre annuaire.
	DE 56/56	DES_56_56	Activer, Désactiver	Activez ou désactivez le chiffrement DES 56/56 pour sécuriser les communications entre les contrôleurs de domaine de votre annuaire.

Type	Nom du paramè	Nom d'API	Valeurs potentielles	Description du paramètre
	RC2 40	RC2_40_128	Activer, Désactiver	Activez ou désactivez le chiffrement RC2 40/128 pour sécuriser les communications entre les contrôleurs de domaine de votre annuaire.
	RC2 56	RC2_56_128	Activer, Désactiver	Activez ou désactivez le chiffrement RC2 56/128 pour sécuriser les communications entre les contrôleurs de domaine de votre annuaire.
	RC2 12	RC2_128_128	Activer, Désactiver	Activez ou désactivez le chiffrement RC2 128/128 pour sécuriser les communications entre les contrôleurs de domaine de votre annuaire.

Type	Nom du paramè	Nom d'API	Valeurs potentielles	Description du paramètre
	RC4 40/	RC4_40_128	Activer, Désactiver	Activez ou désactivez le chiffrement RC4 40/128 pour sécuriser les communications entre les contrôleurs de domaine de votre annuaire.
	RC4 56/	RC4_56_128	Activer, Désactiver	Activez ou désactivez le chiffrement RC4 56/128 pour sécuriser les communications entre les contrôleurs de domaine de votre annuaire.
	RC4 64/	RC4_64_128	Activer, Désactiver	Activez ou désactivez le chiffrement RC4 64/128 pour sécuriser les communications entre les contrôleurs de domaine de votre annuaire.

Type	Nom du paramè	Nom d'API	Valeurs potentielles	Description du paramètre
	RC4 12	RC4_128_128	Activer, Désactiver	Activez ou désactivez le chiffrement RC4 128/128 pour sécuriser les communications entre les contrôleurs de domaine de votre annuaire.
	Triple DES 16	3DES_168_168	Activer, Désactiver	Activez ou désactivez le chiffrement Triple DES 168/168 pour sécuriser les communications entre les contrôleurs de domaine de votre annuaire.

Type	Nom du paramè	Nom d'API	Valeurs potentielles	Description du paramètre
Canal sécurisé : protocole	PCT 1.0	PCT_1_0	Activer, Désactiver	Activez ou désactivez le protocole PCT 1.0 pour sécuriser les communications (serveur et client) sur les contrôleurs de domaine de votre annuaire.
	SSL 2.0	SSL_2_0	Activer, Désactiver	Activez ou désactivez le protocole SSL 2.0 pour sécuriser les communications (serveur et client) sur les contrôleurs de domaine de votre annuaire.

Type	Nom du paramè	Nom d'API	Valeurs potentielles	Description du paramètre
	SSL 3.0	SSL_3_0	Activer, Désactiver	Activez ou désactivez le protocole SSL 3.0 pour sécuriser les communications (serveur et client) sur les contrôleurs de domaine de votre annuaire.
	TLS 1.0	TLS_1_0	Activer, Désactiver	Activez ou désactivez le protocole TLS 1.0 pour sécuriser les communications (serveur et client) sur les contrôleurs de domaine de votre annuaire.

Type	Nom du paramè	Nom d'API	Valeurs potentielles	Description du paramètre
	TLS 1.1	TLS_1_1	Activer, Désactiver	Activez ou désactivez le protocole TLS 1.1 pour sécuriser les communications (serveur et client) sur les contrôleurs de domaine de votre annuaire.

Configurer le AWS Private CA connecteur pour AD

Vous pouvez intégrer votre Microsoft AD AWS géré à AWS Private Certificate Authority (CA) pour émettre et gérer des certificats pour les utilisateurs, les groupes et les machines associés à votre domaine Active Directory. AWS Private CA Le Connector for Active Directory vous permet d'utiliser une solution de remplacement entièrement AWS Private CA gérée pour les autorités de certification autogérées de votre entreprise sans avoir à déployer, corriger ou mettre à jour des agents locaux ou des serveurs proxy.

> **Note**
>
> L'inscription de certificats LDAPS côté serveur pour les contrôleurs de domaine AWS Microsoft AD gérés avec AWS Private CA Connector for Active Directory n'est pas prise en charge. Pour activer le protocole LDAPS côté serveur pour votre annuaire, consultez Comment activer le protocole LDAPS côté serveur pour votre AWS annuaire Microsoft AD géré.

Vous pouvez configurer AWS Private CA l'intégration à votre annuaire via la console Directory Service, la console AWS Private CA Connector for Active Directory ou en appelant l'`CreateTemplate`API. Pour configurer l'intégration de Private CA via la console AWS Private CA

Connector for Active Directory, reportez-vous à la section Création d'un modèle de connecteur. Vous trouverez ci-dessous les étapes à suivre pour configurer cette intégration depuis la AWS Directory Service console.

Pour configurer AWS Private CA Connector pour AD

1. Connectez-vous à la AWS Directory Service console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/directoryservicev2/.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sous l'onglet Réseau et sécurité, sous AWS Private CA Connecteur pour AD, choisissez Configurer le AWS Private CA connecteur pour AD. La page Créer un certificat CA privé pour Active Directory apparaît. Suivez les étapes indiquées sur la console pour créer votre autorité de certification privée pour le Active Directory connecteur afin de vous inscrire auprès de votre autorité de certification privée. Pour de plus amples informations, veuillez consulter Creating a connector (français non garanti).
4. Après avoir créé votre connecteur, suivez les étapes ci-dessous pour afficher les détails, notamment le statut du connecteur et le statut de l'autorité de certification privée associée.

Pour afficher AWS Private CA Connector for AD

1. Connectez-vous à la AWS Directory Service console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/directoryservicev2/.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sous Réseau et sécurité, sous AWS Private CA Connecteur pour AD, vous pouvez afficher vos connecteurs d'autorité de certification privée et votre autorité de certification privée associée. Par défaut, les champs suivants s'affichent :

    a. AWS Private CA ID du connecteur : identifiant unique d'un AWS Private CA connecteur. Cliquez dessus pour accéder à la page de détails de ce AWS Private CA connecteur.

    b. AWS Private CA objet — Informations sur le nom distinctif de l'autorité de certification. Cliquez dessus pour accéder à la page de détails de cet élément AWS Private CA.

    c. État — Sur la base d'une vérification de l'état du AWS Private CA connecteur et du AWS Private CA. Si les deux contrôles sont réussis, Actif s'affiche. Si l'une des vérifications échoue, la mention 1/2 checks failed (1 vérifications sur 2 a échoué) s'affiche. Si les deux vérifications échouent, la mention Failed (Échec) s'affiche. Pour plus d'informations sur

un état d'échec, passez le pointeur de la souris sur le lien hypertexte pour savoir quelle vérification a échoué. Suivez les instructions de la console pour résoudre le problème.

d. Date de création — Le jour où le AWS Private CA connecteur a été créé.

Pour plus d'informations, veuillez consulter View connector details (français non garanti).

Surveiller votre AWS Managed Microsoft AD

Vous pouvez surveiller votre annuaire AWS Managed Microsoft AD à l'aide des méthodes suivantes :

Rubriques

- Comprendre le statut de votre annuaire
- Configurer les notifications d'état de l'annuaire avec Amazon SNS
- Vérification de vos journaux d'annuaire AWS Managed Microsoft AD
- Activer le transfert de journaux
- Surveiller vos contrôleurs de domaine grâce à des métriques de performance

Comprendre le statut de votre annuaire

Voici les différents statuts possibles pour un annuaire.

Actif

L'annuaire fonctionne normalement. Aucun problème n'a été détecté par AWS Directory Service pour votre annuaire.

Création

L'annuaire est en cours de création. La création de l'annuaire prend généralement entre 20 et 45 minutes, mais peut varier selon la charge du système.

Supprimé

L'annuaire a été supprimé. Toutes les ressources de l'annuaire ont été libérées. Une fois qu'un annuaire se trouve dans cet état, il ne peut pas être récupéré.

Suppression en cours

L'annuaire est en cours de suppression. L'annuaire restera dans cet état jusqu'à ce qu'il soit totalement supprimé. Une fois qu'un annuaire se trouve dans cet état, l'opération de suppression ne peut pas être annulée, et l'annuaire ne peut pas être récupéré.

Échec

L'annuaire n'a pas pu être créé. Veuillez supprimer cet annuaire. Si le problème persiste, veuillez contacter le centre AWS Support.

Dégradé

L'annuaire est en cours d'exécution dans un état dégradé. Un ou plusieurs problèmes ont été détectés. Il se peut que toutes les opérations liées à l'annuaire ne puissent pas être totalement opérationnelles. Il existe de nombreuses raisons pouvant expliquer que l'annuaire se trouve dans cet état. Parmi ces raisons, citons une opération de maintenance d'exploitation normale comme une application de correctif ou une rotation d'instance EC2, la création temporaire d'un point chaud par une application sur l'un de vos contrôleurs de domaine ou des modifications que vous avez apportées à votre réseau et qui ont interrompu les communications de l'annuaire. Pour plus d'informations, veuillez consulter Résolution des problèmes liés AWS à Managed Microsoft AD, Résolution des problèmes liés à AD Connector, Résolution des problèmes de Simple AD. Pour les problèmes normaux liés à la maintenance, AWS les problèmes sont résolus dans les 40 minutes. Si, après avoir consulté la rubrique de dépannage, votre annuaire reste à l'état Dégradé pendant plus de 40 minutes, nous vous recommandons de contacter le centre AWS Support.

> **Important**
>
> Ne restaurez pas un instantané lorsqu'un annuaire est dans un état dégradé. Il est rare qu'une restauration d'instantané soit nécessaire pour résoudre les problèmes d'état dégradé. Pour plus d'informations, consultez Création d'un instantané ou d'une restauration de votre annuaire.

Demandé

La demande de création de votre annuaire est actuellement en attente.

RestoreFailed

Échec de la restauration de l'annuaire à partir d'un instantané. Renouvelez l'opération de restauration. Si le problème persiste, utilisez un autre instantané ou contactez le centre AWS Support.

Restauration en cours

L'annuaire est en cours de restauration à partir d'un instantané automatique ou manuel. La restauration à partir d'un instantané prend généralement plusieurs minutes, selon la taille des données de l'annuaire dans l'instantané.

Configurer les notifications d'état de l'annuaire avec Amazon SNS

Avec Amazon Simple Notification Service (Amazon SNS), vous pouvez recevoir des e-mails ou des messages texte (SMS) lorsque le statut de votre annuaire change. Vous êtes averti si votre annuaire passe du statut Actif à l'état Inactif. Vous recevez également une notification lorsque l'annuaire renvoie un statut Active (Actif).

Comment ça marche

Amazon SNS utilise des « rubriques » pour collecter et diffuser des messages. Chaque rubrique compte un ou plusieurs abonnés qui reçoivent les messages qui ont été publiés dans cette rubrique. En suivant les étapes ci-dessous, vous pouvez ajouter un article AWS Directory Service en tant qu'éditeur à une rubrique Amazon SNS. Lorsqu'il AWS Directory Service détecte un changement dans le statut de votre annuaire, il publie un message sur ce sujet, qui est ensuite envoyé aux abonnés du sujet.

Vous pouvez associer plusieurs annuaires en tant que diffuseurs de publication à une même rubrique. Vous pouvez également ajouter des messages de statut de l'annuaire aux rubriques que vous avez créées précédemment dans Amazon SNS. Vous avez un contrôle détaillé sur les personnes autorisées à publier et à s'abonner à une rubrique. Pour obtenir des informations détaillées sur Amazon SNS, veuillez consulter Qu'est-ce qu'Amazon SNS ?

> **Note**
>
> Les notifications d'état du répertoire sont une fonctionnalité régionale de AWS Managed Microsoft AD. Si vous utilisez Réplication multi-régions, les procédures suivantes doivent

être appliquées séparément dans chaque région. Pour plus d'informations, consultez Caractéristiques mondiales et régionales.

Pour activer la messagerie SNS pour votre annuaire

1. Connectez-vous à la AWS Directory Service console AWS Management Console et ouvrez-la.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), procédez de l'une des manières suivantes :
   - Si plusieurs régions apparaissent sous Réplication multi-régions, sélectionnez la région dans laquelle vous souhaitez activer la messagerie SNS, puis cliquez sur l'onglet Maintenance. Pour plus d'informations, consultez Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication multi-régions, sélectionnez l'onglet Maintenance.
4. Dans la section Surveillance de l'annuaire, choisissez Actions, puis sélectionnez Create notification (Créer une notification).
5. Sur la page Créer une notification, sélectionnez Choisir un type de notification, puis choisissez Créer une notification. Si vous avez déjà une rubrique SNS existante, vous pouvez également choisir Associer une rubrique SNS existante pour envoyer des messages de statut de cet annuaire à cette rubrique.

   > **Note**
   >
   > Si vous choisissez Créer une nouvelle notification, mais que vous utilisez le même nom de rubrique pour une rubrique SNS qui existe déjà, Amazon SNS ne crée pas de rubrique, mais ajoute simplement les nouvelles informations d'abonnement à la rubrique existante.
   > Si vous choisissez Associer une rubrique SNS existante, vous ne pourrez choisir qu'une rubrique SNS située dans la même région que l'annuaire.

6. Choisissez le type de destinataire et saisissez les coordonnées du destinataire. Si vous saisissez un numéro de téléphone pour les SMS, utilisez uniquement des chiffres. N'incluez pas de tirets, d'espaces, ni de parenthèses.
7. (Facultatif) Donnez un nom à votre rubrique et un nom d'affichage SNS. Le nom d'affichage est un nom court de 10 caractères maximum inclus dans tous les messages SMS de cette rubrique. Lorsque vous utilisez l'option SMS, le nom d'affichage est obligatoire.

> **Note**
>
> Si vous êtes connecté à l'aide d'un utilisateur ou d'un rôle IAM doté uniquement de la politique DirectoryServiceFullAccessgérée, le nom de votre rubrique doit commencer par « DirectoryMonitoring ». Si vous souhaitez personnaliser davantage le nom de votre rubrique, vous aurez besoin de privilèges supplémentaires pour SNS.

8. Sélectionnez Create (Créer).

Si vous souhaitez désigner des abonnés SNS supplémentaires, tels qu'une adresse e-mail supplémentaire, des files d'attente Amazon SQS AWS Lambda ou, vous pouvez le faire depuis la console Amazon SNS.

Pour supprimer les messages de statut de l'annuaire d'une rubrique

1. Connectez-vous à la AWS Directory Service console AWS Management Console et ouvrez-la.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), procédez de l'une des manières suivantes :
   - Si plusieurs régions apparaissent sous Réplication multi-régions, sélectionnez la région dans laquelle vous souhaitez supprimer les messages de statut, puis cliquez sur l'onglet Maintenance. Pour plus d'informations, consultez Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication multi-régions, sélectionnez l'onglet Maintenance.
4. Dans la section Surveillance de l'annuaire, sélectionnez le nom d'une rubrique SNS dans la liste, choisissez Actions, puis sélectionnez Supprimer.
5. Sélectionnez Remove (Supprimer).

Cela supprime votre annuaire en tant que diffuseur de publication pour la rubrique SNS sélectionnée. Si vous souhaitez supprimer le sujet dans son intégralité, vous pouvez le faire depuis la console Amazon SNS.

> **Note**
>
> Avant de supprimer une rubrique Amazon SNS à l'aide de la console SNS, vous devez vous assurer qu'aucun annuaire n'envoie de messages de statut à cette rubrique.

Si vous supprimez une rubrique Amazon SNS à l'aide de la console SNS, cette modification ne sera pas immédiatement reflétée dans la console Directory Services. Vous ne serez averti que la prochaine fois qu'un annuaire publiera une notification concernant la rubrique supprimée, auquel cas vous verrez un statut mis à jour dans l'onglet Surveillance de l'annuaire indiquant que la rubrique est introuvable.
Par conséquent, pour éviter de manquer des messages importants sur le statut du répertoire, avant de supprimer toute rubrique recevant des messages AWS Directory Service, associez votre annuaire à une autre rubrique Amazon SNS.

Vérification de vos journaux d'annuaire AWS Managed Microsoft AD

Les journaux de sécurité des instances de contrôleur de domaine AWS Managed Microsoft AD sont archivés pendant un an. Vous pouvez également configurer votre annuaire AWS Managed Microsoft AD pour transmettre les journaux du contrôleur de domaine à Amazon CloudWatch Logs en temps quasi réel. Pour de plus amples informations, veuillez consulter Activer le transfert de journaux.

AWS enregistre les événements suivants à des fins de conformité.

Catégorie de surveillance	Définition de stratégie	État d'audit
Connexion au compte	Audit de validation des identifiants	Réussite, échec
	Audit des autres événements d'ouverture de session de compte	Réussite, échec
Gestion de compte	Audit de la gestion des comptes informatiques	Réussite, échec
	Audit des autres événements de gestion des comptes	Réussite, échec
	Audit de la gestion des groupes de sécurité	Réussite, échec

Catégorie de surveillance	Définition de stratégie	État d'audit
	Audit de la gestion des comptes d'utilisateur	Réussite, échec
Suivi détaillé	Audit d'activité DPAPI	Réussite, échec
	Audit d'activité PNP	Réussite
	Audit de la création de processus	Réussite, échec
Accès DS	Audit de l'accès aux services d'annuaire	Réussite, échec
	Audit des changements de services d'annuaire	Réussite, échec
Connexion/déconnexion	Audit de verrouillage de compte	Réussite, échec
	Audit de déconnexion	Réussite
	Audit de connexion	Réussite, échec
	Audit des autres événement s d'ouverture/fermeture de session	Réussite, échec
	Audit des connexions spéciales	Réussite, échec
Accès aux objets	Audit des autres événements d'accès aux objets	Réussite, échec
	Audit des supports de stockage amovibles	Réussite, échec
	Audit du transfert des stratégie s d'accès centrales	Réussite, échec

Catégorie de surveillance	Définition de stratégie	État d'audit
Modifications des stratégies	Audit de modification des stratégies	Réussite, échec
	Audit de modification des stratégies d'authentification	Réussite, échec
	Audit de modification des stratégies d'autorisation	Réussite, échec
	Audit de modification de la stratégie au niveau des règles MPSSVC	Réussite
	Audit des autres événements de modification de stratégie	Échec
Utilisation des privilèges	Audit de l'utilisation des privilèges sensibles	Réussite, échec
Système	Audit du pilote IPsec	Réussite, échec
	Audit des autres événements système	Réussite, échec
	Audit des changements d'état de sécurité	Réussite, échec
	Audit de l'extension du système de sécurité	Réussite, échec
	Audit de l'intégrité du système	Réussite, échec

Activer le transfert de journaux

Vous pouvez utiliser la console AWS Directory Service ou les API pour transmettre les journaux d'événements de sécurité du contrôleur de domaine vers Amazon CloudWatch Logs. Cela vous

aide à répondre à vos exigences en matière de sécurité, d'audit et de conservation des journaux en assurant la transparence des événements de sécurité dans votre annuaire.

CloudWatch Logs peut également transférer ces événements vers d'autres comptes AWS, services AWS ou applications tierces. Cela facilite la surveillance et la configuration centralisées des alertes afin de détecter et de réagir de manière proactive aux activités inhabituelles en temps quasi réel.

Une fois le service activé, vous pouvez ensuite utiliser la console CloudWatch Logs pour récupérer les données du groupe de journaux que vous avez spécifié lors de l'activation. Ce groupe de journaux contient les journaux de sécurité de vos contrôleurs de domaine.

Pour plus d'informations sur les groupes de journaux et la lecture de leurs données, consultez Utilisation des groupes de journaux et des flux de journaux dans le Guide de l'utilisateur d'Amazon CloudWatch Logs.

> **Note**
>
> Le transfert de journaux est une fonctionnalité régionale de AWS Managed Microsoft AD. Si vous utilisez Réplication multi-régions, les procédures suivantes doivent être appliquées séparément dans chaque région. Pour de plus amples informations, veuillez consulter Caractéristiques mondiales et régionales.

Pour activer le transfert de journaux

1. Dans le panneau de navigation de la console AWS Directory Service, choisissez Annuaires.
2. Choisissez l'ID de l'annuaire AWS Managed Microsoft AD que vous souhaitez partager.
3. Sur la page Directory details (Détails de l'annuaire), procédez de l'une des manières suivantes :
   - Si plusieurs régions apparaissent sous Multi-Region replication (Réplication multi-régions), sélectionnez la région dans laquelle vous souhaitez activer le transfert de journaux, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour de plus amples informations, veuillez consulter Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Multi-Regions replication (Réplication multi-régions), choisissez l'onglet Networking & security (Réseau et sécurité).
4. Dans la section Transfert de journaux, choisissez Activer.
5. Dans la boîte de dialogue Activer le transfert de journaux vers CloudWatch, choisissez l'une des options suivantes :

a. Choisissez Create a new CloudWatch log group (Créer un nouveau groupe de journaux CloudWatch), sous CloudWatch Log group name (Nom du groupe de journaux CloudWatch), précisez un nom auquel vous pouvez faire référence dans CloudWatch Logs.

b. Sélectionnez Choisir un groupe de journaux CloudWatch existant, puis sous Groupes de journaux CloudWatch existants, sélectionnez un groupe de journaux dans le menu.

6. Passez en revue les informations de tarification et le lien, puis choisissez Activer.

Pour désactiver le transfert de journaux

1. Dans le panneau de navigation de la console AWS Directory Service, choisissez Annuaires.
2. Choisissez l'ID de l'annuaire AWS Managed Microsoft AD que vous souhaitez partager.
3. Sur la page Directory details (Détails de l'annuaire), procédez de l'une des manières suivantes :

   - Si plusieurs régions apparaissent sous Multi-Region replication (Réplication multi-régions), sélectionnez la région dans laquelle vous souhaitez désactiver le transfert de journaux, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour de plus amples informations, veuillez consulter Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Multi-Regions replication (Réplication multi-régions), choisissez l'onglet Networking & security (Réseau et sécurité).

4. Dans la section Transfert de journaux, choisissez Désactiver.
5. Une fois que vous avez lu les informations de la boîte de dialogue Désactiver le transfert de journaux, choisissez Désactiver.

Utilisation de l'interface de ligne de commande pour activer le transfert de journaux

Avant de pouvoir utiliser la commande `ds create-log-subscription`, vous devez créer un groupe de journaux Amazon CloudWatch, puis créer une politique de ressources IAM qui accorde l'autorisation nécessaire à ce groupe. Pour activer le transfert de journaux à l'aide de l'interface de ligne de commande, suivez toutes les étapes ci-dessous.

Étape 1 : création d'un groupe de journaux dans CloudWatch Logs

Créez un groupe de journaux qui servira à recevoir les journaux de sécurité de vos contrôleurs de domaine. Nous vous conseillons de faire précéder le nom de `/aws/directoryservice/`, mais ce n'est pas obligatoire. Par exemple :

EXEMPLE DE COMMANDE DE LIGNE DE COMMANDE

```
aws logs create-log-group --log-group-name '/aws/directoryservice/
d-9876543210'
```

EXEMPLE DE COMMANDE POWERSHELL

```
New-CWLLogGroup -LogGroupName '/aws/directoryservice/d-9876543210'
```

Pour en savoir plus sur comment créer un groupe CloudWatch Logs, consultez Créer un groupe de journaux dans CloudWatch Logs dans le Guide de l'utilisateur Amazon CloudWatch Logs.

Étape 2 : création d'une politique de ressources CloudWatch Logs dans IAM

Créez une politique de ressources CloudWatch Logs accordant à AWS Directory Service des droits pour ajouter des journaux dans le nouveau groupe de journaux créé à l'étape 1. Vous pouvez spécifier l'ARN précis du groupe de journaux pour limiter l'accès de AWS Directory Service aux autres groupes de journaux ou utiliser un caractère générique pour inclure tous les groupes de journaux. La politique de l'exemple suivant utilise la méthode du caractère générique pour inclure tous les groupes de journaux commençant par `/aws/directoryservice/` pour le compte AWSdans lequel votre annuaire.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ds.amazonaws.com"
            },
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:YOUR_REGION:YOUR_ACCOUNT_NUMBER:log-group:/aws/
directoryservice/*"
        }
    ]
}
```

Vous devez enregistrer cette stratégie dans un fichier texte (par exemple DSPolicy.json) sur votre station de travail locale, car vous devrez l'exécuter à partir de l'interface de ligne de commande. Par exemple :

EXEMPLE DE COMMANDE DE LIGNE DE COMMANDE

```
aws logs put-resource-policy --policy-name DSLogSubscription --policy-document file://DSPolicy.json
```

EXEMPLE DE COMMANDE POWERSHELL

```
$PolicyDocument = Get-Content .\DSPolicy.json –Raw

Write-CWLResourcePolicy -PolicyName DSLogSubscription -PolicyDocument $PolicyDocument
```

Étape 3 : création d'un abonnement aux journaux AWS Directory Service

Dans cette étape finale, vous pouvez maintenant passer à l'activation du transfert de journaux en créant l'abonnement aux journaux. Par exemple :

EXEMPLE DE COMMANDE DE LIGNE DE COMMANDE

```
aws ds create-log-subscription --directory-id 'd-9876543210' --log-group-name '/aws/directoryservice/d-9876543210'
```

EXEMPLE DE COMMANDE POWERSHELL

```
New-DSLogSubscription -DirectoryId 'd-9876543210' -LogGroupName '/aws/directoryservice/d-9876543210'
```

Surveiller vos contrôleurs de domaine grâce à des métriques de performance

AWS Directory Service s'intègre CloudWatch à Amazon pour vous fournir des indicateurs de performance importants pour chaque contrôleur de domaine de votreActive Directory. Cela signifie que vous pouvez surveiller les compteurs de performance des contrôleurs de domaine, tels que l'utilisation du processeur et de la mémoire. Vous pouvez également configurer des alarmes et lancer des actions automatisées pour répondre aux périodes de forte utilisation. Par exemple, vous pouvez configurer une alarme pour une utilisation du processeur du contrôleur de domaine supérieure à 70 % et créer une rubrique SNS pour vous avertir lorsque cela se produit. Vous pouvez utiliser cette rubrique SNS pour lancer des automatisations, telles que des AWS Lambda fonctions, afin d'augmenter le nombre de contrôleurs de domaine sur votreActive Directory.

Pour plus d'informations sur la surveillance des contrôleurs de domaine, veuillez consulter Déterminez quand ajouter des contrôleurs de domaine avec des CloudWatch métriques.

Des frais sont associés à Amazon CloudWatch. Pour plus d'informations, consultez la section CloudWatchfacturation et coûts.

> **Important**
>
> Les indicateurs de performance des contrôleurs de domaine ne CloudWatch sont pas disponibles dans la région du Canada Ouest (Calgary).

Trouvez les indicateurs de performance des contrôleurs de domaine dans CloudWatch

Dans la CloudWatch console Amazon, les métriques d'un service donné sont d'abord regroupées en fonction de l'espace de noms du service. Vous pouvez ajouter des filtres métriques subordonnés à cet espace de noms. Utilisez la procédure suivante pour localiser l'espace de noms et la métrique subordonnée appropriés requis pour configurer les métriques du contrôleur de domaine Managed AWS Microsoft AD dans. CloudWatch

Pour trouver les métriques du contrôleur de domaine dans la CloudWatch console

1. Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Dans la liste des métriques, sélectionnez l'espace de noms Directory Service, puis dans la liste, sélectionnez la métrique AWS Managed Microsoft AD.

Pour obtenir des instructions sur la façon de configurer les métriques du contrôleur de domaine à l'aide de la CloudWatch console, consultez Comment automatiser le dimensionnement de AWS Managed Microsoft AD en fonction des métriques d'utilisation dans le blog sur la AWS sécurité.

Déterminez quand ajouter des contrôleurs de domaine avec des CloudWatch métriques

L'équilibrage de charge entre tous vos contrôleurs de domaine est important pour la résilience et les performances de votreActive Directory. Pour vous aider à optimiser les performances de vos contrôleurs de domaine dans AWS Managed Microsoft AD, nous vous recommandons de commencer par surveiller les indicateurs importants CloudWatch afin de constituer une base de

référence. Au cours de ce processus, vous analysez votre taux d'utilisation Active Directory au fil du temps afin d'identifier votre taux d'Active Directoryutilisation moyen et maximal. Après avoir déterminé votre base de référence, vous pouvez surveiller régulièrement ces indicateurs afin de déterminer à quel moment ajouter un contrôleur de domaine à votreActive Directory.

Les métriques suivantes sont importantes à surveiller de façon régulière. Pour obtenir la liste complète des métriques de contrôleur de domaine disponibles dans CloudWatch, voirAWS Compteurs de performance Microsoft AD gérés.

- Métriques spécifiques au contrôleur de domaine, telles que :
  - Processeur
  - Mémoire
  - Disque logique
  - Interface réseau
- AWS Mesures spécifiques à l'annuaire Microsoft AD gérées, telles que :
  - Recherches LDAP
  - Liaisons
  - Requêtes DNS
  - Lectures de l'annuaire
  - Écritures de l'annuaire

Pour obtenir des instructions sur la façon de configurer les métriques du contrôleur de domaine à l'aide de la CloudWatch console, consultez Comment automatiser le dimensionnement de AWS Managed Microsoft AD en fonction des métriques d'utilisation dans le blog sur la AWS sécurité. Pour obtenir des informations générales sur les métriques dans CloudWatch, consultez la section Utilisation CloudWatch des métriques Amazon dans le guide de CloudWatch l'utilisateur Amazon.

Pour des informations générales sur la planification des contrôleurs de domaine, consultez la section Planification des capacités pour les services de Active Directory domaine sur le site Web de Microsoft.

AWS Compteurs de performance Microsoft AD gérés

Le tableau suivant répertorie tous les compteurs de performance disponibles sur Amazon CloudWatch pour suivre les performances des contrôleurs de domaine et des annuaires dans AWS Managed Microsoft AD.

Catégorie de la métrique	Nom de la métrique
Base de données ==> Instances (NTDSA)	Résultats en % du cache de bases de données
	Latence de moyenne de lectures de bases de données I/O
	Lectures de bases de données I/O par seconde
	Latence de moyenne d'écritures de journaux I/O
DirectoryServices (MNT)	Temps de liaison LDAP
	Opérations de réplication en attente de DRA
	Synchronisations des réplications en attente de DRA
DNS	Requêtes récursives par seconde
	Échec de la requête récursive par seconde
	Requête TCP reçue par seconde
	Total requête reçue par seconde
	Réponse totale envoyée par seconde
	Requête UDP reçue par seconde
LogicalDisk	Avg. Longueur de la file d'attente de disque
	Espace libre en %
Mémoire	% d'octets validés en cours d'utilisation
	Durée de vie moyenne du cache en veille à long terme(s)
Interface réseau	Octets envoyés/s

Catégorie de la métrique	Nom de la métrique
	Octets reçus/s
	Bande passante actuelle
NTDS	Délai d'attente estimé ATQ
	Latence des demandes ATQ
	Lectures de l'annuaire DS par seconde
	Recherches de l'annuaire DS par seconde
	Écritures de l'annuaire DS par seconde
	Sessions client LDAP
	Recherches LDAP par seconde
	Liaisons réussies LDAP par seconde
Processeur	Temps de traitement en %
Statistiques de sécurité à l'échelle du système	Authentifications Kerberos
	Authentifications NTLM

Réplication multi-régions

La réplication multirégionale peut être utilisée pour répliquer automatiquement les données de votre annuaire AWS Microsoft AD géré sur plusieurs. Régions AWSCette réplication peut améliorer les performances des utilisateurs et des applications dans des zones géographiques dispersées. AWS Managed Microsoft AD utilise la réplication native d'Active Directory pour répliquer les données de votre annuaire en toute sécurité dans la nouvelle région.

La réplication multirégionale n'est prise en charge que pour l'édition Enterprise de AWS Managed Microsoft AD.

Vous pouvez utiliser la réplication multi-régions automatisée dans la plupart des régions où AWS Managed Microsoft AD est disponible.

Important

La réplication multirégionale n'est pas disponible dans les régions optionnelles suivantes :

- Afrique (Le Cap) af-south-1
- Asie-Pacifique (Hong Kong) ap-east-1
- Asie-Pacifique (Hyderabad) ap-south-2
- Asie-Pacifique (Jakarta) ap-southeast-3
- Asie-Pacifique (Melbourne) ap-southeast-4
- Canada Ouest (Calgary) ca-ouest-1
- Europe (Milan) eu-south-1
- Europe (Espagne) eu-south-2
- Europe (Zurich) eu-central-2
- Israël (Tel Aviv) il-central-1
- Moyen-Orient (Bahreïn) me-south-1
- Moyen-Orient (Émirats arabes unis) me-central-1

Pour plus d'informations sur les régions optionnelles et sur la façon de les activer, consultez la section Spécifiez les régions que Régions AWS votre compte peut utiliser dans le AWS Account Management Guide.

Avantages

Avec la réplication multirégionale dans AWS Managed Microsoft AD, les applications compatibles avec Active Directory utilisent l'annuaire localement pour des performances élevées et la fonctionnalité multirégion pour la résilience. Vous pouvez utiliser la réplication multirégionale avec des applications compatibles avec Active Directory telles que SQL Server SharePoint Always On, ainsi que des AWS services tels qu'Amazon RDS for SQL Server et FSx for Windows File Server. Voici d'autres avantages de la réplication multi-régions.

- Il vous permet de déployer rapidement une seule instance Microsoft AD AWS gérée dans le monde entier et élimine le lourd fardeau lié à l'autogestion d'une infrastructure Active Directory mondiale.

- Il vous permet de déployer et de gérer les charges de travail Windows et Linux plus facilement et à moindre coût dans plusieurs AWS régions. La réplication multirégionale automatisée permet d'optimiser les performances de vos applications globales compatibles avec Active Directory. Toutes les applications déployées dans des instances Windows ou Linux utilisent Microsoft AD AWS géré localement dans la région, ce qui permet de répondre aux demandes des utilisateurs depuis la région la plus proche possible.
- Elle assure la résilience multi-régions. Déployé dans l'infrastructure AWS gérée à haute disponibilité, AWS Managed Microsoft AD gère les mises à jour logicielles automatisées, la surveillance, la restauration et la sécurité de l'infrastructure Active Directory sous-jacente dans toutes les régions. Cela vous permet de vous concentrer sur le développement de vos applications.

Rubriques

Caractéristiques mondiales et régionales

Lorsque vous ajoutez une AWS région à votre répertoire à l'aide de la réplication multirégionale, cela AWS Directory Service améliore la portée de toutes les fonctionnalités afin qu'elles prennent en compte les régions. Ces fonctionnalités sont répertoriées dans différents onglets de la page de détails qui apparaît lorsque vous choisissez l'ID de l'annuaire dans la console AWS Directory Service . Cela signifie que toutes les fonctionnalités sont activées, configurées ou gérées en fonction de la région que vous sélectionnez dans la section Réplication multi-régions de la console. Les modifications que vous apportez aux fonctionnalités de chaque région sont appliquées à l'échelle mondiale ou par région.

La réplication multirégionale n'est prise en charge que pour l'édition Enterprise de AWS Managed Microsoft AD.

Fonctionnalités mondiales

Toutes les modifications que vous apportez aux fonctionnalités mondiales alors que la Région principale est sélectionnée seront appliquées à toutes les régions.

Vous pouvez identifier les fonctionnalités utilisées à l'échelle mondiale sur la page Directory details (Détails de l'annuaire), car la mention Applied to all replicated Regions (Appliquée à toutes les régions répliquées) s'affiche à côté. Sinon, si vous avez sélectionné une autre région dans la liste qui n'est pas la région principale, vous pouvez identifier les fonctionnalités utilisées à l'échelle mondiale, car elles affichent la mention Inherited from primary Region (Hérité de la région principale).

Caractéristiques régionales

Toutes les modifications que vous apportez à une fonctionnalité dans une Région supplémentaire seront appliquées uniquement à cette région.

Vous pouvez identifier les fonctionnalités qui sont régionales sur la page Directory details (Détails de l'annuaire), car les mentions Applied to all replicated Regions (Appliquée à toutes les régions répliquées) ou Inherited from primary Region (Hérité de la région principale) ne s'affichent pas à côté.

Régions principales et régions supplémentaires

Avec la réplication multirégionale, AWS Managed Microsoft AD utilise les deux types de régions suivants pour différencier la manière dont les fonctionnalités globales ou régionales doivent être appliquées dans votre annuaire.

Région principale

La région initiale dans laquelle vous avez créé votre annuaire pour la première fois est appelée région principale. Vous ne pouvez effectuer que des opérations mondiales au niveau de l'annuaire, telles que la création d'approbations Active Directory et la mise à jour du schéma AD à partir de la région principale.

La région principale peut toujours être identifiée comme étant la première région, car elle figure en haut de la liste dans la section Multi-Region replication (Réplication multi-régions) et se termine par - Primary (Principale). Par exemple, USA Est (Virginie du Nord) - Principale.

Toutes les modifications que vous apportez aux Fonctionnalités mondiales alors que la région principale est sélectionnée seront appliquées à toutes les régions.

Vous ne pouvez ajouter des régions que lorsque la région principale est sélectionnée. Pour de plus amples informations, veuillez consulter Ajouter une région répliquée.

Région supplémentaire

Toutes les régions que vous avez ajoutées à votre annuaire sont appelées régions supplémentaires.

Bien que certaines fonctionnalités puissent être gérées à l'échelle mondiale pour toutes les régions, d'autres sont gérées individuellement par région. Pour gérer une fonctionnalité pour une région supplémentaire (région non principale), vous devez d'abord sélectionner la région supplémentaire dans la liste de la section Multi-Region replication (Réplication multi-régions) de la page Directory details (Détails de l'annuaire). Vous pouvez ensuite procéder à la gestion de la fonctionnalité.

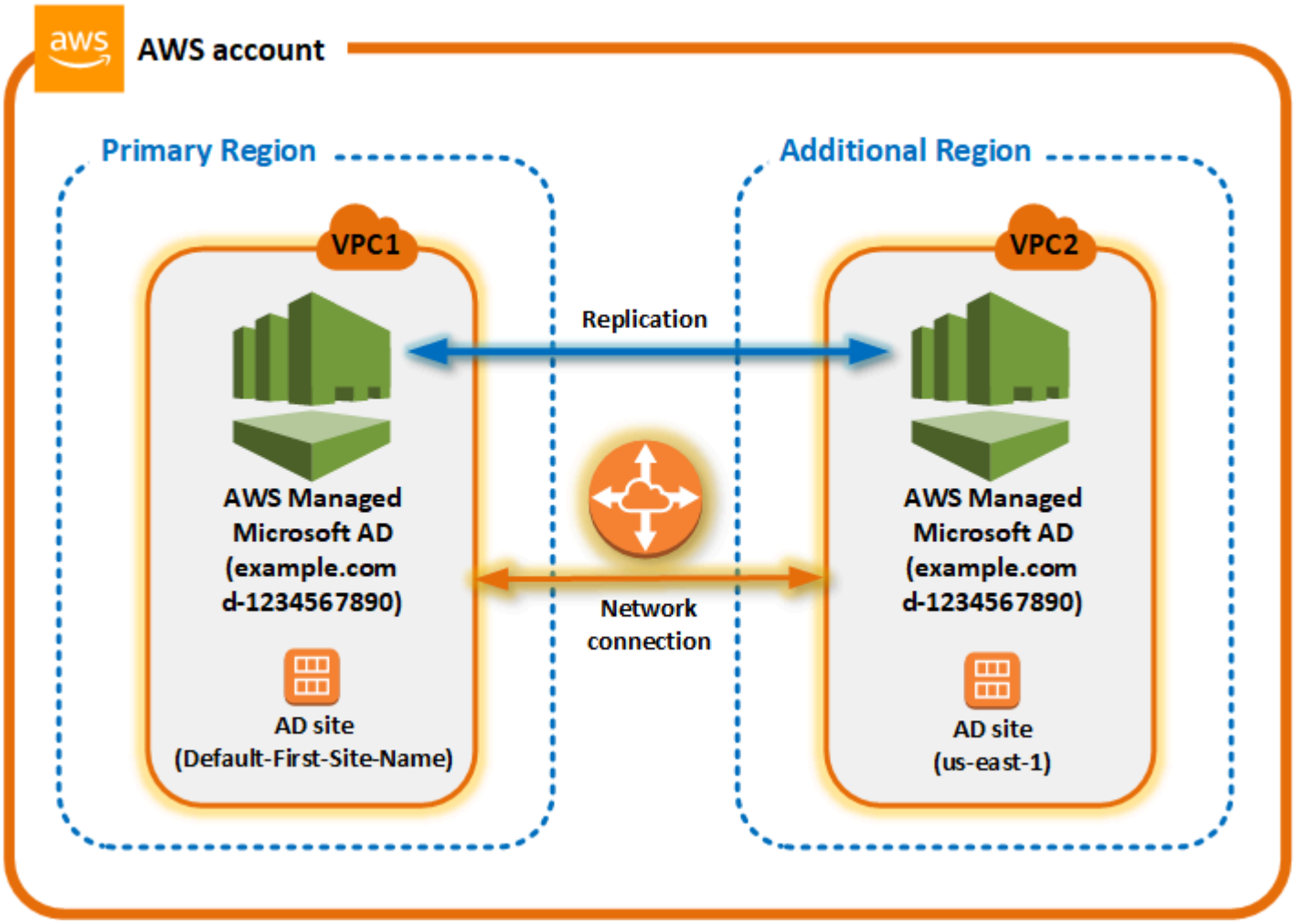
Toutes les modifications que vous apportez aux Caractéristiques régionales alors qu'une région supplémentaire est sélectionnée ne seront appliquées qu'à cette région.

Fonctionnement de la réplication multi-régions

Grâce à la fonctionnalité de réplication multirégionale, AWS Managed Microsoft AD élimine le fardeau indifférencié lié à la gestion d'une infrastructure Active Directory mondiale. Une fois configuré, il AWS réplique toutes les données de l'annuaire des clients, y compris les utilisateurs, les groupes, les politiques de groupe et le schéma dans plusieurs AWS régions.

Une fois qu'une nouvelle région a été ajoutée, les opérations suivantes se produisent automatiquement, comme indiqué dans l'illustration :

- AWS Managed Microsoft AD crée deux contrôleurs de domaine dans le VPC sélectionné et les déploie dans la nouvelle région avec le même compte. AWS L'identifiant de votre annuaire (`directory_id`) reste le même dans toutes les régions. Vous pouvez ajouter d'autres contrôleurs de domaine ultérieurement si vous le souhaitez.
- AWS Managed Microsoft AD configure la connexion réseau entre la région principale et la nouvelle région.
- AWS Managed Microsoft AD crée un nouveau site Active Directory et lui donne le même nom que la région, tel que us-east-1. Vous pouvez également le renommer ultérieurement à l'aide de l'outil Active Directory Sites and Services.
- AWS Managed Microsoft AD réplique tous les objets et configurations Active Directory dans la nouvelle région, y compris les utilisateurs, les groupes, les politiques de groupe, les approbations Active Directory, les unités organisationnelles et le schéma Active Directory. Les liens de sites Active Directory sont configurés pour utiliser Change Notification (Notification de modification). Lorsque la notification des modifications entre sites est activée, les modifications sont propagées vers le site distant à la même fréquence qu'au sein du site source, y compris les modifications qui nécessitent une réplication urgente.
- S'il s'agit de la première région que vous ajoutez, AWS Managed Microsoft AD rend toutes les fonctionnalités compatibles avec plusieurs régions. Pour de plus amples informations, veuillez consulter Caractéristiques mondiales et régionales.



Sites Active Directory

La réplication multirégionale prend en charge plusieurs sites Active Directory (un site Active Directory par région). Lorsqu'une nouvelle région est ajoutée, elle reçoit le même nom que la région, par exemple, us-east-1. Vous pouvez également le renommer ultérieurement à l'aide de Active Directory Sites and Services.

AWS services

AWS des services tels qu'Amazon RDS for SQL Server et Amazon FSx se connectent aux instances locales de l'annuaire global. Cela permet à vos utilisateurs de se connecter une seule fois aux applications compatibles avec Active Directory qui s'exécutent, AWS ainsi qu'à des AWS services tels qu'Amazon RDS for SQL Server dans n'importe quelle région. AWS Pour ce faire, les utilisateurs ont besoin d'informations d'identification provenant de AWS Managed Microsoft AD ou d'Active Directory local lorsque vous avez confiance en votre AWS Managed Microsoft AD.

Vous pouvez utiliser les AWS services suivants avec la fonctionnalité de réplication multirégionale.

- Amazon EC2
- FSx for Windows File Server
- Amazon RDS for SQL Server
- Amazon RDS for Oracle
- Amazon RDS for MySQL
- Amazon RDS for PostgreSQL
- Amazon RDS for MariaDB
- Amazon Aurora for MySQL
- Amazon Aurora for PostgreSQL

Basculement

Si tous les contrôleurs de domaine d'une région sont en panne, AWS Managed Microsoft AD récupère les contrôleurs de domaine et réplique automatiquement les données de l'annuaire. Pendant ce temps, les contrôleurs de domaine des autres régions restent opérationnels.

Ajouter une région répliquée

Lorsque vous ajoutez une région à l'aide de Réplication multi-régions cette fonctionnalité, AWS Managed Microsoft AD crée deux contrôleurs de domaine dans la AWS région sélectionnée, Amazon Virtual Private Cloud (VPC) et le sous-réseau. AWS Managed Microsoft AD crée également les groupes de sécurité associés qui permettent aux charges de travail Windows de se connecter à votre annuaire dans la nouvelle région. Il crée également ces ressources en utilisant le même AWS compte sur lequel votre répertoire est déjà déployé. Pour ce faire, choisissez la région, spécifiez le VPC et fournissez les configurations pour la nouvelle région.

La réplication multirégionale n'est prise en charge que pour l'édition Enterprise de AWS Managed Microsoft AD.

Prérequis

Avant de poursuivre les étapes d'ajout d'une nouvelle région de réplication, nous vous recommandons de consulter d'abord les tâches préalables suivantes.

- Vérifiez que vous disposez des autorisations AWS Identity and Access Management (IAM) nécessaires, de la configuration Amazon VPC et de la configuration du sous-réseau dans la nouvelle région vers laquelle vous souhaitez répliquer le répertoire.
- Si vous souhaitez utiliser vos informations d'identification Active Directory locales existantes pour accéder aux charges de travail compatibles avec Active Directory et les gérer AWS, vous devez créer une relation de confiance Active Directory entre Managed AWS Microsoft AD et votre infrastructure AD locale. Pour plus d'informations sur les approbations, veuillez consulter Connectez-vous à votre infrastructure Active Directory existante.
- Si vous avez déjà établi une relation de confiance entre votre instance Active Directory locale et que vous souhaitez ajouter une région répliquée, vous devez vérifier que vous disposez de la configuration de sous-réseau et de VPC Amazon nécessaire dans la nouvelle région vers laquelle vous souhaitez répliquer l'annuaire.

Ajouter une région

Utilisez la procédure suivante pour ajouter une région répliquée à votre répertoire Microsoft AD AWS géré.

Pour ajouter une région répliquée

1. Dans le panneau de navigation de la consoleAWS Directory Service, choisissez Annuaires.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sous Multi-Region replication (Réplication multi-régions), choisissez la région principale dans la liste, puis choisissez Add Region (Ajouter une région).

   > **Note**
   >
   > Vous ne pouvez ajouter des régions que lorsque la région principale est sélectionnée. Pour de plus amples informations, veuillez consulter Région principale.

4. Sur la page Add Region (Ajouter une région), sous Region, choisissez la région que vous souhaitez ajouter dans la liste.
5. Sous VPC, sélectionnez le VPC à utiliser pour cette région.

> **Note**
>
> Ce VPC ne doit pas avoir de routage inter-domaines sans classe (CIDR) qui est identique à celui d'un VPC utilisé par cet annuaire dans une autre région.

6. Sous Subnets (Sous-réseaux), sélectionnez le sous-réseau à utiliser pour cette région.
7. Passez en revue les informations sous Pricing (Tarification), puis choisissez Add (Ajouter).
8. Lorsque AWS Managed Microsoft AD termine le processus de déploiement du contrôleur de domaine, la région affiche le statut Actif. Vous pouvez désormais apporter des mises à jour à cette région selon vos besoins.

Étapes suivantes

Une fois que vous avez ajouté votre nouvelle région, vous devez envisager les étapes suivantes :

- Déployez des contrôleurs de domaine supplémentaires (jusqu'à 20) dans votre nouvelle région selon vos besoins. Le nombre de contrôleurs de domaine lorsque vous ajoutez une nouvelle région est de 2 par défaut, qui est le minimum requis pour des raisons de tolérance aux pannes et de haute disponibilité. Pour de plus amples informations, veuillez consulter Ajout ou suppression de contrôleurs de domaine supplémentaires.
- Partagez votre annuaire avec un plus grand nombre de AWS comptes par région. Les configurations de partage d'annuaires ne sont pas répliquées automatiquement depuis la région principale. Pour de plus amples informations, veuillez consulter Partagez votre annuaire.
- Activez le transfert de journaux pour récupérer les journaux de sécurité de votre annuaire à l'aide d'Amazon CloudWatch Logs depuis la nouvelle région. Lorsque vous activez le transfert de journaux, vous devez fournir un nom de groupe de journaux dans chaque région dans laquelle vous avez répliqué votre annuaire. Pour de plus amples informations, veuillez consulter Activer le transfert de journaux.
- Activez Amazon Simple Notification Service (Amazon SNS) pour la nouvelle région afin de suivre l'état d'intégrité de votre annuaire par région. Pour de plus amples informations, veuillez consulter Configurer les notifications d'état de l'annuaire avec Amazon SNS.

Supprimer une région répliquée

Utilisez la procédure suivante pour supprimer une région pour votre répertoire Microsoft AD AWS géré. Avant de supprimer une région, assurez-vous qu'elle ne possède aucun des éléments suivants :

- Applications autorisées qui y sont associées.
- Annuaires partagés qui lui sont associés.

Pour supprimer une région répliquée

1. Dans le panneau de navigation de la consoleAWS Directory Service, choisissez Annuaires.
2. Dans la barre de navigation, sélectionnez le sélecteur Regions (Régions), puis sélectionnez la région où votre annuaire est stocké.
3. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
4. Sur la page Directory details (Détails de l'annuaire), sous Multi-Region replication (Réplication multi-régions), choisissez Delete Region (Supprimer la région).
5. Dans la boîte de dialogue Delete Region (Supprimer la région), passez en revue les informations, puis saisissez le nom de la région pour confirmer. Ensuite, choisissez Supprimer.

> **Note**
>
> Vous ne pouvez pas mettre à jour la région pendant sa suppression.

Partagez votre annuaire

AWS Managed Microsoft AD s'intègre étroitement avec AWS Organizations pour autoriser un partage d'annuaire transparent entre différents comptes AWS. Vous pouvez partager un seul annuaire avec d'autres comptes AWS approuvés au sein de la même organisation ou partager l'annuaire avec d'autres comptes AWS en dehors de votre organisation. Vous pouvez également partager votre annuaire lorsque votre compte AWS n'est pas membre d'une organisation.

> **Note**
>
> AWS facture des frais supplémentaires pour le partage d'annuaire. Pour en savoir plus, consultez la page Tarification du site Web AWS Directory Service.

Le partage d'annuaire fait de AWS Managed Microsoft AD une méthode plus économique d'intégration avec Amazon EC2 dans différents comptes et VPC. Le partage d'annuaire est disponible dans toutes les régions AWS proposant AWS Managed Microsoft AD.

> **Note**
>
> Dans la région AWS Chine (Ningxia), cette fonctionnalité est uniquement disponible en cas d'utilisation de AWS Systems Manager (SSM) pour joindre vos instances Amazon EC2 de façon transparente.

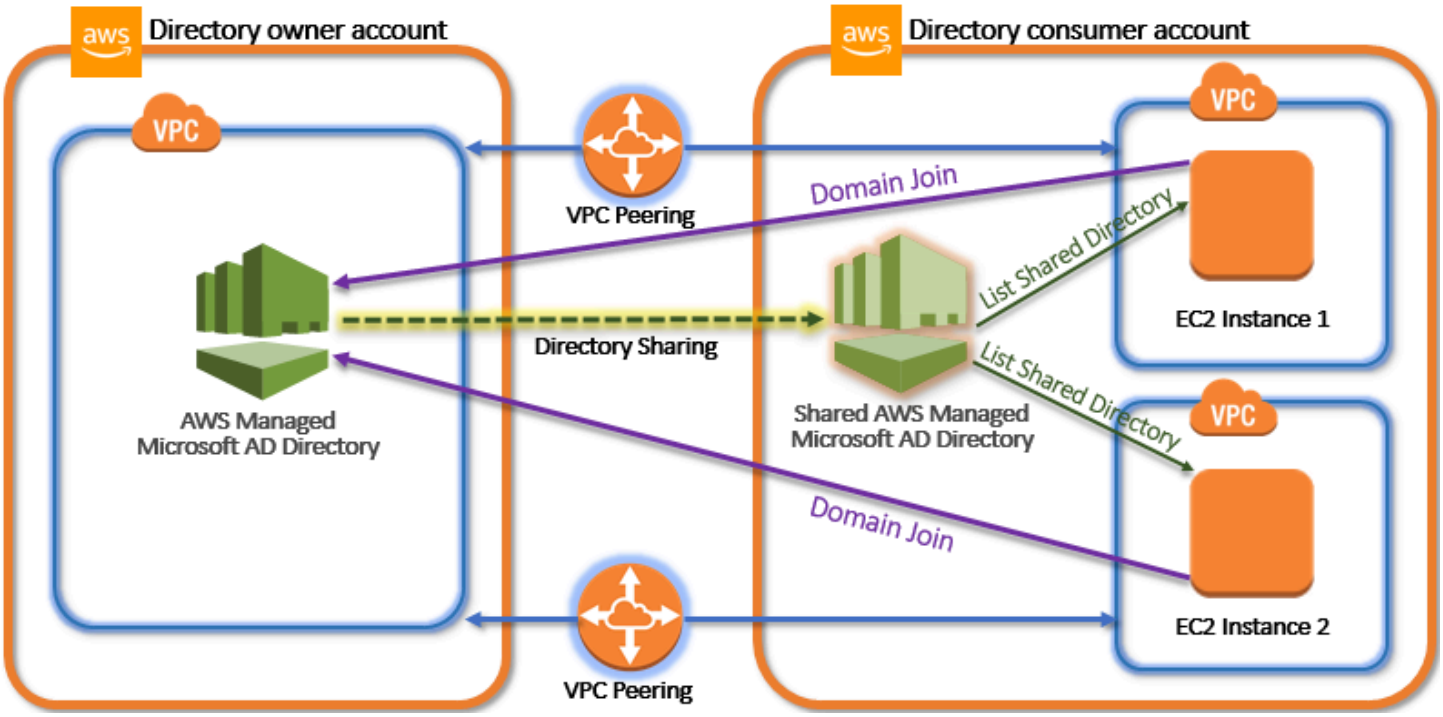
Pour plus d'informations sur le partage d'annuaire et pour savoir comment étendre la portée de votre annuaire AWS Managed Microsoft AD au-delà des limites du compte AWS, consultez les rubriques suivantes.

Rubriques

- Concepts clés du partage d'annuaire
- Tutoriel : Partage de votre répertoire Microsoft AD AWS géré pour une jonction de domaine EC2 fluide
- Annulation du partage de l'annuaire

Concepts clés du partage d'annuaire

Vous tirerez le meilleur parti de la fonction de partage d'annuaire en vous familiarisant avec les concepts clés suivants.



Compte propriétaire de l'annuaire

Le propriétaire de l'annuaire est le titulaire du Compte AWS qui possède l'annuaire d'origine dans la relation d'annuaire partagé. Un administrateur de ce compte initie le flux de partage d'annuaire en spécifiant avec quels Comptes AWS leur annuaire doit être partagé. Les propriétaires d'annuaires peuvent voir avec qui ils ont partagé un annuaire depuis l'onglet Mettre à l'échelle et partager pour un annuaire donné dans la console AWS Directory Service.

Compte consommateur de l'annuaire

Dans une relation d'annuaire partagé, le consommateur de l'annuaire représente le Compte AWS avec lequel le propriétaire de l'annuaire a partagé l'annuaire. En fonction de la méthode de partage utilisée, un administrateur de ce compte peut avoir besoin d'accepter une invitation envoyée depuis le propriétaire de l'annuaire avant de pouvoir commencer à utiliser l'annuaire partagé.

Le processus de partage d'annuaire crée un annuaire partagé dans le compte consommateur de l'annuaire. Cet annuaire partagé contient les métadonnées qui permettent de joindre l'instance EC2 de façon transparente au domaine, ce qui place l'annuaire d'origine dans le compte propriétaire de l'annuaire. Chaque annuaire partagé dans le compte consommateur de l'annuaire possède un identifiant unique (ID de l'annuaire partagé).

Méthodes de partage

AWS Managed Microsoft AD fournit deux méthodes de partage d'annuaire :

- AWS Organizations : cette méthode simplifie le partage de l'annuaire au sein de votre organisation. En effet, elle vous permet de parcourir et de confirmer les comptes consommateurs de l'annuaire. Pour utiliser cette option, votre organisation doit avoir Toutes les fonctions activées et votre annuaire doit être situé dans le compte de gestion de l'organisation. Cette méthode de partage simplifie votre configuration, car elle n'oblige pas les comptes consommateurs de l'annuaire à accepter votre invitation de partage d'annuaire. Dans la console, cette méthode est appelée Partager cet annuaire avec les Comptes AWS de votre organisation.
- Handshake (Poignée de main) : cette méthode permet le partage d'annuaire lorsque vous n'utilisez pas AWS Organizations. Cette méthode de la « poignée de main » oblige le compte consommateur de l'annuaire à accepter la demande de partage d'annuaire. Dans la console, cette méthode est appelée Partager cet annuaire avec d'autres Comptes AWS.

La connectivité réseau

La connectivité réseau est une condition préalable à la création d'une relation de partage d'annuaire entre les Comptes AWS. AWS prend en charge de nombreuses solutions pour connecter vos VPC, notamment l'appairage de VPC, Transit Gateway, et VPN. Consultez Tutoriel : Partage de votre répertoire Microsoft AD AWS géré pour une jonction de domaine EC2 fluide pour démarrer.

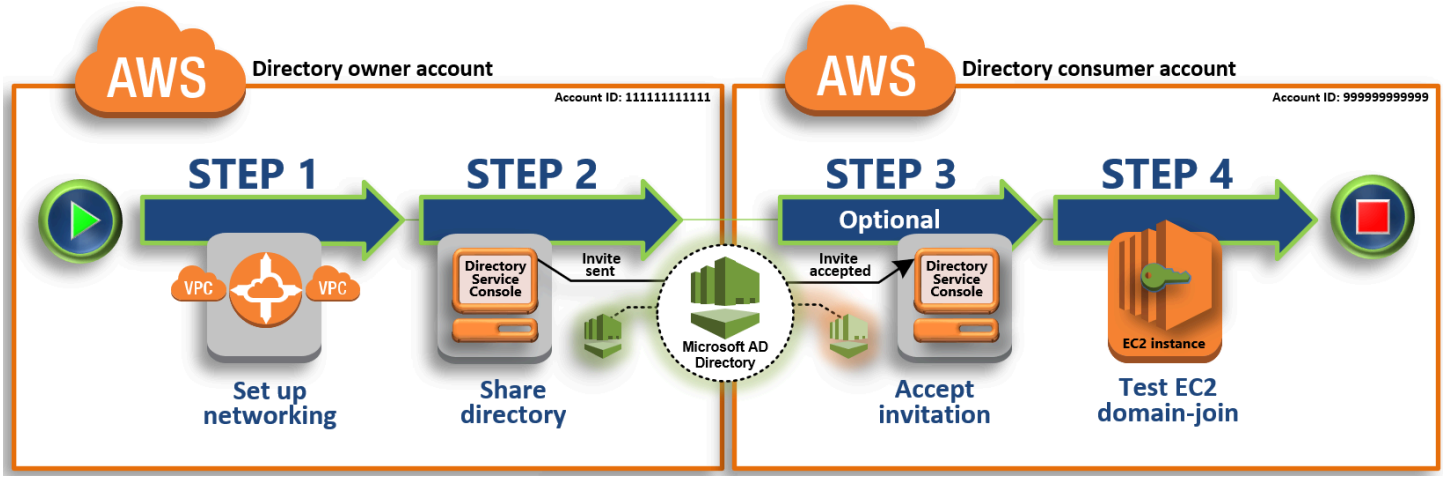
Tutoriel : Partage de votre répertoire Microsoft AD AWS géré pour une jonction de domaine EC2 fluide

Ce didacticiel explique comment partager votre annuaire Microsoft AD AWS géré (le compte du propriétaire du répertoire) avec un autre Compte AWS (le compte client de l'annuaire). Une fois que les conditions préalables à la mise en réseau sont remplies, vous partagerez un répertoire entre deux Comptes AWS. Ensuite, vous apprendrez à joindre en toute transparence une instance EC2 à un domaine dans le compte consommateur de l'annuaire.

Nous vous recommandons d'examiner les concepts clés du partage d'annuaire et le contenu des cas d'utilisation avant de commencer à travailler avec ce didacticiel. Pour plus d'informations, consultez Concepts clés du partage d'annuaire.

Le processus de partage de votre annuaire varie selon que vous le partagez avec un autre Compte AWS membre de la même AWS organisation ou avec un compte externe à l' AWS organisation. Pour plus d'informations sur le partage, veuillez consulter Méthodes de partage.

Ce flux de travail se compose de quatre étapes de base.



[Étape 1 : configurez votre environnement de mise en réseau]

Dans le compte propriétaire de l'annuaire, vous configurez tous les prérequis de mise en réseau nécessaires pour le processus de partage d'annuaire.

[Étape 2 : partagez votre annuaire]

Une fois connecté avec les informations d'identification d'administrateur propriétaire de l'annuaire, vous ouvrez la console AWS Directory Service et démarrez le flux de partage d'annuaire. Celui-ci envoie une invitation au compte consommateur de l'annuaire.

[Étape 3 : Accepter l'invitation à un répertoire partagé - Facultatif]

Lorsque vous êtes connecté avec les informations d'identification de l'administrateur utilisateur de l'annuaire, vous ouvrez la AWS Directory Service console et acceptez l'invitation de partage d'annuaire.

[Étape 4 : testez de manière transparente l'action de jointure d'une instance EC2 pour Windows Server à un domaine]

Enfin, en tant qu'administrateur consommateur de l'annuaire, vous tentez de joindre une instance EC2 à votre domaine et vérifiez si cela fonctionne.

Ressources supplémentaires

- [Cas d'utilisation : partagez votre annuaire pour joindre des instances Amazon EC2 en toute transparence à un domaine sur Comptes AWS]

- AWS Article de blog sur la sécurité : Comment joindre des instances Amazon EC2 provenant de plusieurs comptes et VPC à un seul annuaire AWS Microsoft AD géré

Étape 1 : configurez votre environnement de mise en réseau

Avant d'exécuter les procédures fournies dans ce didacticiel, vous devez commencer par effectuer les opérations suivantes :

- Créez-en deux nouveaux Comptes AWS à des fins de test dans la même région. Lorsque vous créez un Compte AWS, il crée automatiquement un cloud privé virtuel (VPC) dédié dans chaque compte. Prenez note de l'ID du VPC dans chaque compte. Vous en aurez besoin ultérieurement.
- Créez une connexion d'appairage de VPC entre les deux VPC dans chaque compte en procédant comme décrit dans cette étape.

> **Note**
>
> Bien qu'il existe plusieurs façons de connecter des VPC de comptes de propriétaire d'annuaire et de comptes de consommateur, ce didacticiel utilisera la méthode d'appairage de VPC. Pour plus d'options d'appairage de VPC, reportez-vous à la section La connectivité réseau.

Configurez une connexion d'appairage de VPC entre le compte propriétaire de l'annuaire et le compte consommateur de l'annuaire

La connexion d'appairage de VPC que vous créez est établie entre les VPC du consommateur de l'annuaire et du propriétaire de l'annuaire. Procédez comme suit pour configurer une connexion d'appairage de VPC pour accéder au compte consommateur de l'annuaire. Cette connexion vous permet d'acheminer le trafic entre les deux VPC au moyen d'adresses IP privées.

Pour créer une connexion d'appairage de VPC entre le compte propriétaire de l'annuaire et le compte consommateur de l'annuaire

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/. Assurez-vous de vous connecter en tant qu'administrateur au compte propriétaire de l'annuaire.
2. Dans le volet de navigation, choisissez Peering Connections (Connexions d'appairage). Ensuite, choisissez Créer une connexion d'appairage.
3. Configurez les informations suivantes :

- Balise de nom de connexion d'appairage : Choisissez un nom qui identifie clairement cette connexion avec le VPC du compte consommateur de l'annuaire.
- VPC (Demandeur) : Sélectionnez l'ID de VPC correspondant au compte propriétaire de l'annuaire.
- Dans Sélectionner un autre VPC auquel s'appairer, assurez-vous que les options Mon compte et Cette région sont sélectionnées.
- VPC (Accepteur) : Sélectionnez l'ID de VPC correspondant au compte consommateur de l'annuaire.

4. Choisissez Créer une connexion d'appairage. Dans la boîte de dialogue de confirmation, choisissez OK.

Étant donné que les deux VPC se trouvent dans la même région, l'administrateur du compte propriétaire de l'annuaire qui a envoyé la demande d'appairage de VPC peut également accepter la demande d'appairage au nom du compte consommateur de l'annuaire.

Pour accepter la demande d'appairage au nom du compte consommateur de l'annuaire

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Peering Connections.
3. Sélectionnez la connexion d'appairage de VPC en attente. (Son statut est En attente d'acceptation.) Choisissez Actions, Accepter la demande.
4. Dans la boîte de dialogue de confirmation, choisissez Yes, Accept (Oui, accepter). Dans la boîte de dialogue de confirmation qui suit, choisissez Modifier mes tables de routage maintenant pour accéder directement à la page des tables de routage.

Maintenant que votre connexion d'appairage de VPC est active, vous devez ajouter une entrée dans la table de routage de votre VPC dans le compte propriétaire de l'annuaire. Ceci permet d'acheminer le trafic vers le VPC du compte consommateur de l'annuaire.

Pour ajouter une entrée dans la table de routage du VPC dans le compte propriétaire de l'annuaire

1. Dans la section Tables de routage de la console Amazon VPC, sélectionnez la table de routage correspondant au VPC propriétaire de l'annuaire.
2. Choisissez l'onglet Routes, choisissez Modifier les routes, puis Ajouter une route.

3. Dans la colonne Destination, saisissez le bloc d'adresse CIDR pour le VPC consommateur de l'annuaire.
4. Dans la colonne Cible, saisissez l'ID de la connexion d'appairage de VPC (par exemple, **pcx-123456789abcde000**) correspondant à la connexion d'appairage que vous avez créée précédemment dans le compte propriétaire de l'annuaire.
5. Sélectionnez Enregistrer les modifications.

Pour ajouter une entrée dans la table de routage du VPC dans le compte consommateur de l'annuaire

1. Dans la section Tables de routage de la console Amazon VPC, sélectionnez la table de routage correspondant au VPC consommateur de l'annuaire.
2. Choisissez l'onglet Routes, choisissez Modifier les routes, puis Ajouter une route.
3. Dans la colonne Destination, saisissez le bloc d'adresse CIDR pour le VPC propriétaire de l'annuaire.
4. Dans la colonne Cible, saisissez l'ID de la connexion d'appairage de VPC (par exemple, **pcx-123456789abcde001**) correspondant à la connexion d'appairage que vous avez créée précédemment dans le compte consommateur de l'annuaire.
5. Sélectionnez Enregistrer les modifications.

Assurez-vous de configurer le groupe de sécurité de vos VPC consommateurs de l'annuaire afin d'autoriser le trafic sortant. Pour cela, ajoutez les protocoles Active Directory et les ports dans la table de règles sortantes. Pour plus d'informations, veuillez consulter Security groups for your VPC et AWS Managed Microsoft AD prerequisites (français non garanti).

Étape suivante

Étape 2 : partagez votre annuaire

Étape 2 : partagez votre annuaire

Utilisez les procédures suivantes pour commencer le flux de partage d'annuaire depuis le compte propriétaire de l'annuaire.

> **Note**
>
> Le partage d'annuaires est une fonctionnalité régionale de AWS Managed Microsoft AD. Si vous utilisez Réplication multi-régions, les procédures suivantes doivent être appliquées séparément dans chaque région. Pour plus d'informations, consultez Caractéristiques mondiales et régionales.

Pour partager votre annuaire depuis le compte propriétaire de l'annuaire

1. Connectez-vous au compte du propriétaire du répertoire à l' AWS Management Console aide des informations d'identification d'administrateur et ouvrez la AWS Directory Service console à l'adresse https://console.aws.amazon.com/directoryservicev2/.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
3. Choisissez l'ID de répertoire du répertoire Microsoft AD AWS géré que vous souhaitez partager.
4. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :
   - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région dans laquelle vous souhaitez partager votre annuaire, puis cliquez sur l'onglet Mettre à l'échelle et partager. Pour plus d'informations, consultez Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Mettre à l'échelle et partager.
5. Dans la section Annuaires partagés, choisissez Actions, puis Créer un nouvel annuaire partagé.
6. Sur la page Choisissez avec qui Comptes AWS partager, choisissez l'une des méthodes de partage suivantes en fonction des besoins de votre entreprise :
   a. Partager ce répertoire avec les Comptes AWS membres de votre organisation : avec cette option, vous pouvez sélectionner le répertoire avec lequel Comptes AWS vous souhaitez partager votre répertoire dans une liste répertoriant tous les éléments Comptes AWS internes de votre AWS organisation. Vous devez activer l'accès sécurisé avec AWS Directory Service avant de partager un annuaire. Pour plus d'informations, veuillez consulter How to enable or disable trusted access (français non garanti).

> **Note**
>
> Pour utiliser cette option, votre organisation doit avoir Toutes les fonctions activées et votre annuaire doit être situé dans le compte de gestion de l'organisation.

i. Comptes AWS Dans votre organisation, sélectionnez le répertoire avec Comptes AWS lequel vous souhaitez partager le répertoire et cliquez sur Ajouter.

ii. Passez en revue les informations de tarification, puis choisissez Partager.

iii. Passez à l'étape 4 de ce guide. Comme tous Comptes AWS font partie de la même organisation, il n'est pas nécessaire de suivre l'étape 3.

b. Partager ce répertoire avec d'autres Comptes AWS personnes : avec cette option, vous pouvez partager un répertoire avec des comptes internes ou externes à votre AWS organisation. Vous pouvez également utiliser cette option lorsque votre annuaire n'est pas membre d'une AWS organisation et que vous souhaitez le partager avec une autre Compte AWS.

i. Dans ID Compte AWS , saisissez tous les ID Compte AWS avec lesquels vous souhaitez partager l'annuaire, puis cliquez sur Ajouter.

ii. Dans Envoyer un message, saisissez un message à l'attention de l'administrateur de l'autre Compte AWS.

iii. Passez en revue les informations de tarification, puis choisissez Partager.

iv. Passez à l'étape 3.

Étape suivante

Étape 3 : Accepter l'invitation à un répertoire partagé - Facultatif

Étape 3 : Accepter l'invitation à un répertoire partagé - Facultatif

Si vous avez choisi l'option Partager cet annuaire avec d'autres Comptes AWS (méthode de l'établissement de liaison) dans la procédure précédente, procédez comme suit pour terminer le flux de partage d'annuaire. Si vous avez choisi l'option Partager ce répertoire avec Comptes AWS les membres de votre organisation, ignorez cette étape et passez à l'étape 4.

Pour accepter l'invitation de partage d'annuaire

1. Connectez-vous au compte consommateur du répertoire à l' AWS Management Console aide des informations d'identification d'administrateur et ouvrez la AWS Directory Service console à l'adresse https://console.aws.amazon.com/directoryservicev2/.
2. Dans le volet de navigation, choisissez Annuaires partagés avec moi.
3. Dans la colonne ID de l'annuaire partagé, choisissez l'ID de l'annuaire qui affiche l'état En attente d'acceptation.
4. Dans la page Détails de l'annuaire partagé, choisissez Vérifier.
5. Dans la boîte de dialogue Invitation en attente pour l'annuaire partagé, passez en revue le message, les détails sur le propriétaire de l'annuaire et les informations de tarification. Si vous êtes d'accord, choisissez Accepter pour commencer à utiliser l'annuaire.

Étape suivante

Étape 4 : testez de manière transparente l'action de jointure d'une instance EC2 pour Windows Server à un domaine

Étape 4 : testez de manière transparente l'action de jointure d'une instance EC2 pour Windows Server à un domaine

Vous pouvez utiliser l'une des deux méthodes suivantes pour tester une jonction totalement transparente d'une instance EC2 à un domaine.

Méthode 1 : test de la jonction de domaine à l'aide de la console Amazon EC2

Effectuez ces étapes dans le compte consommateur de l'annuaire.

1. Connectez-vous à la console Amazon EC2 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation, choisissez le même répertoire Région AWS que le répertoire existant.
3. Sur le EC2 Dashboard (tableau de bord EC2), dans la section Launch instance (Lancer une instance), choisissez Launch instance (Lancer une instance).
4. Sur la page Launch an instance (Lancer une instance), dans la section Name and Tags (Nom et balises), saisissez le nom que vous souhaitez utiliser pour votre instance Windows EC2.

5. (Facultatif) Sélectionnez Add additional tags (Ajouter des balises supplémentaires) pour ajouter une ou plusieurs paires clé-valeur d'identification afin d'organiser, de suivre ou de contrôler l'accès pour cette instance EC2.
6. Dans la section Application and OS Image (Amazon Machine Image) [Image de l'application et du système d'exploitation (Amazon Machine Image)], sélectionnez Windows dans le volet Quick Start (Démarrage rapide). Vous pouvez modifier Windows Amazon Machine Image (AMI) dans la liste déroulante Amazon Machine Image (AMI).
7. Dans la section Type d'instance, choisissez le type d'instance que vous souhaitez utiliser dans la liste déroulante Type d'instance.
8. Dans la section Paire de clés (connexion), vous pouvez choisir de créer une nouvelle paire de clés ou choisir une paire de clés existante.

   a. Pour créer une nouvelle paire de clés, choisissez Créer une paire de clés.

   b. Entrez le nom de la paire de clés et sélectionnez une option pour le type de paire de clés et le format de fichier de clé privée.

   c. 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.

   d. Choisissez Créer une paire de clés.

   e. Le fichier de clé privée est automatiquement téléchargé dans votre navigateur. Enregistrez le fichier de clé privée en lieu sûr.

   > ⚠ Important
   >
   > C'est votre seule occasion d'enregistrer le fichier de clé privée.

9. Sur la page Lancer une instance, dans la section Paramètres réseau, choisissez Modifier. Choisissez le VPC dans lequel votre répertoire a été créé dans la liste déroulante VPC obligatoire.
10. Choisissez l'un des sous-réseaux publics de votre VPC dans la liste déroulante Sous-réseau. Tout le trafic externe du sous-réseau que vous choisissez doit être acheminé vers une passerelle Internet. Sinon, vous ne pourrez pas vous connecter à l'instance à distance.

    Pour obtenir plus d'informations sur la manière de se connecter à une passerelle Internet, veuillez consulter la section Connect to the internet using an internet gateway (français non garanti) dans le Guide de l'utilisateur Amazon VPC.

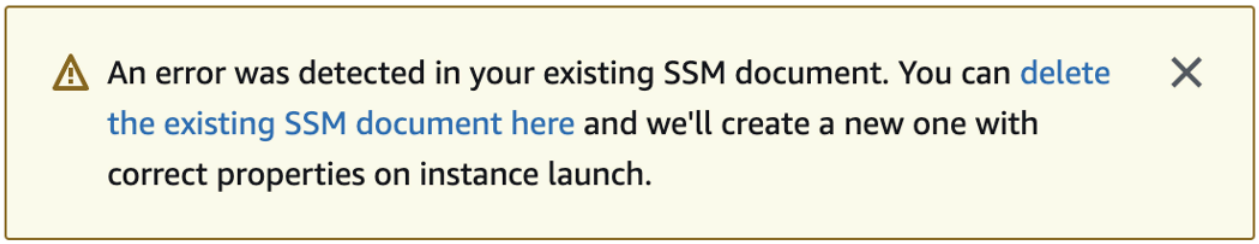
11. Sous Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique), choisissez Enable (Activer).

    Pour plus d'informations sur les adresses IP publiques et privées, veuillez consulter la section Amazon EC2 instance IP addressing (français non garanti) dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.

12. Pour les paramètres Firewall (security groups) [Pare-feu (groupes de sécurité)], vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.

13. Pour les paramètres Configure storage (Configurer le stockage), vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.

14. Choisissez la section Advanced details (Détails avancés), puis sélectionnez votre domaine dans la liste déroulante Domain join directory (Annuaire de jonction de domaines).

    > **Note**
    >
    > Après avoir choisi le répertoire de jointure du domaine, vous pouvez voir :
    >
    > 
    >
    >
    > Cette erreur se produit si l'assistant de lancement EC2 identifie un document SSM existant présentant des propriétés inattendues. Vous pouvez effectuer l'une des actions suivantes :
    >
    > - Si vous avez déjà modifié le document SSM et que les propriétés sont attendues, choisissez Fermer et lancez l'instance EC2 sans aucune modification.
    > - Cliquez sur le lien Supprimer le document SSM existant ici pour supprimer le document SSM. Cela permettra de créer un document SSM avec les propriétés correctes. Le document SSM sera automatiquement créé lorsque vous lancerez l'instance EC2.

15. Pour l'IAM instance profile (profil d'instance IAM), vous pouvez sélectionner un profil d'instance IAM existant ou en créer un nouveau. Sélectionnez un profil d'instance IAM DirectoryServiceAccess auquel sont associées les politiques AWS gérées AmazonSSM ManagedInstanceCore et AmazonSSM dans la liste déroulante des profils d'instance IAM. Pour

en créer un nouveau, choisissez Créer un nouveau lien de profil IAM, puis procédez comme suit :

1. Sélectionnez Créer un rôle.
2. Sous Select trusted entity (Sélectionner une entité approuvée), choisissez service AWS .
3. Sous Use case (Cas d'utilisation), choisissez EC2.
4. Sous Ajouter des autorisations, dans la liste des politiques, sélectionnez les politiques AmazonSSM ManagedInstanceCore et DirectoryServiceAccessAmazonSSM. Pour filtrer la liste, tapez **`SSM`** dans la zone de recherche. Choisissez Suivant.

   > **Note**
   >
   > AmazonSSM DirectoryServiceAccess fournit les autorisations nécessaires pour joindre des instances à une instance Active Directory gérée par. AWS Directory ServiceAmazonSSM ManagedInstanceCore fournit les autorisations minimales nécessaires pour utiliser le AWS Systems Manager service. Pour plus d'informations sur la création d'un rôle doté de ces autorisations, ainsi que sur les autres autorisations et politiques que vous pouvez attribuer à votre rôle IAM, veuillez consulter la section Create an IAM instance profile for Systems Manager (français non garanti) dans le Guide de l'utilisateur AWS Systems Manager .

5. Sur la page Name, review, and create (Nommer, vérifier et créer), saisissez un Role name (Nom du rôle). Vous aurez besoin de ce nom de rôle pour l'attacher à l'instance EC2.
6. (Facultatif) Vous pouvez fournir une description du profil d'instance IAM dans le champ Description.
7. Sélectionnez Créer un rôle.
8. Revenez à la page Launch an instance (Lancer une instance) et choisissez l'icône d'actualisation à côté du profil d'instance IAM. Votre nouveau profil d'instance IAM doit être visible dans la liste déroulante des IAM instance profile (profil d'instance IAM). Choisissez le nouveau profil et laissez le reste de paramètres avec leurs valeurs par défaut.

16. Choisissez Launch instance (Lancer une instance).

Méthode 2 : tester la jointure de domaine en utilisant AWS Systems Manager

Effectuez ces étapes dans le compte consommateur de l'annuaire. Pour effectuer cette procédure, vous aurez besoin de certaines informations sur le compte du propriétaire de l'annuaire, telles que l'ID de l'annuaire, le nom de l'annuaire et les adresses IP DNS.

Prérequis

- Configuration AWS Systems Manager.
  - Pour de plus amples informations sur Systems Manager, veuillez consulter General setup for AWS Systems Manager (français non garanti).
- Les instances auxquelles vous souhaitez rejoindre le domaine Microsoft Active Directory AWS géré doivent être associées à un rôle IAM contenant les politiques gérées par AmazonSSM ManagedInstanceCore et DirectoryServiceAccessAmazonSSM.
  - Pour plus d'informations sur ces stratégies gérées et sur les autres stratégies que vous pouvez attacher à un profil d'instance pour Systems Manager consultez Création d'un profil d'instance IAM pour Systems Manager dans le Guide de l'utilisateur AWS Systems Manager . Pour plus d'informations sur les stratégies gérées, veuillez consulter AWS Managed policies (français non garanti) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur l'utilisation de Systems Manager pour joindre des instances EC2 à un domaine Microsoft Active Directory AWS géré, voir Comment associer une instance EC2 Windows en cours d'exécution à mon domaine AWS Directory Service ? AWS Systems Manager .

1. Ouvrez la AWS Systems Manager console à l'adressehttps://console.aws.amazon.com/systems-manager/.
2. Dans le panneau de navigation, sous Gestion des nœuds, choisissez Exécuter la commande.
3. Sélectionnez Run Command (Exécuter la commande).
4. Sur la page Exécuter la commande, recherchez `AWS-JoinDirectoryServiceDomain`. Lorsqu'elle s'affiche dans les résultats de recherche, sélectionnez l'option `AWS-JoinDirectoryServiceDomain`.
5. Faites défiler jusqu'à la section Paramètres de la commande. Vous devez fournir les paramètres suivants :

> **Note**
>
> Vous pouvez localiser l'ID du répertoire, le nom du répertoire et les adresses IP DNS en revenant à la AWS Directory Service console, en sélectionnant Répertoires partagés avec moi, puis en sélectionnant votre répertoire. L'ID de votre annuaire se trouve dans la section Détails du répertoire partagé. Vous pouvez trouver les valeurs du nom du répertoire et des adresses IP DNS dans la section Détails de l'annuaire propriétaire.

- Pour ID de répertoire, entrez le nom du répertoire Microsoft Active Directory AWS géré.
- Pour Nom de l'annuaire, entrez le nom de l'annuaire AWS Managed Microsoft Active Directory (pour le compte du propriétaire de l'annuaire).
- Pour les adresses IP DNS, entrez les adresses IP des serveurs DNS dans le répertoire Microsoft Active Directory AWS géré (pour le compte du propriétaire de l'annuaire).

6. Pour Cibles, choisissez Choisir les instances manuellement, puis sélectionnez les instances que vous souhaitez joindre au domaine.
7. Pour le reste du formulaire, laissez les valeurs par défaut, faites défiler la page, puis choisissez Exécuter.
8. Le statut de la commande passe de En attente à Réussi une fois que les instances ont joint le domaine avec succès. Vous pouvez afficher le résultat de la commande en sélectionnant l'ID d'instance de l'instance qui a joint le domaine et Afficher le résultat.

Après avoir terminé l'une ou l'autre de ces étapes, vous devriez désormais être en mesure de joindre votre instance EC2 au domaine. Une fois cela fait, vous pouvez vous connecter à votre instance à l'aide d'un client RDP (Remote Desktop Protocol) avec les informations d'identification de votre compte utilisateur Microsoft AD AWS géré.

Annulation du partage de l'annuaire

Utilisez la procédure suivante pour annuler le partage d'un annuaire AWS Managed Microsoft AD.

Pour annuler le partage de votre annuaire

1. Dans le panneau de navigation de la console AWS Directory Service, sous Active Directory, sélectionnez Annuaires.

2. Choisissez l'ID d'annuaire de l'annuaire AWS Managed Microsoft AD dont vous souhaitez annuler le partage.
3. Sur la page Directory details (Détails de l'annuaire), procédez de l'une des manières suivantes :
   - Si plusieurs régions apparaissent sous Multi-Region replication (Réplication multi-régions), sélectionnez la région dans laquelle vous souhaitez annuler le partage de votre annuaire, puis cliquez sur l'onglet Scale & share (Mettre à l'échelle et partager). Pour de plus amples informations, veuillez consulter Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Multi-Region replication (Réplication multi-régions), choisissez l'onglet Mettre à l'échelle et partager.
4. Dans la section Annuaires partagés, sélectionnez l'annuaire partagé dont vous souhaitez annuler le partage, choisissez Actions, puis choisissez Annuler le partage.
5. Dans la boîte de dialogue Annuler le partage de l'annuaire, choisissez Annuler le partage.

Ressources supplémentaires

- Cas d'utilisation : partagez votre annuaire pour joindre des instances Amazon EC2 de façon transparente à un domaine entre plusieurs comptes AWS
- Article du blog sur la sécurité AWS : Comment joindre des instances Amazon EC2 à partir de plusieurs comptes et VPC vers un seul annuaire AWS Managed Microsoft AD
- Regrouper vos instances Amazon RDS DB des différents comptes dans un seul domaine partagé

Joindre une instance Amazon EC2 à votre compte AWS Microsoft AD géré Active Directory

Vous pouvez facilement joindre une instance Amazon EC2 à votre Active Directory domaine lorsque l'instance est lancée. Pour plus d'informations, consultez Associez facilement une instance Windows Amazon EC2 à votre compte AWS Microsoft AD géré Active Directory. Vous pouvez également lancer une instance EC2 et la joindre à un Active Directory domaine directement depuis la AWS Directory Service console avec AWS Systems Manager Automation.

Si vous devez joindre manuellement une instance EC2 à votre Active Directory domaine, vous devez lancer l'instance dans la région et le groupe de sécurité ou le sous-réseau appropriés, puis joindre l'instance au domaine.

Pour pouvoir vous connecter à distance à ces instances, vous devez disposer d'une connectivité IP aux instances depuis le réseau à partir duquel vous vous connectez. Dans la plupart des cas, cela nécessite qu'une passerelle Internet soit attachée à votre VPC et que l'instance possède une adresse IP publique.

Rubriques

- Lancez une instance d'administration d'annuaire dans votre AWS Managed Microsoft AD Active Directory
- Associez facilement une instance Windows Amazon EC2 à votre compte AWS Microsoft AD géré Active Directory
- Joindre manuellement une Windows instance Amazon EC2 à votre Managed AWS Microsoft AD Active Directory
- Joignez facilement une instance Linux Amazon EC2 à votre annuaire AWS Microsoft AD Active Directory géré
- Joindre manuellement une instance Linux Amazon EC2 à votre annuaire AWS Microsoft AD Active Directory géré
- Joindre manuellement une instance Linux Amazon EC2 à votre répertoire AWS Microsoft AD Active Directory géré à l'aide de Winbind
- Joindre manuellement une instance Mac Amazon EC2 à votre annuaire AWS Microsoft AD Active Directory géré
- Délégation des privilèges de jonction d'annuaire pour AWS Managed Microsoft AD
- Création ou modification d'un ensemble d'options DHCP

Lancez une instance d'administration d'annuaire dans votre AWS Managed Microsoft AD Active Directory

Cette procédure lance une Windows instance d'administration d'annuaires Amazon EC2 en AWS Management Console utilisant AWS Systems Manager Automation pour gérer vos annuaires. Vous pouvez également y parvenir en exécutant directement l'automatisation AWS-CreateDS ManagementInstance dans la console AWS Systems Manager Automation.

Prérequis

Pour lancer une instance EC2 d'administration d'annuaire depuis la console, les autorisations suivantes doivent être activées dans votre compte.

- ds:DescribeDirectories
- ec2:AuthorizeSecurityGroupIngress
- ec2:CreateSecurityGroup
- ec2:CreateTags
- ec2:DeleteSecurityGroup
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeKeyPairs
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcs
- ec2:RunInstances
- ec2:TerminateInstances
- iam:AddRoleToInstanceProfile
- iam:AttachRolePolicy
- iam:CreateInstanceProfile
- iam:CreateRole
- iam:DeleteInstanceProfile
- iam:DeleteRole
- iam:DetachRolePolicy
- iam:GetInstanceProfile
- iam:GetRole
- iam:ListAttachedRolePolicies
- iam:ListInstanceProfiles
- iam:ListInstanceProfilesForRole
- iam:PassRole
- iam:RemoveRoleFromInstanceProfile
- iam:TagInstanceProfile
- iam:TagRole
- ssm:CreateDocument
- ssm:DeleteDocument

- `ssm:DescribeInstanceInformation`
- `ssm:GetAutomationExecution`
- `ssm:GetParameters`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:ListDocuments`
- `ssm:SendCommand`
- `ssm:StartAutomationExecution`
- `ssm:GetDocument`

Pour lancer une instance EC2 d'administration d'annuaire dans le AWS Management Console

1. Connectez-vous à la console AWS Directory Service.
2. Sous Active Directory, sélectionnez Directories (Annuaires).
3. Choisissez l'ID du répertoire dans lequel vous souhaitez lancer une instance EC2 d'administration d'annuaire.
4. Sur la page de l'annuaire, dans le coin supérieur droit, sélectionnez Actions.
5. Dans la liste déroulante Actions, choisissez Launch directory administration EC2 instance.
6. Sur la page Launch directory administration EC2 instance (Lancer une instance EC2 d'administration d'annuaire), sous Input parameters (Paramètres d'entrée), renseignez les champs.

    a. (Facultatif) Vous pouvez fournir une paire de clés pour l'instance. Dans la liste déroulante Nom de la paire de clés - facultatif, sélectionnez une paire de clés.

    b. (Facultatif) Choisissez la AWS CLI commande Afficher pour voir un exemple que vous utilisez AWS CLI pour exécuter cette automatisation.
7. Sélectionnez Envoyer.
8. Vous êtes renvoyé à la page d'annuaire. Une barre de progression verte s'affiche en haut de votre écran pour indiquer que vous avez réussi le lancement.

Pour afficher l'instance EC2 d'administration d'annuaires

Si vous n'avez lancé aucune instance EC2 pour un annuaire, un tiret (-) s'affiche sous Directory administration EC2 instance (Instance EC2 d'administration de l'annuaire).

1. Sous Active Directory, choisissez Directories (Annuaires) et sélectionnez l'annuaire que vous souhaitez consulter.
2. Sous Directory details (Détails de l'annuaire), sous Directory administration EC2 instance (Instance EC2 d'administration de l'annuaire), choisissez l'une ou l'ensemble de vos instances à consulter.
3. Lorsque vous choisissez une instance, vous êtes acheminé vers la page Connect to EC2 instance (Se connecter à une instance EC2) pour connecter un poste de travail distant à votre instance.

Associez facilement une instance Windows Amazon EC2 à votre compte AWS Microsoft AD géré Active Directory

Cette procédure permet de joindre facilement une Windows instance Amazon EC2 à votre Managed AWS Microsoft AD. Si vous devez effectuer une jointure fluide entre plusieurs domaines Comptes AWS, consultezTutoriel : Partage de votre répertoire Microsoft AD AWS géré pour une jonction de domaine EC2 fluide. Pour plus d'informations sur Amazon EC2, veuillez consulter What is Amazon EC2? (français non garanti).

Pour rejoindre facilement une instance Amazon EC2 Windows

1. Connectez-vous à la console Amazon EC2 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation, choisissez le même répertoire Région AWS que le répertoire existant.
3. Sur le EC2 Dashboard (tableau de bord EC2), dans la section Launch instance (Lancer une instance), choisissez Launch instance (Lancer une instance).
4. Sur la page Launch an instance (Lancer une instance), dans la section Name and Tags (Nom et balises), saisissez le nom que vous souhaitez utiliser pour votre instance Windows EC2.
5. (Facultatif) Sélectionnez Add additional tags (Ajouter des balises supplémentaires) pour ajouter une ou plusieurs paires clé-valeur d'identification afin d'organiser, de suivre ou de contrôler l'accès pour cette instance EC2.
6. Dans la section Application and OS Image (Amazon Machine Image) [Image de l'application et du système d'exploitation (Amazon Machine Image)], sélectionnez Windows dans le volet Quick Start (Démarrage rapide). Vous pouvez modifier Windows Amazon Machine Image (AMI) dans la liste déroulante Amazon Machine Image (AMI).

7. Dans la section Type d'instance, choisissez le type d'instance que vous souhaitez utiliser dans la liste déroulante Type d'instance.
8. Dans la section Paire de clés (connexion), vous pouvez choisir de créer une nouvelle paire de clés ou choisir une paire de clés existante.

   a. Pour créer une nouvelle paire de clés, choisissez Créer une paire de clés.

   b. Entrez le nom de la paire de clés et sélectionnez une option pour le type de paire de clés et le format de fichier de clé privée.

   c. 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.

   d. Choisissez Créer une paire de clés.

   e. Le fichier de clé privée est automatiquement téléchargé dans votre navigateur. Enregistrez le fichier de clé privée en lieu sûr.

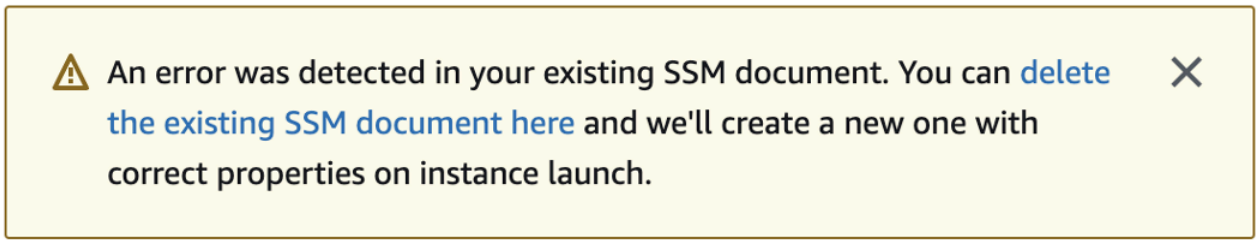
   > ⚠ Important
   >
   > C'est votre seule occasion d'enregistrer le fichier de clé privée.

9. Sur la page Lancer une instance, dans la section Paramètres réseau, choisissez Modifier. Choisissez le VPC dans lequel votre répertoire a été créé dans la liste déroulante VPC obligatoire.
10. Choisissez l'un des sous-réseaux publics de votre VPC dans la liste déroulante Sous-réseau. Tout le trafic externe du sous-réseau que vous choisissez doit être acheminé vers une passerelle Internet. Sinon, vous ne pourrez pas vous connecter à l'instance à distance.

    Pour obtenir plus d'informations sur la manière de se connecter à une passerelle Internet, veuillez consulter la section Connect to the internet using an internet gateway (français non garanti) dans le Guide de l'utilisateur Amazon VPC.
11. Sous Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique), choisissez Enable (Activer).

    Pour plus d'informations sur les adresses IP publiques et privées, veuillez consulter la section Amazon EC2 instance IP addressing (français non garanti) dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.

12. Pour les paramètres Firewall (security groups) [Pare-feu (groupes de sécurité)], vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
13. Pour les paramètres Configure storage (Configurer le stockage), vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
14. Choisissez la section Advanced details (Détails avancés), puis sélectionnez votre domaine dans la liste déroulante Domain join directory (Annuaire de jonction de domaines).

> **Note**
>
> Après avoir choisi le répertoire de jointure du domaine, vous pouvez voir :
>
> 
>
>
> Cette erreur se produit si l'assistant de lancement EC2 identifie un document SSM existant présentant des propriétés inattendues. Vous pouvez effectuer l'une des actions suivantes :
>
> - Si vous avez déjà modifié le document SSM et que les propriétés sont attendues, choisissez Fermer et lancez l'instance EC2 sans aucune modification.
> - Cliquez sur le lien Supprimer le document SSM existant ici pour supprimer le document SSM. Cela permettra de créer un document SSM avec les propriétés correctes. Le document SSM sera automatiquement créé lorsque vous lancerez l'instance EC2.

15. Pour l'IAM instance profile (profil d'instance IAM), vous pouvez sélectionner un profil d'instance IAM existant ou en créer un nouveau. Sélectionnez un profil d'instance IAM DirectoryServiceAccess auquel sont associées les politiques AWS gérées AmazonSSM ManagedInstanceCore et AmazonSSM dans la liste déroulante des profils d'instance IAM. Pour en créer un nouveau, choisissez Créer un nouveau lien de profil IAM, puis procédez comme suit :

    1. Sélectionnez Créer un rôle.
    2. Sous Select trusted entity (Sélectionner une entité approuvée), choisissez service AWS .
    3. Sous Use case (Cas d'utilisation), choisissez EC2.

4. Sous Ajouter des autorisations, dans la liste des politiques, sélectionnez les politiques AmazonSSM ManagedInstanceCore et DirectoryServiceAccessAmazonSSM. Pour filtrer la liste, tapez **SSM** dans la zone de recherche. Choisissez Suivant.

   > **Note**
   >
   > AmazonSSM DirectoryServiceAccess fournit les autorisations nécessaires pour joindre des instances à une instance Active Directory gérée par. AWS Directory ServiceAmazonSSM ManagedInstanceCore fournit les autorisations minimales nécessaires pour utiliser le AWS Systems Manager service. Pour plus d'informations sur la création d'un rôle doté de ces autorisations, ainsi que sur les autres autorisations et politiques que vous pouvez attribuer à votre rôle IAM, veuillez consulter la section Create an IAM instance profile for Systems Manager (français non garanti) dans le Guide de l'utilisateur AWS Systems Manager .

5. Sur la page Name, review, and create (Nommer, vérifier et créer), saisissez un Role name (Nom du rôle). Vous aurez besoin de ce nom de rôle pour l'attacher à l'instance EC2.
6. (Facultatif) Vous pouvez fournir une description du profil d'instance IAM dans le champ Description.
7. Sélectionnez Créer un rôle.
8. Revenez à la page Launch an instance (Lancer une instance) et choisissez l'icône d'actualisation à côté du profil d'instance IAM. Votre nouveau profil d'instance IAM doit être visible dans la liste déroulante des IAM instance profile (profil d'instance IAM). Choisissez le nouveau profil et laissez le reste de paramètres avec leurs valeurs par défaut.

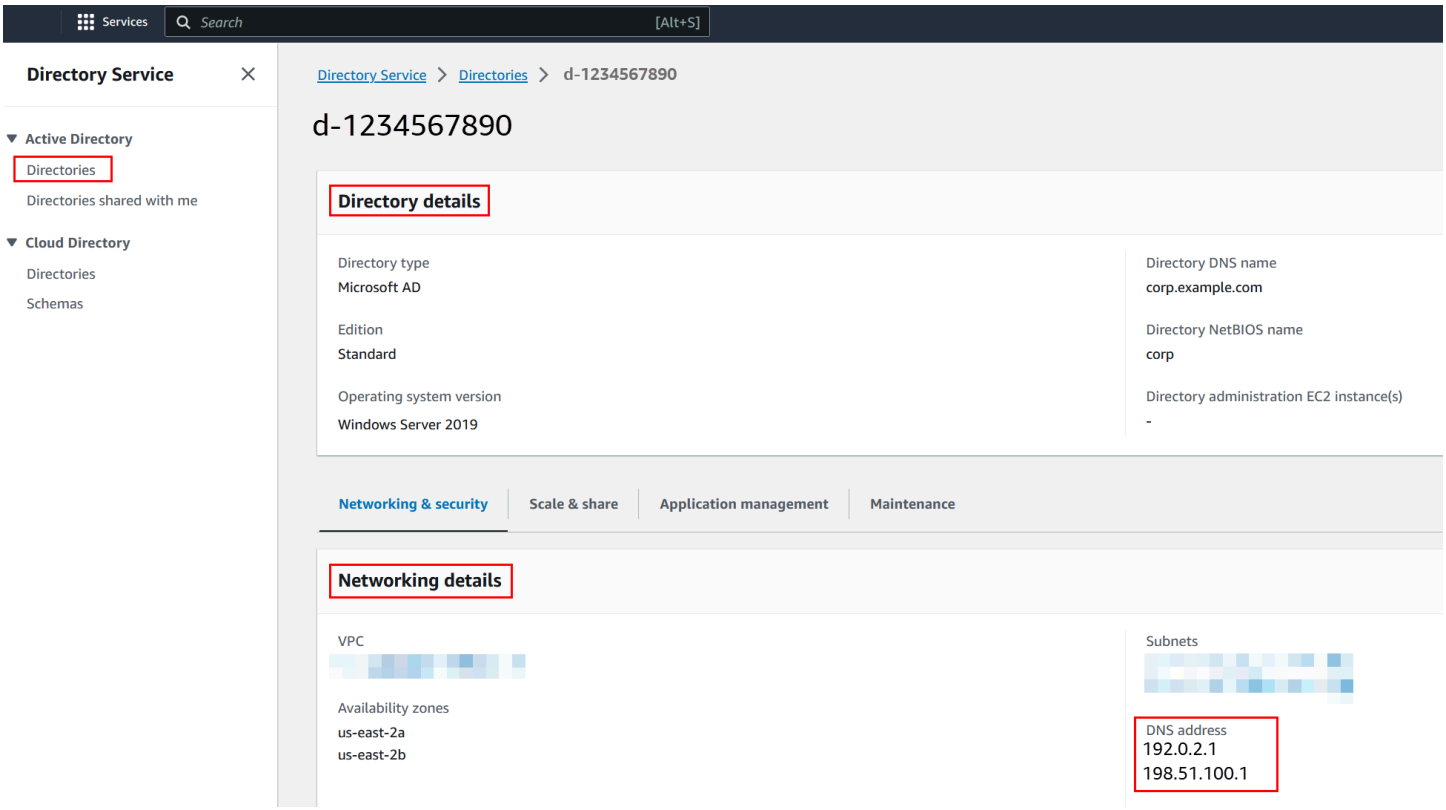
16. Choisissez Launch instance (Lancer une instance).

Joindre manuellement une Windows instance Amazon EC2 à votre Managed AWS Microsoft AD Active Directory

Pour joindre manuellement une Windows instance Amazon EC2 existante à un AWS Microsoft AD géréActive Directory, l'instance doit être lancée à l'aide des paramètres spécifiés dans. Associez facilement une instance Windows Amazon EC2 à votre compte AWS Microsoft AD géré Active Directory

Vous aurez besoin des adresses IP des serveurs DNS Microsoft AD AWS gérés. Ces informations se trouvent sous Directory Services (Services d'annuaire) > Directories (Annuaires) > le lien Directory

ID (ID de l'annuaire) de votre annuaire > Directory details (Détails de l'annuaire) puis les sections Networking & Security Réseau et sécurité.



Pour joindre une instance Windows à un Microsoft AD AWS géré Active Directory

1. Connectez-vous à l'instance à l'aide d'un client RDP (Remote Desktop Protocol).
2. Ouvrez la boîte de dialogue des propriétés TCP/IPv4 sur l'instance.

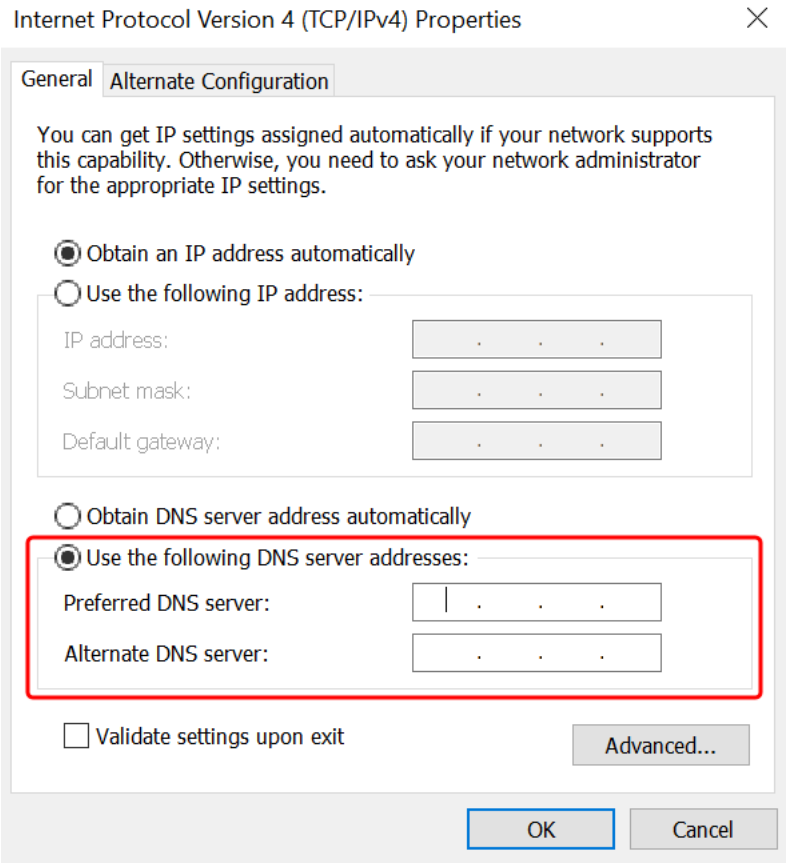
   a. Ouvrez Network Connections (Connexions réseau).

   > **Tip**
   >
   > Vous pouvez ouvrir Network Connections (Connexions réseau) directement en exécutant ce qui suit à partir d'une invite de commande sur l'instance.
   >
   > ```
   > %SystemRoot%\system32\control.exe ncpa.cpl
   > ```

   b. Ouvrez le menu contextuel (clic droit) pour toute connexion de réseau active, puis choisissez Properties (Propriétés).

c. Dans la boîte de dialogue des propriétés de connexion, ouvrez (double-cliquez) Internet Protocol version 4.

3. Sélectionnez Utiliser les adresses de serveur DNS suivantes, remplacez les adresses du serveur DNS préféré et du serveur DNS secondaire par les adresses IP de vos serveurs DNS AWS gérés par Microsoft AD, puis cliquez sur OK.



4. Ouvrez la boîte de dialogue System Properties (Propriétés système) de l'instance, sélectionnez l'onglet Computer Name (Nom de l'ordinateur), puis choisissez Change (Modifier).

> **Tip**
>
> Vous pouvez ouvrir la boîte de dialogue System Properties (Propriétés du système) directement en exécutant ce qui suit à partir d'une invite de commande sur l'instance.
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. Dans le champ Membre de, sélectionnez Domaine, entrez le nom complet de votre annuaire Microsoft AD Active Directory AWS géré, puis cliquez sur OK.

6. Lorsque vous êtes invité à saisir le nom et le mot de passe de l'administrateur du domaine, entrez le nom d'utilisateur et le mot de passe d'un compte doté de privilèges de connexion au domaine. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter Délégation des privilèges de jonction d'annuaire pour AWS Managed Microsoft AD.

   > **Note**
   >
   > Vous pouvez saisir le nom complet de votre domaine ou le nom NetBIOS, suivi d'une barre oblique inverse (\), puis du nom d'utilisateur. Le nom d'utilisateur serait Admin. Par exemple, **`corp.example.com\admin`** ou **`corp\admin`**.

7. Après avoir reçu le message de bienvenue dans le domaine, redémarrez l'instance pour que les modifications prennent effet.

Maintenant que votre instance a été jointe au domaine Microsoft AD Active Directory AWS géré, vous pouvez vous connecter à distance à cette instance et installer des utilitaires pour gérer le répertoire, tels que l'ajout d'utilisateurs et de groupes. Les outils d'administration Active Directory peuvent être utilisés pour créer des utilisateurs et des groupes. Pour plus d'informations, consultez Installation des outils d'administration Active Directory pour Microsoft AD AWS géré.

> **Note**
>
> Vous pouvez également utiliser Amazon Route 53 pour traiter les requêtes DNS au lieu de modifier manuellement les adresses DNS de vos instances Amazon EC2. Pour plus d'informations, consultez la section Intégration de la résolution DNS de votre service d'annuaire à votre réseau Amazon Route 53 Resolver et transfert de requêtes DNS sortantes vers votre réseau.

Joignez facilement une instance Linux Amazon EC2 à votre annuaire AWS Microsoft AD Active Directory géré

Cette procédure permet de joindre facilement une instance Linux Amazon EC2 à votre annuaire AWS Microsoft AD Active Directory géré. Si vous devez effectuer une jonction de domaine fluide entre plusieurs AWS comptes, vous pouvez éventuellement choisir d'activer le partage d'annuaires.

Les distributions et les versions d'instance Linux suivantes sont prises en charge :

- AMI Amazon Linux 2018.03.0
- Amazon Linux 2 (64 bits x86)
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS et Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Les distributions antérieures à Ubuntu 14 et Red Hat Enterprise Linux 7 ne prennent pas en charge la fonctionnalité de jonction de domaine transparente.

Pour une démonstration du processus permettant de joindre facilement une instance Linux à votre annuaire Microsoft AD Active Directory AWS géré, regardez la YouTube vidéo suivante.

Démonstration de jonction transparente à un domaine AD d'Amazon EC2 pour Linux

Prérequis

Avant de pouvoir configurer une jointure de domaine fluide à une instance Linux, vous devez suivre les procédures décrites dans cette section.

Sélectionnez votre compte de service de jonction transparente à un domaine

Vous pouvez facilement associer des ordinateurs Linux à votre domaine Microsoft AD Active Directory AWS géré. Pour ce faire, vous devez utiliser un compte utilisateur autorisé à créer un compte d'ordinateur pour joindre les machines au domaine. Bien que les administrateurs délégués AWS ou les membres d'autres groupes puissent disposer de privilèges suffisants pour joindre des ordinateurs au domaine, nous vous déconseillons ce type d'utilisation. À titre de bonne pratique, nous vous recommandons d'utiliser un compte de service disposant des privilèges minimaux nécessaires pour joindre les ordinateurs au domaine.

Pour déléguer un compte doté des privilèges minimaux nécessaires pour associer les ordinateurs au domaine, vous pouvez exécuter les PowerShell commandes suivantes. Vous devez exécuter ces commandes à partir d'un ordinateur Windows joint au domaine sur lequel le Installation des outils d'administration Active Directory pour Microsoft AD AWS géré est installé. En outre, vous devez

utiliser un compte autorisé à modifier les autorisations sur l'unité d'organisation ou le conteneur de votre ordinateur. La PowerShell commande définit les autorisations permettant au compte de service de créer des objets informatiques dans le conteneur d'ordinateurs par défaut de votre domaine.

```
$AccountName = 'awsSeamlessDomain'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$Domain = Get-ADDomain -ErrorAction Stop
$BaseDn = $Domain.DistinguishedName
$ComputersContainer = $Domain.ComputersContainer
$SchemaNamingContext = Get-ADRootDSE | Select-Object -ExpandProperty
 'schemaNamingContext'
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase $SchemaNamingContext
 -Filter { lDAPDisplayName -eq 'Computer' } -Properties 'schemaIDGUID').schemaIDGUID
# Getting Service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for the Computers container.
$ObjectAcl = Get-ACL -Path "AD:\$ComputersContainer"
# Setting ACL allowing the service account the ability to create child computer objects
 in the Computers container.
$AddAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'CreateChild',
 'Allow', $ServicePrincipalNameGUID, 'All'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$ComputersContainer"
```

Si vous préférez utiliser une interface utilisateur graphique (GUI), vous pouvez utiliser le processus manuel décrit dans Délégation de privilèges à votre compte de service.

Créer les secrets pour stocker le compte de service de domaine

Vous pouvez l'utiliser AWS Secrets Manager pour stocker le compte de service de domaine.

Pour créer des secrets et stocker les informations du compte de service de domaine

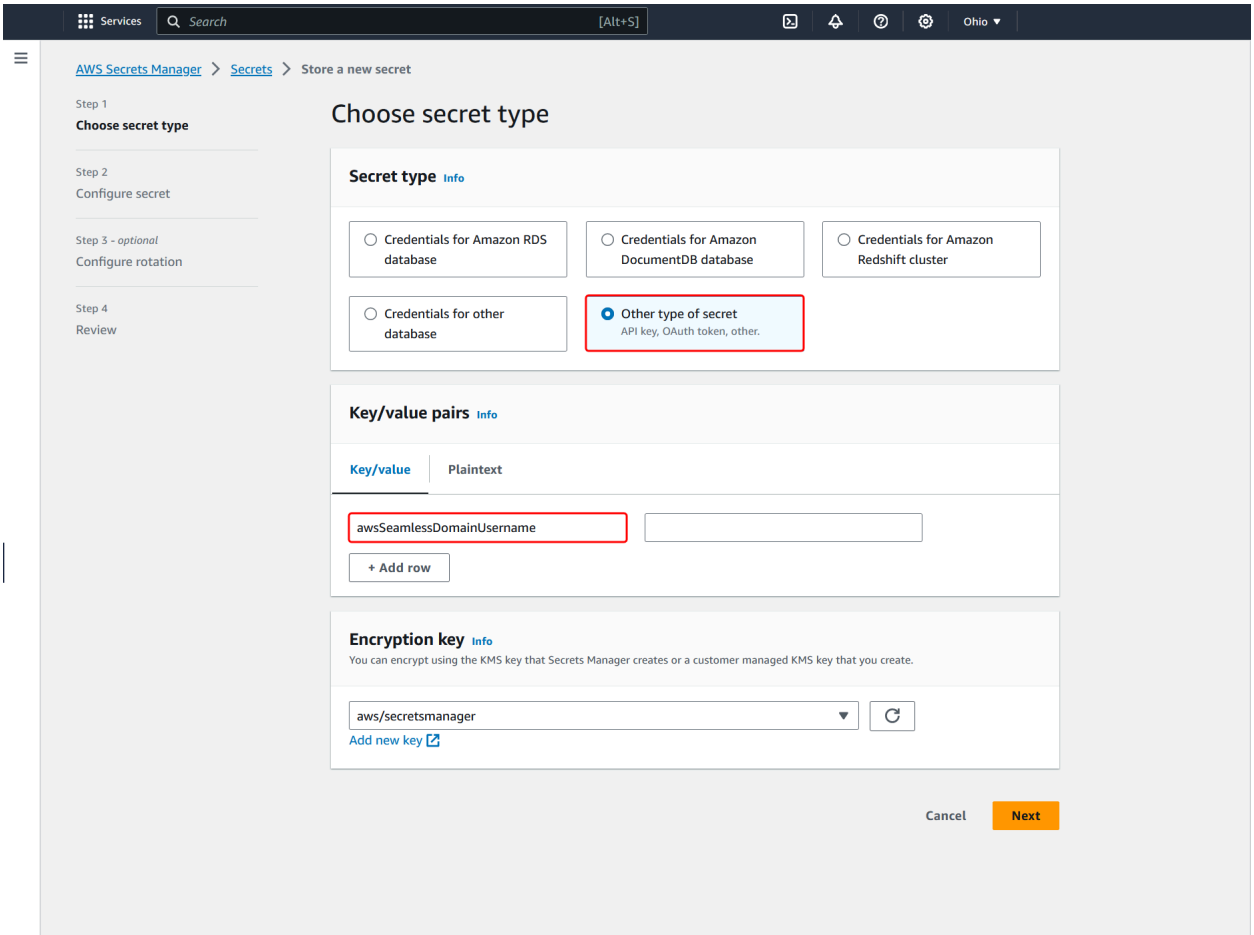
1. Connectez-vous à la AWS Secrets Manager console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/secretsmanager/.
2. Choisissez Store a new secret (Stocker un nouveau secret).
3. Sur la page Store a new secret (Stocker un nouveau secret), procédez comme suit :

a. Sous Type de secret, sélectionnez Autre type de secret.

b. Sous Paires clé/valeur, procédez comme suit :

i. Dans la première case, saisissez **`awsSeamlessDomainUsername`**. Sur la même ligne, dans la case suivante, entrez le nom d'utilisateur de votre compte de service. Par exemple, si vous avez déjà utilisé la PowerShell commande, le nom du compte de service serait**`awsSeamlessDomain`**.

> **Note**
>
> Vous devez saisir **`awsSeamlessDomainUsername`** exactement tel quel. Assurez-vous qu'il n'y a pas d'espaces au début ni à la fin. Sinon, la jonction de domaine échouera.



ii. Choisissez Add row (Ajouter une ligne).

iii. Sur la nouvelle ligne, dans la première case, saisissez **`awsSeamlessDomainPassword`**. Sur la même ligne, dans la case suivante, saisissez le mot de passe de votre compte de service.

> **Note**
>
> Vous devez saisir **`awsSeamlessDomainPassword`** exactement tel quel. Assurez-vous qu'il n'y a pas d'espaces au début ni à la fin. Sinon, la jonction de domaine échouera.

iv. Sous Clé de chiffrement, laissez la valeur par défaut`aws/secretsmanager`. AWS Secrets Manager chiffre toujours le secret lorsque vous choisissez cette option. Vous pouvez également choisir une clé que vous avez créée.

> **Note**
>
> Des frais sont associés AWS Secrets Manager, selon le secret que vous utilisez. Pour obtenir la liste de prix actuelle complète, consultez Tarification AWS Secrets Manager.
> Vous pouvez utiliser la clé AWS `aws/secretsmanager` gérée créée par Secrets Manager pour chiffrer vos secrets gratuitement. Si vous créez vos propres clés KMS pour chiffrer vos secrets, cela vous AWS sera facturé au AWS KMS tarif en vigueur. Pour plus d'informations, consultez Tarification d'AWS Key Management Service.

v. Choisissez Suivant.

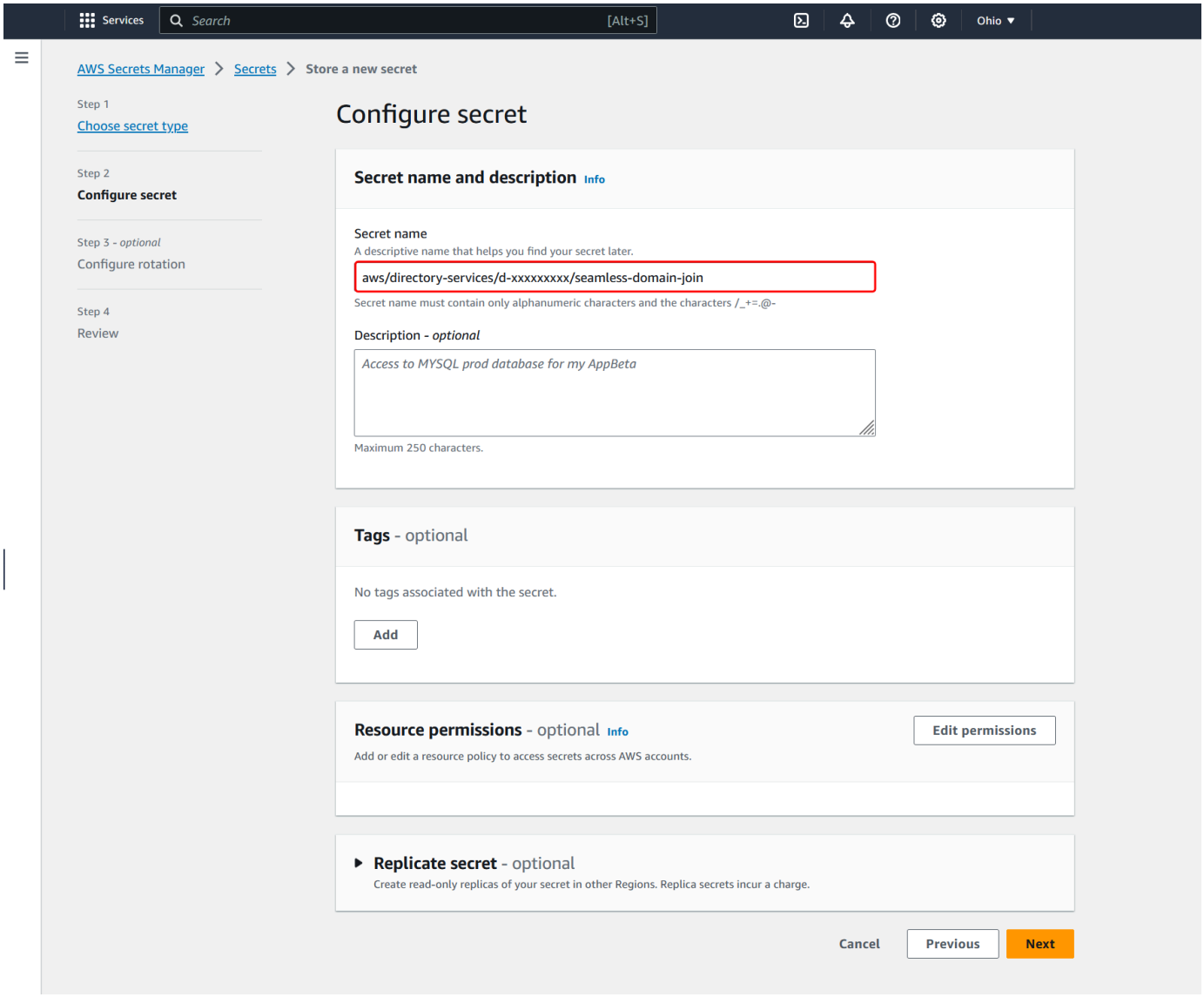
4. Sous Nom secret, entrez un nom secret qui inclut votre identifiant de répertoire en utilisant le format suivant, en remplaçant *`d-xxxxxxxxx`* par votre identifiant de répertoire :

```
aws/directory-services/d-xxxxxxxxx/seamless-domain-join
```

Cela servira à récupérer des secrets dans l'application.

> **Note**
>
> Vous devez saisir **`aws/directory-services/d-xxxxxxxxx/seamless-domain-join`** exactement tel quel, mais remplacez *`d-xxxxxxxxx`* par votre ID d'annuaire.

Assurez-vous qu'il n'y a pas d'espaces au début ni à la fin. Sinon, la jonction de domaine échouera.



5. Laissez le reste des paramètres définis par défaut, puis choisissez Next (Suivant).
6. Sous Configure automatic rotation (Configurer la rotation automatique), choisissez Disable automatic rotation (Désactiver la rotation automatique), puis cliquez sur Next (Suivant).

   Vous pouvez activer la rotation pour ce secret après l'avoir enregistré.
7. Vérifiez les paramètres, puis choisissez Store (Stocker) pour enregistrer vos modifications. La console Secrets Manager vous redirige à la liste des secrets de votre compte, où votre nouveau secret est désormais inclus.

8. Choisissez le nom du secret que vous venez de créer dans la liste et prenez note de la valeur de l'ARN secret. Vous en aurez besoin pour la section suivante.

Activer la rotation pour le secret du compte de service de domaine

Nous vous recommandons d'alterner régulièrement les secrets afin d'améliorer votre niveau de sécurité.

Pour activer la rotation pour le secret du compte de service de domaine

- Suivez les instructions de la section Configurer la rotation automatique pour les AWS Secrets Manager secrets dans le Guide de AWS Secrets Manager l'utilisateur.

  Pour l'étape 5, utilisez le modèle de rotation des informations d'identification Microsoft Active Directory dans le guide de AWS Secrets Manager l'utilisateur.

  Pour obtenir de l'aide, consultez la section Résolution des problèmes AWS Secrets Manager de rotation dans le Guide de AWS Secrets Manager l'utilisateur.

Créez le rôle et la politique IAM requis

Suivez les étapes préalables suivantes pour créer une politique personnalisée qui autorise un accès en lecture seule à votre secret de jonction de domaine transparent Secrets Manager (que vous avez créé précédemment) et pour créer un nouveau rôle IAM DomainJoin LinuxEC2.

Créer la politique de lecture IAM Secrets Manager

Utilisez la console IAM pour créer une politique qui accorde un accès en lecture seule à votre secret Secrets Manager.

Pour créer la politique de lecture IAM Secrets Manager

1. Connectez-vous au en AWS Management Console tant qu'utilisateur autorisé à créer des politiques IAM. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, Gestion des accès, sélectionnez Policies.
3. Choisissez Créer une politique.
4. Choisissez l'onglet JSON et copiez le texte du document de politique JSON suivant. Collez-le ensuite dans la zone de texte JSON.

> **Note**
>
> Assurez-vous de remplacer l'ARN de la région et de la ressource par la région et l'ARN réels du secret que vous avez créé précédemment.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:xxxxxxxxx:secret:aws/directory-
services/d-xxxxxxxxx/seamless-domain-join"
            ]
        }
    ]
}
```

5. Lorsque vous avez terminé, choisissez Next. Le programme de validation des politiques signale les éventuelles erreurs de syntaxe. Pour plus d'informations, veuillez consulter la section Validating IAM policies (français non garanti).
6. Sur la page Review policy (Réviser la politique), saisissez un nom pour la politique, tel que **`SM-Secret-Linux-DJ-d-xxxxxxxxxx-Read`**. Vérifiez la section Summary (Récapitulatif) pour voir les autorisations accordées par votre politique. Sélectionnez Create Policy (Créer une politique) pour enregistrer vos changements. La nouvelle politique s'affiche dans la liste des politiques gérées et est prête à être attachée à une identité.

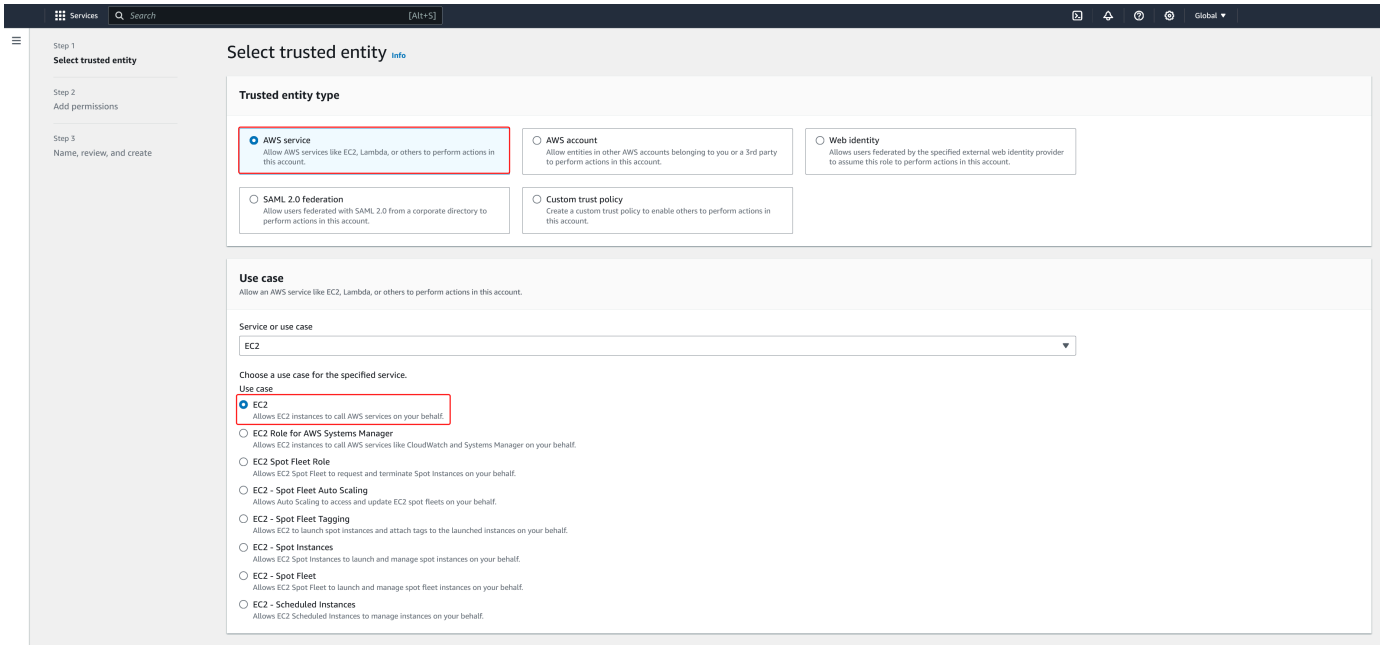
> **Note**
>
> Nous vous recommandons de créer une politique par secret. Cela garantit que les instances n'ont accès qu'au secret approprié et minimise les répercussions si une instance est compromise.

Création du rôle LinuxEC2 DomainJoin

Utilisez la console IAM pour créer le rôle que vous utiliserez pour joindre un domaine à votre instance Linux EC2.

Pour créer le rôle LinuxEC2 DomainJoin

1. Connectez-vous au en AWS Management Console tant qu'utilisateur autorisé à créer des politiques IAM. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, sous Gestion des accès, sélectionnez Rôles.
3. Dans le panneau de contenu, sélectionnez Create role (Créer un rôle).
4. Sous Select type of trusted entity (Sélectionner le type d'entité approuvée), choisissez service AWS .
5. Sous Cas d'utilisation, choisissez EC2, puis Next.



6. Pour Filter policies (Filtrer les politiques), procédez comme suit :

   a. Saisissez **`AmazonSSMManagedInstanceCore`**. Cochez ensuite la case correspondant à cet élément de la liste.

   b. Saisissez **`AmazonSSMDirectoryServiceAccess`**. Cochez ensuite la case correspondant à cet élément de la liste.

   c. Saisissez **`SM-Secret-Linux-DJ-`*`d-xxxxxxxxxx`*`-Read`** (ou le nom de la politique que vous avez créée dans la procédure précédente). Cochez ensuite la case correspondant à cet élément de la liste.

d. Après avoir ajouté les trois politiques répertoriées ci-dessus, sélectionnez Créer un rôle.

> **Note**
>
> AmazonSSM DirectoryServiceAccess fournit les autorisations nécessaires pour joindre des instances à une instance Active Directory gérée par. AWS Directory Service AmazonSSM ManagedInstanceCore fournit les autorisations minimales nécessaires pour utiliser le AWS Systems Manager service. Pour plus d'informations sur la création d'un rôle doté de ces autorisations, ainsi que sur les autres autorisations et politiques que vous pouvez attribuer à votre rôle IAM, veuillez consulter la section Create an IAM instance profile for Systems Manager (français non garanti) dans le Guide de l'utilisateur AWS Systems Manager .

7. Entrez un nom pour votre nouveau rôle, par exemple un autre nom que vous préférez dans le champ Nom du rôle. **`LinuxEC2DomainJoin`**
8. (Facultatif) Pour Role description (Description du rôle), entrez une description.
9. (Facultatif) Choisissez Ajouter une nouvelle balise à l'étape 3 : Ajouter des balises pour ajouter des balises. Les paires clé-valeur de balise sont utilisées pour organiser, suivre ou contrôler l'accès pour ce rôle.
10. Sélectionnez Créer un rôle.

Rejoignez facilement votre instance Linux

Maintenant que vous avez configuré toutes les tâches prérequises, vous pouvez utiliser la procédure suivante pour rejoindre facilement votre instance EC2 Linux.

Pour rejoindre facilement votre instance Linux

1. Connectez-vous à la console Amazon EC2 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le sélecteur de région de la barre de navigation, choisissez le même répertoire Région AWS que le répertoire existant.
3. Sur le EC2 Dashboard (tableau de bord EC2), dans la section Launch instance (Lancer une instance), choisissez Launch instance (Lancer une instance).
4. Sur la page Lancer une instance, dans la section Nom et balises, entrez le nom que vous souhaitez utiliser pour votre instance Linux EC2.

5. (Facultatif) Sélectionnez Add additional tags (Ajouter des balises supplémentaires) pour ajouter une ou plusieurs paires clé-valeur d'identification afin d'organiser, de suivre ou de contrôler l'accès pour cette instance EC2.
6. Dans la section Image de l'application et du système d'exploitation (Amazon Machine Image), choisissez l'AMI Linux que vous souhaitez lancer.

> **Note**
>
> L'AMI utilisée doit avoir la version 2.3.1644.0 ou supérieure AWS Systems Manager (agent SSM). Pour vérifier la version de l'agent SSM installée dans votre AMI en lançant une instance à partir de cette AMI, veuillez consulter Getting the currently installed SSM Agent version (français non garanti). Si vous devez mettre à niveau l'agent SSM, veuillez consulter Installing and configuring SSM Agent on EC2 instances for Linux (français non garanti).
> SSM utilise le `aws:domainJoin` plugin pour joindre une instance Linux à un Active Directory domaine. *`Le plugin remplace le nom d'hôte des instances Linux par le format EC2AMAZ-XXXXXXX.`* Pour plus d'informations`aws:domainJoin`, consultez la référence du plug-in du document de AWS Systems Manager commande dans le guide de AWS Systems Manager l'utilisateur.

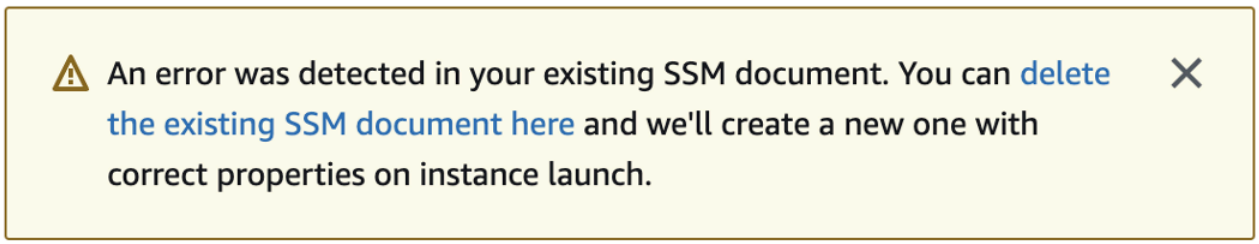
7. Dans la section Type d'instance, choisissez le type d'instance que vous souhaitez utiliser dans la liste déroulante Type d'instance.
8. Dans la section Paire de clés (connexion), vous pouvez choisir de créer une nouvelle paire de clés ou choisir une paire de clés existante. Pour créer une nouvelle paire de clés, choisissez Créer une paire de clés. Entrez le nom de la paire de clés et sélectionnez une option pour le type de paire de clés et le format de fichier de 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. Choisissez Créer une paire de clés. Le fichier de clé privée est automatiquement téléchargé dans votre navigateur. Enregistrez le fichier de clé privée en lieu sûr.

> **Important**
>
> C'est votre seule occasion d'enregistrer le fichier de clé privée.

9. Sur la page Lancer une instance, dans la section Paramètres réseau, choisissez Modifier. Choisissez le VPC dans lequel votre répertoire a été créé dans la liste déroulante VPC obligatoire.
10. Choisissez l'un des sous-réseaux publics de votre VPC dans la liste déroulante Sous-réseau. Tout le trafic externe du sous-réseau que vous choisissez doit être acheminé vers une passerelle Internet. Sinon, vous ne pourrez pas vous connecter à l'instance à distance.

    Pour obtenir plus d'informations sur la manière de se connecter à une passerelle Internet, veuillez consulter la section Connect to the internet using an internet gateway (français non garanti) dans le Guide de l'utilisateur Amazon VPC.
11. Sous Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique), choisissez Enable (Activer).

    Pour plus d'informations sur les adresses IP publiques et privées, veuillez consulter la section Amazon EC2 instance IP addressing (français non garanti) dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.
12. Pour les paramètres Firewall (security groups) [Pare-feu (groupes de sécurité)], vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
13. Pour les paramètres Configure storage (Configurer le stockage), vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
14. Choisissez la section Advanced details (Détails avancés), puis sélectionnez votre domaine dans la liste déroulante Domain join directory (Annuaire de jonction de domaines).

> **Note**
>
> Après avoir choisi le répertoire de jointure du domaine, vous pouvez voir :
>
> 
>
>
> Cette erreur se produit si l'assistant de lancement EC2 identifie un document SSM existant présentant des propriétés inattendues. Vous pouvez effectuer l'une des actions suivantes :

- Si vous avez déjà modifié le document SSM et que les propriétés sont attendues, choisissez Fermer et lancez l'instance EC2 sans aucune modification.
- Cliquez sur le lien Supprimer le document SSM existant ici pour supprimer le document SSM. Cela permettra de créer un document SSM avec les propriétés correctes. Le document SSM sera automatiquement créé lorsque vous lancerez l'instance EC2.

15. Pour le profil d'instance IAM, choisissez le rôle IAM que vous avez créé précédemment dans la section des prérequis Étape 2 : Création du rôle LinuxEC2. DomainJoin
16. Choisissez Launch instance (Lancer une instance).

> **Note**
>
> Si vous effectuez une jonction de domaine transparente avec SUSE Linux, un redémarrage est nécessaire pour que les authentifications fonctionnent. Pour redémarrer SUSE depuis le terminal Linux, tapez sudo reboot.

Joindre manuellement une instance Linux Amazon EC2 à votre annuaire AWS Microsoft AD Active Directory géré

Outre les instances Windows Amazon EC2, vous pouvez également joindre certaines instances Amazon EC2 Linux à votre annuaire Microsoft AD Active AWS Directory géré. Les distributions et les versions d'instance Linux suivantes sont prises en charge :

- AMI Amazon Linux 2018.03.0
- Amazon Linux 2 (64 bits x86)
- AMI Amazon Linux 2023
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS et Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> D'autres distributions et versions Linux peuvent fonctionner, mais n'ont pas été testées.

Joindre une instance Linux à votre Microsoft AD AWS géré

Avant de pouvoir joindre une instance Amazon Linux, CentOS, Red Hat ou Ubuntu à votre annuaire, l'instance doit d'abord être lancée comme indiqué dans Rejoignez facilement votre instance Linux.

> **Important**
>
> Certaines des procédures suivantes peuvent rendre votre instance inaccessible ou non utilisable si elles ne sont pas effectuées correctement. Par conséquent, nous vous conseillons vivement de faire une sauvegarde ou de prendre un instantané de votre instance avant d'exécuter ces procédures.

Pour joindre une instance Linux à votre annuaire

Suivez les étapes pour votre instance Linux spécifique à l'aide de l'un des onglets suivants :

Amazon Linux

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP des serveurs DNS AWS Directory Service fournis. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez la définir manuellement, veuillez consulter How do I assign a static DNS server to a private Amazon EC2 instance (français non garanti) dans le Centre de connaissances AWS pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version particulières de Linux.
3. Assurez-vous que votre instance Amazon Linux - 64 bits est à jour.

   ```
   sudo yum -y update
   ```

4. Installez les paquets Amazon Linux requis sur votre instance Linux.

> **Note**
>
> Certains de ces packages peuvent être déjà installés.
> Au fur et à mesure que vous installez les packages, plusieurs fenêtres de configuration contextuelles peuvent apparaître. Vous pouvez généralement laisser les champs de ces écrans vides.

Amazon Linux

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli
 krb5-workstation
```

> **Note**
>
> Pour vous aider à déterminer la version d'Amazon Linux que vous utilisez, veuillez consulter la section Identifying Amazon Linux images (français non garanti) dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.

5. Joignez l'instance à l'annuaire avec la commande suivante.

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

Un compte dans le domaine *example.com* qui dispose de privilèges de jointure de domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter Délégation des privilèges de jonction d'annuaire pour AWS Managed Microsoft AD.

example.com

Nom DNS complet de votre annuaire.

```
...
 * Successfully enrolled machine in realm
```

6. Définissez le service SSH pour permettre l'authentification du mot de passe.

a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

```
sudo vi /etc/ssh/sshd_config
```

b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

```
PasswordAuthentication yes
```

c. Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

Autrement :

```
sudo service sshd restart
```

7. Une fois l'instance redémarrée, connectez-vous à celle-ci avec n'importe quel client SSH et ajoutez le groupe AWS Delegated Administrators à la liste des sudoers en effectuant les étapes suivantes :

a. Ouvrez le fichier `sudoers` avec la commande suivante :

```
sudo visudo
```

b. Ajoutez les éléments suivants en bas du fichier `sudoers` et enregistrez-le.

```
## Add the "AWS Delegated Administrators" group from the example.com domain.
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

CentOS

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP des serveurs DNS AWS Directory Service fournis. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC

ou la définir manuellement sur l'instance. Si vous souhaitez la définir manuellement, veuillez consulter How do I assign a static DNS server to a private Amazon EC2 instance (français non garanti) dans le Centre de connaissances AWS pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version particulières de Linux.

3. Assurez-vous que votre instance CentOS 7 est à jour.

```
sudo yum -y update
```

4. Installez les paquets CentOS 7 obligatoires sur votre instance Linux.

> **Note**
>
> Certains de ces packages peuvent être déjà installés.
> Au fur et à mesure que vous installez les packages, plusieurs fenêtres de configuration contextuelles peuvent apparaître. Vous pouvez généralement laisser les champs de ces écrans vides.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Joignez l'instance à l'annuaire avec la commande suivante.

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

Un compte dans le domaine *example.com* qui dispose de privilèges de jointure de domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter Délégation des privilèges de jonction d'annuaire pour AWS Managed Microsoft AD.

example.com

Nom DNS complet de votre annuaire.

```
...
 * Successfully enrolled machine in realm
```

6. Définissez le service SSH pour permettre l'authentification du mot de passe.

a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

```
sudo vi /etc/ssh/sshd_config
```

b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

```
PasswordAuthentication yes
```

c. Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

Autrement :

```
sudo service sshd restart
```

7. Une fois l'instance redémarrée, connectez-vous à celle-ci avec n'importe quel client SSH et ajoutez le groupe AWS Delegated Administrators à la liste des sudoers en effectuant les étapes suivantes :

a. Ouvrez le fichier `sudoers` avec la commande suivante :

```
sudo visudo
```

b. Ajoutez les éléments suivants en bas du fichier `sudoers` et enregistrez-le.

```
## Add the "AWS Delegated Administrators" group from the example.com domain.
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

Red Hat

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP des serveurs DNS AWS Directory Service fournis. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC

ou la définir manuellement sur l'instance. Si vous souhaitez la définir manuellement, veuillez consulter How do I assign a static DNS server to a private Amazon EC2 instance (français non garanti) dans le Centre de connaissances AWS pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version particulières de Linux.

3. Assurez-vous que l'instance Red Hat - 64 bits est à jour.

```
sudo yum -y update
```

4. Installez les packages Red Hat obligatoires sur votre instance Linux.

> **Note**
>
> Certains de ces packages peuvent être déjà installés.
> Au fur et à mesure que vous installez les packages, plusieurs fenêtres de configuration contextuelles peuvent apparaître. Vous pouvez généralement laisser les champs de ces écrans vides.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Joignez l'instance à l'annuaire avec la commande suivante.

```
sudo realm join -v -U join_account example.com --install=/
```

join_account

Le SAM AccountName pour un compte du domaine *exemple.com* doté de privilèges de connexion à un domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter Délégation des privilèges de jonction d'annuaire pour AWS Managed Microsoft AD.

example.com

Nom DNS complet de votre annuaire.

```
...
 * Successfully enrolled machine in realm
```

6. Définissez le service SSH pour permettre l'authentification du mot de passe.

a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

```
sudo vi /etc/ssh/sshd_config
```

b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

```
PasswordAuthentication yes
```

c. Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

Autrement :

```
sudo service sshd restart
```

7. Une fois l'instance redémarrée, connectez-vous à celle-ci avec n'importe quel client SSH et ajoutez le groupe AWS Delegated Administrators à la liste des sudoers en effectuant les étapes suivantes :

a. Ouvrez le fichier `sudoers` avec la commande suivante :

```
sudo visudo
```

b. Ajoutez les éléments suivants en bas du fichier `sudoers` et enregistrez-le.

```
## Add the "AWS Delegated Administrators" group from the example.com domain.
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

SUSE

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP de serveur DNS des serveurs DNS fournis par AWS Directory Service. Pour cela, vous pouvez la configurer dans le jeu d'options

DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez la définir manuellement, veuillez consulter How do I assign a static DNS server to a private Amazon EC2 instance (français non garanti) dans le Centre de connaissances AWS pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version particulières de Linux.

3. Assurez-vous que votre instance SUSE Linux 15 est à jour.

   a. Connectez le référentiel de packages.

   ```
   sudo SUSEConnect -p PackageHub/15.1/x86_64
   ```

   b. Mettre à jour SUSE.

   ```
   sudo zypper update -y
   ```

4. Installez les paquets SUSE Linux 15 requis sur votre instance Linux.

   > **Note**
   >
   > Certains de ces packages peuvent être déjà installés.
   > Au fur et à mesure que vous installez les packages, plusieurs fenêtres de configuration contextuelles peuvent apparaître. Vous pouvez généralement laisser les champs de ces écrans vides.

   ```
   sudo zypper -n install realmd adcli sssd sssd-tools sssd-ad samba-client krb5-client
   ```

5. Joignez l'instance à l'annuaire avec la commande suivante.

   ```
   sudo realm join -U join_account example.com --verbose
   ```

   join_account

   Le SAM AccountName du domaine *exemple.com* doté de privilèges de jonction de domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter Délégation des privilèges de jonction d'annuaire pour AWS Managed Microsoft AD.

example.com

Nom DNS complet de votre annuaire.

```
…
realm: Couldn't join realm: Enabling SSSD in nsswitch.conf and PAM failed.
```

Notez que les deux retours suivants sont attendus.

```
! Couldn't authenticate with keytab while discovering which salt to use:
! Enabling SSSD in nsswitch.conf and PAM failed.
```

6. Activez manuellement SSSD dans PAM.

```
sudo pam-config --add --sss
```

7. Modifier nsswitch.conf pour activer SSSD dans nsswitch.conf

```
sudo vi /etc/nsswitch.conf
```

```
passwd: compat sss
group:  compat sss
shadow: compat sss
```

8. Ajoutez la ligne suivante à /etc/pam.d/common-session pour créer automatiquement un annuaire de base lors de la connexion initiale

```
sudo vi /etc/pam.d/common-session
```

```
session optional        pam_mkhomedir.so skel=/etc/skel umask=077
```

9. Redémarrez l'instance pour terminer le processus de jointure de domaine.

```
sudo reboot
```

10. Reconnectez-vous à l'instance à l'aide d'un client SSH pour vérifier que la jointure de domaine s'est terminée avec succès et finalisez les étapes supplémentaires.

    a. Pour confirmer que l'instance a été inscrite sur le domaine

```
sudo realm list
```

```
example.com
  type: kerberos
  realm-name: EXAMPLE.COM
  domain-name: example.com
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: adcli
  required-package: samba-client
  login-formats: %U@example.com
  login-policy: allow-realm-logins
```

b. Pour vérifier l'état du démon SSSD

```
systemctl status sssd
```

```
sssd.service - System Security Services Daemon
   Loaded: loaded (/usr/lib/systemd/system/sssd.service; enabled; vendor
 preset: disabled)
   Active: active (running) since Wed 2020-04-15 16:22:32 UTC; 3min 49s ago
 Main PID: 479 (sssd)
    Tasks: 4
   CGroup: /system.slice/sssd.service
           ##479 /usr/sbin/sssd -i --logger=files
           ##505 /usr/lib/sssd/sssd_be --domain example.com --uid 0 --gid 0 --
logger=files
           ##548 /usr/lib/sssd/sssd_nss --uid 0 --gid 0 --logger=files
           ##549 /usr/lib/sssd/sssd_pam --uid 0 --gid 0 --logger=files
```

11. Pour autoriser l'accès d'un utilisateur via SSH et la console

```
sudo realm permit join_account@example.com
```

Pour autoriser un accès à un groupe de domaines via SSH et la console

```
sudo realm permit -g 'AWS Delegated Administrators'
```

Ou pour permettre à tous les utilisateurs d'accéder

```
sudo realm permit --all
```

12. Définissez le service SSH pour permettre l'authentification du mot de passe.

    a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

    ```
    sudo vi /etc/ssh/sshd_config
    ```

    b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

    ```
    PasswordAuthentication yes
    ```

    c. Redémarrez le service SSH.

    ```
    sudo systemctl restart sshd.service
    ```

    Autrement :

    ```
    sudo service sshd restart
    ```

13. 13. Une fois l'instance redémarrée, connectez-vous à celle-ci avec n'importe quel client SSH et ajoutez le groupe AWS Delegated Administrators à la liste des sudoers en effectuant les étapes suivantes :

    a. Ouvrez le fichier sudoers avec la commande suivante :

    ```
    sudo visudo
    ```

    b. Ajoutez les éléments suivants en bas du fichier sudoers et enregistrez-le.

    ```
    ## Add the "Domain Admins" group from the awsad.com domain.
    %AWS\ Delegated\ Administrators@example.com ALL=(ALL) NOPASSWD: ALL
    ```

Ubuntu

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP des serveurs DNS AWS Directory Service fournis. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez la définir manuellement, veuillez consulter How do I assign a static DNS server to a private Amazon EC2 instance (français non garanti) dans le Centre de connaissances AWS pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version particulières de Linux.
3. Assurez-vous que l'instance Ubuntu - 64 bits est à jour.

```
sudo apt-get update
sudo apt-get -y upgrade
```

4. Installez les packages Ubuntu obligatoires sur votre instance Linux.

> **Note**
>
> Certains de ces packages peuvent être déjà installés.
> Au fur et à mesure que vous installez les packages, plusieurs fenêtres de configuration contextuelles peuvent apparaître. Vous pouvez généralement laisser les champs de ces écrans vides.

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. Désactivez la résolution DNS inversée et définissez le domaine par défaut sur le nom de domaine complet de votre domaine. Les instances Ubuntu doivent pouvoir faire l'objet d'une résolution inverse dans le DNS pour qu'un domaine puisse fonctionner. Sinon, vous devez désactiver la résolution DNS inverse dans /etc/krb5.conf de la façon suivante :

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. Joignez l'instance à l'annuaire avec la commande suivante.

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

Le SAM AccountName pour un compte du domaine *exemple.com* doté de privilèges de connexion à un domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter Délégation des privilèges de jonction d'annuaire pour AWS Managed Microsoft AD.

example.com

Nom DNS complet de votre annuaire.

```
...
 * Successfully enrolled machine in realm
```

7. Définissez le service SSH pour permettre l'authentification du mot de passe.
   a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Redémarrez le service SSH.

   ```
   sudo systemctl restart sshd.service
   ```

   Autrement :

   ```
   sudo service sshd restart
   ```

8. Une fois l'instance redémarrée, connectez-vous à celle-ci avec n'importe quel client SSH et ajoutez le groupe AWS Delegated Administrators à la liste des sudoers en effectuant les étapes suivantes :
   a. Ouvrez le fichier `sudoers` avec la commande suivante :

```
sudo visudo
```

b. Ajoutez les éléments suivants en bas du fichier `sudoers` et enregistrez-le.

```
## Add the "AWS Delegated Administrators" group from the example.com domain.
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

Restriction de l'accès de connexion à un compte

Comme tous les comptes sont définis dans Active Directory, par défaut, tous les utilisateurs de l'annuaire peuvent se connecter à l'instance. Vous pouvez autoriser uniquement certains utilisateurs à se connecter à l'instance à l'aide de la commande ad_access_filterdans sssd.conf. Par exemple :

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Indique que les utilisateurs ne peuvent accéder qu'à l'instance s'ils sont membres d'un groupe spécifique.

cn

Nom canonique du groupe disposant d'un accès. Dans cet exemple, le nom du groupe est *admins*.

ou

Il s'agit de l'unité d'organisation dans laquelle se trouve le groupe ci-dessus. Dans cet exemple, l'unité d'organisation est *Testou*.

dc

Il s'agit du composant de domaine de votre domaine. Dans cet exemple, *example*.

dc

Il s'agit d'un composant de domaine supplémentaire. Dans cet exemple, *com*.

Vous devez ajouter manuellement ad_access_filter à votre /etc/sssd/sssd.conf.

Ouvrez le fichier /etc/sssd/sssd.conf dans un éditeur de texte.

```
sudo vi /etc/sssd/sssd.conf
```

Une fois l'opération effectuée, votre commande sssd.conf pourrait ressembler à ce qui suit :

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

Pour que la configuration soit appliquée, vous devez redémarrer le service sssd :

```
sudo systemctl restart sssd.service
```

Vous pouvez également utiliser :

```
sudo service sssd restart
```

Comme tous les comptes sont définis dans Active Directory, par défaut, tous les utilisateurs de l'annuaire peuvent se connecter à l'instance. Vous pouvez autoriser uniquement certains utilisateurs à se connecter à l'instance à l'aide de la commande ad_access_filterdans sssd.conf.

Par exemple :

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Indique que les utilisateurs ne peuvent accéder qu'à l'instance s'ils sont membres d'un groupe spécifique.

cn

Nom canonique du groupe disposant d'un accès. Dans cet exemple, le nom du groupe est *admins*.

ou

Il s'agit de l'unité d'organisation dans laquelle se trouve le groupe ci-dessus. Dans cet exemple, l'unité d'organisation est *Testou*.

dc

Il s'agit du composant de domaine de votre domaine. Dans cet exemple, *example*.

dc

Il s'agit d'un composant de domaine supplémentaire. Dans cet exemple, *com*.

Vous devez ajouter manuellement ad_access_filter à votre /etc/sssd/sssd.conf.

1. Ouvrez le fichier /etc/sssd/sssd.conf dans un éditeur de texte.

   ```
   sudo vi /etc/sssd/sssd.conf
   ```

2. Une fois l'opération effectuée, votre commande sssd.conf pourrait ressembler à ce qui suit :

   ```
   [sssd]
   domains = example.com
   config_file_version = 2
   services = nss, pam

   [domain/example.com]
   ad_domain = example.com
   krb5_realm = EXAMPLE.COM
   realmd_tags = manages-system joined-with-samba
   cache_credentials = True
   ```

```
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

3. Pour que la configuration soit appliquée, vous devez redémarrer le service sssd :

```
sudo systemctl restart sssd.service
```

Vous pouvez également utiliser :

```
sudo service sssd restart
```

Cartographie des identifiants

Le mappage des identifiants peut être effectué par deux méthodes afin de maintenir une expérience unifiée entre les identités UNIX/Linux User Identifier (UID) et Group Identifier (GID) et Windows et Active Directory Security Identifier (SID).

1. Centralisé
2. Distribué

> **Note**
>
> Le mappage centralisé de l'identité utilisateur Active Directory nécessite une interface de système d'exploitation portable ou POSIX.

Cartographie centralisée de l'identité des utilisateurs

Active Directoryou un autre service LDAP (Lightweight Directory Access Protocol) fournit un UID et un GID aux utilisateurs de Linux. DansActive Directory, ces identifiants sont stockés dans les attributs des utilisateurs :

- UID - Le nom d'utilisateur Linux (chaîne)

- Numéro UID : numéro d'identification utilisateur Linux (entier)
- Numéro GID : numéro d'identification du groupe Linux (entier)

Pour configurer une instance Linux afin d'utiliser l'UID et le GID à partir deActive Directory, définissez-les `ldap_id_mapping = False` dans le fichier sssd.conf. Avant de définir cette valeur, vérifiez que vous avez ajouté un UID, un numéro UID et un numéro GID aux utilisateurs et aux groupes dans. Active Directory

Cartographie distribuée de l'identité des utilisateurs

S'il Active Directory ne possède pas l'extension POSIX ou si vous choisissez de ne pas gérer de manière centralisée le mappage des identités, Linux peut calculer les valeurs UID et GID. Linux utilise l'identifiant de sécurité (SID) unique de l'utilisateur pour garantir la cohérence.

Pour configurer le mappage d'ID utilisateur distribué, définissez-le `ldap_id_mapping = True` dans le fichier sssd.conf.

Connect à l'instance Linux

Lorsqu'un utilisateur se connecte à l'instance à l'aide d'un client SSH, il est invité à indiquer son nom d'utilisateur. L'utilisateur peut entrer le nom d'utilisateur au format `username@example.com` ou au format `EXAMPLE\username`. La réponse ressemblera à la suivante, selon la distribution Linux que vous utilisez :

Amazon Linux, Red Hat Enterprise Linux et CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)

As "root" (sudo or sudo -i) use the:
  - zypper command for package management
  - yast command for configuration management

Management and Config: https://www.suse.com/suse-in-the-cloud-basics
```

```
Documentation: https://www.suse.com/documentation/sles-15/
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud

Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

  System information as of Sat Apr 18 22:03:35 UTC 2020

  System load:  0.01              Processes:           102
  Usage of /:   18.6% of 7.69GB   Users logged in:     2
  Memory usage: 16%               IP address for eth0: 10.24.34.1
  Swap usage:   0%
```

Joindre manuellement une instance Linux Amazon EC2 à votre répertoire AWS Microsoft AD Active Directory géré à l'aide de Winbind

Vous pouvez utiliser le service Winbind pour joindre manuellement vos instances Amazon EC2 Linux à un domaine Microsoft AD Active Directory AWS géré. Cela permet aux utilisateurs Active Directory locaux existants d'utiliser leurs informations d'identification Active Directory lorsqu'ils accèdent aux instances Linux jointes à votre annuaire Microsoft AD Active Directory AWS géré. Les distributions et les versions d'instance Linux suivantes sont prises en charge :

- AMI Amazon Linux 2018.03.0
- Amazon Linux 2 (64 bits x86)
- AMI Amazon Linux 2023
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS et Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> D'autres distributions et versions Linux peuvent fonctionner, mais n'ont pas été testées.

Joindre une instance Linux à votre répertoire Microsoft AD Active Directory AWS géré

> **Important**
>
> Certaines des procédures suivantes peuvent rendre votre instance inaccessible ou non utilisable si elles ne sont pas effectuées correctement. Par conséquent, nous vous conseillons vivement de faire une sauvegarde ou de prendre un instantané de votre instance avant d'exécuter ces procédures.

Pour joindre une instance Linux à votre annuaire

Suivez les étapes pour votre instance Linux spécifique à l'aide de l'un des onglets suivants :

Amazon Linux/CENTOS/REDHAT

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP de serveur DNS des serveurs DNS fournis par AWS Directory Service. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez la définir manuellement, veuillez consulter How do I assign a static DNS server to a private Amazon EC2 instance (français non garanti) dans le Centre de connaissances AWS pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version particulières de Linux.
3. Assurez-vous que votre instance Linux est à jour.

   ```
   sudo yum -y update
   ```

4. Installez les paquets Samba/Winbind obligatoires sur votre instance Linux.

   ```
   sudo yum -y install authconfig samba samba-client samba-winbind samba-winbind-clients
   ```

5. Faites une sauvegarde du fichier `smb.conf` principal afin de pouvoir y revenir en cas d'échec :

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. Ouvrez le fichier de configuration d'origine [`/etc/samba/smb.conf`] dans un éditeur de texte.

```
sudo vim /etc/samba/smb.conf
```

   Renseignez les informations relatives à votre environnement de domaine Active Directory comme indiqué dans l'exemple ci-dessous :

```
[global]
 workgroup = example
 security = ads
 realm = example.com
 idmap config * : rangesize = 1000000
 idmap config * : range = 1000000-19999999
 idmap config * : backend = autorid
 winbind enum users = no
 winbind enum groups = no
 template homedir = /home/%U@%D
 template shell = /bin/bash
 winbind use default domain = false
```

7. Ouvrez le fichier d'hôtes [`/etc/hosts`] dans un éditeur de texte.

```
sudo vim /etc/hosts
```

   Ajoutez l'adresse IP privée de votre instance Linux comme suit :

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> Si vous n'avez pas indiqué votre adresse IP dans le fichier `/etc/hosts`, le message d'erreur DNS suivant peut s'afficher lorsque vous joignez l'instance au domaine : `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`

Cette erreur signifie que la jonction a réussi, mais que la commande [net ads] n'a pas pu consigner l'enregistrement DNS dans le DNS.

8. Joignez l'instance Linux à Active Directory à l'aide de l'utilitaire net.

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

Un compte dans le domaine *example.com* qui dispose de privilèges de jointure de domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter Délégation des privilèges de jonction d'annuaire pour AWS Managed Microsoft AD.

example.com

Nom DNS complet de votre annuaire.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Modifiez le fichier de configuration PAM, utilisez la commande ci-dessous pour ajouter les entrées nécessaires à l'authentification Winbind :

```
sudo authconfig --enablewinbind --enablewinbindauth  --enablemkhomedir   --update
```

10. Définissez le service SSH pour permettre l'authentification du mot de passe en modifiant le fichier `/etc/ssh/sshd_config`.

    a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

    ```
    sudo vi /etc/ssh/sshd_config
    ```

    b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

    ```
    PasswordAuthentication yes
    ```

    c. Redémarrez le service SSH.

    ```
    sudo systemctl restart sshd.service
    ```

Autrement :

```
sudo service sshd restart
```

11. Une fois que l'instance a redémarré, connectez-vous y avec un client SSH et ajoutez des privilèges racine pour un groupe ou un utilisateur de domaine à la liste sudoers en effectuant les étapes suivantes :

    a. Ouvrez le fichier `sudoers` avec la commande suivante :

    ```
    sudo visudo
    ```

    b. Ajoutez les groupes ou utilisateurs requis à partir de votre domaine approuvé ou d'approbation comme suit, puis enregistrez-les.

    ```
    ## Adding Domain Users/Groups.
    %domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL
    %domainname\\groupname ALL=(ALL:ALL) ALL
    domainname\\username ALL=(ALL:ALL) ALL
    %Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
    Trusted_DomainName\\username ALL=(ALL:ALL) ALL
    ```

    (L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

SUSE

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP de serveur DNS des serveurs DNS fournis par AWS Directory Service. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez la définir manuellement, veuillez consulter How do I assign a static DNS server to a private Amazon EC2 instance (français non garanti) dans le Centre de connaissances AWS pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version particulières de Linux.
3. Assurez-vous que votre instance SUSE Linux 15 est à jour.

    a. Connectez le référentiel de packages.

```
sudo SUSEConnect -p PackageHub/15.1/x86_64
```

b. Mettre à jour SUSE.

```
sudo zypper update -y
```

4. Installez les paquets Samba/Winbind obligatoires sur votre instance Linux.

```
sudo zypper in -y samba samba-winbind
```

5. Faites une sauvegarde du fichier `smb.conf` principal afin de pouvoir y revenir en cas d'échec :

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. Ouvrez le fichier de configuration d'origine [`/etc/samba/smb.conf`] dans un éditeur de texte.

```
sudo vim /etc/samba/smb.conf
```

Renseignez les informations relatives à l'environnement de votre domaine Active Directory comme indiqué dans l'exemple ci-dessous :

```
[global]
 workgroup = example
 security = ads
 realm = example.com
 idmap config * : rangesize = 1000000
 idmap config * : range = 1000000-19999999
 idmap config * : backend = autorid
 winbind enum users = no
 winbind enum groups = no
 template homedir = /home/%U@%D
 template shell = /bin/bash
 winbind use default domain = false
```

7. Ouvrez le fichier d'hôtes [`/etc/hosts`] dans un éditeur de texte.

```
sudo vim /etc/hosts
```

Ajoutez l'adresse IP privée de votre instance Linux comme suit :

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> Si vous n'avez pas indiqué votre adresse IP dans le fichier `/etc/hosts`, le message d'erreur DNS suivant peut s'afficher lorsque vous joignez l'instance au domaine :
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> Cette erreur signifie que la jonction a réussi, mais que la commande [net ads] n'a pas pu consigner l'enregistrement DNS dans le DNS.

8. Joignez l'instance Linux à l'annuaire avec la commande suivante.

```
sudo net ads join -U join_account@example.com
```

join_account

Le SAM AccountName du domaine *exemple.com* doté de privilèges de jonction de domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter Délégation des privilèges de jonction d'annuaire pour AWS Managed Microsoft AD.

example.com

Nom DNS complet de votre annuaire.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Modifiez le fichier de configuration PAM, utilisez la commande ci-dessous pour ajouter les entrées nécessaires à l'authentification Winbind :

```
sudo pam-config --add --winbind --mkhomedir
```

10. Ouvrez le fichier de configuration Name Service Switch [`/etc/nsswitch.conf`] dans un éditeur de texte.

```
vim /etc/nsswitch.conf
```

Ajoutez la directive Winbind comme indiqué ci-dessous.

```
passwd: files winbind
shadow: files winbind
group:  files winbind
```

11. Définissez le service SSH pour permettre l'authentification du mot de passe en modifiant le fichier `/etc/ssh/sshd_config`.

    a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

    ```
    sudo vim /etc/ssh/sshd_config
    ```

    b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

    ```
    PasswordAuthentication yes
    ```

    c. Redémarrez le service SSH.

    ```
    sudo systemctl restart sshd.service
    ```

    Autrement :

    ```
    sudo service sshd restart
    ```

12. Une fois que l'instance a redémarré, connectez-vous y avec un client SSH et ajoutez des privilèges racine pour un groupe ou un utilisateur de domaine à la liste sudoers en effectuant les étapes suivantes :

    a. Ouvrez le fichier `sudoers` avec la commande suivante :

    ```
    sudo visudo
    ```

    b. Ajoutez les groupes ou utilisateurs requis à partir de votre domaine approuvé ou d'approbation comme suit, puis enregistrez-les.

    ```
    ## Adding Domain Users/Groups.
    %domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL
    ```

```
%domainname\\groupname ALL=(ALL:ALL) ALL
domainname\\username ALL=(ALL:ALL) ALL
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

Ubuntu

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP de serveur DNS des serveurs DNS fournis par AWS Directory Service. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez le configurer manuellement, consultez l'article Comment attribuer un serveur DNS statique à une instance Amazon EC2 privée dans le centre de AWS connaissances pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version Linux spécifiques.
3. Assurez-vous que votre instance Linux est à jour.

   ```
   sudo yum -y update
   ```

   ```
   sudo apt-get -y upgrade
   ```

4. Installez les paquets Samba/Winbind obligatoires sur votre instance Linux.

   ```
   sudo apt -y install samba winbind libnss-winbind libpam-winbind
   ```

5. Faites une sauvegarde du fichier `smb.conf` principal afin de pouvoir y revenir en cas d'échec.

   ```
   sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
   ```

6. Ouvrez le fichier de configuration d'origine [`/etc/samba/smb.conf`] dans un éditeur de texte.

   ```
   sudo vim /etc/samba/smb.conf
   ```

   Renseignez les informations relatives à l'environnement de votre domaine Active Directory comme indiqué dans l'exemple ci-dessous :

```
[global]
 workgroup = example
 security = ads
 realm = example.com
 idmap config * : rangesize = 1000000
 idmap config * : range = 1000000-19999999
 idmap config * : backend = autorid
 winbind enum users = no
 winbind enum groups = no
 template homedir = /home/%U@%D
 template shell = /bin/bash
 winbind use default domain = false
```

7. Ouvrez le fichier d'hôtes [`/etc/hosts`] dans un éditeur de texte.

```
sudo vim /etc/hosts
```

Ajoutez l'adresse IP privée de votre instance Linux comme suit :

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> Si vous n'avez pas indiqué votre adresse IP dans le fichier `/etc/hosts`, le message d'erreur DNS suivant peut s'afficher lorsque vous joignez l'instance au domaine : `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER` Cette erreur signifie que la jonction a réussi, mais que la commande [net ads] n'a pas pu consigner l'enregistrement DNS dans le DNS.

8. Joignez l'instance Linux à Active Directory à l'aide de l'utilitaire net.

```
sudo net ads join -U join_account@example.com
```

`join_account@example.com`

Un compte dans le domaine *`example.com`* qui dispose de privilèges de jointure de domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations

sur la délégation de ces privilèges, veuillez consulter Délégation des privilèges de jonction d'annuaire pour AWS Managed Microsoft AD.

example.com

Nom DNS complet de votre annuaire.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Modifiez le fichier de configuration PAM, utilisez la commande ci-dessous pour ajouter les entrées nécessaires à l'authentification Winbind :

```
sudo pam-auth-update --add --winbind --enable mkhomedir
```

10. Ouvrez le fichier de configuration Name Service Switch [`/etc/nsswitch.conf`] dans un éditeur de texte.

```
vim /etc/nsswitch.conf
```

Ajoutez la directive Winbind comme indiqué ci-dessous.

```
passwd: compat winbind
group:  compat winbind
shadow: compat winbind
```

11. Définissez le service SSH pour permettre l'authentification du mot de passe en modifiant le fichier `/etc/ssh/sshd_config`.

a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

```
sudo vim /etc/ssh/sshd_config
```

b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

```
PasswordAuthentication yes
```

c. Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

Autrement :

```
sudo service sshd restart
```

12. Une fois que l'instance a redémarré, connectez-vous y avec un client SSH et ajoutez des privilèges racine pour un groupe ou un utilisateur de domaine à la liste sudoers en effectuant les étapes suivantes :

    a. Ouvrez le fichier `sudoers` avec la commande suivante :

    ```
    sudo visudo
    ```

    b. Ajoutez les groupes ou utilisateurs requis à partir de votre domaine approuvé ou d'approbation comme suit, puis enregistrez-les.

    ```
    ## Adding Domain Users/Groups.
    %domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL
    %domainname\\groupname ALL=(ALL:ALL) ALL
    domainname\\username ALL=(ALL:ALL) ALL
    %Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
    Trusted_DomainName\\username ALL=(ALL:ALL) ALL
    ```

    (L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

Connect à l'instance Linux

Lorsqu'un utilisateur se connecte à l'instance à l'aide d'un client SSH, il est invité à indiquer son nom d'utilisateur. L'utilisateur peut entrer le nom d'utilisateur au format `username@example.com` ou au format `EXAMPLE\username`. La réponse ressemblera à la suivante, selon la distribution Linux que vous utilisez :

Amazon Linux, Red Hat Enterprise Linux et CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)
```

```
As "root" (sudo or sudo -i) use the:
  - zypper command for package management
  - yast command for configuration management

Management and Config: https://www.suse.com/suse-in-the-cloud-basics
Documentation: https://www.suse.com/documentation/sles-15/
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud

Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

  System information as of Sat Apr 18 22:03:35 UTC 2020

  System load:  0.01              Processes:           102
  Usage of /:   18.6% of 7.69GB   Users logged in:     2
  Memory usage: 16%               IP address for eth0: 10.24.34.1
  Swap usage:   0%
```

Joindre manuellement une instance Mac Amazon EC2 à votre annuaire AWS Microsoft AD Active Directory géré

Cette procédure joint manuellement une instance Mac Amazon EC2 à votre annuaire AWS Microsoft AD Active Directory géré.

Prérequis

- Les instances Mac Amazon EC2 nécessitent des hôtes dédiés Amazon EC2. Vous devez allouer un hôte dédié et lancer une instance sur l'hôte. Pour plus d'informations, consultez Lancer une instance Mac dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.
- Nous vous recommandons de créer un ensemble d'options DHCP pour votre répertoire Microsoft AD Active Directory AWS géré. Cela permettra à toutes les instances de votre Amazon VPC de

pointer vers le domaine spécifié et aux serveurs DNS de résoudre leurs noms de domaine. Pour plus d'informations, consultez Création ou modification d'un ensemble d'options DHCP.

> **Note**
>
> Le tarif des hôtes dédiés varie en fonction de l'option de paiement que vous sélectionnez. Pour plus d'informations, consultez la section Tarification et facturation dans le guide de l'utilisateur Amazon EC2 pour les instances Linux.

Pour rejoindre manuellement une instance Mac

1. Utilisez la commande SSH suivante pour vous connecter à votre instance Mac. Pour plus d'informations sur la connexion à votre instance Mac, consultez la section Se connecter à votre instance Mac.

   ```
   ssh -i /path/key-pair-name.pem ec2-user@my-instance-public-dns-name
   ```

2. Une fois connecté à votre instance Mac, créez un mot de passe pour le compte *ec2-user* à l'aide de la commande suivante :

   ```
   sudo passwd ec2-user
   ```

3. Lorsque vous y êtes invité sur la ligne de commande, entrez un mot de passe pour le compte *ec2-user*. Vous pouvez mettre à jour votre système d'exploitation et vos logiciels en suivant la procédure décrite dans Mettre à jour le système d'exploitation et le logiciel dans le guide de l'utilisateur Amazon EC2 pour les instances Linux.

4. Utilisez la commande *dsconfigad* suivante pour joindre votre instance Mac au domaine Managed AWS Microsoft AD Active Directory. Assurez-vous de remplacer le nom de domaine, le nom de l'ordinateur et l'unité organisationnelle par les informations de votre domaine AWS Managed Microsoft AD Active Directory. Pour plus d'informations, voir Configuration de l'accès au domaine dans Directory Utility sur Mac sur le site Web d'Apple.

   > **Warning**
   >
   > Le nom de l'ordinateur ne doit pas contenir de tiret. Les traits d'union peuvent empêcher la liaison avec le répertoire AWS Microsoft AD Active Directory géré.

```
sudo dsconfigad -add domainName -computer computerName -username Username -
ou "Your-AWS-Delegated-Organizational-Unit"
```

L'exemple suivant montre à quoi doit ressembler la commande lorsque vous rejoignez un utilisateur administratif sur une instance Mac **myec2mac01** associée au **example.com** domaine :

```
sudo dsconfigad -add example.com -computer myec2mac01 -username admin -
ou "OU=Computers,OU=Example,DC=Example,DC=com"
```

5. Utilisez la commande suivante pour ajouter les administrateurs AWS délégués à l'utilisateur administratif sur votre instance Mac :

```
sudo dsconfigad -group "EXAMPLE\aws delegated administrators
```

6. Utilisez la commande suivante pour confirmer que la jointure du domaine AWS Managed Microsoft AD Active Directory a réussi :

```
dsconfigad -show
```

Vous avez joint avec succès votre instance Mac à votre annuaire Microsoft AD Active Directory AWS géré. Vous pouvez désormais vous connecter à votre instance Mac à l'aide de vos informations d'identification Microsoft AD Active Directory AWS gérées.

Lorsque vous vous connectez pour la première fois à votre instance Mac, vous devriez avoir la possibilité de vous connecter en tant qu'utilisateur « Autre ». À ce stade, vous pouvez utiliser vos informations d'identification de domaine Active Directory pour vous connecter à l'instance Mac. Si le message « Autre » ne s'affiche pas sur l'écran de connexion après avoir effectué ces étapes, connectez-vous en tant qu'utilisateur ec2, puis déconnectez-vous.

Pour vous connecter à l'aide de l'interface utilisateur graphique avec un utilisateur de domaine, suivez les étapes décrites dans la section Connexion à l'interface utilisateur graphique (GUI) de votre instance dans le guide de l'utilisateur Amazon EC2 pour les instances Linux.

Délégation des privilèges de jonction d'annuaire pour AWS Managed Microsoft AD

Pour joindre un ordinateur à votre annuaire, vous devez disposer d'un compte doté des privilèges de jonction des ordinateurs à l'annuaire.

Avec AWS Directory Service for Microsoft Active Directory, les membres des groupes Admins et AWS Delegated Server Administrators disposent de ces privilèges.

Cependant, en tant que bonne pratique, vous devez utiliser un compte disposant uniquement des privilèges minimum nécessaires. La procédure suivante montre comment créer un nouveau groupe appelé `Joiners` et déléguer les privilèges à ce groupe qui sont nécessaires pour joindre des ordinateurs à l'annuaire.

Vous devez effectuer cette procédure sur un ordinateur qui est joint à votre annuaire et qui dispose du composant logiciel enfichable Utilisateurs et ordinateurs Active Directory. Vous devez également être connecté en tant qu'administrateur de domaine.

Pour déléguer les privilèges d'adhésion pour AWS Managed Microsoft AD

1. Ouvrez Utilisateurs et ordinateurs Active Directory et sélectionnez l'unité d'organisation ayant votre nom NetBIOS dans l'arborescence de navigation, puis sélectionnez l'unité d'organisation Utilisateurs.

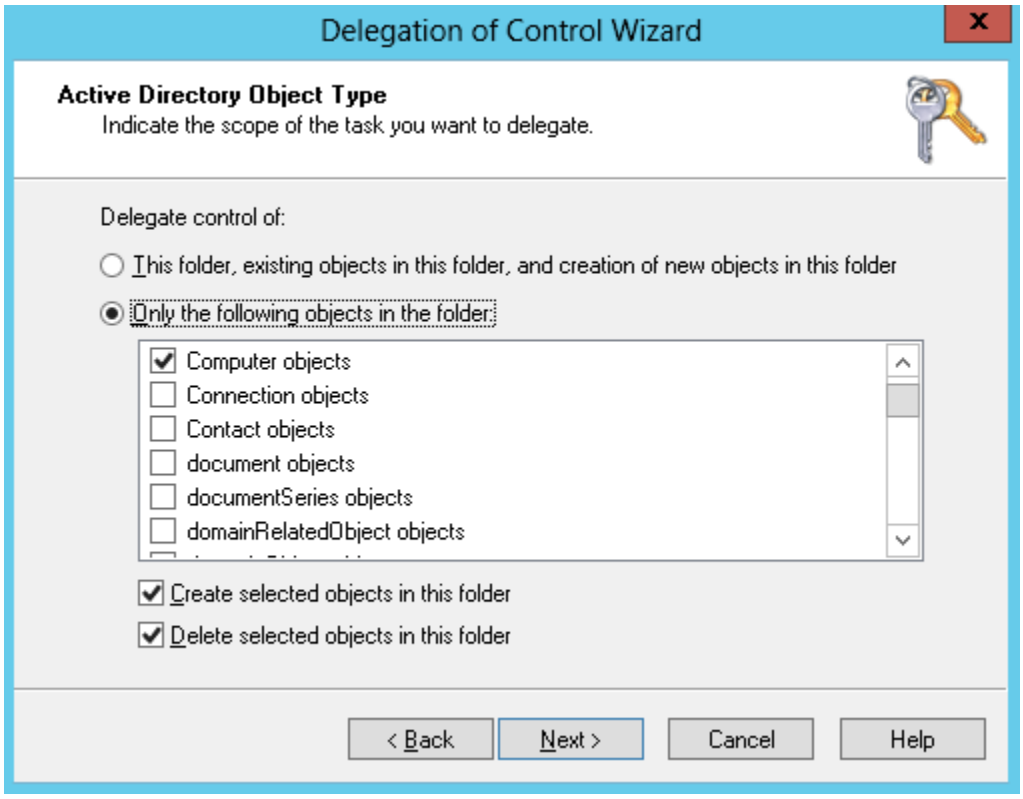
   > **Important**
   >
   > Lorsque vous lancez un service d' AWS annuaire pour Microsoft Active Directory, il AWS crée une unité organisationnelle (UO) qui contient tous les objets de votre annuaire. Cette unité d'organisation, qui porte le nom NetBIOS que vous avez saisi lorsque vous avez créé votre annuaire, est située dans la racine du domaine. La racine du domaine est détenue et gérée par AWS. Vous ne pouvez pas apporter des modifications à la racine du domaine lui-même, par conséquent, vous devez créer le groupe **`Joiners`** au sein de l'unité d'organisation qui détient votre nom NetBIOS.

2. Ouvrez le menu contextuel (clic droit) pour Utilisateurs, choisissez Nouveau, puis choisissez Groupe.
3. Dans la zone Nouvel objet - groupe, saisissez ce qui suit et choisissez OK.

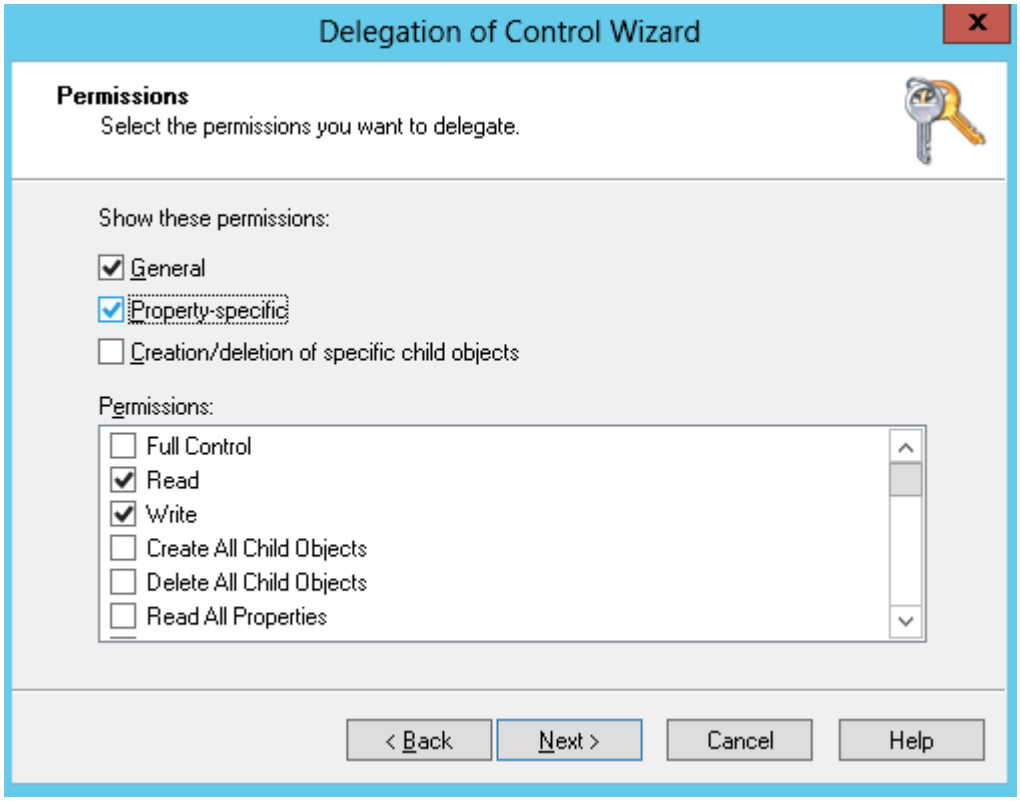
   - Pour Nom du groupe, tapez **`Joiners`**.
   - Pour Étendue du groupe, choisissez Global.

- Pour Type de groupe, choisissez Sécurité.

4. Dans l'arborescence de navigation, sélectionnez le conteneur Ordinateurs sous votre nom NetBIOS. A partir du menu Action, choisissez Déléguer le contrôle.
5. Sur la page Delegation of Control Wizard, choisissez Next, puis choisissez Add.
6. Dans la zone Select Users, Computers, or Groups, saisissez `Joiners`, puis choisissez OK. Si vous trouvez plusieurs objets, sélectionnez le groupe `Joiners` créé précédemment. Choisissez Suivant.
7. Sur la page Tâches à déléguer, sélectionnez Créer une tâche personnalisée à déléguer, puis choisissez Suivant.
8. Sélectionnez Only the following objects in the folder, puis Computer objects.
9. Sélectionnez Créer les objets sélectionnés dans ce dossier et Supprimer les objets sélectionnés dans ce dossier. Ensuite, sélectionnez Suivant.



10. Sélectionnez Lecture et Ecriture, puis choisissez Suivant.



11. Vérifiez les informations de la page Fin de l'Assistant Délégation de contrôle, puis choisissez Terminer.
12. Créez un utilisateur avec un mot de passe fort et ajoutez-le au groupe `Joiners`. Cet utilisateur doit figurer dans le conteneur Utilisateurs qui est sous votre nom NetBIOS. L'utilisateur aura alors les privilèges nécessaires pour connecter les instances à l'annuaire.

Création ou modification d'un ensemble d'options DHCP

AWS vous recommande de créer un ensemble d'options DHCP pour votre AWS Directory Service répertoire et d'attribuer le jeu d'options DHCP au VPC dans lequel se trouve votre répertoire. Cela permet à toutes les instances de ce VPC de pointer vers le domaine spécifié, et aux serveurs DNS de résoudre leurs noms de domaine.

Pour en savoir plus sur les jeux d'options DHCP, veuillez consulter la section DHCP options sets (français non garanti) dans le Guide de l'utilisateur Amazon VPC.

Pour créer un jeu d'options DHCP défini pour votre annuaire

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.

2. Dans le volet de navigation, choisissez DHCP Options Sets, puis sélectionnez Create DHCP options set.
3. Dans la page Créer un jeu d'options DHCP, saisissez les valeurs suivantes pour votre annuaire :

   Nom

   Une balise facultative pour le jeu d'options.

   Nom de domaine

   Nom complet de votre annuaire, par exemple `corp.example.com`.

   Serveurs de noms de domaine

   Les adresses IP des serveurs DNS du répertoire AWS que vous avez fourni.

   > **Note**
   >
   > Vous pouvez trouver ces adresses en accédant au volet de navigation de la console AWS Directory Service, en sélectionnant Directories (Annuaires), puis en choisissant l'ID d'annuaire correct.

   Serveurs NTP

   Laissez ce champ vide.

   Serveur de nom NetBIOS

   Laissez ce champ vide.

   Type de nœud NetBIOS

   Laissez ce champ vide.
4. Choisissez Créer un jeu d'options DHCP. Le nouveau jeu d'options DHCP apparaît dans votre liste d'options DHCP.
5. Notez l'ID du nouveau jeu d'options DHCP (dopt-*xxxxxxxx*). Vous l'utilisez pour associer le nouveau jeu d'options à votre VPC.

Pour modifier le jeu d'options DHCP associé à un VPC

Vous ne pouvez pas modifier un jeu d'options DHCP après l'avoir créé. Si vous voulez que votre VPC utilise un jeu différent d'options DHCP, vous devez créer un nouveau jeu et l'associer à votre VPC. Vous pouvez également configurer votre VPC pour ne pas utiliser d'options DHCP du tout.

1. Ouvrez la console VPC d'Amazon sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sélectionnez Your VPCs (Vos VPC).
3. Sélectionnez le VPC, puis choisissez Actions, Modifier les paramètres du VPC.
4. Pour le jeu d'options DHCP, sélectionnez-en un ou choisissez No DHCP options set (Aucun jeu d'option DHCP), puis sélectionnez Save (Enregistrer).

Pour modifier le jeu d'options DHCP associé à un VPC à l'aide de la ligne de commande, consultez ce qui suit :

- AWS CLI: associate-dhcp-options
- AWS Tools for Windows PowerShell: Register-EC2DhcpOption

Gérer des utilisateurs et des groupes dans AWS Managed Microsoft AD

Les utilisateurs représentent des individus ou des entités individuelles qui ont accès à votre annuaire. Les groupes sont très utiles pour octroyer ou refuser des privilèges à des groupes d'utilisateurs, plutôt que d'appliquer ces privilèges à chaque utilisateur. Si un utilisateur change d'organisation, déplacez-le dans un autre groupe. Il reçoit alors automatiquement les privilèges nécessaires pour la nouvelle organisation.

Pour créer des utilisateurs et des groupes dans un annuaire AWS Directory Service, vous devez utiliser une instance (soit sur site, soit EC2) associée à votre annuaire AWS Directory Service, et être connecté en tant qu'utilisateur disposant des privilèges requis pour créer des utilisateurs et des groupes. Vous devrez également installer les outils Active Directory sur votre instance EC2 afin de pouvoir ajouter vos utilisateurs et vos groupes avec le composant logiciel enfichable Active Directory Users and Computers.

Vous pouvez déployer une instance EC2 préconfigurée avec des outils d'administration Active Directory préinstallés depuis la console de gestion AWS Directory Service. Pour de plus amples informations, veuillez consulter Lancez une instance d'administration d'annuaire dans votre AWS Managed Microsoft AD Active Directory.

Si vous devez déployer une instance EC2 autogérée avec des outils d'administration et installer les outils nécessaires, consultez Étape 3 : Déployer une instance Amazon EC2 pour gérer votre annuaire AWS Microsoft AD Active Directory géré.

> **Note**
>
> Vos comptes d'utilisateur doivent avoir une pré-authentification Kerberos activée. Il s'agit du paramètre par défaut pour les nouveaux comptes d'utilisateur, mais il ne doit pas être modifié. Pour plus d'informations sur ce paramètre, consultez Preauthentication sur Microsoft TechNet.

Les rubriques suivantes expliquent comment créer et gérer des utilisateurs et des groupes.

Rubriques

- Installation des outils d'administration Active Directory pour Microsoft AD AWS géré
- Créez un utilisateur
- Suppression d'un utilisateur
- Réinitialiser un mot de passe utilisateur
- Créez un groupe
- Ajouter un utilisateur à un groupe

Installation des outils d'administration Active Directory pour Microsoft AD AWS géré

Pour gérer votre compte Active Directory à partir d'une instance Windows Server Amazon EC2, vous devez l'installer Active Directory Domain Services and Active Directory Lightweight Directory Services Tools sur l'instance. Utilisez la procédure suivante pour installer ces outils sur une instance Windows Server EC2.

Prérequis

Avant de commencer cette procédure, effectuez les opérations suivantes :

1. Créez un Microsoft AD AWS géréActive Directory. Pour plus d'informations, consultez Créez votre Microsoft AD AWS géré.
2. Lancez une instance Windows Server EC2 et joignez-la à votre répertoire Microsoft AD Active Directory AWS géré. L'instance EC2 a besoin des politiques suivantes pour créer des utilisateurs

et des groupes : **AWSSSMManagedInstanceCore** et**AmazonSSMDirectoryServiceAccess**. Pour plus d'informations, consultez Lancez une instance d'administration d'annuaire dans votre AWS Managed Microsoft AD Active Directory et Associez facilement une instance Windows Amazon EC2 à votre compte AWS Microsoft AD géré Active Directory.

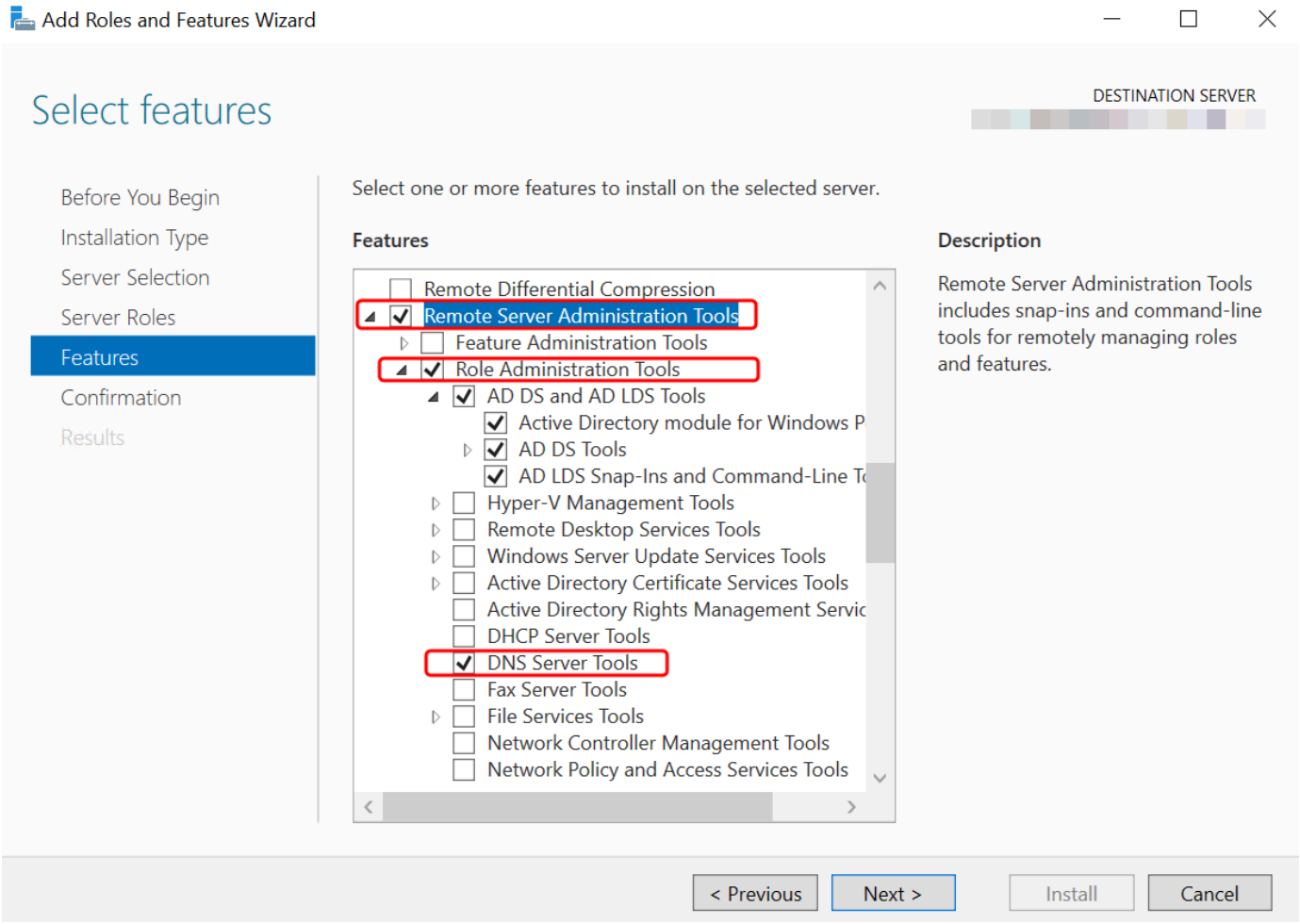
3. Vous aurez besoin des informations d'identification de votre administrateur Active Directory de domaine. Ces informations d'identification ont été créées lors de la création de AWS Managed Microsoft AD. Si vous avez suivi la procédure décrite dansCréez votre Microsoft AD AWS géré, votre nom d'utilisateur d'administrateur inclut votre nom NetBIOS,. **corp\admin**

Installation des outils d'administration Active Directory sur une instance Windows Server EC2

Pour installer les outils d'administration Active Directory sur une instance Windows Server EC2

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la console Amazon EC2, choisissez Instances, sélectionnez l'instance Windows Server, puis sélectionnez Se connecter.
3. Dans la page Se connecter à l'instance, sélectionnez Client RDP.
4. Dans l'onglet Client RDP, sélectionnez Télécharger le fichier Bureau à distance, puis choisissez Obtenir le mot de passe pour récupérer votre mot de passe.
5. Dans le champ Obtenir le mot de passe Windows, sélectionnez Chargement du fichier de clé privée. Choisissez le fichier de clé privée .pem associé à l'instance Windows Server. Après avoir chargé le fichier de clé privée, sélectionnez Déchiffrer le mot de passe.
6. Dans la boîte de dialogue de sécurité Windows, copiez vos informations d'identification d'administrateur local pour que l'ordinateur Windows Server puisse se connecter. Le nom d'utilisateur peut être dans les formats suivants : ***NetBIOS-Name*\admin** ou***DNS-Name*\admin**. Par exemple, **corp\admin** ce serait le nom d'utilisateur si vous avez suivi la procédure dansCréez votre Microsoft AD AWS géré.
7. Une fois connecté à l'instance Windows Server, ouvrez le Gestionnaire de serveur dans le menu Démarrer en choisissant Gestionnaire de serveur.
8. Dans le tableau de bord du Gestionnaire de serveur, choisissez Ajouter des rôles et des fonctionnalités.
9. Dans l'Assistant Ajout de rôles et de fonctionnalités, choisissez Type d'installation, sélectionnez Installation basée sur un rôle ou une fonctionnalité, puis choisissez Suivant.
10. Sous Sélection de serveur, vérifiez que le serveur local est sélectionné, puis choisissez Fonctionnalités dans le volet de navigation de gauche.

11. Dans l'arborescence Fonctionnalités, sélectionnez et ouvrez Outils d'administration de serveur distant, Outils d'administration de rôles et Outils AD DS et AD LDS. Lorsque les outils AD DS et AD LDS sont sélectionnés, le Active Directorymodule pour, les outils AD DSWindows PowerShell, les composants logiciels enfichables et les outils de ligne de commande AD LDS sont sélectionnés. Faites défiler la page vers le bas et sélectionnez Outils du serveur DNS, puis cliquez sur Suivant.



12. Passez en revue les informations, puis choisissez Installer. Lorsque l'installation des fonctionnalités est terminée, les outils Active Directory Domain Services et Active Directory Lightweight Directory Services sont disponibles sur l'écran Démarrer dans le dossier Outils d'administration.

Méthodes alternatives pour installer les outils d'administration Active Directory sur une instance Windows Server EC2

- Voici d'autres méthodes pour installer les outils d'administration Active Directory :

- Vous pouvez éventuellement choisir d'installer les outils d'administration Active Directory à l'aide deWindows PowerShell. Par exemple, vous pouvez installer les outils d'administration à distance Active Directory à partir d'une PowerShell invite en utilisant`Install-WindowsFeature RSAT-ADDS`. Pour plus d'informations, consultez Install- WindowsFeature sur le site Web de Microsoft.
- Vous pouvez également lancer une instance d'administration d'annuaire EC2 dans AWS Management Console laquelle les services de domaine Active Directory et les outils Active Directory Lightweight Directory Services sont déjà installés en suivant les procédures décrites dansLancez une instance d'administration d'annuaire dans votre AWS Managed Microsoft AD Active Directory.

Créez un utilisateur

Utilisez la procédure suivante pour créer un utilisateur avec une instance EC2 jointe à votre annuaire Managed Microsoft AD AWS . Avant de créer des utilisateurs, vous devez suivre les procédures décrites dans la section Installation des outils d'administration Active Directory.

Vous pouvez utiliser l'une des méthodes suivantes pour créer un utilisateur :

- Active DirectoryOutils d'administration
- Windows PowerShell

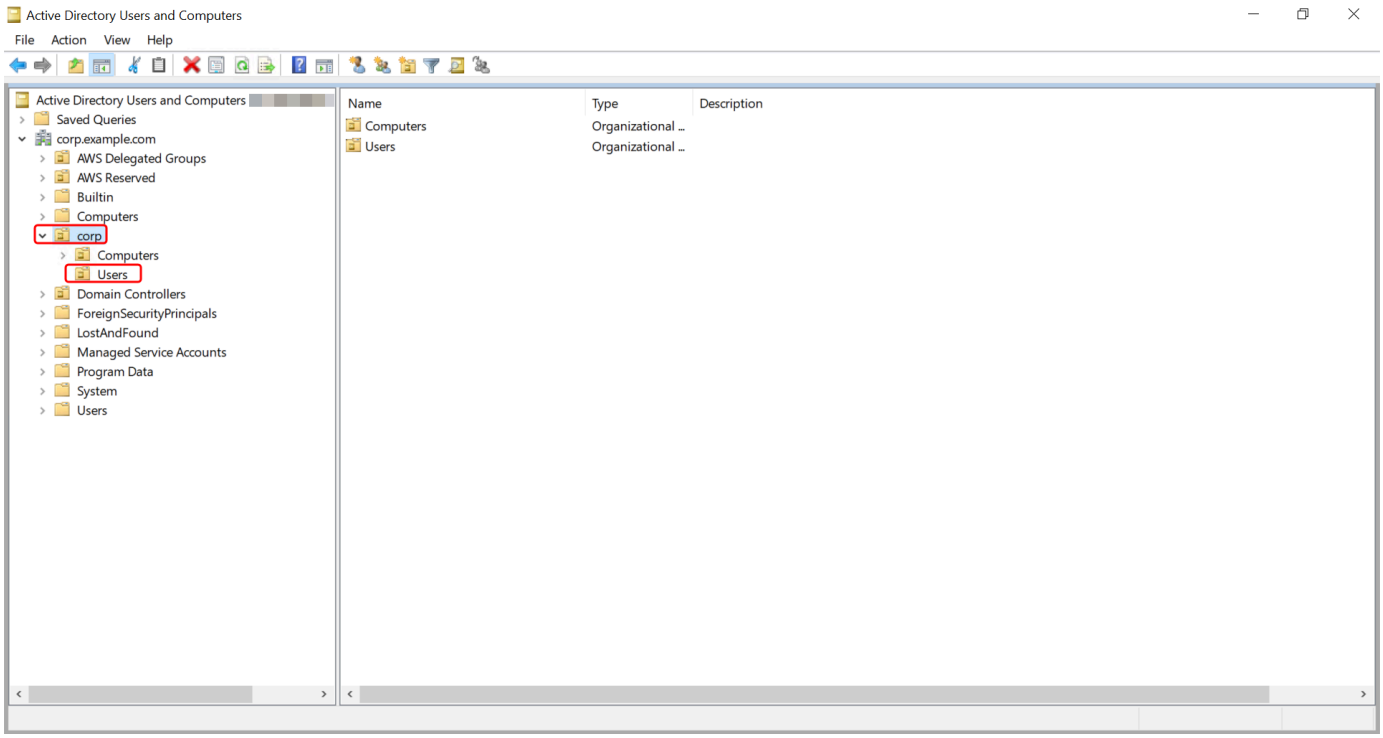
Création d'un utilisateur à l'aide des outils d'Active Directoryadministration

1. Connectez-vous à l'instance où les outils d'administration Active Directory ont été installés.
2. Ouvrez l'outil Utilisateurs et ordinateurs Active Directory dans le menu Démarrer de Windows. Un raccourci vers cet outil se trouve dans le dossier Outils d'administration de Windows.

   > **Tip**
   >
   > Vous pouvez exécuter ce qui suit à partir d'une invite de commande sur l'instance pour ouvrir directement la boîte à outils Utilisateurs et ordinateurs Active Directory.
   >
   > ```
   > %SystemRoot%\system32\dsa.msc
   > ```

3. Dans l'arborescence du répertoire, sélectionnez une unité d'organisation sous le nom NetBIOS de votre répertoire ou dans laquelle vous souhaitez enregistrer votre utilisateur (par exemple,**`corp\Users`**). Pour plus d'informations sur la structure de l'UO utilisée par les

annuaires dans AWS, consultezQu'est-ce qui est créé avec votre annuaire Microsoft AD Active Directory AWS géré.



4. Dans le menu Action, choisissez Nouveau, puis sélectionnez Utilisateur pour ouvrir l'assistant de création d'utilisateurs.
5. Sur la première page de l'assistant, entrez les valeurs des champs suivants, puis sélectionnez Suivant.
   - Prénom
   - Nom
   - Nom de connexion de l'utilisateur
6. Sur la deuxième page de l'assistant, entrez un mot de passe temporaire dans Mot de passe et Confirmer le mot de passe. Assurez-vous que l'utilisateur doit modifier le mot de passe lors de sa prochaine connexion. Aucune autre option ne doit être sélectionnée. Choisissez Suivant.
7. Sur la troisième page de l'assistant Nouvel utilisateur, vérifiez que les informations du nouvel utilisateur sont correctes, puis choisissez Terminer. Le nouvel utilisateur s'affiche dans le dossier Utilisateurs.

Créez un utilisateur dans Windows PowerShell

1. Connectez-vous à l'instance jointe à votre Active Directory domaine en tant qu'Active Directoryadministrateur.
2. Ouvrir Windows PowerShell.
3. Tapez la commande suivante en remplaçant le nom **`jane.doe`** d'utilisateur par le nom d'utilisateur de l'utilisateur que vous souhaitez créer. Vous serez invité Windows PowerShell à fournir un mot de passe pour le nouvel utilisateur. Pour plus d'informations sur les exigences relatives à la complexité des mots de Active Directory passe, consultez Microsoftla documentation. Pour plus d'informations sur la commande New-ADUser, consultez Microsoft la documentation.

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -AsSecureString
 'Password')
```

Suppression d'un utilisateur

Suivez la procédure ci-dessous pour supprimer un utilisateur joint à votre AWS Managed Microsoft ADActive Directory.

Vous pouvez utiliser l'une des méthodes suivantes pour supprimer un utilisateur :

- Active DirectoryOutils d'administration
- Windows PowerShell

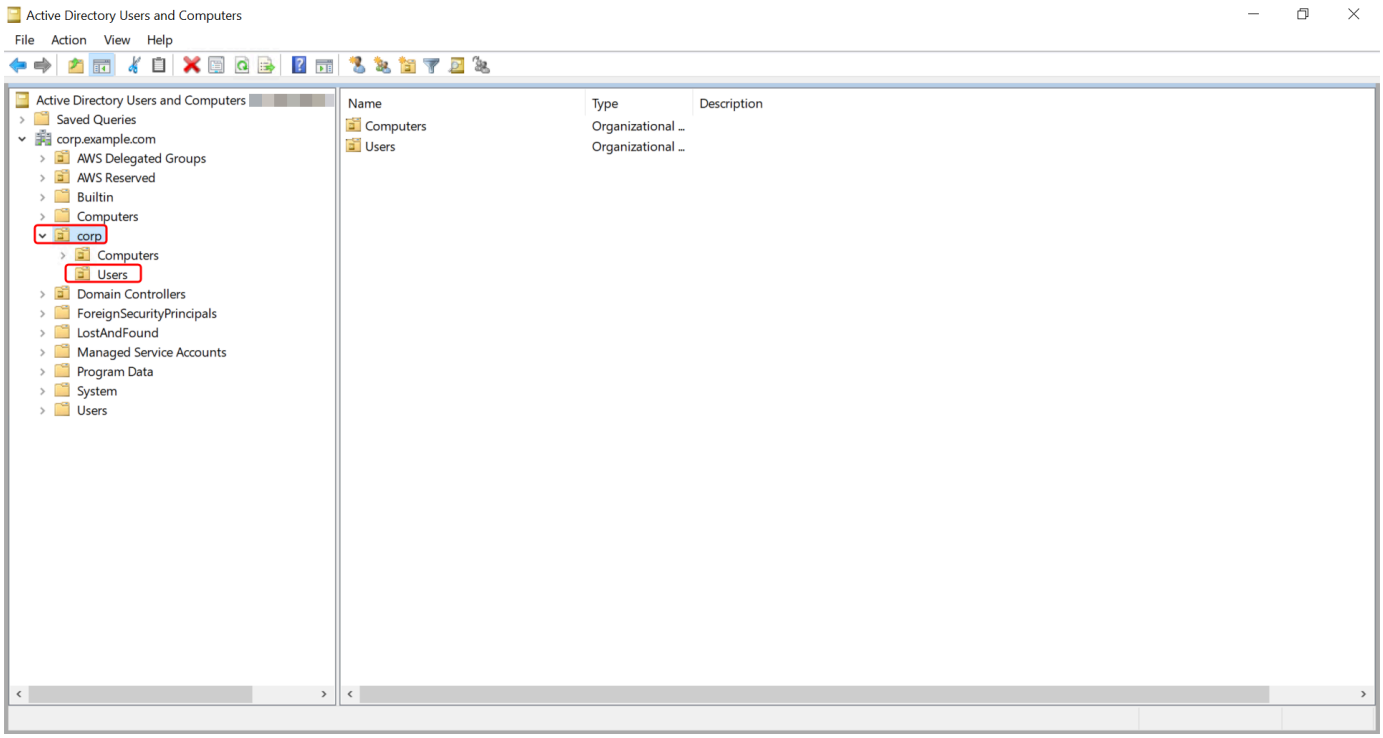
Supprimer un utilisateur à l'aide des outils d'Active Directoryadministration

1. Connectez-vous à l'instance où les outils d'administration Active Directory ont été installés.
2. Ouvrez l'outil Utilisateurs et ordinateurs Active Directory dans le menu Démarrer de Windows. Un raccourci vers cet outil se trouve dans le dossier Outils d'administration de Windows.

> **Tip**
>
> Vous pouvez exécuter ce qui suit à partir d'une invite de commande sur l'instance pour ouvrir directement la boîte à outils Utilisateurs et ordinateurs Active Directory.

```
%SystemRoot%\system32\dsa.msc
```

3. Dans l'arborescence du répertoire, sélectionnez l'unité d'organisation contenant l'utilisateur que vous souhaitez supprimer (par exemple,**`corp\Users`**).



4. Sélectionnez l'utilisateur que vous souhaitez supprimer. Dans le menu Action, sélectionnez Supprimer.
5. Une boîte de dialogue vous demande de confirmer que vous souhaitez supprimer l'utilisateur. Choisissez Oui pour supprimer l'utilisateur. Cette action supprime définitivement l'utilisateur sélectionné.

Supprimer un utilisateur dans Windows PowerShell

1. Connectez-vous à l'instance jointe à votre Active Directory domaine en tant qu'Active Directoryadministrateur.
2. Ouvrir Windows PowerShell.
3. Tapez la commande suivante en remplaçant le nom **`jane.doe`** d'utilisateur par le nom d'utilisateur de l'utilisateur que vous souhaitez supprimer. Pour plus d'informations sur la commande Remove-ADUser, consultez la documentation. Microsoft

```
Remove-ADUser -Identity "jane.doe"
```

Considérations relatives à la corbeille AD

Les utilisateurs supprimés sont stockés temporairement dans la corbeille AD. Pour plus d'informations sur la corbeille AD, consultez La corbeille AD : compréhension, mise en œuvre, meilleures pratiques et résolution des problèmes dans le blog Ask the Directory Services Team Microsoft de l'équipe des services d'annuaire.

Réinitialiser un mot de passe utilisateur

Les utilisateurs doivent respecter les politiques relatives aux mots de passe définies dans leActive Directory. Parfois, cela peut prendre le dessus sur les utilisateurs, y compris l'Active Directoryadministrateur, et ils oublient leur mot de passe. Dans ce cas, vous pouvez rapidement réinitialiser le mot de passe de l'utilisateur en AWS Directory Service indiquant s'il réside dans AWS Managed Microsoft AD.

Vous devez être connecté en tant qu'utilisateur avec les autorisations nécessaires pour réinitialiser les mots de passe. Pour plus d'informations sur les autorisations, consultez Vue d'ensemble de la gestion des autorisations d'accès à vos AWS Directory Service ressources.

Vous pouvez réinitialiser le mot de passe de n'importe quel utilisateur, à l'Active Directoryexception des exceptions suivantes :

- Vous pouvez réinitialiser le mot de passe de n'importe quel utilisateur de l'unité organisationnelle (UO) en fonction du nom NetBIOS que vous avez utilisé lors de la création de votre. Active Directory Par exemple, si vous avez suivi la procédure indiquée dans Créez votre Microsoft AD AWS géré votre NetBIOS, le nom serait CORP et les mots de passe des utilisateurs que vous pourriez réinitialiser seraient membres de l'unité d'organisation Corp/Users.
- Vous ne pouvez pas réinitialiser le mot de passe d'un utilisateur extérieur à l'unité d'organisation en fonction du nom NetBIOS que vous avez utilisé lors de la création de votre. Active Directory Par exemple, vous ne pouvez pas réinitialiser le mot de passe d'un utilisateur dans l'unité d'organisation AWS réservée. Pour plus d'informations sur la structure de l'unité organisationnelle de AWS Managed Microsoft AD, consultezQu'est-ce qui est créé avec votre annuaire Microsoft AD Active Directory AWS géré.

Pour plus d'informations sur la façon dont les politiques de mot de passe sont appliquées lorsqu'un mot de passe est réinitialisé dans AWS Managed Microsoft AD, consultezComment les politiques relatives aux mots de passe sont appliquées.

Vous pouvez utiliser l'une des méthodes suivantes pour réinitialiser le mot de passe d'un utilisateur :

- AWS Management Console
- AWS CLI
- Windows PowerShell

Réinitialisez un mot de passe utilisateur dans AWS Management Console

1. Dans le volet de navigation de la AWS Directory Service console Active Directory, sous, choisissez Répertoires, puis sélectionnez le répertoire Active Directory dans lequel vous souhaitez réinitialiser un mot de passe utilisateur.
2. Sur la page des détails de l'annuaire, choisissez Actions, puis Réinitialiser le mot de passe utilisateur.
3. Dans la boîte de dialogue Réinitialiser le mot de passe utilisateur, dans Nom d'utilisateur, tapez le nom d'utilisateur de l'utilisateur dont le mot de passe doit être modifié.
4. Entrez un mot de passe dans Nouveau mot de passe et Confirmer le mot de passe, puis choisissez Réinitialiser le mot de passe.

Réinitialiser un mot de passe utilisateur dans AWS CLI

1. Pour installer le AWS CLI, voir Installer ou mettre à jour la dernière version du AWS CLI.
2. Ouvrez le AWS CLI.
3. Tapez la commande suivante et remplacez l'ID de répertoire, le nom d'utilisateur **`jane.doe`** et le mot de passe **`P@ssw0rd`** par votre ID de Active Directory répertoire et les informations d'identification souhaitées. Consultez reset-user-passwordle manuel de référence des AWS CLI commandes pour plus d'informations.

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-
password "P@ssw0rd"
```

Réinitialiser un mot de passe utilisateur dans Windows PowerShell

1. Connectez-vous à l'instance jointe à votre Active Directory domaine en tant qu'Active Directoryadministrateur.
2. Ouvrir Windows PowerShell.
3. Tapez la commande suivante en remplaçant le nom d'utilisateur**`jane.doe`**, l'ID de répertoire et le mot de passe **`P@ssw0rd`** par votre ID de Active Directory répertoire et les informations d'identification souhaitées. Consultez l'UserPassword applet de commande Reset-DS pour plus d'informations.

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword
 "P@ssw0rd"
```

Créez un groupe

Utilisez la procédure suivante pour créer un groupe de sécurité avec une instance EC2 jointe à votre répertoire AWS Managed Microsoft AD. Avant de créer des groupes de sécurité, vous devez suivre les procédures décrites dans la section Installation des outils d'administration Active Directory.

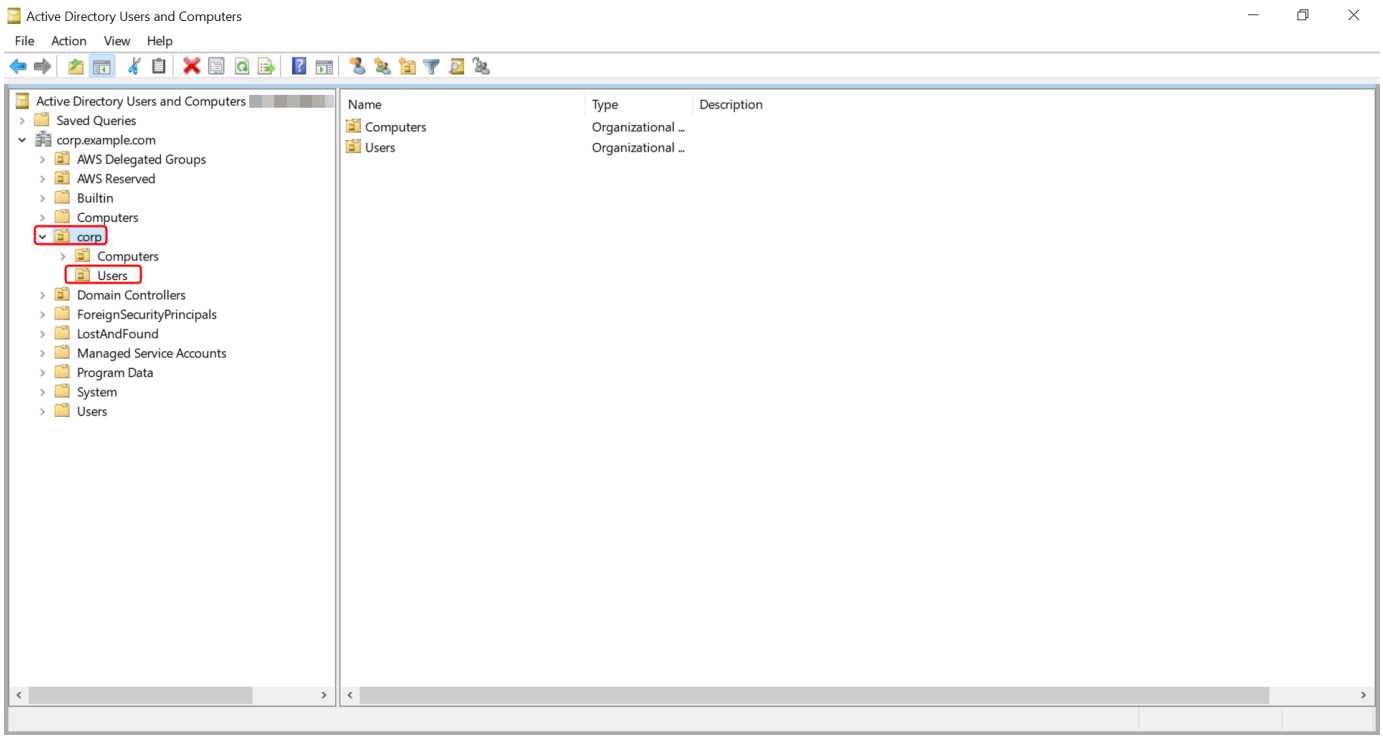
Vous pouvez également utiliser des Windows PowerShell commandes pour créer des groupes. Pour plus d'informations, consultez New-ADGroup dans la documentation de Windows Server 2022 PowerShell .

Pour créer un groupe

1. Connectez-vous à l'instance où les outils d'administration Active Directory ont été installés.
2. Ouvrez l'outil Utilisateurs et ordinateurs Active Directory. Il existe un raccourci vers cet outil dans le dossier Outils d'administration.

> **Tip**
>
> Vous pouvez exécuter ce qui suit à partir d'une invite de commande sur l'instance pour ouvrir directement la boîte à outils Utilisateurs et ordinateurs Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Dans l'arborescence du répertoire, sélectionnez une unité d'organisation sous l'unité d'organisation du nom NetBIOS de votre annuaire dans laquelle vous souhaitez stocker votre groupe (par exemple, Corp\Users). Pour plus d'informations sur la structure de l'UO utilisée par les annuaires dans AWS, consultezQu'est-ce qui est créé avec votre annuaire Microsoft AD Active Directory AWS géré.



4. Dans le menu Action, cliquez sur Nouveau, puis sur Groupe pour ouvrir l'assistant de création de nouveaux groupes.
5. Tapez le nom du groupe dans Nom du groupe, sélectionnez une étendue de groupe qui répond à vos besoins, puis sélectionnez Sécurité pour le type de groupe. Pour plus d'informations sur l'étendue des groupes Active Directory et les groupes de sécurité, veuillez consulter la section Groupes de sécurité Active Directory dans la documentation de Microsoft Windows Server.
6. Cliquez sur OK. Le nouveau groupe de sécurité apparaîtra dans le dossier Utilisateurs.

Ajouter un utilisateur à un groupe

Utilisez la procédure suivante pour ajouter un utilisateur à un groupe de sécurité avec une instance EC2 qui est jointe à votre annuaire AWS Managed Microsoft AD.

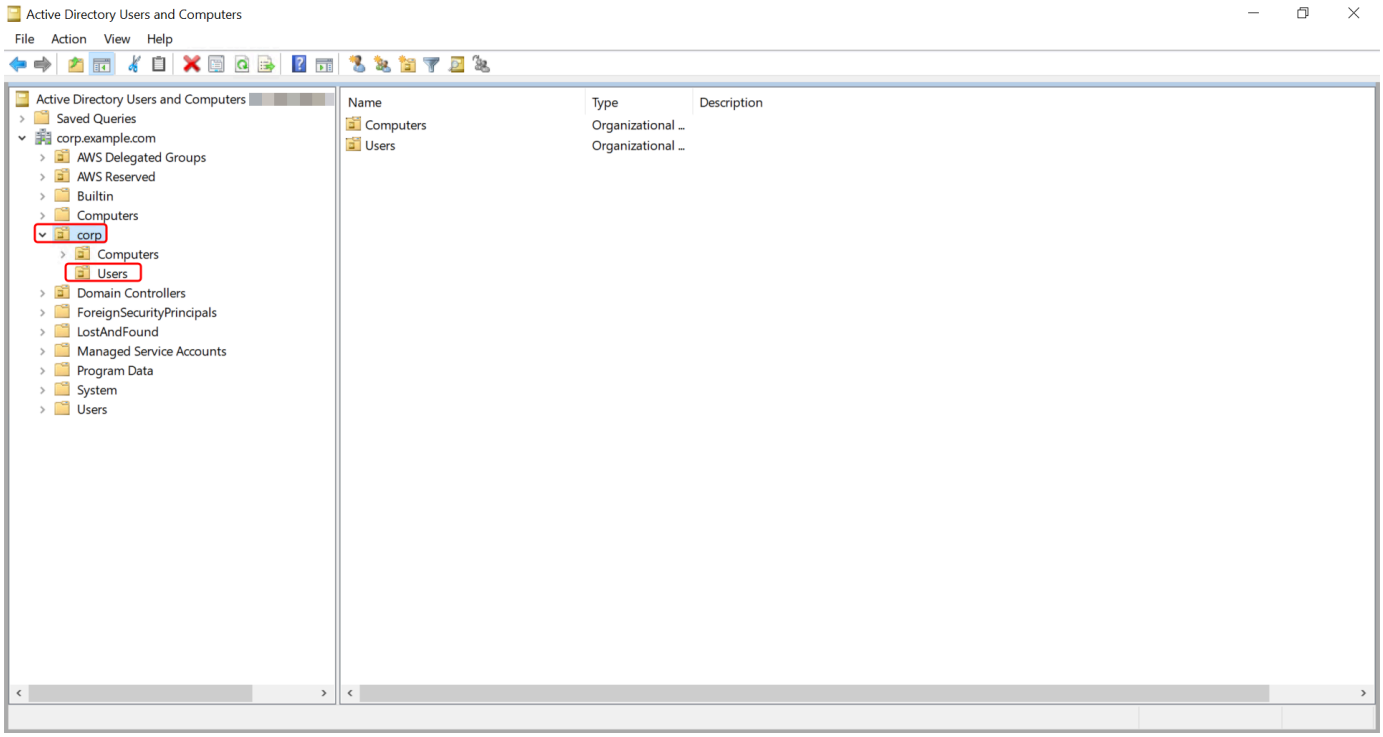
Pour ajouter un utilisateur à un groupe

1. Connectez-vous à l'instance où les outils d'administration Active Directory ont été installés.

2. Ouvrez l'outil Utilisateurs et ordinateurs Active Directory. Il existe un raccourci vers cet outil dans le dossier Outils d'administration.

> **Tip**
>
> Vous pouvez exécuter ce qui suit à partir d'une invite de commande sur l'instance pour ouvrir directement la boîte à outils Utilisateurs et ordinateurs Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Dans l'arborescence de l'annuaire, sélectionnez l'unité d'organisation sous l'unité d'organisation du nom NetBIOS de votre annuaire dans laquelle vous avez enregistré votre groupe, puis sélectionnez le groupe auquel vous souhaitez ajouter un utilisateur en tant que membre.



4. Dans le menu Action, cliquez sur Propriétés pour ouvrir la boîte de dialogue des propriétés du groupe.
5. Sélectionnez l'onglet Membres, puis cliquez sur Ajouter.
6. Pour Entrez les noms des objets à sélectionner, tapez le nom d'utilisateur que vous souhaitez ajouter et cliquez sur OK. Le nom sera affiché dans la liste Membres. Cliquez à nouveau sur OK pour mettre à jour les membres du groupe.

7. Vérifiez que l'utilisateur est désormais membre du groupe en le sélectionnant dans le dossier Utilisateurs et en cliquant sur Propriétés dans le menu Action pour ouvrir la boîte de dialogue des propriétés. Sélectionnez l'onglet Membre de. Le nom du groupe doit apparaître dans la liste des groupes auxquels appartient l'utilisateur.

Connectez-vous à votre infrastructure Active Directory existante

Cette section décrit comment configurer les relations de confiance entre AWS Managed Microsoft AD et votre infrastructure Active Directory existante.

Rubriques

- Création d'une relation d'approbation
- Ajout de routes IP lors de l'utilisation d'adresses IP publiques
- Didacticiel : créer une relation d'approbation entre votre AWS Managed Microsoft AD et votre domaine Active Directory.
- Didacticiel : créer une relation d'approbation entre deux domaines AWS Managed Microsoft AD

Création d'une relation d'approbation

Vous pouvez configurer des relations d'approbation externes et forestières unidirectionnelles ou bidirectionnelles entre votre Service d' AWS annuaire pour Microsoft Active Directory et les annuaires autogérés (sur site), ainsi qu'entre plusieurs annuaires AWS Microsoft AD gérés dans le cloud. AWS AWS Managed Microsoft AD prend en charge les trois directions des relations de confiance : entrante, sortante et bidirectionnelle (bidirectionnelle).

Pour plus d'informations sur les relations de confiance, voir Tout ce que vous vouliez savoir sur les approbations avec AWS Managed Microsoft AD.

> **Note**
>
> Lorsque vous configurez des relations de confiance, vous devez vous assurer que votre annuaire autogéré est et reste compatible avec AWS Directory Service s. Pour plus d'informations sur vos responsabilités, veuillez consulter notre modèle de responsabilité partagée.

AWS Managed Microsoft AD prend en charge les approbations externes et forestières. Pour passer en revue un exemple de scénario montrant comment créer une approbation de forêt, veuillez consulter Didacticiel : créer une relation d'approbation entre votre AWS Managed Microsoft AD et votre domaine Active Directory..

Une confiance bidirectionnelle est requise pour les applications AWS d'entreprise telles qu'Amazon Chime, Amazon Connect, QuickSight Amazon AWS IAM Identity Center, Amazon WorkDocs, Amazon WorkMail, WorkSpaces Amazon et le. AWS Management Console AWS Managed Microsoft AD doit être en mesure d'interroger les utilisateurs et les groupes de votre service autogéréActive Directory.

Amazon EC2, Amazon RDS et Amazon FSx fonctionneront avec une confiance unidirectionnelle ou bidirectionnelle.

Prérequis

La création de l'approbation s'effectue en quelques étapes seulement, mais vous devez d'abord effectuer plusieurs étapes préalables à la phase de configuration de la relation d'approbation.

> **Note**
>
> AWS Managed Microsoft AD ne prend pas en charge la confiance avec les domaines à étiquette unique.

Connexion au VPC

Si vous créez une relation de confiance avec votre annuaire autogéré, vous devez d'abord connecter votre réseau autogéré au VPC Amazon contenant votre Microsoft AD géré AWS . Le pare-feu de vos réseaux Microsoft AD AWS autogérés et gérés doit avoir les ports réseau ouverts répertoriés dans WindowsServer 2008 et versions ultérieures dans Microsoft la documentation.

Pour utiliser votre nom NetBIOS au lieu de votre nom de domaine complet pour l'authentification auprès de vos AWS applications telles qu'Amazon ou WorkDocs Amazon QuickSight, vous devez autoriser le port 9389. Pour plus d'informations sur les ports et protocoles Active Directory, consultez la section Présentation des services et exigences relatives aux ports réseau Windows dans Microsoft la documentation.

Il s'agit des ports minimum requis pour vous permettre de vous connecter à votre annuaire. Votre configuration spécifique peut nécessiter l'ouverture de ports supplémentaires.

Configuration de votre VPC

Le VPC qui contient votre AWS Microsoft AD géré doit disposer des règles sortantes et entrantes appropriées.

Pour configurer vos règles sortantes VPC

1. Dans la AWS Directory Service console, sur la page Détails du répertoire, notez votre ID d'annuaire Microsoft AD AWS géré.
2. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
3. Choisissez Security Groups.
4. Recherchez votre ID d'annuaire Microsoft AD AWS géré. Dans les résultats de recherche, sélectionnez l'élément avec la description « groupe de sécuritéAWS créé pour les contrôleurs de répertoire ID ».

   > **Note**
   >
   > Le groupe de sécurité sélectionné est un groupe de sécurité qui est créé automatiquement lorsque vous créez initialement votre annuaire.

5. Accédez à l'onglet Outbound Rules de ce groupe de sécurité. Sélectionnez Edit, puis Add another rule. Pour la nouvelle règle, saisissez les valeurs suivantes :

   - Type : All Traffic
   - Protocole : All
   - La Destination détermine le trafic qui peut quitter vos contrôleurs de domaine et les directions possible sur votre réseau autogéré. Indiquez une adresse IP unique ou une plage d'adresses IP dans une notation CIDR (par exemple, 203.0.113.5/32). Vous pouvez également indiquer le nom ou l'ID d'un autre groupe de sécurité dans la même région. Pour plus d'informations, consultez Comprenez la configuration et l'utilisation AWS des groupes de sécurité de votre annuaire.
6. Sélectionnez Save.

Activation de l'authentification préalable Kerberos

Vos comptes d'utilisateur doivent avoir une pré-authentification Kerberos activée. Pour plus d'informations sur ce paramètre, consultez la section Préauthentification sur Microsoft TechNet.

Configuration des redirecteurs conditionnels DNS sur votre domaine autogéré

Vous devez configurer des redirecteurs conditionnels DNS sur votre domaine autogéré. Reportez-vous à la section Affecter un redirecteur conditionnel pour un nom de domaine sur Microsoft TechNet pour plus de détails sur les redirecteurs conditionnels.

Pour effectuer les étapes suivantes, vous devez avoir accès aux outils Windows Server suivants pour votre domaine autogéré :

- Outils AD DS et AD LDS
- DNS

Pour configurer les redirecteurs conditionnels sur votre domaine autogéré

1. Vous devez d'abord obtenir des informations sur votre AWS Managed Microsoft AD. Connectez-vous à AWS Management Console et ouvrez la console AWS Directory Service.
2. Dans le volet de navigation, sélectionnez Directories.
3. Choisissez l'ID de répertoire de votre AWS Managed Microsoft AD.
4. Prenez note du nom de domaine complet (FQDN) et des adresses DNS de votre annuaire.
5. Retournez maintenant à votre contrôleur de domaine autogéré. Ouvrez le Gestionnaire de serveur.
6. Dans le menu Tools, choisissez DNS.
7. Dans l'arborescence de la console, développez le serveur DNS du domaine pour lequel vous configurez la relation d'approbation.
8. Dans l'arborescence de la console, sélectionnez Conditional Forwarders.
9. Dans le menu Action, choisissez New conditional forwarder.
10. Dans le domaine DNS, tapez le nom de domaine complet (FQDN) de votre AWS Managed Microsoft AD, comme vous l'avez indiqué précédemment.
11. Choisissez les adresses IP des serveurs principaux et saisissez les adresses DNS de votre répertoire AWS Managed Microsoft AD, comme vous l'avez indiqué précédemment.

    Après avoir saisi les adresses DNS, il se peut que l'erreur « timeout » ou « Impossible à résoudre » s'affiche. Vous pouvez généralement ignorer ces erreurs.
12. Sélectionnez Store this conditional forwarder in Active Directory and replicate as follows: All DNS servers in this domain. Choisissez OK.

Mot de passe de relation d'approbation

Si vous créez une relation d'approbation avec un domaine existant, configurez la relation d'approbation sur ce domaine à l'aide des outils d'administration de Windows Server. Pensez à relever le mot de passe de la relation d'approbation que vous utilisez. Vous devrez utiliser ce même mot de passe lors de la configuration de la relation de confiance sur AWS Managed Microsoft AD. Pour plus d'informations, consultez la section Gestion des approbations sur Microsoft TechNet.

Vous êtes maintenant prêt à créer la relation de confiance sur votre AWS Managed Microsoft AD.

Noms de domaine et NetBIOS

Les noms de domaine et NetBIOS doivent être uniques et ne peuvent pas être identiques pour établir une relation d'approbation.

Création, vérification ou suppression d'une relation d'approbation

> **Note**
>
> Les relations de confiance sont une fonctionnalité globale de AWS Managed Microsoft AD. Si vous utilisez Réplication multi-régions, les procédures suivantes doivent être effectuées dans Région principale. Les modifications seront appliquées automatiquement à toutes les régions répliquées. Pour plus d'informations, consultez Caractéristiques mondiales et régionales.

Pour créer une relation de confiance avec votre Microsoft AD AWS géré

1. Ouvrez la AWS Directory Service console.
2. Sur la page Répertoires, choisissez votre identifiant Microsoft AD AWS géré.
3. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :
   - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région principale, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour plus d'informations, consultez Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Réseau et sécurité.
4. Dans la section Trust relationships (Relations d'approbation), choisissez Actions, puis sélectionnez Add trust relationship (Ajouter une relation d'approbation).

5. Sur la page Ajouter une relation d'approbation, fournissez les informations requises, y compris le type d'approbation, le nom de domaine complet (FQDN) de votre domaine approuvé, le mot de passe et la direction d'approbation.
6. (Facultatif) Si vous souhaitez autoriser uniquement les utilisateurs autorisés à accéder aux ressources de votre répertoire AWS Managed Microsoft AD, vous pouvez éventuellement cocher la case Authentification sélective. Pour des informations générales sur l'authentification sélective, consultez la section Considérations relatives à la sécurité pour les entreprises de confiance chez Microsoft TechNet.
7. Pour Redirecteur conditionnel, saisissez l'adresse IP de votre serveur DNS autogéré. Si vous avez créé précédemment des redirecteurs conditionnels, vous pouvez saisir le nom de domaine complet de votre domaine autogéré au lieu d'une adresse IP DNS.
8. (Facultatif) Choisissez Add another IP (Ajouter une autre adresse IP) et entrez l'adresse IP d'un autre serveur DNS autogéré. Vous pouvez répéter cette étape pour chaque adresse de serveur DNS applicable pour un total de quatre adresses.
9. Choisissez Ajouter.
10. Si le serveur DNS ou le réseau de votre domaine autogéré utilise un espace d'adresse IP publique (non RFC 1918), accédez à la section IP routing (Routage IP) et choisissez Actions, puis Add route (Ajouter une route). Tapez le bloc d'adresse IP de votre serveur DNS ou réseau autogéré selon le format CIDR, par exemple 203.0.113.0/24. Cette étape n'est pas nécessaire si votre serveur DNS et votre réseau autogéré utilisent des espaces d'adressage IP RFC 1918.

    > **Note**
    >
    > Lorsque vous définissez un espace d'adressage IP publique, assurez-vous de ne pas utiliser l'une des plages d'adresses IP AWS ; en effet, celles-ci ne peuvent pas être exploitées dans ce type de cas.

11. (Facultatif) Nous vous recommandons de sélectionner Add routes to the security group for this directory's VPC (Ajouter des routes au groupe de sécurité pour le VPC de cet annuaire) pendant que vous êtes sur la page Add routes (Ajouter des routes). Cela va permettre de configurer les groupes de sécurité comme indiqué ci-dessus dans la section « Configuration de votre VPC ». Ces règles de sécurité ont un impact sur une interface réseau interne qui n'est pas exposée publiquement. Si cette option n'est pas disponible, un message s'affichera pour indiquer que vous avez déjà personnalisé vos groupes de sécurité.

Vous devez configurer la relation d'approbation sur les deux domaines. Les relations doivent être complémentaires. Par exemple, si vous créez une relation d'approbation sortante sur un domaine, vous devez créer une relation d'approbation entrante sur l'autre.

Si vous créez une relation d'approbation avec un domaine existant, configurez la relation d'approbation sur ce domaine à l'aide des outils d'administration de Windows Server.

Vous pouvez créer plusieurs approbations entre votre Microsoft AD AWS géré et différents domaines Active Directory. Cependant, vous ne pouvez avoir qu'une seule relation d'approbation par paire. Par exemple, si vous avez une relation d'approbation unidirectionnelle dans la « direction entrante » et que vous souhaitez configurer une autre relation d'approbation dans la « direction sortante », vous devrez supprimer la relation d'approbation existante et créer une nouvelle approbation « bidirectionnelle ».

Pour vérifier une relation d'approbation sortante

1. Ouvrez la AWS Directory Service console.
2. Sur la page Répertoires, choisissez votre identifiant Microsoft AD AWS géré.
3. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :
   - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région principale, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour plus d'informations, consultez Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Réseau et sécurité.
4. Dans la section Trust relationships (Relations d'approbation), sélectionnez la relation d'approbation que vous voulez vérifier et choisissez Actions, puis Verify trust relationship (Vérifier la relation d'approbation).

Ce processus vérifie uniquement le sens sortant d'une confiance bidirectionnelle. AWS ne prend pas en charge la vérification des trusts entrants. Pour plus d'informations sur la façon de vérifier une approbation depuis ou vers votre Active Directory autogéré, consultez Vérifier une approbation sur Microsoft TechNet.

Suppression d'une relation d'approbation existante

1. Ouvrez la AWS Directory Service console.
2. Sur la page Répertoires, choisissez votre identifiant Microsoft AD AWS géré.

3. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :

   - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région principale, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour plus d'informations, consultez Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Réseau et sécurité.
4. Dans la section Trust relationships (Relations d'approbation), sélectionnez la relation d'approbation que vous voulez supprimer et choisissez Actions, puis Delete trust relationship (Supprimer la relation d'approbation).
5. Sélectionnez Supprimer.

Ajout de routes IP lors de l'utilisation d'adresses IP publiques

Vous pouvez utiliser AWS Directory Service for Microsoft Active Directory pour tirer profit de nombreuses fonctionnalités puissantes d'Active Directory, y compris l'établissement d'approbation avec d'autres annuaires. Toutefois, si les serveurs DNS des réseaux d'autres annuaires utilisent des adresses IP publiques (non RFC 1918), vous devez spécifier ces adresses IP dans le cadre de la configuration de la relation d'approbation. Vous pourrez trouver des informations à ce sujet dans Création d'une relation d'approbation.

De même, vous devez également entrer les adresses IP lors du routage du trafic entre votre AWS Managed Microsoft AD sur AWS et un VPC AWS homologue, si l'ordinateur virtuel utilise des plages d'adresses IP publiques.

Lorsque vous ajoutez les adresses IP comme décrit dans Création d'une relation d'approbation, vous avez la possibilité de sélectionner Add routes to the security group for this directory's VPC. Cette option doit être sélectionnée, sauf si vous avez déjà personnalisé votre groupe de sécurité pour autoriser le trafic nécessaire comme indiqué ci-dessous. Pour de plus amples informations, veuillez consulter Comprenez la configuration et l'utilisation AWS des groupes de sécurité de votre annuaire.

Didacticiel : créer une relation d'approbation entre votre AWS Managed Microsoft AD et votre domaine Active Directory.

Ce didacticiel vous guide à travers toutes les étapes nécessaires pour configurer une relation d'approbation entre AWS Service d'annuaire pour Microsoft Active Directory et votre annuaire Microsoft Active Directory (sur site) autogéré. Même si la création de la relation d'approbation ne requiert que quelques étapes, vous devez d'abord effectuer les étapes préalables suivantes.

Rubriques

Voir aussi

Création d'une relation d'approbation

Prérequis

Le didacticiel présume que vous avez déjà effectué les étapes suivantes :

> **Note**
>
> AWS Managed Microsoft AD ne prend pas en charge les approbations avec domaines à étiquette unique.

- Un annuaire AWS Managed Microsoft AD créé sur AWS. Si vous avez besoin d'aide pour effectuer l'opération, consultez Commencer à utiliser AWS Managed Microsoft AD.
- Instance EC2 exécutant Windows ajoutée à cet annuaire AWS Managed Microsoft AD. Si vous avez besoin d'aide pour effectuer l'opération, consultez Joindre manuellement une Windows instance Amazon EC2 à votre Managed AWS Microsoft AD Active Directory.

  > **Important**
  >
  > Le compte d'administrateur de votre AWS Managed Microsoft AD doit disposer d'un accès administratif à cette instance.

- Outils Windows Server suivants installés sur cette instance :
  - Outils AD DS et AD LDS
  - DNS

  Si vous avez besoin d'aide pour effectuer l'opération, consultez Installation des outils d'administration Active Directory pour Microsoft AD AWS géré.

- Annuaire Microsoft Active Directory (sur site) autogéré

  Vous devez disposer d'un accès administratif à cet annuaire. Les mêmes outils Windows Server comme indiqué ci-dessus doivent être également disponibles pour cet annuaire.
- Une connexion active entre votre réseau autogéré et le VPC contenant votre AWS Managed Microsoft AD. Si vous avez besoin d'aide pour effectuer l'opération, consultez la section Amazon Virtual Private Cloud Connectivity Options.
- Une politique de sécurité locale définie correctement. Vérifiez `Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously` et assurez-vous que ce paramètre contient au moins les trois canaux nommés suivants :
  - netlogon
  - samr
  - lsarpc
- Les noms de domaine et NetBIOS doivent être uniques et ne peuvent pas être identiques pour établir une relation de confiance.

Pour plus d'informations sur les prérequis relatifs à la création d'une relation de confiance, consultez Création d'une relation d'approbation.

Configuration du didacticiel

Pour ce didacticiel, nous avons déjà créé un domaine AWS Managed Microsoft AD et un domaine autogéré. Le réseau autogéré est connecté au VPC de l'annuaire AWS Managed Microsoft AD. Voici les propriétés des deux annuaires :

AWS Managed Microsoft AD s'exécutant sur AWS

- Nom de domaine (FQDN) : MyManagedAD.example.com
- Nom NetBIOS : MyManagedAD
- Adresses DNS : 10.0.10.246, 10.0.20.121
- CIDR VPC : 10.0.0.0/16

AWS Managed Microsoft AD géré réside dans l'ID VPC : vpc-12345678.

Domaine autogéré ou AWS Managed Microsoft AD

- Nom de domaine (FQDN) : corp.example.com
- Nom NetBIOS : CORP
- Adresses DNS : 172.16.10.153
- CIDR autogéré : 172.16.0.0/16

Étape suivante

Étape 1 : préparer votre domaine AD autogéré

Étape 1 : préparer votre domaine AD autogéré

Tout d'abord, vous devez suivre plusieurs étapes préalables sur votre domaine (sur site) autogéré.

Configurer votre pare-feu autogéré

Vous devez configurer votre pare-feu autogéré de manière à ce que les ports suivants soient ouverts aux CIDR pour tous les sous-réseaux utilisés par le VPC qui contient votre Microsoft AD géré. AWS Dans ce didacticiel, nous autorisons le trafic entrant et sortant depuis la version 10.0.0.0/16 (le bloc CIDR du VPC de notre Managed AWS Microsoft AD) sur les ports suivants :

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Authentification Kerberos
- TCP/UDP 389 - Protocole LDAP (Lightweight Directory Access Protocol)
- TCP 445 - Bloc de messages du serveur (SMB)
- TCP 9389 - Active Directory Web Services (ADWS) (facultatif - Ce port doit être ouvert si vous souhaitez utiliser votre nom NetBIOS au lieu de votre nom de domaine complet pour vous authentifier auprès d'applications telles qu'Amazon ou AWS Amazon.) WorkDocs QuickSight

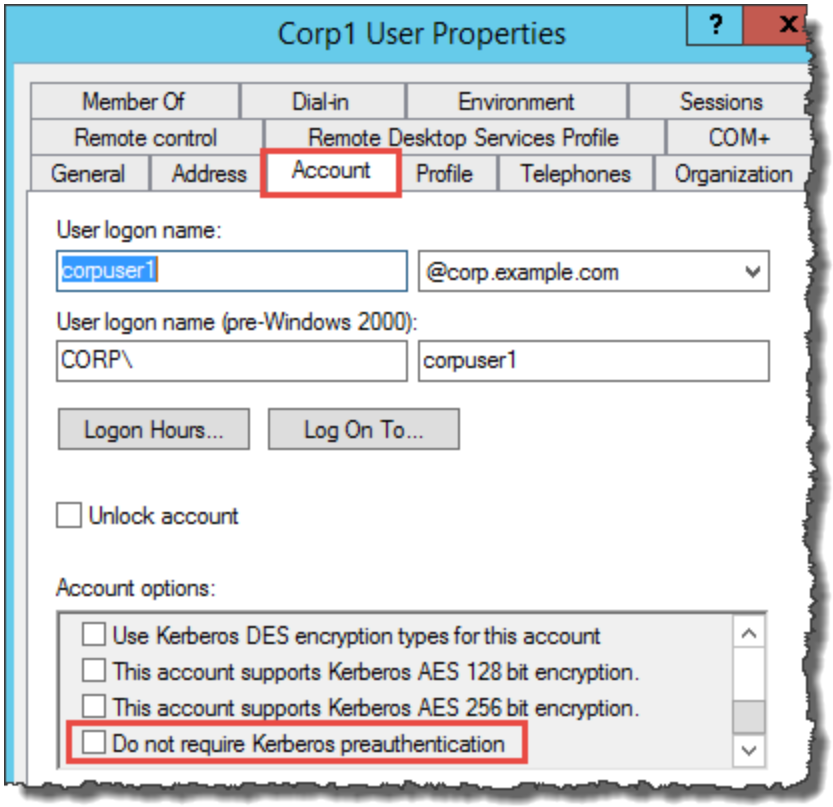
> **Note**
>
> SMBv1 n'est plus pris en charge.
> Il s'agit des ports minimum nécessaires pour connecter le VPC à l'annuaire autogéré. Votre configuration spécifique peut nécessiter l'ouverture de ports supplémentaires.

Vérification de l'activation de l'authentification préalable Kerberos

Les comptes d'utilisateur dans les deux annuaires doivent avoir une pré-authentification Kerberos activée. Il s'agit de la configuration par défaut, mais vérifiez les propriétés d'un utilisateur choisi de manière aléatoire afin de vous assurer que rien n'a changé.

Pour afficher les paramètres Kerberos de l'utilisateur

1. Sur votre contrôleur de domaine autogéré, ouvrez le Gestionnaire de serveur.
2. Dans le menu Tools, choisissez Active Directory Users and Computers.
3. Choisissez le dossier Utilisateurs et ouvrez le menu contextuel (clic droit). Sélectionnez un compte utilisateur de manière aléatoire parmi ceux répertoriés dans le volet droit. Choisissez Propriétés.
4. Choisissez l'onglet Account. Parcourez la liste Account options vers le bas pour vérifier que l'option Do not require Kerberos preauthentication n'est pas cochée.



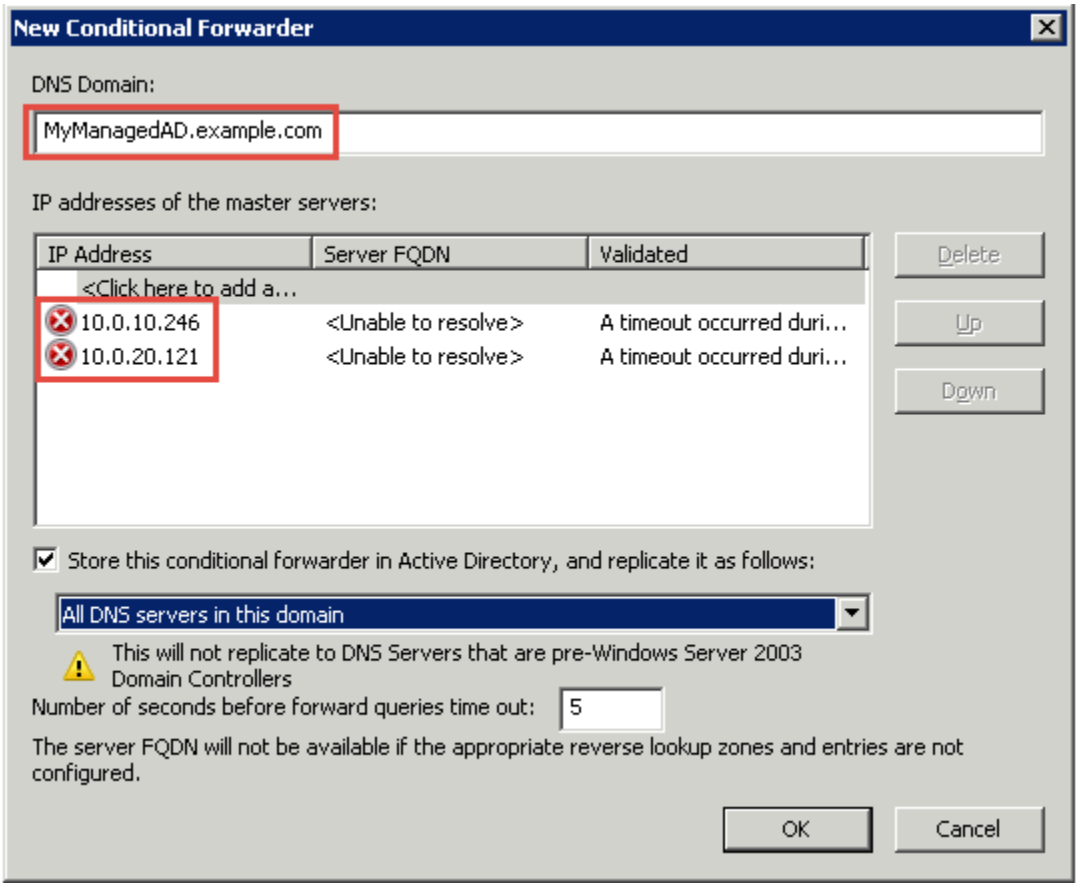
Configuration des redirecteurs conditionnels DNS pour votre domaine autogéré

Vous devez configurer des redirecteurs conditionnels DNS sur chaque domaine. Avant de procéder à cette opération sur votre domaine autogéré, vous allez d'abord obtenir des informations sur votre AWS Managed Microsoft AD.

Pour configurer les redirecteurs conditionnels sur votre domaine autogéré

1. Connectez-vous à la AWS Directory Service console AWS Management Console et ouvrez-la.
2. Dans le volet de navigation, sélectionnez Directories.
3. Choisissez l'ID de répertoire de votre AWS Managed Microsoft AD.
4. Sur la page Details (Détails), notez les valeurs des zones Directory name (Nom de l'annuaire) et DNS address (Adresse DNS) de votre annuaire.
5. Retournez maintenant à votre contrôleur de domaine autogéré. Ouvrez le Gestionnaire de serveur.
6. Dans le menu Tools, choisissez DNS.
7. Dans l'arborescence de la console, développez le serveur DNS du domaine pour lequel vous configurez la relation d'approbation. Notre serveur s'intitule WIN-5V70CN7VJ0.corp.example.com.
8. Dans l'arborescence de la console, sélectionnez Conditional Forwarders.
9. Dans le menu Action, choisissez New conditional forwarder.
10. Dans le domaine DNS, tapez le nom de domaine complet (FQDN) de votre AWS Managed Microsoft AD, comme vous l'avez indiqué précédemment. Dans cet exemple, le FQDN est MyManaged AD.Example.com.
11. Choisissez les adresses IP des serveurs principaux et saisissez les adresses DNS de votre répertoire AWS Managed Microsoft AD, comme vous l'avez indiqué précédemment. Dans cet exemple, il s'agit de : 10.0.10.246, 10.0.20.121

    Après avoir saisi les adresses DNS, il se peut que l'erreur « timeout » ou « Impossible à résoudre » s'affiche. Vous pouvez généralement ignorer ces erreurs.



12. Sélectionnez Store this conditional forwarder in Active Directory, and replicate it as follows.
13. Sélectionnez All DNS servers in this domain, puis cliquez sur OK.

Étape suivante

Étape 2 : préparer votre AWS Managed Microsoft AD

Étape 2 : préparer votre AWS Managed Microsoft AD

Préparons maintenant votre Microsoft AD AWS géré pour la relation de confiance. Une grande partie des étapes suivantes est quasi-identique aux opérations que vous venez d'effectuer pour votre domaine autogéré. Toutefois, cette fois, vous travaillez avec votre AWS Managed Microsoft AD.

Configuration de vos groupes de sécurité et sous-réseaux VPC

Vous devez autoriser le trafic de votre réseau autogéré vers le VPC contenant votre Microsoft AD AWS géré. Pour ce faire, vous devez vous assurer que les ACL associées aux sous-réseaux utilisés pour déployer votre Managed AWS Microsoft AD et les règles de groupe de sécurité configurées sur vos contrôleurs de domaine autorisent toutes deux le trafic requis pour soutenir les approbations.

Les exigences relatives aux ports varient en fonction de la version de Windows Server utilisée par vos contrôleurs de domaine et les services ou applications qui utiliseront l'approbation. Dans le cadre de ce didacticiel, vous devez ouvrir les ports suivants :

Entrant

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Authentification Kerberos
- UDP 123 - NTP
- TCP 135 - RPC
- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB
- TCP/UDP 464 - Authentification Kerberos
- TCP 636 - LDAPS (LDAP sur TLS/SSL)
- TCP 3268-3269 - Catalogue global
- TCP/UDP 49152-65535 - Ports éphémères pour RPC

> **Note**
>
> SMBv1 n'est plus pris en charge.

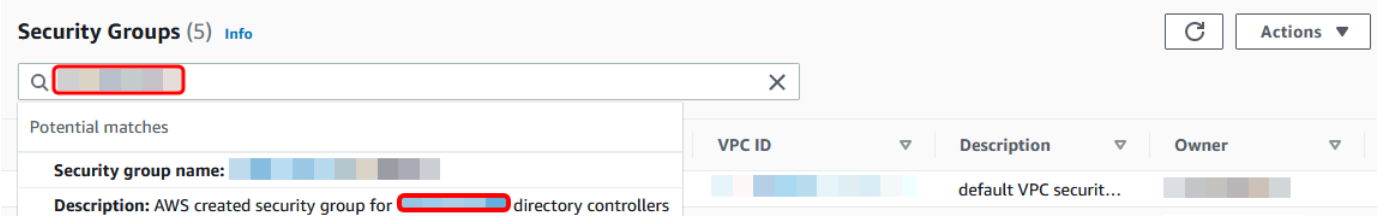
Sortant

- ALL

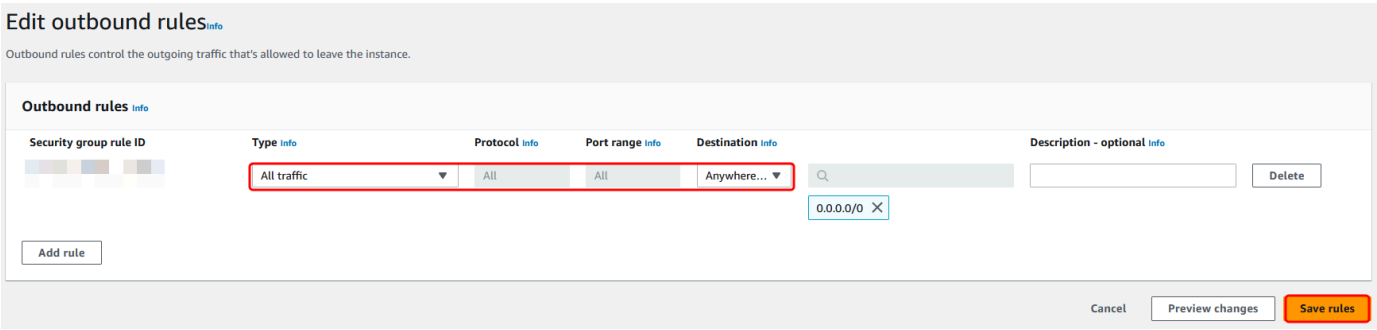
> **Note**
>
> Il s'agit des ports minimum nécessaires pour connecter le VPC et l'annuaire autogéré. Votre configuration spécifique peut nécessiter l'ouverture de ports supplémentaires.

Pour configurer les règles sortantes et entrantes de votre contrôleur de domaine Microsoft AD AWS géré

1. Revenez à la console AWS Directory Service. Dans la liste des annuaires, notez l'ID du répertoire de votre annuaire Microsoft AD AWS géré.
2. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
3. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité).
4. Utilisez le champ de recherche pour rechercher votre ID d'annuaire Microsoft AD AWS géré. Dans les résultats de recherche, sélectionnez le groupe de sécurité avec la description**`AWS created security group for yourdirectoryID directory controllers`**.



5. Accédez à l'onglet Outbound Rules de ce groupe de sécurité. Choisissez Modifier les règles sortantes, puis Ajouter une règle. Pour la nouvelle règle, saisissez les valeurs suivantes :
   - Type : ALL Traffic
   - Protocole : ALL
   - La Destination détermine le trafic qui peut quitter vos contrôleurs de domaine et où il peut aller. Indiquez une adresse IP unique ou une plage d'adresses IP dans une notation CIDR (par exemple, 203.0.113.5/32). Vous pouvez également indiquer le nom ou l'ID d'un autre groupe de sécurité dans la même région. Pour plus d'informations, consultez Comprenez la configuration et l'utilisation AWS des groupes de sécurité de votre annuaire.
6. Sélectionnez Enregistrer la règle.

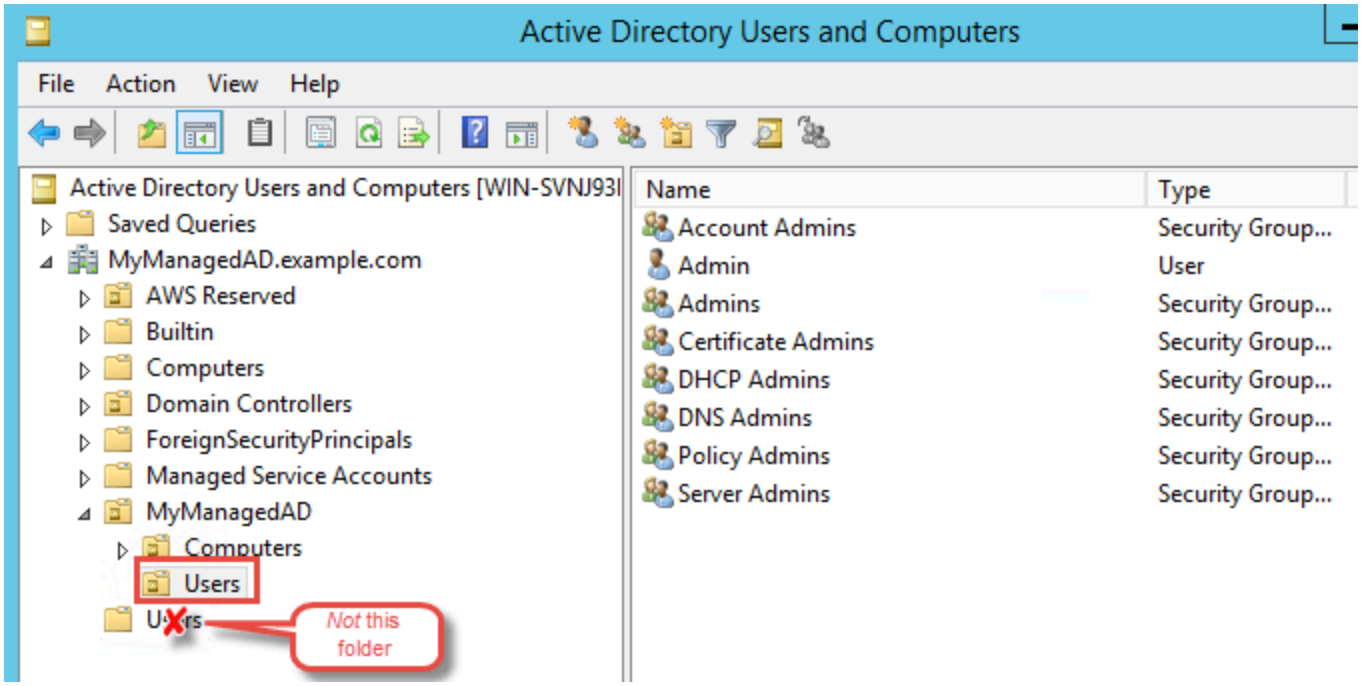


Vérification de l'activation de l'authentification préalable Kerberos

Vous souhaitez maintenant vérifier que la pré-authentification Kerberos est également activée pour les utilisateurs de votre compte Microsoft AD AWS géré. Il s'agit du même processus que celui que vous venez d'effectuer pour votre annuaire autogéré. Il s'agit de la valeur par défaut, mais nous allons vérifier que rien n'a changé.

Pour afficher les paramètres Kerberos utilisateur

1. Connectez-vous à une instance membre de votre annuaire Microsoft AD AWS géré en utilisant soit le compte correspondant au Autorisations pour le compte administrateur domaine, soit un compte auquel des autorisations ont été déléguées pour gérer les utilisateurs du domaine.
2. Si ce n'est pas encore fait, installez les outils Utilisateurs et ordinateurs Active Directory et DNS. Découvrez comment installer ces outils dans Installation des outils d'administration Active Directory pour Microsoft AD AWS géré.
3. Ouvrez le Gestionnaire de serveur. Dans le menu Tools, choisissez Active Directory Users and Computers.
4. Choisissez le dossier Users dans votre domaine. Notez qu'il s'agit du dossier Users sous votre nom NetBIOS, et non du dossier Users sous le nom de domaine complet (FQDN).



5. Dans la liste des utilisateurs, cliquez avec le bouton droit sur un utilisateur, puis choisissez Properties (Propriétés).

6. Choisissez l'onglet Account. Dans la liste Account options, vérifiez que l'option Do not require Kerberos preauthentication n'est pas cochée.

Étape suivante

Étape 3 : créer la relation d'approbation

Étape 3 : créer la relation d'approbation

Maintenant que le travail de préparation est terminé, les étapes finales consistent à créer les approbations. Dans un premier temps, commencez par créer la relation d'approbation sur votre domaine sur site, puis sur votre AWS Managed Microsoft AD. Si vous avez des problèmes lors du processus de création de la relation d'approbation, veuillez consulter Raisons liées aux statuts de création d'une relation d'approbation pour obtenir de l'aide.

Configurer l'approbation dans votre annuaire Active Directory autogéré

Dans ce didacticiel, configurez une relation d'approbation de forêt bidirectionnelle. Toutefois, si vous créez une relation d'approbation de forêt unidirectionnelle, sachez que les directions d'approbation sur chacun de vos domaines doivent être complémentaires. Par exemple, si vous créez une relation d'approbation unidirectionnelle sortante sur votre domaine autogéré, vous devez créer une relation d'approbation unidirectionnelle entrante sur votre AWS Managed Microsoft AD.

> **Note**
>
> AWS Managed Microsoft AD prend également en charge les approbations externes. Toutefois, dans le cadre de ce didacticiel, vous allez créer une approbation de forêt birectionnelle.

Pour configurer la confiance dans votre Active Directory autogéré

1. Ouvrez le Gestionnaire de serveur, puis dans le menu Tools, choisissez Active Directory Domains and Trusts.
2. Ouvrez le menu contextuel (clic droit) de votre domaine, puis choisissez Properties.
3. Choisissez l'onglet Trusts, puis choisissez New trust. Tapez le nom de votre AWS Managed Microsoft AD, puis choisissez Suivant.
4. Choisissez Forest trust. Choisissez Suivant.

5. Choisissez Two-way. Choisissez Suivant.
6. Choisissez This domain only. Choisissez Suivant.
7. Choisissez Forest-wide authentication. Choisissez Suivant.
8. Saisissez un mot de passe d'approbation. Prenez soin de retenir ce mot de passe, car vous en aurez besoin lorsque vous configurerez l'approbation pour votre AWS Managed Microsoft AD.
9. Dans la boîte de dialogue suivante, confirmez vos paramètres et choisissez Next. Confirmez que la relation d'approbation a été créée avec succès, puis choisissez à nouveau Next.
10. Choisissez No, do not confirm the outgoing trust. Choisissez Suivant.
11. Choisissez No, do not confirm the incoming trust. Choisissez Suivant.

Configurer l'approbation dans votre annuaire AWS Managed Microsoft AD

Pour finir, configurez la relation d'approbation de forêt avec votre annuaire AWS Managed Microsoft AD. Étant donné que vous avez créé une relation d'approbation de forêt bidirectionnelle sur le domaine sur site, vous devez également créer une relation d'approbation bidirectionnelle en utilisant votre annuaire AWS Managed Microsoft AD.

> **Note**
>
> Les relations d'approbation sont une fonctionnalité globale de AWS Managed Microsoft AD. Si vous utilisez Réplication multi-régions, les procédures suivantes doivent être effectuées dans Région principale. Les modifications seront appliquées automatiquement à toutes les régions répliquées. Pour en savoir plus, consultez Caractéristiques mondiales et régionales.

Pour configurer l'approbation dans votre annuaire AWS Managed Microsoft AD

1. Revenez à la console AWS Directory Service.
2. Sur la page Annuaires, choisissez votre ID AWS Managed Microsoft AD.
3. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :

   - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région principale, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour en savoir plus, consultez Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Réseau et sécurité.

4. Dans la section Trust relationships (Relations d'approbation), choisissez Actions, puis sélectionnez Add trust relationship (Ajouter une relation d'approbation).
5. Sur la page Ajouter une relation d'approbation, spécifiez le type de confiance. Dans ce cas, nous avons choisi Approbation de forêt. Entrez le nom de domaine complet de votre domaine autogéré (dans ce didacticiel **`corp.example.com`**). Tapez le même mot de passe de relation d'approbation que vous avez utilisé lors de la création de la relation d'approbation sur votre domaine autogéré. Spécifiez la direction. Dans ce cas, nous choisissons Bidirectionnelle.
6. Dans le champ Redirecteur conditionnel, entrez l'adresse IP de votre serveur DNS autogéré. Pour cet exemple, entrez 172.16.10.153.
7. (Facultatif) Choisissez Ajouter une autre adresse IP, puis entrez une deuxième adresse IP pour votre serveur DNS sur site. Vous pouvez spécifier un maximum de quatre serveurs DNS.
8. Choisissez Ajouter.

Félicitations ! Vous disposez désormais d'une relation de confiance entre votre domaine autogéré (corp.exemple.com) et votre AWS Microsoft AD géré (AD.Example.com). MyManaged Une seule relation peut être configurée entre ces deux domaines. Si vous souhaitez par exemple passer à une direction d'approbation unidirectionnelle, vous devrez tout d'abord supprimer cette relation d'approbation existante, puis en créer une autre.

Pour plus d'informations, notamment pour obtenir les instructions de vérification ou de suppression d'une approbation, veuillez consulter Création d'une relation d'approbation.

Didacticiel : créer une relation d'approbation entre deux domaines AWS Managed Microsoft AD

Ce didacticiel vous guide à travers toutes les étapes nécessaires pour configurer une relation d'approbation entre deux domaines AWS Service d'annuaire pour Microsoft Active Directory.

Rubriques

- Étape 2 : préparer votre AWS Managed Microsoft AD
- Étape 2 : créer la relation d'approbation avec un autre domaine AWS Managed Microsoft AD

Voir aussi

Création d'une relation d'approbation

Étape 2 : préparer votre AWS Managed Microsoft AD

Dans cette section, vous préparerez votre Microsoft AD AWS géré à établir une relation de confiance avec un autre Microsoft AD AWS géré. Une grande partie des étapes suivantes est quasi-identique aux opérations que vous avez effectuées pour votre domaine dans Didacticiel : créer une relation d'approbation entre votre AWS Managed Microsoft AD et votre domaine Active Directory.. Toutefois, cette fois-ci, vous configurez vos environnements Microsoft AD AWS gérés pour qu'ils fonctionnent les uns avec les autres.

Configuration de vos groupes de sécurité et sous-réseaux VPC

Vous devez autoriser le trafic d'un réseau Microsoft AD AWS géré vers le VPC contenant votre autre réseau AWS Microsoft AD géré. Pour ce faire, vous devez vous assurer que les ACL associées aux sous-réseaux utilisés pour déployer votre Managed AWS Microsoft AD et les règles de groupe de sécurité configurées sur vos contrôleurs de domaine autorisent toutes deux le trafic requis pour soutenir les approbations.

Les exigences relatives aux ports varient en fonction de la version de Windows Server utilisée par vos contrôleurs de domaine et les services ou applications qui utiliseront l'approbation. Dans le cadre de ce didacticiel, vous devez ouvrir les ports suivants :

Entrant

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Authentification Kerberos
- UDP 123 - NTP
- TCP 135 - RPC
- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB

> **Note**
>
> SMBv1 n'est plus pris en charge.

- TCP/UDP 464 - Authentification Kerberos
- TCP 636 - LDAPS (LDAP sur TLS/SSL)
- TCP 3268-3269 - Catalogue global
- TCP/UDP 1024-65535 - Ports éphémères pour RPC

Sortant

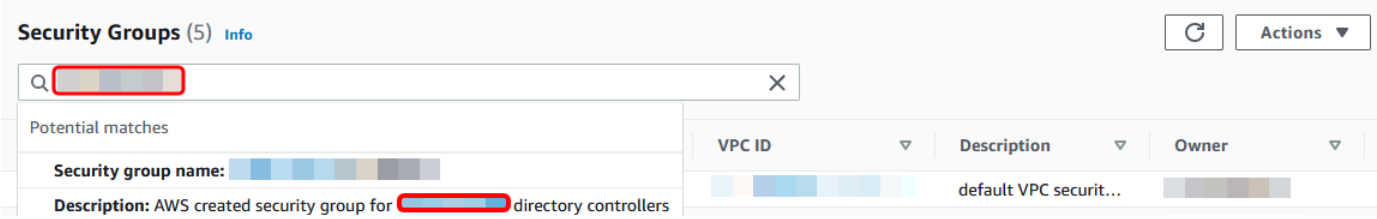
- ALL

> **Note**
>
> Il s'agit des ports minimum nécessaires pour connecter les VPC depuis les deux AWS Managed Microsoft AD. Votre configuration spécifique peut nécessiter l'ouverture de ports supplémentaires. Pour en savoir plus, veuillez consulter How to configure a firewall for Active Directory domains and trusts (français non garanti) sur le site web de Microsoft.

Pour configurer les règles sortantes de votre contrôleur de domaine Microsoft AD AWS géré

> **Note**
>
> Répétez les étapes 1 à 6 ci-dessous pour chaque annuaire.

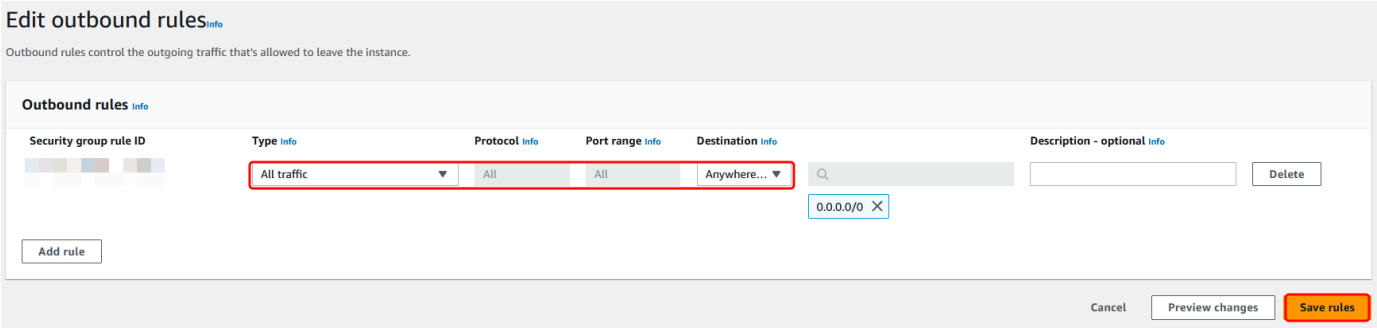
1. Accédez à la console AWS Directory Service. Dans la liste des annuaires, notez l'ID du répertoire de votre annuaire Microsoft AD AWS géré.
2. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
3. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité).
4. Utilisez le champ de recherche pour rechercher votre ID d'annuaire Microsoft AD AWS géré. Dans les résultats de recherche, sélectionnez l'élément avec la description**`AWS created security group for yourdirectoryID directory controllers`**.



5. Accédez à l'onglet Outbound Rules de ce groupe de sécurité. Choisissez Edit, puis Add another rule. Pour la nouvelle règle, saisissez les valeurs suivantes :
   - Type : ALL Traffic
   - Protocole : ALL

- La Destination détermine le trafic qui peut quitter vos contrôleurs de domaine et où il peut aller. Indiquez une adresse IP unique ou une plage d'adresses IP dans une notation CIDR (par exemple, 203.0.113.5/32). Vous pouvez également indiquer le nom ou l'ID d'un autre groupe de sécurité dans la même région. Pour plus d'informations, consultez Comprenez la configuration et l'utilisation AWS des groupes de sécurité de votre annuaire.

6. Sélectionnez Save.

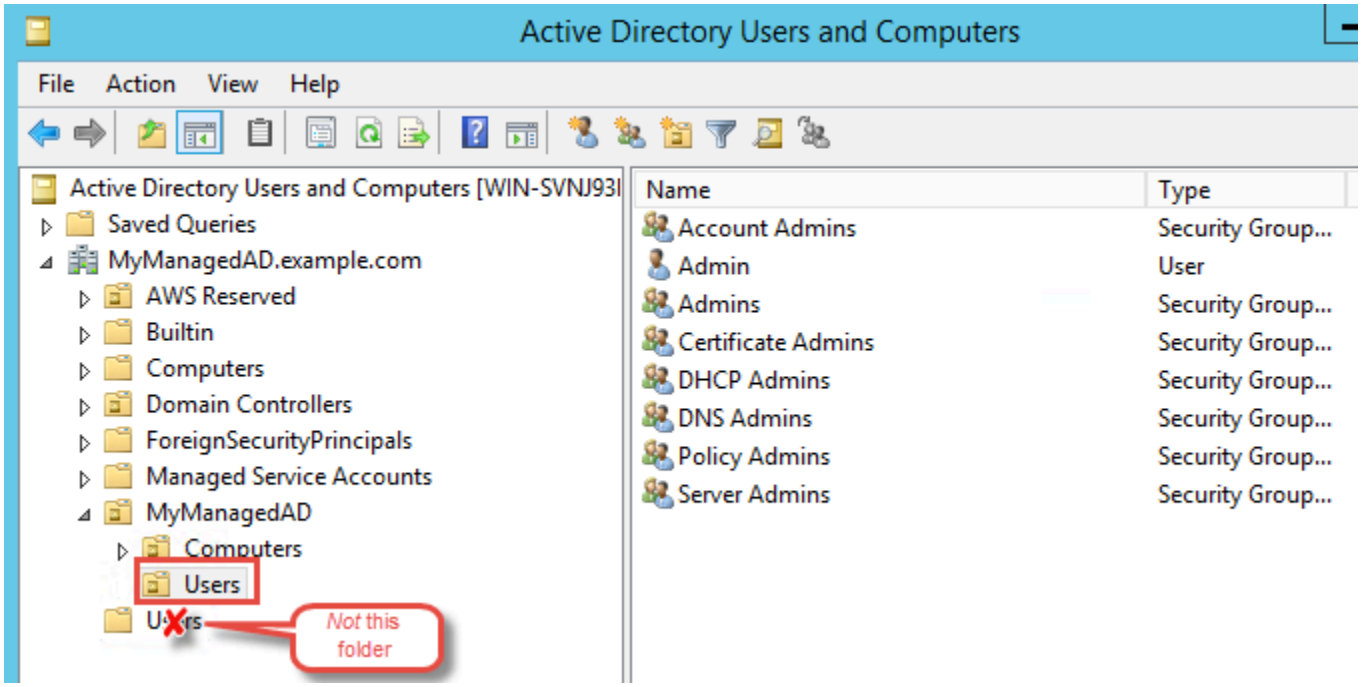


Vérification de l'activation de l'authentification préalable Kerberos

Vous souhaitez maintenant vérifier que la pré-authentification Kerberos est également activée pour les utilisateurs de votre compte Microsoft AD AWS géré. Il s'agit du même processus que celui que vous venez d'effectuer pour votre annuaire sur site. Il s'agit de la valeur par défaut, mais nous allons vérifier que rien n'a changé.

Pour afficher les paramètres Kerberos utilisateur

1. Connectez-vous à une instance membre de votre annuaire Microsoft AD AWS géré en utilisant soit le compte correspondant au Autorisations pour le compte administrateur domaine, soit un compte auquel des autorisations ont été déléguées pour gérer les utilisateurs du domaine.
2. Si ce n'est pas encore fait, installez les outils Utilisateurs et ordinateurs Active Directory et DNS. Découvrez comment installer ces outils dans Installation des outils d'administration Active Directory pour Microsoft AD AWS géré.
3. Ouvrez le Gestionnaire de serveur. Dans le menu Tools, choisissez Active Directory Users and Computers.
4. Choisissez le dossier Users dans votre domaine. Notez qu'il s'agit du dossier Users sous votre nom NetBIOS, et non du dossier Users sous le nom de domaine complet (FQDN).



5. Dans la liste des utilisateurs, cliquez avec le bouton droit sur un utilisateur, puis choisissez Properties (Propriétés).
6. Choisissez l'onglet Account. Dans la liste Account options, vérifiez que l'option Do not require Kerberos preauthentication n'est pas cochée.

Étape suivante

Étape 2 : créer la relation d'approbation avec un autre domaine AWS Managed Microsoft AD

Étape 2 : créer la relation d'approbation avec un autre domaine AWS Managed Microsoft AD

Maintenant que le travail de préparation est terminé, les étapes finales consistent à créer les approbations entre les deux domaines AWS Managed Microsoft AD. Si vous avez des problèmes lors du processus de création de la relation d'approbation, consultez Raisons liées aux statuts de création d'une relation d'approbation pour obtenir de l'aide.

Configurez l'approbation dans votre premier domaine AWS Managed Microsoft AD

Dans ce didacticiel, configurez une relation d'approbation de forêt bidirectionnelle. Toutefois, si vous créez une relation d'approbation de forêt unidirectionnelle, sachez que les directions d'approbation sur chacun de vos domaines doivent être complémentaires. Par exemple, si vous créez une relation d'approbation unidirectionnelle sortante sur ce premier domaine, vous devez créer une relation d'approbation unidirectionnelle entrante sur votre second domaine AWS Managed Microsoft AD.

> **Note**
>
> AWS Managed Microsoft AD prend également en charge les approbations externes. Toutefois, dans le cadre de ce didacticiel, vous allez créer une approbation de forêt birectionnelle.

Pour configurer l'approbation dans votre premier domaine AWS Managed Microsoft AD

1. Ouvrez la console AWS Directory Service.
2. Sur la page Annuaires, choisissez votre premier ID AWS Managed Microsoft AD.
3. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :
   - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région principale, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour de plus amples informations, veuillez consulter Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Réseau et sécurité.
4. Dans la section Trust relationships (Relations d'approbation), choisissez Actions, puis sélectionnez Add trust relationship (Ajouter une relation d'approbation).
5. Sur la page Ajouter une relation d'approbation, saisissez le nom de domaine complet de votre deuxième domaine AWS Managed Microsoft AD. Prenez soin de retenir ce mot de passe, car vous en aurez besoin lorsque vous configurerez l'approbation pour votre second AWS Managed Microsoft AD. Spécifiez la direction. Dans ce cas, nous choisissons Bidirectionnelle.
6. Dans le champ Redirecteur conditionnel, entrez l'adresse IP de votre second serveur DNS AWS Managed Microsoft AD.
7. (Facultatif) Choisissez Ajouter une autre adresse IP, puis entrez une seconde adresse IP pour votre second serveur DNS AWS Managed Microsoft AD. Vous pouvez spécifier un maximum de quatre serveurs DNS.
8. Choisissez Ajouter. L'approbation échouera à ce stade, ce qui est prévisible jusqu'à ce que nous ayons créé l'autre côté de l'approbation.

Configurez l'approbation dans votre second domaine AWS Managed Microsoft AD

Maintenant, configurez la relation d'approbation de forêt avec votre second annuaire AWS Managed Microsoft AD. Étant donné que vous avez créé une relation d'approbation de forêt bidirectionnelle

sur le premier domaine AWS Managed Microsoft AD, vous devez également créer une approbation bidirectionnelle en utilisant ce domaine AWS Managed Microsoft AD.

Pour configurer l'approbation dans votre second domaine AWS Managed Microsoft AD

1. Revenez à la console AWS Directory Service.
2. Sur la page Annuaires, choisissez votre second ID AWS Managed Microsoft AD.
3. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :
   - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région principale, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour de plus amples informations, veuillez consulter Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Réseau et sécurité.
4. Dans la section Trust relationships (Relations d'approbation), choisissez Actions, puis sélectionnez Add trust relationship (Ajouter une relation d'approbation).
5. Sur la page Ajouter une relation d'approbation, saisissez le nom de domaine complet de votre premier domaine AWS Managed Microsoft AD. Tapez le même mot de passe de relation d'approbation que vous avez utilisé lors de la création de la relation d'approbation sur votre domaine sur site. Spécifiez la direction. Dans ce cas, nous choisissons Bidirectionnelle.
6. Dans le champ Redirecteur conditionnel, entrez l'adresse IP de votre premier serveur DNS AWS Managed Microsoft AD.
7. (Facultatif) Choisissez Ajouter une autre adresse IP, puis entrez une seconde adresse IP pour votre premier serveur DNS AWS Managed Microsoft AD. Vous pouvez spécifier un maximum de quatre serveurs DNS.
8. Choisissez Ajouter. L'approbation doit être vérifiée peu de temps après.
9. Revenez maintenant à l'approbation que vous avez créée dans le premier domaine et vérifiez à nouveau la relation d'approbation.

Félicitations ! Vous disposez désormais d'une relation d'approbation entre vos deux domaines AWS Managed Microsoft AD. Une seule relation peut être configurée entre ces deux domaines. Si vous souhaitez par exemple passer à une direction d'approbation unidirectionnelle, vous devrez tout d'abord supprimer cette relation d'approbation existante, puis en créer une autre.

Connectez votre Microsoft AD AWS géré à Microsoft Entra Connect Sync

Ce didacticiel vous explique les étapes nécessaires à l'installation Microsoft Entra Connect Syncpour vous synchroniser avec votre Microsoft Entra ID AWS Managed Microsoft AD.

Dans ce didacticiel, vous effectuez les opérations suivantes :

1. Créez un utilisateur de domaine Microsoft AD AWS géré.
2. Téléchargement Entra Connect Sync.
3. Windows PowerShellÀ utiliser pour exécuter un script afin de fournir les autorisations appropriées à l'utilisateur nouvellement créé.
4. Installer Entra Connect Sync.

Prérequis

Vous aurez besoin des éléments suivants pour suivre ce didacticiel :

- Un Microsoft AD AWS géré. Pour plus d'informations, consultez the section called “Créez votre Microsoft AD AWS géré”.
- Une instance de Windows serveur Amazon EC2 jointe à votre AWS Microsoft AD géré. Pour plus d'informations, consultez Rejoindre facilement une instance Windows.
- Un Windows serveur EC2 Active Directory Administration Tools installé pour gérer votre Microsoft AD AWS géré. Pour plus d'informations, consultez the section called “Installation des outils d'administration AD pour Microsoft AD AWS géré”.

Étape 1 : créer un utilisateur Active Directory de domaine

Ce didacticiel part du principe que vous disposez déjà d'une instance Microsoft AD AWS gérée et d'une instance de Windows serveur EC2 Active Directory Administration Tools installées. Pour plus d'informations, consultez the section called “Installation des outils d'administration AD pour Microsoft AD AWS géré”.

1. Connectez-vous à l'instance sur laquelle Active Directory Administration Tools ils ont été installés.
2. Créez un utilisateur de domaine Microsoft AD AWS géré. Cet utilisateur deviendra le Active Directory Directory Service (AD DS) Connector account pourEntra Connect Sync. Pour connaître les étapes détaillées de ce processus, voirthe section called “Créez un utilisateur”.

Étape 2 : Téléchargement Entra Connect Sync

- Téléchargez Entra Connect Sync depuis le Microsoftsite Web sur l'instance EC2 qui est l'administrateur Microsoft AD AWS géré.

> **Warning**
>
> Ne l'ouvrez pas ou ne Entra Connect Sync l'exécutez pas à ce stade. Les prochaines étapes fourniront les autorisations nécessaires à l'utilisateur de votre domaine créé à l'étape 1.

Étape 3 : Exécuter Windows PowerShell le script

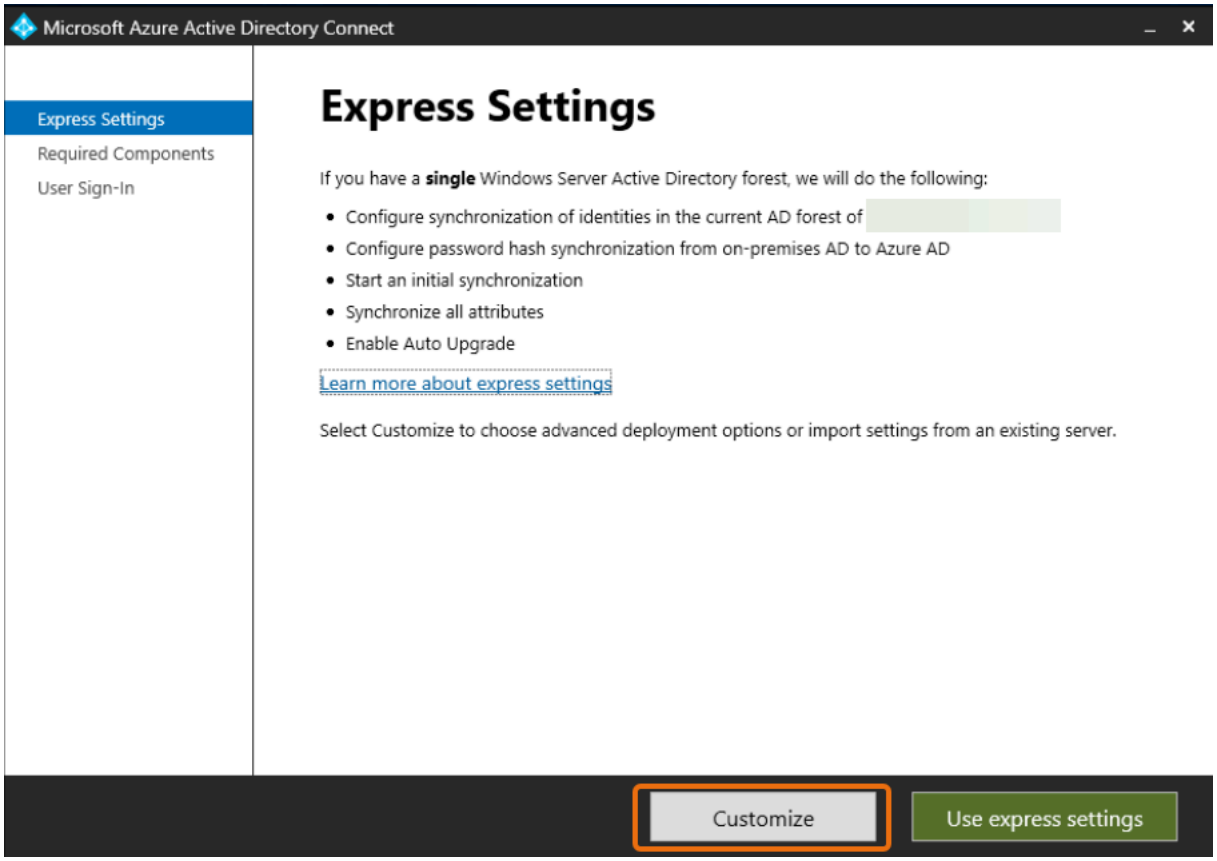
- Ouvrez PowerShell en tant qu'administrateur et exécutez le script suivant. Pendant l'exécution du script, il vous sera demandé de saisir le sAM AccountName pour le nouvel utilisateur de domaine créé à l'étape 1.

```
$modulePath = "C:\Program Files\Microsoft Azure Active Directory Connect\AdSyncConfig
\AdSyncConfig.psm1"

try {
    # Attempt to import the module
    Write-Host -ForegroundColor Green "Importing Module for Azure Entra Connect..."
    Import-Module $modulePath -ErrorAction Stop
    Write-Host -ForegroundColor Green "Success!"
}
catch {
    # Display the exception message
    Write-Host -ForegroundColor Red "An error occurred: $($_.Exception.Message)"
}

Function Set-EntraConnectSvcPerms {
    [CmdletBinding()]
    Param (
        [String]$ServiceAccountName
    )

    #Requires -Modules 'ActiveDirectory' -RunAsAdministrator

    Try {
```

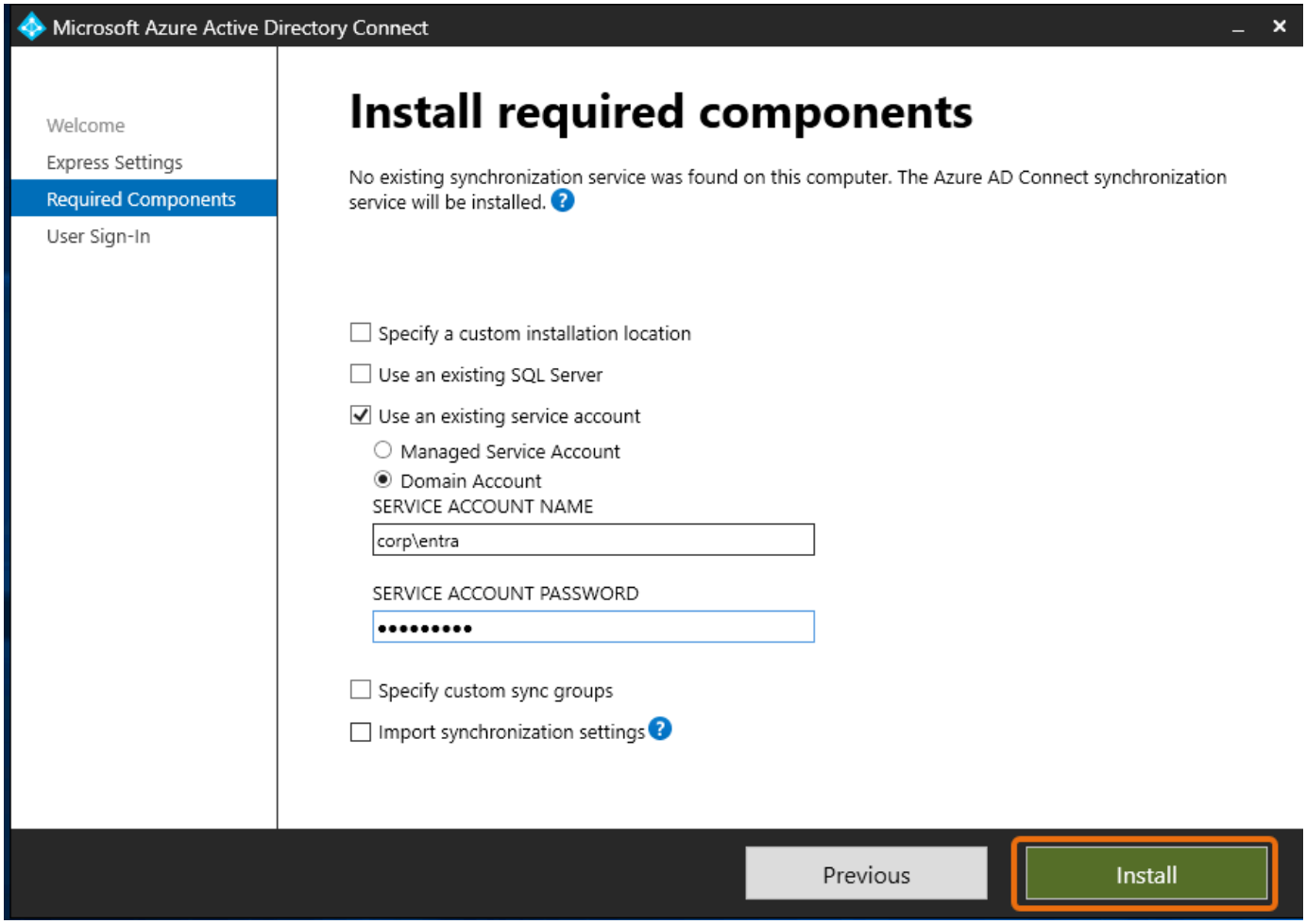
```
        $Domain = Get-ADDomain -ErrorAction Stop
    } Catch [System.Exception] {
        Write-Output "Failed to get AD domain information $_"
    }

    $BaseDn = $Domain | Select-Object -ExpandProperty 'DistinguishedName'
    $Netbios = $Domain | Select-Object -ExpandProperty 'NetBIOSName'

    Try {
        $OUs = Get-ADOrganizationalUnit -SearchBase "OU=$Netbios,$BaseDn" -
SearchScope 'Onelevel' -Filter * -ErrorAction Stop | Select-Object -ExpandProperty
 'DistinguishedName'
    } Catch [System.Exception] {
        Write-Output "Failed to get OUs under OU=$Netbios,$BaseDn $_"
    }

    Try {
        $ADConnectorAccountDN = Get-ADUser -Identity $ServiceAccountName -ErrorAction
 Stop | Select-Object -ExpandProperty 'DistinguishedName'
    } Catch [System.Exception] {
        Write-Output "Failed to get service account DN $_"
    }

    Foreach ($OU in $OUs) {
        try {
        Set-ADSyncMsDsConsistencyGuidPermissions -ADConnectorAccountDN
 $ADConnectorAccountDN -ADobjectDN $OU -Confirm:$false -ErrorAction Stop
        Write-Host "Permissions set successfully for $ADConnectorAccountDN and $OU"

        Set-ADSyncBasicReadPermissions -ADConnectorAccountDN $ADConnectorAccountDN -
ADobjectDN $OU -Confirm:$false -ErrorAction Stop
        Write-Host "Basic read permissions set successfully for $ADConnectorAccountDN
 on OU $OU"
    }
    catch {
        Write-Host "An error occurred while setting permissions for
 $ADConnectorAccountDN on OU $OU : $_"
    }
    }
}
```

Étape 4 : installation de Entra Connect Sync

1. Une fois le script terminé, vous pouvez exécuter le fichier de configuration téléchargé Microsoft Entra Connect (anciennement connu sous le nom de fichierAzure Active Directory Connect).
2. Une Microsoft Azure Active Directory Connect fenêtre s'ouvre après l'exécution du fichier de configuration de l'étape précédente. Dans la fenêtre Express Settings, sélectionnez Personnaliser.



3. Dans la fenêtre Installer les composants requis, cochez la case Utiliser un compte de service existant. Dans NOM DU COMPTE DE SERVICE et MOT DE PASSE DU COMPTE DE SERVICE, entrez le AD DS Connector account nom et le mot de passe de l'utilisateur que vous avez créé à l'étape 1. Par exemple, si votre AD DS Connector account nom est`entra`, le nom du compte sera`corp\entra`. Sélectionnez ensuite Installer.



4. Dans la fenêtre de connexion de l'utilisateur, sélectionnez l'une des options suivantes :

   a. Authentification directe - Cette option vous permet de vous connecter à votre compte à l'aide de votre nom d'utilisateur et Active Directory de votre mot de passe.

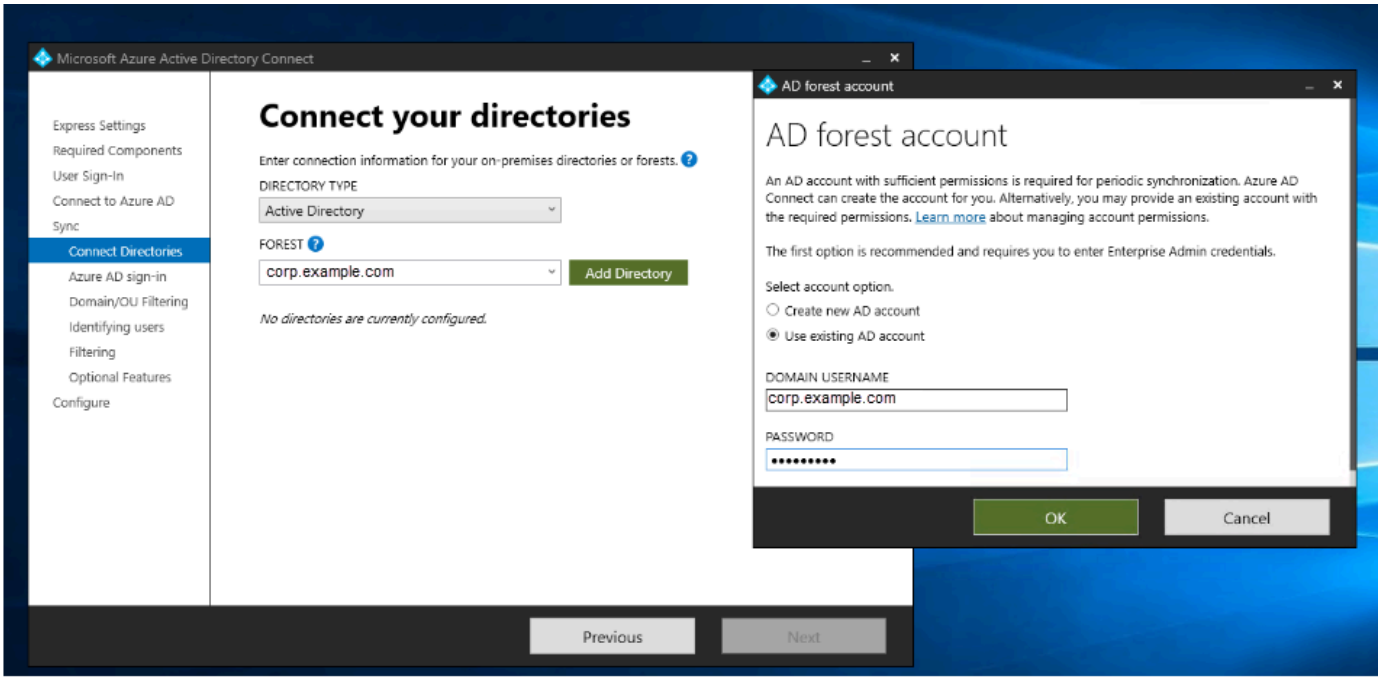
   b. Ne pas configurer : cela vous permet d'utiliser la connexion fédérée avec Microsoft Entra (anciennement connue sous le nom de Azure Active Directory (AzureAD)) ouOffice 365.

   Sélectionnez ensuite Next.

5. Dans la Azure fenêtre Connect to, entrez votre nom d'utilisateur et votre mot de passe d'administrateur global, Entra ID puis sélectionnez Next.

6. Dans la fenêtre Connect your directories, sélectionnez Active DirectoryDIRECTORY TYPE. Choisissez la forêt pour votre AWS Managed Microsoft AD for FOREST. Sélectionnez ensuite Ajouter un répertoire.

7. Une fenêtre contextuelle s'affiche pour vous demander les options de votre compte. Sélectionnez Utiliser un compte AD existant. Entrez le AD DS Connector account nom d'utilisateur et le mot de passe créés à l'étape 1, puis sélectionnez OK. Sélectionnez ensuite Next.



8. Dans la fenêtre de Azure ADconnexion, sélectionnez Continuer sans associer tous les suffixes UPN aux domaines vérifiés, uniquement si aucun domaine personnalisé vérifié n'y a été ajouté. Entra ID Sélectionnez ensuite Next.
9. Dans la fenêtre de filtrage des domaines/OU, sélectionnez les options qui répondent à vos besoins. Pour plus d'informations, voir Entra Connect Sync: Configurer le filtrage dans Microsoft la documentation. Sélectionnez ensuite Next.
10. Dans la fenêtre Identification des utilisateurs, filtrage et fonctionnalités facultatives, conservez les valeurs par défaut et sélectionnez Suivant.
11. Dans la fenêtre Configurer, passez en revue les paramètres de configuration et sélectionnez Configurer. L'installation de Entra Connect Sync sera finalisée et les utilisateurs commenceront à se synchroniser avecMicrosoft Entra ID.

Étendre votre schéma

AWS Managed Microsoft AD utilise des schémas pour organiser et appliquer la façon dont les données d'annuaire sont stockées. Le processus d'ajout de définitions au schéma est appelé « extension de schéma ». Les extensions de schéma vous permettent de modifier le schéma de votre annuaire AWS Managed Microsoft AD à l'aide d'un fichier LDAP Data Interchange Format (LDIF)

valide. Pour plus d'informations sur les schémas AD et comment étendre votre schéma, consultez les rubriques ci-dessous.

Rubriques

- Quand étendre votre schéma AWS Managed Microsoft AD
- Tutoriel : extension de votre schéma Microsoft AD AWS géré

Quand étendre votre schéma AWS Managed Microsoft AD

Vous pouvez étendre votre schéma AWS Managed Microsoft AD en ajoutant de nouveaux attributs et de nouvelles classes d'objet. Par exemple, vous pouvez exécuter cette action si vous disposez d'une application qui nécessite d'apporter des modifications à votre schéma afin de prendre en charge les fonctions d'authentification unique.

Vous pouvez également utiliser des extensions de schéma pour activer la prise en charge des applications qui reposent sur des attributs et classes d'objet Active Directory spécifiques. Cela peut s'avérer particulièrement utile si vous avez besoin de migrer des applications d'entreprise qui dépendent de AWS Managed Microsoft AD vers le cloud AWS.

Chaque attribut ou classe ajouté(e) à un schéma Active Directory existant doit être défini(e) avec un ID unique. De cette manière, lorsque les entreprises ajoutent des extensions au schéma, ces dernières sont assurées d'être uniques et de ne pas entrer en conflit les unes avec les autres. Ces ID sont appelés Identificateurs d'objet (OID) AD et sont stockés dans AWS Managed Microsoft AD.

Consultez Tutoriel : extension de votre schéma Microsoft AD AWS géré pour démarrer.

Rubriques en relation

- Étendre votre schéma
- Éléments du schéma

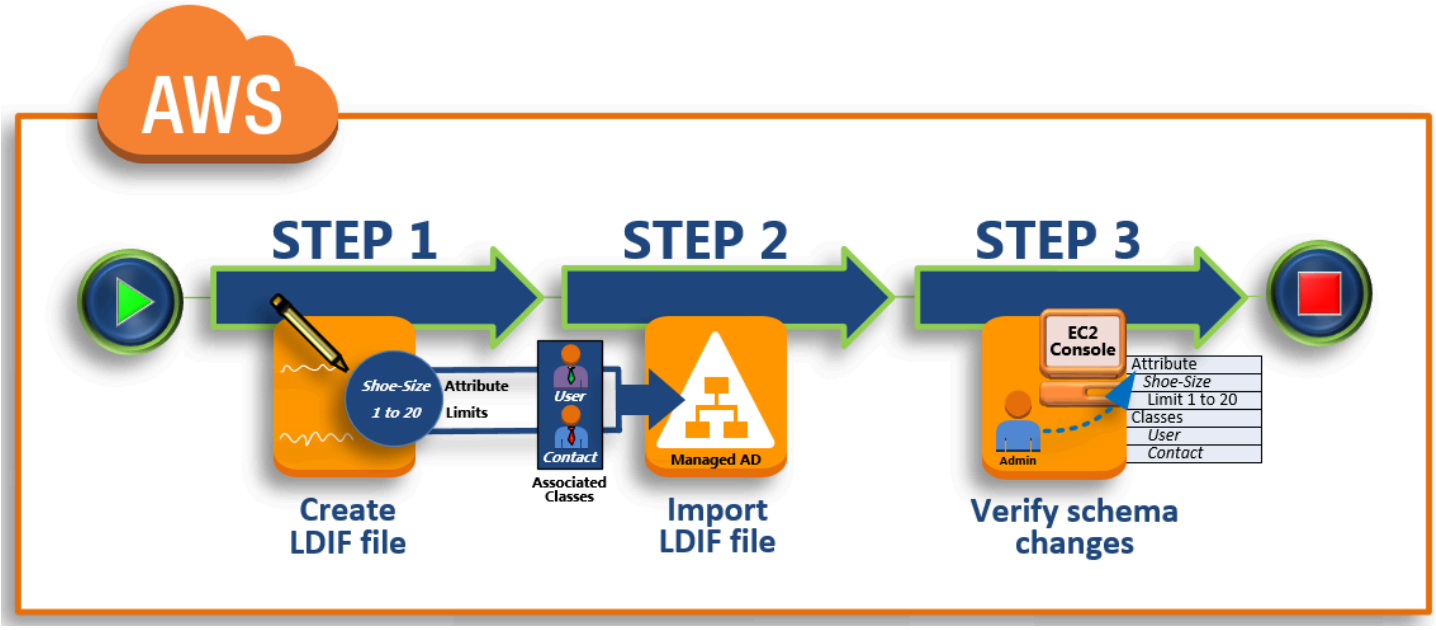
Tutoriel : extension de votre schéma Microsoft AD AWS géré

Dans ce didacticiel, vous allez apprendre à étendre le schéma de votre AWS annuaire Directory Service for Microsoft Active Directory, également connu sous le nom de AWS Managed Microsoft AD, en ajoutant des attributs et des classes uniques répondant à vos besoins spécifiques. AWS Les extensions de schéma Microsoft AD gérées ne peuvent être téléchargées et appliquées qu'à l'aide d'un fichier de script LDIF (Lightweight Directory Interchange Format) valide.

Les attributs (attributeSchema) définissent les champs de la base de données, tandis que les classes (classSchema) définissent les tables de la base de données. Par exemple, tous les objets utilisateur dans Active Directory sont définis par la classe de schéma Utilisateur, tandis que les propriétés individuelles d'un utilisateur, telles que l'adresse e-mail ou le numéro de téléphone, sont chacune définies par un attribut.

Si vous souhaitez ajouter une nouvelle propriété, telle que la taille de chaussure, vous définissez un nouvel attribut, qui serait de type entier. Vous pouvez également définir des limites inférieure et supérieure allant de 1 à 20. Une fois que l'objet attributeSchema taille de chaussure a été créé, vous modifiez ensuite l'objet classSchema Utilisateur pour contenir cet attribut. Les attributs peuvent être liés à plusieurs classes. La taille de chaussure peut être ajoutée à la classe Contact par exemple. Pour plus d'informations sur les schémas Active Directory, veuillez consulter Quand étendre votre schéma AWS Managed Microsoft AD.

Ce flux de travail se compose de trois étapes de base.



Étape 1 : créer votre fichier LDIF

Tout d'abord, vous créez un fichier LDIF et définissez les nouveaux attributs et les classes auxquelles ils doivent être ajoutés. Vous utilisez ce fichier pour la prochaine étape du flux de travail.

Étape 2 : importer votre fichier LDIF

Au cours de cette étape, vous devez utiliser la AWS Directory Service console pour importer le fichier LDIF dans votre environnement Microsoft Active Directory.

Étape 3 : vérifier si l'extension de schéma a réussi

Enfin, en tant qu'administrateur, vous utilisez une instance EC2 pour vérifier que les nouvelles extensions apparaissent dans le composant logiciel enfichable du schéma Active Directory.

Étape 1 : créer votre fichier LDIF

Un fichier LDIF est un format d'échange de données standard en texte brut qui représente le contenu de l'annuaire LDAP (Lightweight Directory Access Protocol) et les demandes de mise à jour. LDIF transmet le contenu de l'annuaire en tant qu'ensemble d'enregistrements, un enregistrement pour chaque objet (ou entrée). Il représente également des demandes de mise à jour, comme Ajouter, Modifier, Supprimer et Renommer en tant qu'ensemble d'enregistrements, un enregistrement pour chaque demande de mise à jour.

AWS Directory Service Importe ensuite votre fichier LDIF avec les modifications de schéma en exécutant l'`ldifde.exe`application sur votre répertoire AWS Microsoft AD géré. Par conséquent, vous trouvez utile pour comprendre la syntaxe de script LDIF. Pour plus d'informations, veuillez consulter LDIF Scripts (français non garanti).

Plusieurs outils LDIF tiers peuvent extraire, nettoyer et mettre à jour vos mises à jour de schéma. Quel que soit l'outil utilisé, vous devez comprendre que tous les identificateurs utilisés dans votre fichier LDIF doivent être uniques.

Nous vous recommandons vivement d'examiner les concepts et conseils suivants avant de créer votre fichier LDIF.

- Éléments du schéma : découvrez les éléments du schéma tels que les attributs, les classes, les ID d'objet et les attributs liés. Pour plus d'informations, consultez Éléments du schéma.

- Séquence d'éléments : veillez à ce que l'ordre dans lequel les éléments de votre fichier LDIF sont disposés respecte le Directory Information Tree (DIT) de haut en bas. Les règles générales pour effectuer le séquençage d'un fichier LDIF incluent les éléments suivants :

  - Séparer les éléments par une ligne vide.
  - Répertorier les éléments enfants en fonction de leurs éléments parents.
  - Veillez à ce que des éléments tels que des attributs ou des classes d'objet existent dans le schéma. S'ils ne sont pas présents, vous devez les ajouter au schéma avant qu'ils puissent être

utilisés. Par exemple, avant que vous puissiez assigner un attribut à une classe, ce dernier doit être créé.

- Format du DN : pour chaque nouvelle instruction dans le fichier LDIF, définissez le nom unique (DN) en tant que première ligne de l'instruction. Le DN identifie un objet Active Directory au sein de l'arborescence de l'objet Active Directory et doit comporter les composants du domaine pour votre annuaire. Par exemple, les composants du domaine pour l'annuaire dans ce didacticiel sont `DC=example,DC=com`.

  Le DN doit contenir le nom commun (CN) de l'objet Active Directory. La première entrée de CN est le nom de l'attribut ou de la classe. Ensuite, vous devez utiliser `CN=Schema,CN=Configuration`. Ce CN garantit que vous pouvez étendre le schéma Active Directory. Comme mentionné auparavant, vous ne pouvez pas ajouter ou modifier le contenu des objets Active Directory. Le format général pour un DN suit.

  ```
  dn: CN=[attribute or class name],CN=Schema,CN=Configuration,DC=[domain_name]
  ```

  Pour ce didacticiel, le DN pour le nouvel attribut taille de chaussure ressemblerait à :

  ```
  dn: CN=Shoe-Size,CN=Schema,CN=Configuration,DC=example,DC=com
  ```

- Avertissements – Examinez les avertissements avant d'étendre votre schéma.
  - Avant d'étendre votre schéma Active Directory, il est important d'examiner les avertissements de Microsoft sur l'impact de cette opération. Pour plus d'informations, veuillez consulter What You Must Know Before Extending the Schema (français non garanti).
  - Vous ne pouvez pas supprimer un attribut ou une classe de schéma. Par conséquent, si vous faites une erreur et ne voulez pas restaurer à partir d'une sauvegarde, vous pouvez uniquement désactiver l'objet. Pour plus d'informations, veuillez consulter Disabling Existing Classes and Attributes (français non garanti).
  - Les modifications apportées à ne defaultSecurityDescriptor sont pas prises en charge.

Pour en savoir plus sur le mode de construction des fichiers LDIF et consulter un exemple de fichier LDIF pouvant être utilisé pour tester les extensions de schéma AWS Microsoft AD gérées, consultez l'article Comment étendre votre schéma de répertoire AWS Microsoft AD géré sur le blog de sécurité. AWS

Étape suivante

Étape 2 : importer votre fichier LDIF

Étape 2 : importer votre fichier LDIF

Vous pouvez étendre votre schéma en important un fichier LDIF depuis la AWS Directory Service console ou à l'aide de l'API. Pour plus d'informations sur la procédure avec les API d'extension de schéma, veuillez consulter AWS Directory Service API Reference (français non garanti). Pour l'instant, AWS ne prend pas en charge les applications externes, telles que Microsoft Exchange, pour d'effectuer directement les mises à jour de schéma.

> **Important**
>
> Lorsque vous mettez à jour votre schéma d'annuaire Microsoft AD AWS géré, l'opération n'est pas réversible. En d'autres termes, une fois que vous créez une nouvelle classe ou un nouvel attribut, Active Directory ne vous autorise pas à la ou le supprimer. Cependant, vous pouvez la ou le désactiver.
> Si vous devez supprimer les modifications de schéma, une option consiste à restaurer l'annuaire à partir d'un instantané précédent. La restauration d'un instantané restaure à la fois le schéma et les données de l'annuaire à un point précédent, pas uniquement le schéma.
> Remarque : la durée maximale prise en charge pour un instantané est de 180 jours. Pour plus d'informations, veuillez consulter la section Useful shelf life of a system-state backup of Active Directory (français non garanti) sur le site web Microsoft.

Avant le début du processus de mise à jour, AWS Managed Microsoft AD prend un instantané pour conserver l'état actuel de votre annuaire.

> **Note**
>
> Les extensions de schéma sont une fonctionnalité globale de AWS Managed Microsoft AD. Si vous utilisez Réplication multi-régions, les procédures suivantes doivent être effectuées dans Région principale. Les modifications seront appliquées automatiquement à toutes les régions répliquées. Pour plus d'informations, consultez Caractéristiques mondiales et régionales.

Pour importer votre fichier LDIF

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).

2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :
   - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région principale, puis cliquez sur l'onglet Maintenance. Pour plus d'informations, consultez Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Maintenance.
4. Dans la sectionSchema extensions (Extensions de schéma), choisissez Actions, puis sélectionnez Upload and update schema (Charger et mettre à jour le schéma).
5. Dans la boîte de dialogue, cliquez sur Parcourir, sélectionnez un fichier LDIF valide, saisissez une description, puis choisissez Update Schema.

> **Important**
>
> L'extension du schéma est une opération critique. N'appliquez aucune mise à jour de schéma à un environnement de production sans l'avoir d'abord tester avec votre application dans un environnement de développement ou de test.

Comment le fichier LDIF est appliqué

Une fois votre fichier LDIF chargé, Managed AWS Microsoft AD prend des mesures pour protéger votre répertoire contre les erreurs en appliquant les modifications dans l'ordre suivant.

1. Valide le fichier LDIF. Étant donné que les scripts LDIF peuvent manipuler n'importe quel objet du domaine, AWS Managed Microsoft AD effectue des vérifications juste après le téléchargement pour s'assurer que l'opération d'importation n'échouera pas. Ces vérifications garantissent les points suivants :
   - Les objets à mettre à jour se trouvent uniquement dans le conteneur de schéma
   - La partie des DC (contrôleurs de domaine) correspond au nom du domaine dans lequel le script LDIF est en cours d'exécution
2. Prend un instantané de votre annuaire. Vous pouvez utiliser l'instantané pour restaurer votre annuaire au cas où vous rencontrez des problèmes avec votre application après la mise à jour du schéma.

3. Applique les modifications à un seul DC. AWS Managed Microsoft AD isole l'un de vos contrôleurs de domaine et applique les mises à jour du fichier LDIF au contrôleur de domaine isolé. Ensuite, il sélectionne l'un de vos DC pour être le schéma principal, supprime ce DC de la réplication de l'annuaire, et applique votre fichier LDIF à l'aide de `Ldifde.exe`.
4. La réplication s'effectue sur tous les contrôleurs de domaine. AWS Managed Microsoft AD réintègre le contrôleur de domaine isolé à la réplication pour terminer la mise à jour. Pendant ce temps, votre annuaire continue de fournir l'Active Directory Service à vos applications sans interruption.

Étape suivante

Étape 3 : vérifier si l'extension de schéma a réussi

Étape 3 : vérifier si l'extension de schéma a réussi

Lorsque vous avez terminé le processus d'importation, il est important de vérifier que les mises à jour de schéma ont été appliquées à votre annuaire. Cette étape est particulièrement importante avant de migrer ou mettre à jour toute application s'appuyant sur la mise à jour de schéma. Pour ce faire, utilisez différents outils LDAP ou écrivez un outil de test qui émet les commandes LDAP appropriées.

Cette procédure utilise le composant logiciel enfichable du schéma Active Directory et/ou PowerShell pour vérifier que les mises à jour du schéma ont été appliquées. Vous devez exécuter ces outils à partir d'un ordinateur joint au domaine à votre AWS Managed Microsoft AD. Il peut s'agir d'un serveur Windows en cours d'exécution dans votre réseau sur site avec accès à votre Virtual Private Cloud (VPC) ou via une connexion de réseau privé virtuel (VPN). Vous pouvez également exécuter ces outils sur une instance Windows Amazon EC2 (consultez Comment lancer une nouvelle instance EC2 avec une jonction de domaine continue).

Pour vérifier à l'aide du composant logiciel enfichable du schéma Active Directory

1. Installez le composant logiciel enfichable du schéma Active Directory en suivant les instructions du site TechNetWeb.
2. Ouvrez la Microsoft Management Console (MMC) et développez l'arborescence Schéma AD pour votre annuaire.
3. Parcourez les dossiers Classes et Attributs jusqu'à ce que vous trouviez les modifications de schéma que vous avez fait précédemment.

Pour vérifier en utilisant PowerShell

1. Ouvrez une PowerShell fenêtre.
2. Utilisez l'applet de commande `Get-ADObject` comme illustré ci-dessous pour vérifier la modification de schéma. Par exemple :

   ```
   get-adobject -Identity 'CN=Shoe-
   Size,CN=Schema,CN=Configuration,DC=example,DC=com' -Properties *
   ```

Étape facultative

Ajouter une valeur au nouvel attribut - Facultatif

Ajouter une valeur au nouvel attribut - Facultatif

Utilisez cette étape facultative lorsque vous avez créé un nouvel attribut et que vous souhaitez ajouter une nouvelle valeur à l'attribut dans votre annuaire Microsoft AD AWS géré.

Pour ajouter une valeur à un attribut

1. Ouvrez l'utilitaire de ligne de Windows PowerShell commande et définissez le nouvel attribut à l'aide de la commande suivante. Dans cet exemple, nous allons ajouter une nouvelle valeur EC2InstanceID à l'attribut pour un ordinateur spécifique.

   ```
   PS C:\> set-adcomputer -Identity computer name -add @{example-
   EC2InstanceID = 'EC2 instance ID'}
   ```
2. Vous pouvez valider si la valeur EC2InstanceID a été ajoutée à l'objet ordinateur en exécutant la commande suivante :

   ```
   PS C:\> get-adcomputer -Identity computer name –Property example-
   EC2InstanceID
   ```

Ressources connexes

Les liens de ressource suivants se trouvent sur le site web Microsoft et fournissent des informations connexes.

- Extension du schéma (Windows)
- Schéma Active Directory (Windows)

- Schéma Active Directory
- Administration Windows : Extension du schéma Active Directory
- Restrictions sur l'extension du schéma (Windows)
- Ldifde

Gérez votre répertoire Microsoft AD AWS géré

Cette section décrit comment gérer les tâches administratives courantes pour votre environnement Microsoft AD AWS géré.

Rubriques

- Ajout de suffixes UPN alternatifs
- Supprimer votre Microsoft AD AWS géré
- Modifier le nom de site de votre annuaire
- Création d'un instantané ou d'une restauration de votre annuaire
- Mettez à niveau votre Microsoft AD AWS géré
- Affichage des informations d'annuaire

Ajout de suffixes UPN alternatifs

Vous pouvez simplifier la gestion des noms de connexion Active Directory (AD) et améliorer l'expérience de connexion de l'utilisateur en ajoutant d'autres suffixes de noms principaux d'utilisateurs (UPN) à votre annuaire AWS Managed Microsoft AD. Pour ce faire, vous devez être connecté avec le compte Admin ou avec un compte qui est un membre du groupe Administrateurs délégués des suffixes de noms principaux d'utilisateurs AWS. Pour en savoir plus sur ce groupe, consultez Qu'est-ce qui est créé avec votre annuaire Microsoft AD Active Directory AWS géré.

Pour ajouter des suffixes UPN alternatifs

1. Ouvrez la console Amazon EC2 sur https://console.aws.amazon.com/ec2/.
2. Localisez une instance Amazon EC2 qui est jointe à votre annuaire AWS Managed Microsoft AD. Sélectionnez l'instance, puis choisissez Connecter.
3. Dans la fenêtre Gestionnaire de serveur, choisissez Outils. Puis choisissez Domaines et approbations Active Directory.

4. Dans le volet de gauche, effectuez un clic droit sur Domaines et approbations Active Directory, puis choisissez Propriétés .
5. Dans l'onglet Suffixes UPN, tapez un suffixe UPN alternatif (par exemple, **`sales.example.com`**). Sélectionnez Ajouter, puis Appliquer.
6. Si vous devez ajouter d'autres suffixes UPN alternatifs, répétez l'étape 5 jusqu'à ce que vous ayez les suffixes UPN dont vous avez besoin.

Supprimer votre Microsoft AD AWS géré

Lorsqu'un Microsoft AD AWS géré est supprimé, toutes les données de l'annuaire et les instantanés sont supprimés et ne peuvent pas être récupérés. Une fois que l'annuaire est supprimé, toutes les instances qui sont jointes à l'annuaire restent intactes. Toutefois, vous ne pouvez pas utiliser les informations d'identification de votre annuaire pour vous connecter à ces instances. Vous devez vous y connecter avec un compte utilisateur qui est local à l'instance.

Pour supprimer un annuaire

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires). Assurez-vous que vous vous trouvez Région AWS là où vous Active Directory êtes déployé. Pour plus d'informations, consultez la section Choix d'une région.
2. Assurez-vous qu'aucune AWS application n'est activée pour le répertoire que vous souhaitez supprimer. AWS Les applications activées vous empêcheront de supprimer votre AWS Managed Microsoft AD ou Simple AD.

   a. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
   b. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications). Dans la section AWS Applications et services, vous pouvez voir quelles AWS applications sont activées pour votre annuaire.

      - Désactivez AWS Management Console l'accès. Pour plus d'informations, consultez Désactiver l'accès à AWS Management Console.
      - Pour désactiver Amazon WorkSpaces, vous devez désenregistrer le service depuis le répertoire de la WorkSpaces console. Pour plus d'informations, consultez la section Désenregistrement d'un annuaire dans le guide d'administration Amazon WorkSpaces .
      - Pour désactiver Amazon WorkDocs, vous devez supprimer le WorkDocs site Amazon dans la WorkDocs console Amazon. Pour plus d'informations, consultez Supprimer un site dans le guide d' WorkDocs administration Amazon.

- Pour désactiver Amazon WorkMail, vous devez supprimer l' WorkMail organisation Amazon dans la WorkMail console Amazon. Pour plus d'informations, consultez Supprimer une organisation dans le manuel Amazon WorkMail Administrator Guide.
- Pour désactiver Amazon FSx for Windows File Server, vous devez supprimer le système de fichiers Amazon FSx du domaine. Pour plus d'informations, consultez la section Travailler avec un Active Directory serveur de fichiers FSx for Windows dans le guide de l'utilisateur d'Amazon FSx for Windows File Server.
- Pour désactiver Amazon Relational Database Service, vous devez supprimer l'instance Amazon RDS du domaine. Pour plus d'informations, veuillez consulter la section Managing a DB instance in a domain (français non garanti) dans le Guide de l'utilisateur Amazon RDS.
- Pour désactiver le AWS Client VPN service, vous devez supprimer le service d'annuaire du point de terminaison VPN du Client. Pour plus d'informations, consultez la section Active DirectoryAuthentification dans le guide de AWS Client VPN l'administrateur.
- Pour désactiver Amazon Connect, vous devez supprimer l'instance Amazon Connect. Pour plus d'informations, veuillez consulter Deleting an Amazon Connect instance (français non garanti) dans le Guide d'administration Amazon Connect.
- Pour désactiver Amazon QuickSight, vous devez vous désinscrire d'Amazon QuickSight. Pour plus d'informations, consultez la section Fermeture de votre Amazon QuickSight compte dans le guide de QuickSight l'utilisateur Amazon.

> **Note**
>
> Si vous l'utilisez AWS IAM Identity Center et que vous l'avez déjà connecté au répertoire AWS Managed Microsoft AD que vous prévoyez de supprimer, vous devez d'abord modifier la source d'identité avant de pouvoir la supprimer. Pour plus d'informations, veuillez consulter la section Change your identity source (français non garanti) dans le Guide de l'utilisateur IAM Identity Center.

3. Dans le volet de navigation, choisissez Directories (Annuaires).
4. Sélectionnez uniquement l'annuaire à supprimer, puis cliquez sur Supprimer. La suppression de l'annuaire prend plusieurs minutes. Lorsque l'annuaire a été supprimé, il est retiré de votre liste d'annuaires.

Modifier le nom de site de votre annuaire

Vous pouvez modifier le nom de site de votre annuaire par défaut AWS Managed Microsoft AD afin qu'il corresponde à vos noms de site Microsoft Active Directory (AD) existants. Il est ainsi plus facile pour AWS Managed Microsoft AD de trouver et d'authentifier vos utilisateurs AD existants dans votre annuaire sur site. Cela offre une meilleure expérience lorsque les utilisateurs se connectent à des ressources AWS telles que des instances Amazon EC2 et Amazon RDS for SQL Server que vous avez jointes à votre annuaire AWS Managed Microsoft AD.

Pour ce faire, vous devez être connecté avec le compte Admin ou avec un compte qui est un membre du groupe Administrateurs AWS délégués des sites et services. Pour en savoir plus sur ce groupe, consultez Qu'est-ce qui est créé avec votre annuaire Microsoft AD Active Directory AWS géré.

Pour prendre connaissance des avantages supplémentaires à renommer votre site en fonction des approbations, veuillez consulter Domain Locator Across a Forest Trust sur le site Web de Microsoft.

Pour modifier le nom de site AWS Managed Microsoft AD

1. Ouvrez la console Amazon EC2 sur https://console.aws.amazon.com/ec2/.
2. Localisez une instance Amazon EC2 jointe à votre annuaire AWS Managed Microsoft AD. Sélectionnez l'instance, puis choisissez Connecter.
3. Dans la fenêtre Gestionnaire de serveur, choisissez Outils. Choisissez ensuite Sites et services Active Directory.
4. Dans le volet de gauche, développez le dossier Sites, effectuez un clic droit sur le nom de site (par défaut, c'est Default-Site-Name), puis choisissez Renommer.
5. Tapez le nouveau nom de site, puis sélectionnez Entrée.

Création d'un instantané ou d'une restauration de votre annuaire

AWS Directory Servicefournit des instantanés quotidiens automatisés et la possibilité de prendre des instantanés manuels des données pour votre répertoire AWS Microsoft AD Active Directory géré. Ces instantanés peuvent être utilisés pour effectuer une point-in-time restauration de votre Active Directory. Vous êtes limité à cinq instantanés manuels pour chaque répertoire Microsoft AD Active Directory AWS géré. Si vous avez déjà atteint cette limite, vous devez supprimer un de vos instantanés manuels existants avant de pouvoir en créer un autre. Il est impossible de prendre des instantanés des annuaires AD Connector.

> **Note**
>
> L'instantané est une fonctionnalité globale de AWS Managed Microsoft AD. Si vous utilisez Réplication multi-régions, les procédures suivantes doivent être effectuées dans Région principale. Les modifications seront appliquées automatiquement à toutes les régions répliquées. Pour en savoir plus, consultez Caractéristiques mondiales et régionales.

Rubriques

- Création d'un instantané de votre annuaire.
- Restauration de l'annuaire à partir d'un instantané.
- Suppression d'un instantané

Création d'un instantané de votre annuaire.

Un instantané vous permet de restaurer votre répertoire tel qu'il était au moment où il a été pris. Pour créer un instantané manuel de votre annuaire, exécutez les étapes suivantes.

> **Note**
>
> Vous êtes limité à 5 instantanés manuels par annuaire. Si vous avez déjà atteint cette limite, vous devez supprimer un de vos instantanés manuels existants avant de pouvoir en créer un autre.

Pour créer un snapshot manuel

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Maintenance.
4. Dans la section Instantanés, choisissez Actions, puis sélectionnez Créer un instantané.
5. Dans la boîte de dialogue Créer un instantané d'annuaire, entrez une description de l'instantané, si vous le souhaitez. Lorsque vous êtes prêt, choisissez Créer.

Selon la taille de votre répertoire, la création de l'instantané peut prendre plusieurs minutes. Lorsque l'instantané est prêt, la valeur Statut devient `Completed`.

Restauration de l'annuaire à partir d'un instantané.

Restaurer un annuaire à partir d'un instantané revient à le déplacer dans le temps. Les instantanés d'annuaire sont propres à l'annuaire à partir duquel ils ont été créés. Un instantané ne peut être restauré que dans l'annuaire à partir duquel il a été créé. En outre, la durée maximale de prise en charge pour un instantané manuel est de 180 jours. Pour plus d'informations, veuillez consulter la section Useful shelf life of a system-state backup of Active Directory (français non garanti) sur le site web Microsoft.

> **Warning**
>
> Nous vous recommandons de contacter le Centre AWS Support avant toute restauration à partir d'un instantané ; nous pourrons peut-être vous aider à éviter d'avoir à effectuer une restauration à partir d'un instantané. Toute restauration à partir d'un instantané peut entraîner une perte de données, car les instantanés correspondent à un moment donné. Il est important que vous sachiez que tous les contrôleurs de domaine et serveurs DNS associés à l'annuaire seront hors ligne jusqu'à ce que l'opération de restauration soit terminée.

Pour restaurer un annuaire à partir d'un instantané, procédez comme suit :

Pour restaurer un annuaire à partir d'un instantané

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Maintenance.
4. Dans la section Instantanés, sélectionnez un instantané dans la liste, choisissez Actions, puis sélectionnez Restaurer l'instantané.
5. Choisissez Restaurer, passez en revue les informations contenues dans la boîte de dialogue, puis sélectionnez Restaurer.

La restauration d'un annuaire AWS Managed Microsoft AD peut prendre de deux à trois heures. Une fois la restauration réussie, la valeur Statut du répertoire devient `Active`. Toutes les modifications apportées à l'annuaire après la date de l'instantané sont remplacées.

Suppression d'un instantané

Pour supprimer un instantané

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Maintenance.
4. Dans la section Instantanés, choisissez Actions, puis Supprimer l'instantané.
5. Vérifiez que vous souhaitez supprimer l'instantané, puis sélectionnez Supprimer.

Mettez à niveau votre Microsoft AD AWS géré

Vous pouvez mettre à niveau votre édition Standard AWS Managed Microsoft AD Active Directory vers l'édition Enterprise en contactant AWS Support. Pour plus d'informations, voir Création de dossiers de support et gestion de dossiers dans le Guide de AWS Support l'utilisateur.

> **Note**
>
> La réplication multirégionale est uniquement disponible dans l'édition AWS Managed Microsoft AD Enterprise pour les régions suivantes :
>
> - USA Est (Ohio)
> - USA Est (Virginie du Nord)
> - USA Ouest (Californie du Nord)
> - USA Ouest (Oregon)
> - Afrique (Le Cap)
> - Asie-Pacifique (Hong Kong)
> - Asie-Pacifique (Mumbai)
> - Asie-Pacifique (Hyderabad)
> - Asie-Pacifique (Osaka)
> - Asia Pacific (Seoul)
> - Asie-Pacifique (Singapour)
> - Asie-Pacifique (Sydney)
> - Asie-Pacifique (Jakarta)

- Asie-Pacifique (Melbourne)
- Asie-Pacifique (Tokyo)
- Canada (Centre)
- Canada Ouest (Calgary)
- Chine (Beijing)
- China (Ningxia)
- Europe (Francfort)
- Europe (Zurich)
- Europe (Irlande)
- Europe (Londres)
- Europe (Paris)
- Europe (Stockholm)
- Europe (Milan)
- Europe (Espagne)
- Israël (Tel Aviv)
- Moyen-Orient (Bahreïn)
- Moyen-Orient (EAU)
- Amérique du Sud (São Paulo)
- AWS GovCloud (US-Ouest)
- AWS GovCloud (USA Est)

Il existe quelques limites à prendre en compte lors de la mise à niveau de votre Microsoft AD AWS géré. Il s'agit des options suivantes :

- La mise à niveau entraînera un coût supplémentaire. Consultez Tarification AWS Directory Service pour plus d'informations.
- Une fois votre Active Directory mis à niveau, il est impossible de revenir à son édition précédente.
- Les instantanés précédents ne peuvent pas être utilisés pour restaurer le fichier Active Directory après sa mise à niveau.

- Les mises à niveau ont lieu à une date et à une heure planifiées convenues avec vous AWS Support. Les mises à niveau ont lieu du lundi au vendredi, de 9 h à 17 h, heure normale du Pacifique.
- Le processus de mise à niveau prend de quatre à cinq heures.
- Au cours du processus de mise à niveau, les contrôleurs de domaine de votre AWS Managed Microsoft AD sont mis à niveau un par un. Cela peut avoir un impact négatif sur vos performances et provoquer des temps d'arrêt pendant votre période de maintenance.
- Si vos applications utilisent les noms d'hôte ou les adresses IP des contrôleurs de domaine au lieu du nom de domaine de votre Active Directory, ces applications devront être mises à jour.
- Si vous utilisez le protocole LDAPS (Lightweight Directory Access Protocol over SSL), les contrôleurs de domaine auront besoin de nouveaux certificats.

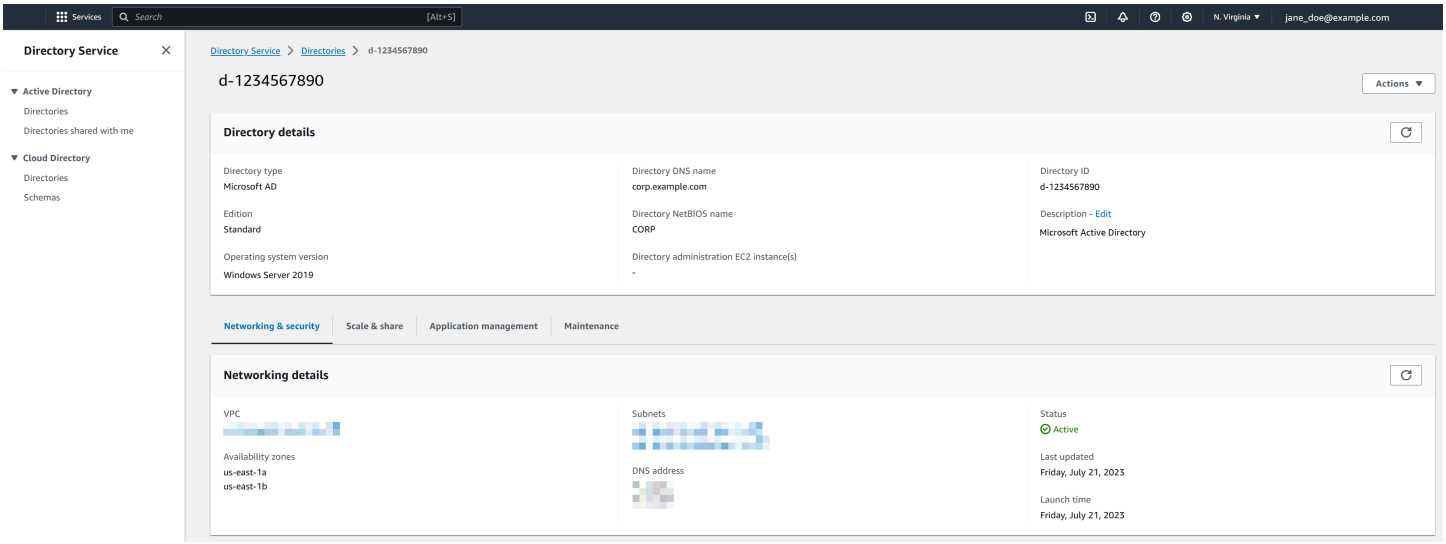
Affichage des informations d'annuaire

Vous pouvez afficher des informations détaillées sur un annuaire.

Pour afficher les informations détaillées de l'annuaire

1. Dans le volet de navigation de la AWS Directory Service console, sous Active Directory, sélectionnez Répertoires.
2. Cliquez sur le lien de l'ID correspondant à votre annuaire. Les informations relatives à l'annuaire sont affichées sur la page Détails de l'annuaire.

Pour de plus amples informations sur le champ Status (Statut), veuillez consulter Comprendre le statut de votre annuaire.



Accorder aux utilisateurs et aux groupes l'accès aux ressources AWS

AWS Directory Service permet aux utilisateurs et aux groupes de votre annuaire d'accéder à des AWS services et à des ressources, tels que l'accès à la console Amazon EC2. Tout comme si vous accordiez aux utilisateurs IAM l'accès à la gestion des annuaires comme décrit dansPolitiques basées sur une identité (politiques IAM), pour que les utilisateurs de votre annuaire aient accès à d'autres AWS ressources, telles qu'Amazon EC2, vous devez attribuer des rôles et des politiques IAM à ces utilisateurs et groupes. Pour de plus amples informations, veuillez consulter IAM roles (français non garanti) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur la manière d'autoriser les utilisateurs à accéder au AWS Management Console, consultezActivation de l'accès à AWS Management Console avec les informations d'identification AD.

Rubriques

- Création d'un rôle
- Modification de la relation d'approbation pour un rôle existant
- Attribution d'utilisateurs et de groupes à un rôle existant
- Affichage des utilisateurs et groupes attribués à un rôle
- Suppression d'un utilisateur ou d'un groupe d'un rôle
- Utilisation des stratégies gérées AWS avec AWS Directory Service

Création d'un rôle

Si vous devez créer un nouveau rôle IAM à utiliser avec AWS Directory Service, vous devez le créer à l'aide de la console IAM. Une fois le rôle créé, vous devez établir une relation de confiance avec ce rôle avant de pouvoir le voir dans la AWS Directory Service console. Pour plus d'informations, consultez Modification de la relation d'approbation pour un rôle existant.

> **Note**
>
> L'utilisateur exécutant cette tâche doit avoir l'autorisation d'effectuer les opérations IAM suivantes. Pour plus d'informations, consultez Politiques basées sur une identité (politiques IAM).
>
> - iam : PassRole
> - iam : GetRole
> - iam : CreateRole
> - iam : PutRolePolicy

Pour créer un nouveau rôle dans la console IAM

1. Dans le panneau de navigation de la console IAM, sélectionnez Roles (Rôles). Pour plus d'informations, veuillez consulter Creating a role (AWS Management Console) (français non garanti) dans le Guide de l'utilisateur IAM.
2. Sélectionnez Créer un rôle.
3. Dans Choisir le service qui utilisera ce rôle, choisissez Directory Service, puis Suivant : Autorisations.
4. Cochez la case à côté de la politique (par exemple, AmazonEC2 FullAccess) que vous souhaitez appliquer aux utilisateurs de votre annuaire, puis choisissez Next.
5. Si nécessaire, ajoutez une balise au rôle, puis choisissez Suivant.
6. Fournissez le Nom du rôle et une Description (facultative), puis choisissez Créer un rôle.

Exemple : Création d'un rôle pour activer l'accès à AWS Management Console

La liste suivante fournit un exemple des tâches que vous devez effectuer pour créer un nouveau rôle qui donnera à des utilisateurs spécifiques de l'annuaire l'accès à la console Amazon EC2.

1. Créez un rôle avec la console IAM à l'aide de la procédure ci-dessus. Lorsque vous êtes invité à saisir une politique, choisissez AmazonEC2 FullAccess.
2. Suivez les étapes décrites dans Modification de la relation d'approbation pour un rôle existant pour modifier le rôle que vous venez de créer, puis ajoutez les informations de relation d'approbation requises au document de stratégie. Cette étape est nécessaire pour que le rôle soit visible immédiatement après avoir activé l'accès AWS Management Console à l'étape suivante.
3. Suivez les étapes de Activation de l'accès à AWS Management Console avec les informations d'identification AD pour configurer l'accès général à AWS Management Console.
4. Suivez les étapes de Attribution d'utilisateurs et de groupes à un rôle existant pour ajouter au nouveau rôle les utilisateurs qui ont besoin d'un accès complet aux ressources EC2.

Modification de la relation d'approbation pour un rôle existant

Vous pouvez attribuer vos rôles IAM existants à vos AWS Directory Service utilisateurs et groupes. Pour ce faire, le rôle doit toutefois entretenir une relation de confiance avec AWS Directory Service. Lorsque vous créez un rôle AWS Directory Service à l'aide de la procédure dansCréation d'un rôle, cette relation de confiance est automatiquement définie. Vous n'avez qu'à établir cette relation d'approbation pour les rôles IAM qui ne sont pas créés par AWS Directory Service.

Pour établir une relation de confiance pour un rôle existant pour AWS Directory Service

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de la console IAM, sous Gestion des accès, choisissez Rôles.

   La console affiche les rôles de votre compte.
3. Choisissez le nom du rôle que vous voulez modifier, puis,une fois dans la page du rôle, sélectionnez Relations d'approbation.
4. Choisissez Edit trust policy (Modifier la politique d'approbation).
5. Sous Modifier la politique d'approbation, collez les informations suivantes, puis choisissez Mettre à jour la stratégie.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ds.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Vous pouvez également mettre à jour ce document de stratégie à l'aide de AWS CLI. Pour plus d'informations, veuillez consulter update-trust dans AWS CLI Command Reference (français non garanti).

Attribution d'utilisateurs et de groupes à un rôle existant

Vous pouvez attribuer un rôle IAM existant à un AWS Directory Service utilisateur ou à un groupe. Pour ce faire, assurez-vous d'avoir effectué les étapes suivantes.

Prérequis

- Créez un Microsoft AD AWS géré.
- Créez un utilisateur ou un groupe.
- Créez un rôle qui entretient une relation de confiance avec AWS Directory Service. Vous pouvez modifier la relation de confiance pour un rôle existant.

> **Note**
>
> L'accès pour les utilisateurs figurant dans des groupes imbriqués au sein de votre annuaire n'est pas pris en charge. Les membres du groupe parent ont accès à la console, mais pas les membres des groupes enfants.

Pour attribuer des utilisateurs ou des groupes à un rôle IAM existant

1. Dans le volet de navigation de la console AWS Directory Service, sous Active Directory, sélectionnez Annuaires.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.

3. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :

   - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Gestion des applications.
   - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région dans laquelle vous souhaitez effectuer vos affectations, puis cliquez sur l'onglet Gestion des applications. Pour plus d'informations, consultez Régions principales et régions supplémentaires.

4. Faites défiler la page jusqu'à la AWS Management Consolesection, sélectionnez Actions et Activer.
5. Dans la section Accès à la console déléguée, choisissez le nom du rôle IAM existant auquel vous souhaitez attribuer des utilisateurs.
6. Sur la page Selected rôle (Rôle sélectionné) sous Manage users and groups for this role (Gérer les utilisateurs et les groupes pour ce rôle), choisissez Add (Ajouter).
7. Sur la page Add users and groups to the role (Ajouter des utilisateurs et groupes aux rôles), en regard de Select Active Directory Forest (Sélectionner la forêt Active Directory), choisissez la forêt AWS Managed Microsoft AD (cette forêt) ou la forêt sur site (forêt approuvée), selon celle qui contient les comptes qui ont besoin d'accéder à AWS Management Console. Pour plus d'informations sur la mise en place d'une forêt approuvée, veuillez consulter Didacticiel : créer une relation d'approbation entre votre AWS Managed Microsoft AD et votre domaine Active Directory..
8. Sous Specify which users or groups to add (Spécifier les utilisateurs ou les groupes à ajouter), sélectionnez Find by user (Rechercher par utilisateur) ou Find by group (Rechercher par groupe), puis tapez le nom de l'utilisateur ou du groupe. Dans la liste de correspondances possibles, choisissez l'utilisateur ou le groupe que vous souhaitez ajouter.
9. Choisissez Add (Ajouter) pour mettre fin à l'affectation des utilisateurs et des groupes au rôle.

Affichage des utilisateurs et groupes attribués à un rôle

Pour afficher les utilisateurs et groupes attribués à un rôle, procédez comme suivant.

Prérequis

- Assignez vos utilisateurs ou groupes à un rôle existant.

Pour afficher les utilisateurs et groupes attribués à un rôle

1. Dans le volet de navigation de la console AWS Directory Service, sous Active Directory, sélectionnez Annuaires.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :
   - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région dans laquelle vous souhaitez afficher vos affectations, puis cliquez sur l'onglet Gestion des applications. Pour plus d'informations, consultez Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Gestion des applications.
4. Dans la section Déléguer l'accès à la console, choisissez le rôle IAM que vous souhaitez afficher.
5. Sur la page Rôle sélectionné, sous Gérer les utilisateurs et les groupes pour ce rôle, vous pouvez afficher les utilisateurs et les groupes attribués au rôle.

Suppression d'un utilisateur ou d'un groupe d'un rôle

Pour supprimer d'un rôle un utilisateur ou un groupe, procédez comme suit.

Pour supprimer un utilisateur ou un groupe d'un rôle

1. Dans le panneau de navigation de la console AWS Directory Service, choisissez Annuaires.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :
   - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région dans laquelle vous souhaitez supprimer vos affectations, puis cliquez sur l'onglet Gestion des applications. Pour plus d'informations, consultez Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Gestion des applications.
4. Dans la section AWS Management Console, choisissez le rôle que vous souhaitez afficher.

5. Sur la page Selected role (Rôle sélectionné), sous Manage users and groups for this role (Gérer les utilisateurs et les groupes pour ce rôle), sélectionnez les utilisateurs ou les groupes pour lesquels supprimer le rôle, puis choisissez Remove (Supprimer). Le rôle est supprimé pour les utilisateurs et les groupes spécifiés, mais il n'est pas supprimé de votre compte.

Utilisation des stratégies gérées AWS avec AWS Directory Service

AWS Directory Service fournit les stratégies gérées AWS suivantes afin de donner à vos utilisateurs et à vos groupes l'accès aux services AWS et ressources, comme l'accès à la console Amazon EC2. Vous devez vous connecter à AWS Management Console avant de pouvoir afficher ces stratégies.

- Accès en lecture seule
- Accès utilisateur avec pouvoir
- AWS Directory Service Accès complet
- AWS Directory Service Accès en lecture seule
- Accès complet à Amazon Cloud Directory
- Accès en lecture seule à Amazon Cloud Directory
- Accès complet à Amazon EC2
- Accès en lecture seule à Amazon EC2
- Accès complet à Amazon VPC
- Accès en lecture seule à Amazon VPC
- Accès complet à Amazon RDS
- Accès en lecture seule à Amazon RDS
- Accès complet à Amazon DynamoDB
- Accès en lecture seule à Amazon DynamoDB
- Accès complet à Amazon S3
- Accès en lecture seule à Amazon S3
- AWS CloudTrail Accès complet
- AWS CloudTrail Accès en lecture seule
- Accès complet à Amazon CloudWatch
- Accès en lecture seule à Amazon CloudWatch

- Accès complet à Amazon CloudWatch Logs
- Accès en lecture seule à Amazon CloudWatch Logs

Pour plus d'informations sur la création de vos propres stratégies, consultez la section Exemples de stratégies de gestion AWS de ressources du .Guide de l'utilisateur IAM.

Permettre l'accès aux AWS applications et aux services

Les utilisateurs peuvent autoriser AWS Managed Microsoft AD à donner à AWS des applications et à des services, tels qu'Amazon WorkSpaces, l'accès à votreActive Directory. Les AWS applications et services suivants peuvent être activés ou désactivés pour fonctionner avec AWS Managed Microsoft AD.

AWS application/service	En savoir plus...
Amazon Chime	Pour plus d'informations, veuillez consulter le Guide d'administration Amazon Chime.
Amazon Connect	Pour plus d'informations, veuillez consulter le Guide d'administration Amazon Connect.
Amazon FSx for Windows File Server	Pour plus d'informations, consultez Utilisation d'Amazon FSx avec AWS Directory Service pour Microsoft Active Directory.
Amazon QuickSight	Pour plus d'informations, consultez le guide de QuickSight l'utilisateur Amazon.
Amazon Relational Database Service	Pour plus d'informations, veuillez consulter le Guide d'utilisateur Amazon RDS.
Amazon WorkDocs	Pour plus d'informations, consultez le guide d' WorkDocs administration Amazon.
Amazon WorkMail	Pour plus d'informations, consultez le guide de WorkMail l'administrateur Amazon.
Amazon WorkSpaces	Vous pouvez créer un Simple AD, AWS Managed Microsoft AD ou AD Connector

AWS application/service	En savoir plus...
	directement à partir de WorkSpaces. Il vous suffit de lancer la configuration avancée lors de la création de votre Workspace. Pour plus d'informations, consultez le guide d' WorkSpaces administration Amazon.
AWS Client VPN	Pour plus d'informations, veuillez consulter le Guide de l'utilisateur AWS Client VPN.
AWS IAM Identity Center	Pour plus d'informations, veuillez consulter le Guide de l'utilisateur AWS IAM Identity Center.
AWS License Manager	Pour plus d'informations, veuillez consulter le Guide de l'utilisateur License Manager.
AWS Management Console	Pour plus d'informations, consultez Activation de l'accès à AWS Management Console avec les informations d'identification AD.
AWS Private Certificate Authority	Pour plus d'informations, consultez AWS Private CA Connector for Active Directory.
AWS Transfer Family	Pour plus d'informations, veuillez consulter le Guide de l'utilisateur AWS Transfer Family.

Une fois activé, vous gérez l'accès à vos annuaires dans la console de l'application ou du service auquel vous souhaitez donner accès à votre répertoire. Pour rechercher les liens vers AWS les applications et les services décrits ci-dessus dans la AWS Directory Service console, effectuez les opérations suivantes.

Pour afficher les applications et les services d'un annuaire

1. Dans le panneau de navigation de la console AWS Directory Service, choisissez Annuaires.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications).

4. Consultez la liste dans la section Applications et services AWS .

Pour plus d'informations sur la manière d'autoriser ou d'annuler l'autorisation d' AWS applications et de services utilisant AWS Directory Service, consultezAutorisation pour AWS les applications et les services utilisant AWS Directory Service.

Rubriques

- Création d'une URL d'accès
- Authentification unique

Création d'une URL d'accès

Une URL d'accès est utilisée avec les applications et services AWS, tels qu'Amazon WorkDocs, pour accéder à une page de connexion associée à votre annuaire. L'URL doit être globalement unique. Vous pouvez créer une URL d'accès pour votre annuaire en effectuant les étapes suivantes.

> **Warning**
>
> Une fois l'URL d'accès aux applications créée pour cet annuaire, elle ne peut pas être modifiée. Une fois votre URL d'accès créée, personne d'autre que vous ne pourra l'utiliser. Si vous supprimez votre annuaire, l'URL d'accès sera également supprimée et pourra alors être utilisée par un autre compte.

> **Note**
>
> L'URL d'accès ne peut être configurée qu'à partir de la région principale lorsque vous utilisez des annuaires sur plusieurs régions.

Pour créer une URL d'accès

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), procédez de l'une des manières suivantes :

- Si plusieurs régions apparaissent sous Multi-Region replication (Réplication multi-régions), sélectionnez la région principale, puis l'onglet Application management (Gestion des applications). Pour de plus amples informations, veuillez consulter Régions principales et régions supplémentaires.
- Si aucune région n'apparaît sous Multi-Region replication (Réplication multi-régions), choisissez l'onglet Application management (Gestion des applications).

4. Dans la section Application access URL (URL d'accès à l'application), si aucune URL d'accès n'a été attribuée à l'annuaire, le bouton Créer s'affiche. Entrez un alias d'annuaire, puis choisissez Créer. Si l'erreur Entity Already Exists (entité déjà existante) est renvoyée, cela veut dire que l'alias de l'annuaire spécifié a déjà été alloué. Choisissez un autre alias et répétez la procédure.

   Votre URL d'accès est affichée au format *<alias>*.awsapps.com. Par défaut, cette URL vous redirigera vers la page de connexion d'Amazon WorkDocs.

Authentification unique

AWS Directory Servicepermet à vos utilisateurs d'accéder à Amazon WorkDocs depuis un ordinateur connecté à l'annuaire sans avoir à saisir leurs informations d'identification séparément.

Avant d'activer l'authentification unique, vous devez prendre des mesures supplémentaires pour permettre aux navigateurs Web de vos utilisateurs de prendre en charge l'authentification unique. Les utilisateurs peuvent avoir besoin de modifier les paramètres de leur navigateur Web pour activer l'authentification unique.

> **Note**
>
> L'authentification unique fonctionne uniquement lorsqu'elle est utilisée sur un ordinateur qui est associé à l'annuaire AWS Directory Service. Elle ne peut pas être utilisée sur les ordinateurs qui ne sont pas joints à l'annuaire.

Si votre annuaire est un annuaire AD Connector et que le compte de service AD Connector ne dispose pas de l'autorisation d'ajouter ou de supprimer son attribut de nom principal de service, vous disposez de deux options pour les étapes 5 et 6 ci-dessous :

1. Vous pouvez continuer et vous serez invité à saisir le nom d'utilisateur et le mot de passe d'un utilisateur d'annuaire qui dispose de cette autorisation pour ajouter ou supprimer l'attribut de nom

principal de service sur le compte de service AD Connector. Ces informations d'identification servent uniquement à activer l'authentification unique et ne sont pas stockées par le service. Les autorisations du compte de service AD Connector ne sont pas modifiées.

2. Vous pouvez déléguer des autorisations pour permettre au compte de service AD Connector d'ajouter ou de supprimer l'attribut du nom principal du service sur lui-même. Vous pouvez exécuter les PowerShell commandes ci-dessous à partir d'un ordinateur joint au domaine à l'aide d'un compte autorisé à modifier les autorisations sur le compte de service AD Connector. La commande ci-dessous donnera au compte de service AD Connector la possibilité d'ajouter et de supprimer un attribut de nom principal de service uniquement pour lui-même.

```
$AccountName = 'ConnectorAccountName'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$RootDse = Get-ADRootDSE
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'servicePrincipalName' } -
Properties 'schemaIDGUID').schemaIDGUID
# Getting AD Connector service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AclPath = $AccountProperties.DistinguishedName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for AD Connector service account.
$ObjectAcl = Get-ACL -Path "AD:\$AclPath"
# Setting ACL allowing the AD Connector service account the ability to add and remove a
 Service Principal Name (SPN) to itself
$AddAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
 'Allow', $ServicePrincipalNameGUID, 'None'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$AclPath"
```

Pour activer ou désactiver l'authentification unique avec Amazon WorkDocs

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.

3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications).
4. Dans la section URL d'accès à l'application, choisissez Activer pour activer l'authentification unique pour Amazon WorkDocs.

   Si vous ne voyez pas le bouton Activer, vous devez d'abord créer une URL d'accès pour pouvoir afficher cette option. Pour plus d'informations sur la création d'une URL d'accès, veuillez consulter Création d'une URL d'accès.
5. Dans la boîte de dialogue Activer l'authentification unique pour cet annuaire, choisissez Activer. L'authentification unique est activée pour l'annuaire.
6. Si vous souhaitez désactiver ultérieurement l'authentification unique avec Amazon WorkDocs, choisissez Disable, puis dans la boîte de dialogue Désactiver l'authentification unique pour ce répertoire, choisissez à nouveau Disable.

Rubriques

- Authentification unique pour IE et Chrome
- Authentification unique pour Firefox

Authentification unique pour IE et Chrome

Pour permettre aux navigateurs Microsoft Internet Explorer (IE) et Google Chrome de prendre en charge l'authentification unique, les tâches suivantes doivent être effectuées sur l'ordinateur client :

- Ajoutez votre URL d'accès (par exemple, https://*<alias>*.awsapps.com) à la liste des sites approuvés pour l'authentification unique.
- Activez le script actif (JavaScript).
- Autorisez l'ouverture de session automatique.
- Activez l'authentification intégrée.

Vous ou vos utilisateurs pouvez effectuer ces tâches manuellement, ou vous pouvez modifier ces paramètres à l'aide des paramètres de politique de groupe.

Rubriques

- Mise à jour manuelle pour authentification unique sous Windows
- Mise à jour manuelle pour authentification unique sous OS X

- Paramètres de stratégie de groupe pour authentification unique

Mise à jour manuelle pour authentification unique sous Windows

Pour activer manuellement l'authentification unique sur un ordinateur Windows, effectuez les étapes suivantes sur l'ordinateur client. Certains de ces paramètres sont peut-être déjà définis correctement.

Pour activer manuellement l'authentification unique pour Internet Explorer et Chrome sous Windows

1. Pour ouvrir la boîte de dialogue Propriétés Internet, sélectionnez le menu Démarrer, tapez `Internet Options` dans la zone de recherche, puis sélectionnez Options Internet.
2. Ajoutez votre URL d'accès à la liste des sites approuvés pour l'authentification unique en effectuant les étapes suivantes :
   a. Dans la boîte de dialogue Propriétés Internet, sélectionnez l'onglet Sécurité.
   b. Sélectionnez Intranet local, puis Sites.
   c. Dans la boîte de dialogue Intranet local, sélectionnez Avancé.
   d. Ajoutez votre URL d'accès à la liste des sites Web et choisissez Fermer.
   e. Dans la boîte de dialogue Intranet local, sélectionnez OK.
3. Pour activer les scripts actifs, effectuez les opérations suivantes :
   a. Dans l'onglet Sécurité de la boîte de dialogue Propriétés Internet, sélectionnez Personnaliser le niveau.
   b. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, faites défiler la page jusqu'à Scripts et sélectionnez Activer sous Scripts actifs.
   c. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, cliquez sur OK.
4. Pour activer la connexion automatique, effectuez les opérations suivantes :
   a. Dans l'onglet Sécurité de la boîte de dialogue Propriétés Internet, sélectionnez Personnaliser le niveau.
   b. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, faites défiler l'écran jusqu'à Authentification utilisateur et sélectionnez Connexion automatique uniquement dans la zone Intranet sous Connexion.
   c. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, cliquez sur OK.

d. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, cliquez sur OK.

5. Pour activer l'authentification intégrée, effectuez les opérations suivantes :

   a. Dans la boîte de dialogue Propriétés Internet, sélectionnez l'onglet Avancé.

   b. Faites défiler la page jusqu'à Sécurité et sélectionnez Activer l'authentification Windows intégrée.

   c. Dans la boîte de dialogue Propriétés Internet, choisissez OK.

6. Fermez puis rouvrez votre navigateur pour que ces modifications prennent effet.

Mise à jour manuelle pour authentification unique sous OS X

Pour activer manuellement l'authentification unique pour Chrome sous OS X, effectuez les étapes suivantes sur l'ordinateur client. Vous devez disposer des droits d'administrateur sur votre ordinateur pour effectuer ces opérations.

Pour activer manuellement l'authentification unique pour Chrome sous OS X

1. Ajoutez votre URL d'accès à la AuthServerAllowlistpolitique en exécutant la commande suivante :

   ```
   defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
   ```

2. Ouvrez les Préférences système, accédez au panneau Profils et supprimez le profil `Chrome Kerberos Configuration`.

3. Redémarrez Chrome et ouvrez chrome://policy dans Chrome pour vérifier que les nouveaux paramètres sont en place.

Paramètres de stratégie de groupe pour authentification unique

L'administrateur de domaine peut implémenter des paramètres de stratégie de groupe pour apporter les modifications d'authentification unique sur les ordinateurs clients joints au domaine.

> **Note**
>
> Si vous gérez les navigateurs Web Chrome sur les ordinateurs de votre domaine à l'aide des politiques Chrome, vous devez y ajouter votre URL d'AuthServerAllowlistaccès. Pour plus

d'informations sur la définition des politiques de Chrome, veuillez consulter la section Policy Settings in Chrome (français non garanti).

Pour activer l'authentification unique pour Internet Explorer et Chrome à l'aide des paramètres de stratégie de groupe

1. Créez un nouvel objet de stratégie de groupe en procédant comme suit :
   a. Ouvrez l'outil de gestion des stratégies de groupe, accédez à votre domaine et sélectionnez Objets de stratégie de groupe.
   b. Dans le menu principal, choisissez Action, puis Nouveau.
   c. Dans la boîte de dialogue New GPO, entrez un nom descriptif pour l'objet de stratégie de groupe, tel que `IAM Identity Center Policy` et laissez Source Starter GPO défini sur (none). Cliquez sur OK.
2. Ajoutez l'URL d'accès à la liste des sites approuvés pour l'authentification unique en effectuant les étapes suivantes :
   a. Dans l'outil de gestion des politiques de groupe, accédez à votre domaine, sélectionnez Objets de stratégie de groupe, ouvrez le menu contextuel (clic droit) de votre politique IAM Identity Center, puis choisissez Modifier.
   b. Dans l'arborescence des politiques, accédez à Configuration utilisateur > Préférences > Paramètres Windows.
   c. Dans la liste Paramètres Windows, ouvrez le menu contextuel (clic droit) pour Registre et choisissez Nouvel élément de Registre.
   d. Dans la boîte de dialogue Propriétés du nouveau registre, entrez les paramètres suivants et cliquez sur OK :

      Action

      ```
      Update
      ```

      Hive

      ```
      HKEY_CURRENT_USER
      ```

Chemin

```
Software\Microsoft\Windows\CurrentVersion\Internet Settings
\ZoneMap\Domains\awsapps.com\<alias>
```

La valeur de *<alias>* est dérivée de votre URL d'accès. Si votre URL d'accès est `https://examplecorp.awsapps.com`, l'alias est `examplecorp` et la clé de registre sera `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\examplecorp`.

Nom de la valeur

```
https
```

Type de la valeur

```
REG_DWORD
```

Données de valeur

```
1
```

3. Pour activer les scripts actifs, effectuez les opérations suivantes :

   a. Dans l'outil de gestion des politiques de groupe, accédez à votre domaine, sélectionnez Objets de stratégie de groupe, ouvrez le menu contextuel (clic droit) de votre politique IAM Identity Center, puis choisissez Modifier.

   b. Dans l'arborescence des politiques, accédez à Configuration informatique > Politiques > Modèles d'administration > Composants Windows > Internet Explorer > Panneau de configuration Internet > Page de sécurité > Zone intranet.

   c. Dans la liste Zone Intranet, ouvrez le menu contextuel (clic droit) pour Autoriser les scripts actifs et choisissez Modifier.

   d. Dans la boîte de dialogue Autoriser les scripts actifs, entrez les paramètres suivants et cliquez sur OK :

      - Sélectionnez le bouton radio Activé.
      - Sous Options, définissez Autoriser les scripts actifs sur Activer.

4. Pour activer la connexion automatique, effectuez les opérations suivantes :

a. Dans l'outil de gestion des politiques de groupe, accédez à votre domaine, sélectionnez Objets de stratégie de groupe, ouvrez le menu contextuel (clic droit) de votre politique SSO (authentification unique), puis choisissez Modifier.

b. Dans l'arborescence des politiques, accédez à Configuration informatique > Politiques > Modèles d'administration > Composants Windows > Internet Explorer > Panneau de configuration Internet > Page de sécurité > Zone intranet.

c. Dans la liste Zone Intranet, ouvrez le menu contextuel (clic droit) pour Options de connexion et choisissez Modifier.

d. Dans la boîte de dialogue Options de connexion, entrez les paramètres suivants et cliquez sur OK :

   - Sélectionnez le bouton radio Activé.
   - Sous Options, définissez les options de connexion sur Connexion automatique uniquement dans la zone Intranet.

5. Pour activer l'authentification intégrée, effectuez les opérations suivantes :

a. Dans l'outil de gestion des politiques de groupe, accédez à votre domaine, sélectionnez Objets de stratégie de groupe, ouvrez le menu contextuel (clic droit) de votre politique IAM Identity Center, puis choisissez Modifier.

b. Dans l'arborescence des politiques, accédez à Configuration utilisateur > Préférences > Paramètres Windows.

c. Dans la liste Paramètres Windows, ouvrez le menu contextuel (clic droit) pour Registre et choisissez Nouvel élément de Registre.

d. Dans la boîte de dialogue Propriétés du nouveau registre, entrez les paramètres suivants et cliquez sur OK :

   Action

   ```
   Update
   ```

   Hive

   ```
   HKEY_CURRENT_USER
   ```

   Chemin

   ```
   Software\Microsoft\Windows\CurrentVersion\Internet Settings
   ```

Nom de la valeur

`EnableNegotiate`

Type de la valeur

`REG_DWORD`

Données de valeur

`1`

6. Fermez la fenêtre de l'éditeur de gestion des politiques de groupe si elle est toujours ouverte.
7. Attribuez la nouvelle politique à votre domaine en procédant comme suit :

   a. Dans l'arborescence Gestion des politiques de groupe, ouvrez le menu contextuel (clic droit) de votre domaine et choisissez Lier un GPO existant.
   b. Dans la liste Objets de politique de groupe, sélectionnez votre politique IAM Identity Center et cliquez sur OK.

Ces modifications prendront effet après la prochaine mise à jour de la politique de groupe sur le client, ou la prochaine fois que l'utilisateur se connectera.

Authentification unique pour Firefox

Pour autoriser le navigateur Mozilla Firefox à prendre en charge l'authentification unique, ajoutez votre URL d'accès (par exemple, https://*<alias>*.awsapps.com) à la liste des sites approuvés pour l'authentification unique. Cela peut être fait manuellement ou automatiquement à l'aide d'un script.

Rubriques

- Mise à jour manuelle pour authentification unique
- Mise à jour automatique pour authentification unique

Mise à jour manuelle pour authentification unique

Pour ajouter manuellement votre URL d'accès à la liste des sites approuvés dans Firefox, effectuez les étapes suivantes sur l'ordinateur client.

Pour ajouter manuellement votre URL d'accès à la liste des sites approuvés dans Firefox

1. Ouvrez Firefox et ouvrez la page `about:config`.

2. Ouvrez la préférence `network.negotiate-auth.trusted-uris` et ajoutez votre URL d'accès à la liste des sites. Utilisez une virgule (,) pour séparer plusieurs entrées.

Mise à jour automatique pour authentification unique

En tant qu'administrateur de domaine, vous pouvez utiliser un script pour ajouter votre URL d'accès aux préférences utilisateur de Firefox `network.negotiate-auth.trusted-uris` sur tous les ordinateurs de votre réseau. Pour de plus amples informations, veuillez consulter https://support.mozilla.org/en-US/questions/939037.

Activation de l'accès à AWS Management Console avec les informations d'identification AD

AWS Directory Service vous permet d'accorder aux membres de votre annuaire l'accès à AWS Management Console. Par défaut, les utilisateurs et les groupes de votre annuaire n'ont pas accès à toutes les ressources AWS. Vous attribuez des rôles IAM aux membres de votre annuaire pour leur donner accès aux différents services et ressources AWS. Le rôle IAM définit les services, les ressources et le niveau d'accès des membres de votre annuaire.

Avant que vous puissiez accorder l'accès à la console aux membres de votre annuaire, celui-ci doit disposer d'une URL d'accès. Pour plus d'informations sur la manière d'afficher les détails du répertoire et d'obtenir votre URL d'accès, veuillez consulter Affichage des informations d'annuaire. Pour plus d'informations sur la création d'une URL d'accès, consultez Création d'une URL d'accès.

Pour plus d'informations sur la façon de créer et d'attribuer des rôles IAM; aux membres de votre annuaire, consultez Accorder aux utilisateurs et aux groupes l'accès aux ressources AWS.

Rubriques

- Activer l'accès à AWS Management Console
- Désactiver l'accès à AWS Management Console
- Définir la durée de la session de connexion

Article du blog sur la sécurité AWS connexe

- How to Access the AWS Management Console Using AWS Managed Microsoft AD and Your On-Premises Credentials

> **Note**
>
> L'accès au AWS Management Console est une fonctionnalité régionale de AWS Managed Microsoft AD. Si vous utilisez Réplication multi-régions, les procédures suivantes doivent être appliquées séparément dans chaque région. Pour de plus amples informations, veuillez consulter Caractéristiques mondiales et régionales.

Activer l'accès à AWS Management Console

Par défaut, l'accès à la console n'est activé pour aucun annuaire. Pour activer l'accès à la console pour les utilisateurs et les groupes de votre annuaire, effectuez les opérations suivantes :

Pour activer l'accès à la console

1. Dans le panneau de navigation de la console AWS Directory Service, choisissez Annuaires.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :
   - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région dans laquelle vous souhaitez activer l'accès à AWS Management Console, puis cliquez sur l'onglet Gestion des applications. Pour de plus amples informations, veuillez consulter Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication sur plusieurs régions, sélectionnez l'onglet Gestion d'applications.
4. Dans la section AWS Management Console, choisissez Activer. L'accès à la console est désormais activé pour votre annuaire.

   Avant que les utilisateurs puissent se connecter à la console avec votre URL d'accès, vous devez d'abord ajouter vos utilisateurs au rôle. Pour des informations générales sur l'attribution d'utilisateurs à des rôles IAM, consultez. Attribution d'utilisateurs et de groupes à un rôle existant Une fois les rôles IAM attribués, les utilisateurs peuvent accéder à la console à l'aide de votre URL d'accès. Par exemple, si l'URL d'accès à votre annuaire est example-corp.awsapps.com, l'URL permettant d'accéder à la console est https://example-corp.awsapps.com/console/.

Désactiver l'accès à AWS Management Console

Pour désactiver l'accès à la console pour les utilisateurs et les groupes de votre annuaire, effectuez les opérations suivantes :

Pour désactiver l'accès à la console

1. Dans le panneau de navigation de la console AWS Directory Service, choisissez Annuaires.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :
   - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région dans laquelle vous souhaitez désactiver l'accès à AWS Management Console, puis cliquez sur l'onglet Gestion d'applications. Pour de plus amples informations, veuillez consulter Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication sur plusieurs régions, sélectionnez l'onglet Gestion d'applications.
4. Dans la section AWS Management Console, choisissez Désactiver. L'accès à la console est désormais désactivé pour votre annuaire.
5. Si des rôles IAM ont été attribués à des utilisateurs ou à des groupes dans l'annuaire, le bouton Désactiver n'est peut-être pas disponible. Dans ce cas, vous devez supprimer toutes les affectations de rôles IAM correspondant à l'annuaire avant de continuer, y compris les affectations d'utilisateurs ou de groupes de votre annuaire qui ont été supprimées et qui apparaissent sous le libellé Utilisateur supprimé ou Groupe supprimé.

   Une fois que toutes les affectations de rôles IAM ont été supprimées, répétez les étapes ci-dessus.

Définir la durée de la session de connexion

Par défaut, les utilisateurs disposent d'une heure pour utiliser leur session après s'être correctement connectés à la console avant d'être déconnectés. Ensuite, les utilisateurs doivent se reconnecter pour démarrer la prochaine session d'une heure avant d'être à nouveau déconnectés. Vous pouvez utiliser la procédure suivante pour modifier la durée jusqu'à 12 heures par session.

Définir la durée de la session de connexion

1. Dans le panneau de navigation de la console AWS Directory Service, choisissez Annuaires.

2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :

   - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région dans laquelle vous souhaitez définir la durée de la session de connexion, puis cliquez sur l'onglet Gestion d'applications. Pour de plus amples informations, veuillez consulter Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication sur plusieurs régions, sélectionnez l'onglet Gestion d'applications.
4. Sous la section Applications et services AWS, choisissez AWS Management Console.
5. Dans la boîte de dialogue Gérer l'accès à la ressource AWS, choisissez Continuer.
6. Sur la page Affecter des utilisateurs et des groupes à des rôles IAM, sous Définir la durée de la session de connexion, modifiez la valeur numérotée, puis choisissez Enregistrer.

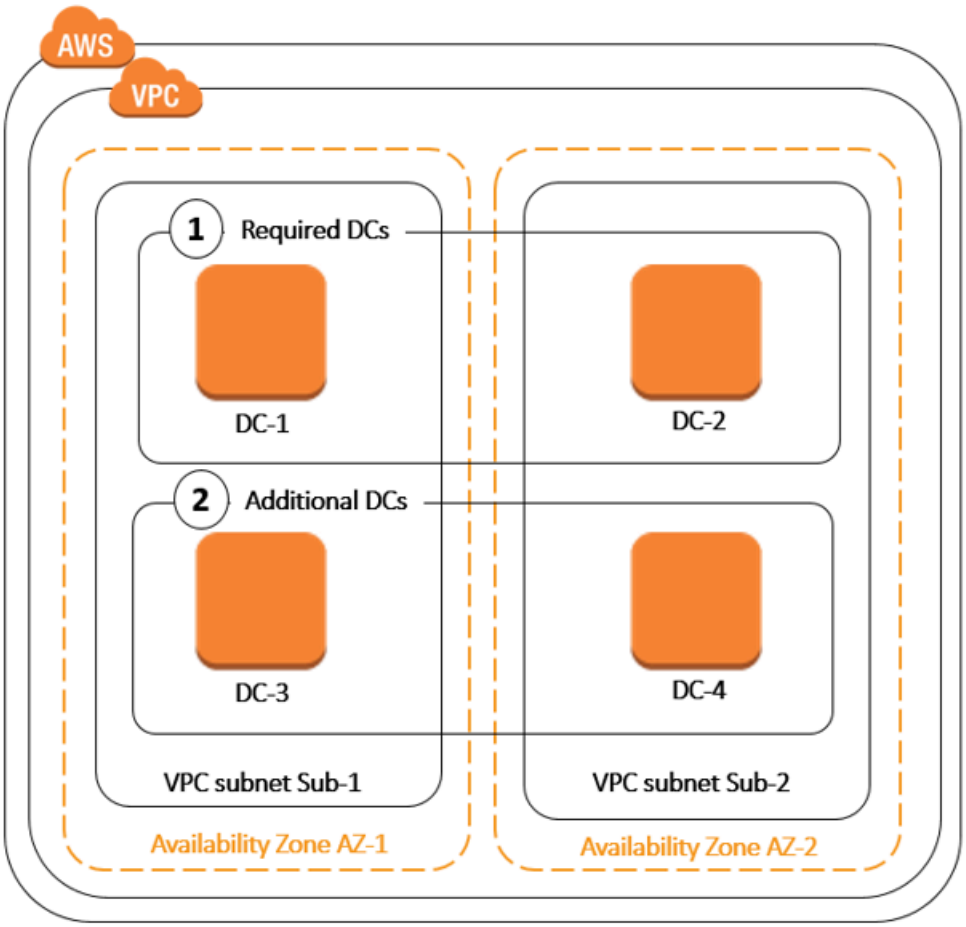
Déploiement de contrôleurs de domaine supplémentaires

Le déploiement de contrôleurs de domaine supplémentaires permet d'augmenter la redondance, ce qui se traduit par une plus grande résilience et une plus grande disponibilité. Ceci améliore également les performances de votre annuaire, grâce à la prise en charge d'un plus grand nombre de demandes Active Directory. Par exemple, vous pouvez désormais utiliser AWS Managed Microsoft AD pour prendre en charge plusieurs applications .NET déployées sur de vastes flottes d'instances Amazon EC2 et Amazon RDS for SQL Server.

Lorsque vous créez votre annuaire pour la première fois, AWS Managed Microsoft AD déploie deux contrôleurs de domaine dans plusieurs zones de disponibilité, ce qui est nécessaire à des fins de haute disponibilité. Plus tard, vous pouvez facilement déployer des contrôleurs de domaine supplémentaires via la AWS Directory Service console en spécifiant simplement le nombre total de contrôleurs de domaine que vous souhaitez. AWS Managed Microsoft AD distribue les contrôleurs de domaine supplémentaires aux zones de disponibilité et aux sous-réseaux Amazon VPC sur lesquels votre annuaire est exécuté.

Par exemple, dans l'illustration ci-dessous, DC-1 et DC-2 représentent les deux contrôleurs de domaine qui ont été initialement créés avec votre annuaire. La AWS Directory Service console désigne ces contrôleurs de domaine par défaut par le terme « Obligatoire ». AWS Managed Microsoft AD localise intentionnellement chacun de ces contrôleurs de domaine dans des zones de disponibilité distinctes lors du processus de création de l'annuaire. Vous pouvez ensuite décider d'ajouter deux contrôleurs de domaine supplémentaires pour mieux répartir la charge

d'authentification sur les pics de connexion. DC-3 et DC-4 représentent les nouveaux contrôleurs de domaine, que la console désigne comme des contrôleurs Supplémentaires. Comme auparavant, AWS Managed Microsoft AD place à nouveau automatiquement les nouveaux contrôleurs de domaine dans différentes zones de disponibilité afin de garantir la haute disponibilité de votre domaine.



Grâce à ce processus, vous n'avez plus besoin de configurer manuellement la réplication des données d'annuaire, la génération automatique des instantanés quotidiens ou la surveillance des contrôleurs de domaine supplémentaires. Il simplifie également la migration et l'exécution des charges de travail stratégiques intégrées à Active Directory dans le cloud AWS sans avoir à déployer et à tenir à jour votre propre infrastructure Active Directory. Vous pouvez également déployer ou supprimer des contrôleurs de domaine supplémentaires pour AWS Managed Microsoft AD à l'aide de l'UpdateNumberOfDomainControllersAPI.

> **Note**
>
> Les contrôleurs de domaine supplémentaires constituent une fonctionnalité régionale de AWS Managed Microsoft AD. Si vous utilisez Réplication multi-régions, les procédures suivantes

doivent être appliquées séparément dans chaque région. Pour plus d'informations, consultez Caractéristiques mondiales et régionales.

Ajout ou suppression de contrôleurs de domaine supplémentaires

Avant d'ajouter ou de supprimer des contrôleurs de domaine supplémentaires, voici plus d'informations sur les exigences relatives aux contrôleurs de domaine :

- Après le déploiement de contrôleurs de domaine supplémentaires, vous pouvez ramener à deux le nombre de contrôleurs de domaine, ce qui correspond au minimum requis pour garantir la tolérance aux pannes et la haute disponibilité.
- Les contrôleurs de domaine supprimés seront supprimés de la liste des contrôleurs de domaine supplémentaires. Les contrôleurs de domaine principal et secondaire sont obligatoires et ne peuvent pas être supprimés.
- Si vous avez configuré votre AWS Managed Microsoft AD pour activer LDAPS, LDAPS sera également activé automatiquement sur tous les contrôleurs de domaine supplémentaires que vous ajouterez. Pour plus d'informations, consultez Activer le protocole LDAP ou LDAPS sécurisé.

Utilisez la procédure suivante pour déployer ou supprimer des contrôleurs de domaine supplémentaires dans votre annuaire AWS Managed Microsoft AD.

Pour ajouter ou supprimer des contrôleurs de domaine supplémentaires

1. Dans le panneau de navigation de la console AWS Directory Service, choisissez Annuaires.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), procédez de l'une des manières suivantes :
   - Si plusieurs régions apparaissent sous Multi-Region replication (Réplication multi-régions), sélectionnez la région dans laquelle vous souhaitez ajouter ou supprimer des contrôleurs de domaine, puis cliquez sur l'onglet Scale & share (Mettre à l'échelle et partager). Pour plus d'informations, consultez Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Multi-Region replication (Réplication multi-régions), choisissez l'onglet Mettre à l'échelle et partager.
4. Dans la section Domain controllers (Contrôleurs de domaine), choisissez Edit (Modifier).

5. Spécifiez le nombre de contrôleurs de domaine à ajouter ou supprimer de votre annuaire, puis choisissez Modify (Modifier).
6. Lorsque AWS Managed Microsoft AD termine le processus de déploiement, tous les contrôleurs de domaine affichent le statut Actif, et la zone de disponibilité et les sous-réseaux Amazon VPC attribués apparaissent. Les nouveaux contrôleurs de domaine sont également répartis sur les zones de disponibilité et sur les sous-réseaux sur lesquels votre annuaire est déjà déployé.

Article AWS de blog sur la sécurité connexe

- Comment augmenter la redondance et les performances de AWS Microsoft AD AWS Directory Service pour Managed en ajoutant des contrôleurs de domaine

Migrer les utilisateurs d'Active Directory vers AWS Managed Microsoft AD

Vous pouvez utiliser le kit de migration Active Directory (ADMT) ainsi que le service d'exportation de mots de passe (PES) pour faire migrer les utilisateurs de votre Active Directory autogéré vers votre répertoire AWS Microsoft AD géré. Cela vous permet de migrer plus facilement les objets Active Directory et les mots de passe chiffrés pour vos utilisateurs.

Pour obtenir des instructions détaillées, veuillez consulter How to migrate your on-premises domain to AWS Managed Microsoft AD using ADMT (français non garanti) sur le blog consacré à la sécurité AWS.

AWS Quotas Managed Microsoft AD

Les quotas par défaut pour AWS Managed Microsoft AD sont les suivants. Sauf indication contraire, chaque quota est spécifique à une région.

AWS Quotas Managed Microsoft AD

Ressource	Quota par défaut
AWS Répertoires Managed Microsoft AD	20
Instantanés manuels *	5 par AWS Managed Microsoft AD
Durée des instantanés manuels **	180 jours

Ressource	Quota par défaut
Nombre maximal de contrôleurs de domaine par annuaire	20
Domaines partagés via Microsoft AD standard ***	5
Domaines partagés via Microsoft AD Entreprise ***	125
Nombre maximal de certificats d'autorité de certification enregistrés par annuaire	5
Nombre maximum de régions AWS au total dans un seul répertoire AWS Managed Microsoft AD (édition Entreprise) ****	5

* Le quota d'instantanés manuels ne peut pas être modifié.

** La durée maximale de prise en charge pour un instantané manuel est de 180 jours et ne peut pas être modifiée. Cela est dû à l'attribut appelé « Tombstone-Lifetime » des objets supprimés. Il définit la durée de conservation d'une sauvegarde de l'état du système d'Active Directory. Il n'est pas possible d'effectuer une restauration à partir d'un instantané datant de plus de 180 jours. Pour plus d'informations, consultez la section Durée de conservation d'une sauvegarde de l'état du système d'Active Directory sur le site Web Microsoft.

*** Le quota par défaut du domaine partagé fait référence au nombre de comptes avec lesquels un répertoire individuel peut être partagé.

**** Cela inclut 1 région principale et jusqu'à 4 régions supplémentaires. Pour de plus amples informations, veuillez consulter Régions principales et régions supplémentaires.

> **Note**
>
> Vous ne pouvez pas attacher une adresse IP publique à votre interface réseau Elastic (ENI) AWS.

Pour plus d'informations concernant la conception d'applications et de la répartition des charges, consultez Programmation de vos applications.

Pour les quotas de stockage et d'objets, veuillez consulter la Table de comparaison sur la page Tarification de Directory ServiceAWS.

Compatibilité des applications pour AWS Managed Microsoft AD

AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) est compatible avec de nombreux AWS services et applications tierces.

Voici une liste des AWS applications et services compatibles :

- Amazon Chime : pour obtenir des instructions détaillées, veuillez consulter la section Connect to your Active Directory (français non garanti).
- Amazon Connect : pour plus d'informations, veuillez consulter la section How Amazon Connect works (français non garanti).
- Amazon EC2 : pour plus d'informations, veuillez consulter Joindre une instance Amazon EC2 à votre compte AWS Microsoft AD géré Active Directory.
- Amazon QuickSight - Pour plus d'informations, consultez la section Gestion des comptes utilisateurs dans Amazon QuickSight Enterprise Edition.
- Amazon RDS for MySQL : pour plus d'informations, veuillez consulter la section Using Kerberos authentication for MySQL (français non garanti).
- Amazon RDS for Oracle : pour plus d'informations, veuillez consulter la section Using Kerberos authentication with Amazon RDS for Oracle (français non garanti).
- Amazon RDS for PostgreSQL : pour plus d'informations, veuillez consulter la section Using Kerberos authentication with Amazon RDS for PostgreSQL (français non garanti).
- Amazon RDS for SQL Server : pour plus d'informations, veuillez consulter la section Using Windows authentication with an Amazon RDS Microsoft SQL Server DB instance (français non garanti).
- Amazon WorkDocs - Pour obtenir des instructions détaillées, consultez Connexion à votre annuaire local avec AWS Managed Microsoft AD.
- Amazon WorkMail - Pour des instructions détaillées, consultez Intégrer Amazon WorkMail à un annuaire existant (configuration standard).
- AWS Client VPN - Pour des instructions détaillées, voir Authentification et autorisation du client.

- AWS IAM Identity Center - Pour des instructions détaillées, voir Connect IAM Identity Center à un Active Directory local.
- AWS License Manager - Pour plus d'informations, consultez la section Abonnements basés sur les utilisateurs dans AWS License Manager.
- AWS Management Console — Pour plus d'informations, voirActivation de l'accès à AWS Management Console avec les informations d'identification AD.
- FSx for Windows File Server : pour plus d'informations, veuillez consulter What is FSx for Windows File Server? (français non garanti).
- WorkSpaces - Pour des instructions détaillées, voir Lancer un WorkSpace à l'aide de AWS Managed Microsoft AD.

En raison de l'ampleur des off-the-shelf applications personnalisées et commerciales qui utilisent Active Directory, AWS elle n'effectue pas et ne peut pas effectuer de vérification formelle ou étendue de la compatibilité des applications tierces avec AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD). Bien que AWS nous travaillons avec les clients pour tenter de surmonter les éventuels problèmes d'installation d'applications qu'ils pourraient rencontrer, nous ne sommes pas en mesure de garantir qu'une application est ou continuera d'être compatible avec AWS Managed Microsoft AD.

Les applications tierces suivantes sont compatibles avec AWS Managed Microsoft AD :

- Activation Active Directory (ADBA)
- Active Directory Certificate Services (AD CS): Enterprise Certificate Authority
- Active Directory Federation Services (AD FS)
- Active Directory Users and Computers (ADUC)
- Application Server (.NET)
- Microsoft Entra(anciennement connu sous le nom de Azure Active Directory (AzureAD))
- Microsoft Entra Connect(anciennement connu sous le nom deAzure Active Directory Connect)
- Réplication de systèmes de fichiers distribués (DFSR)
- Espaces de noms de système de fichiers distribués (DFSN)
- Microsoft Remote Desktop Services Licensing Server
- Microsoft SharePoint Server
- Microsoft SQL Server(y compris les groupes de disponibilité Always On de SQL Server)

- Microsoft System Center Configuration Manager(SCCM) - L'utilisateur qui déploie SCCM doit être membre du groupe des administrateurs de gestion du système AWS délégués.
- Microsoft Windows and Windows Server OS
- Office 365

Remarque : il se peut que certaines des configurations de ces applications ne soient pas prises en charge.

Directives de compatibilité

Bien que les applications peuvent parfois avoir des configurations qui ne sont pas compatibles, les configurations de déploiement d'applications sont souvent capables de surmonter une incompatibilité. La section suivante décrit les motifs les plus courants d'incompatibilité d'une application. Les clients peuvent utiliser ces informations pour étudier les caractéristiques de compatibilité d'une application donnée et identifier les éventuelles modifications à apporter à son déploiement.

- Autorisations de l'administrateur du domaine ou autres autorisations privilégiées – Certaines applications requièrent que vous les installiez en tant qu'administrateur du domaine. Étant donné que vous AWS devez conserver le contrôle exclusif de ce niveau d'autorisation afin de fournir Active Directory en tant que service géré, vous ne pouvez pas agir en tant qu'administrateur de domaine pour installer de telles applications. Cependant, vous pouvez souvent installer de telles applications en déléguant des autorisations spécifiques, moins privilégiées et AWS prises en charge à la personne qui effectue l'installation. Contactez votre fournisseur d'applications pour en savoir plus sur les autorisations précises que requiert votre application. Pour plus d'informations sur les autorisations qui vous AWS permettent de déléguer, consultezQu'est-ce qui est créé avec votre annuaire Microsoft AD Active Directory AWS géré.
- Accès à Active Directory des conteneurs privilégiés : au sein de votre annuaire, AWS Managed Microsoft AD fournit une unité organisationnelle (UO) sur laquelle vous avez un contrôle administratif total. Vous ne possédez pas d'autorisations de création ou d'écriture, mais vous pouvez détenir des autorisations limitées de lecture des conteneurs qui se trouvent à un niveau supérieur dans l'arborescence Active Directory que votre unité d'organisation. Les applications qui créent ou accèdent à des conteneurs, et pour lesquelles vous n'avez pas d'autorisation, peuvent ne pas fonctionner. Toutefois, ces applications ont souvent la capacité d'utiliser un conteneur que vous créez dans votre unité d'organisation comme alternative. Consultez votre fournisseur d'applications pour trouver des moyens de créer et d'utiliser un conteneur dans votre unité

d'organisation comme alternative. Pour en savoir plus sur la gestion de votre unité d'organisation (UO), veuillez consulter la section Comment administrer AWS Managed Microsoft AD.

- Modifications du schéma au cours du processus d'installation — Certaines Active Directory applications nécessitent des modifications du schéma Active Directory par défaut, et elles peuvent tenter d'installer ces modifications dans le cadre du flux de travail d'installation de l'application. En raison de la nature privilégiée des extensions de schéma, cela AWS est possible en important des fichiers LDIF (Lightweight Directory Interchange Format) uniquement via la console AWS Directory Service , la CLI ou le SDK. Ces applications sont souvent accompagnées d'un fichier LDIF que vous pouvez appliquer au répertoire par le biais du processus de mise à jour du AWS Directory Service schéma. Pour en savoir plus sur le fonctionnement du processus d'importation LDIF, veuillez consulter la section Tutoriel : extension de votre schéma Microsoft AD AWS géré. Vous pouvez installer l'application de sorte à contourner l'installation du schéma pendant le processus d'installation.

Applications incompatibles connues

La liste suivante répertorie les off-the-shelf applications commerciales fréquemment demandées pour lesquelles nous n'avons pas trouvé de configuration compatible avec AWS Managed Microsoft AD. AWS met à jour cette liste de temps à autre, à sa seule discrétion, par courtoisie afin de vous aider à éviter des efforts improductifs. AWS fournir ces informations sans garantie ni réclamation concernant la compatibilité actuelle ou future.

- Active Directory Certificate Services (AD CS): Certificate Enrollment Web Service
- Active Directory Certificate Services (AD CS): Certificate Enrollment Policy Web Service
- Microsoft Exchange Server
- Microsoft Skype for Business Server

AWS Tutoriels de laboratoire de test Microsoft AD gérés

Cette section propose une série de didacticiels guidés destinés à vous aider à créer un environnement de laboratoire de test dans AWS lequel vous pourrez expérimenter avec AWS Managed Microsoft AD.

Rubriques

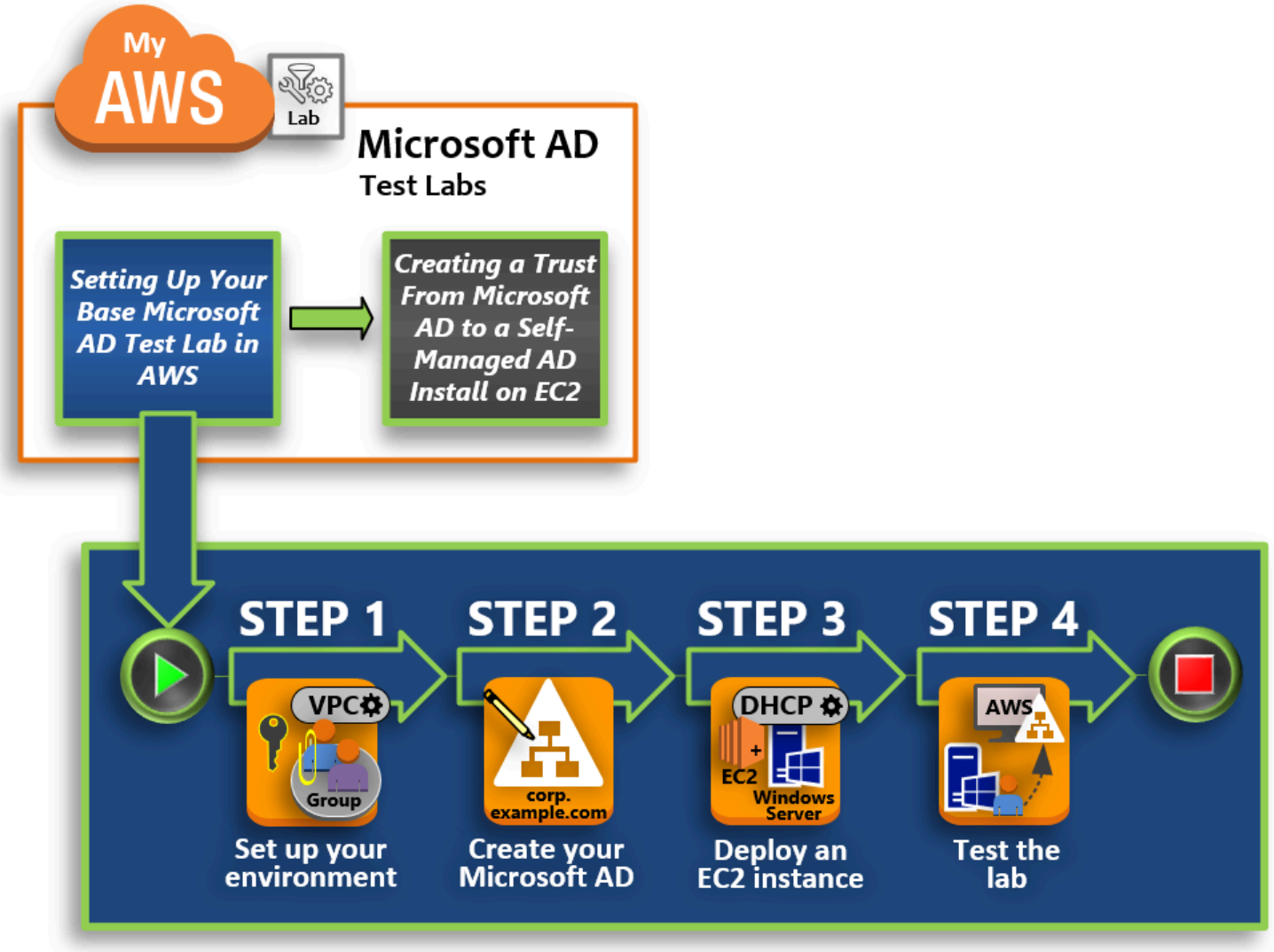
- Tutoriel : Configuration de votre laboratoire de test Microsoft AD AWS géré de base dans AWS

- Tutoriel : Création d'une relation de confiance entre AWS Managed Microsoft AD et une installation Active Directory autogérée sur Amazon EC2

Tutoriel : Configuration de votre laboratoire de test Microsoft AD AWS géré de base dans AWS

Ce didacticiel vous explique comment configurer votre AWS environnement pour préparer une nouvelle installation de AWS Managed Microsoft AD qui utilise une nouvelle instance Amazon EC2 exécutant Windows Server 2019. Il vous apprend ensuite à utiliser les outils d'administration Active Directory classiques pour gérer votre environnement Microsoft AD AWS géré à partir de votre instance Windows EC2. À la fin du didacticiel, vous aurez défini les conditions requises pour le réseau et configuré une nouvelle forêt Microsoft AD AWS gérée.

Comme le montre l'illustration suivante, l'atelier que vous créez à partir de ce didacticiel est l'élément de base de l'apprentissage pratique de AWS Managed Microsoft AD. Vous pourrez ensuite ajouter des didacticiels facultatifs pour améliorer votre expérience pratique. Cette série de didacticiels est idéale pour toute personne qui débute avec AWS Managed Microsoft AD et qui souhaite bénéficier d'un environnement de test à des fins d'évaluation. Ce didacticiel vous prendra environ 1 heure.



[Étape 1 : Configuration de votre AWS environnement pour AWS Managed Microsoft AD Active Directory]

Une fois que vous avez terminé vos tâches prérequises, vous créez et configurez un Amazon VPC dans votre instance EC2.

[Étape 2 : Création de votre répertoire Microsoft AD Active Directory AWS géré]

Au cours de cette étape, vous configurez AWS Managed Microsoft AD AWS pour la première fois.

[Étape 3 : Déployer une instance Amazon EC2 pour gérer votre annuaire AWS Microsoft AD Active Directory géré]

Vous allez ici exécuter les différentes tâches post-déploiement nécessaires pour que les ordinateurs clients puissent se connecter à votre nouveau domaine et configurer un nouveau système Windows Server dans EC2.

[Étape 4 : vérifier que l'atelier de test de base est opérationnel]

Enfin, en tant qu'administrateur, vous devez vérifier que vous pouvez vous identifier et vous connecter à AWS Managed Microsoft AD depuis votre système Windows Server dans EC2. Une fois que vous aurez confirmé que le laboratoire est opérationnel, vous pourrez continuer d'ajouter d'autres modules guides de votre atelier de test.

Prérequis

Si vous prévoyez de suivre uniquement les étapes de l'interface utilisateur décrites dans ce didacticiel pour créer votre atelier de test, vous pouvez ignorer cette section préalable et passer directement à l'étape 1. Toutefois, si vous prévoyez d'utiliser des AWS CLI commandes ou des AWS Tools for Windows PowerShell modules pour créer votre environnement de laboratoire de test, vous devez d'abord configurer les éléments suivants :

- Utilisateur IAM avec l'accès et la clé d'accès secrète — Un utilisateur IAM avec une clé d'accès est requis si vous souhaitez utiliser les modules AWS CLI or AWS Tools for Windows PowerShell . Si vous n'avez pas de clé d'accès, veuillez consulter la section Creating, modifying, and viewing access keys (AWS Management Console) (français non garanti).
- AWS Command Line Interface (facultatif) — Téléchargez et installez AWS CLI le sous Windows. Une fois installé, ouvrez l'invite de commande ou Windows PowerShell la fenêtre, puis tapez`aws configure`. Notez que vous avez besoin de la clé d'accès et de la clé secrète pour effectuer la configuration. Référez-vous au premier prérequis pour savoir comment procéder. Vous devrez renseigner les informations suivantes :
  - AWS ID de clé d'accès [Aucun] : `AKIAIOSFODNN7EXAMPLE`
  - AWS clé d'accès secrète [Aucune] : `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`
  - Default Region name [None] : `us-west-2`
  - Default output format [None] : `json`
- AWS Tools for Windows PowerShell (facultatif) – Téléchargez et installez la dernière version de AWS Tools for Windows PowerShell depuis https://aws.amazon.com/powershell/, puis exécutez la commande suivante. Notez que vous avez besoin de votre clé d'accès et de votre clé secrète pour effectuer la configuration. Référez-vous au premier prérequis pour savoir comment procéder.

```
Set-AWSCredentials -AccessKey {AKIAIOSFODNN7EXAMPLE} -SecretKey
{wJalrXUtnFEMI/K7MDENG/ bPxRfiCYEXAMPLEKEY} -StoreAs {default}
```

Étape 1 : Configuration de votre AWS environnement pour AWS Managed Microsoft AD Active Directory

Avant de créer AWS Managed Microsoft AD dans votre laboratoire de AWS test, vous devez d'abord configurer votre paire de clés Amazon EC2 afin que toutes les données de connexion soient cryptées.

Création d'une paire de clés

Si vous possédez déjà une paire de clés, vous pouvez ignorer cette étape. Pour plus d'informations sur les paires de clés Amazon EC2, consultez la section Créer des paires de clés.

Création d'une paire de clés

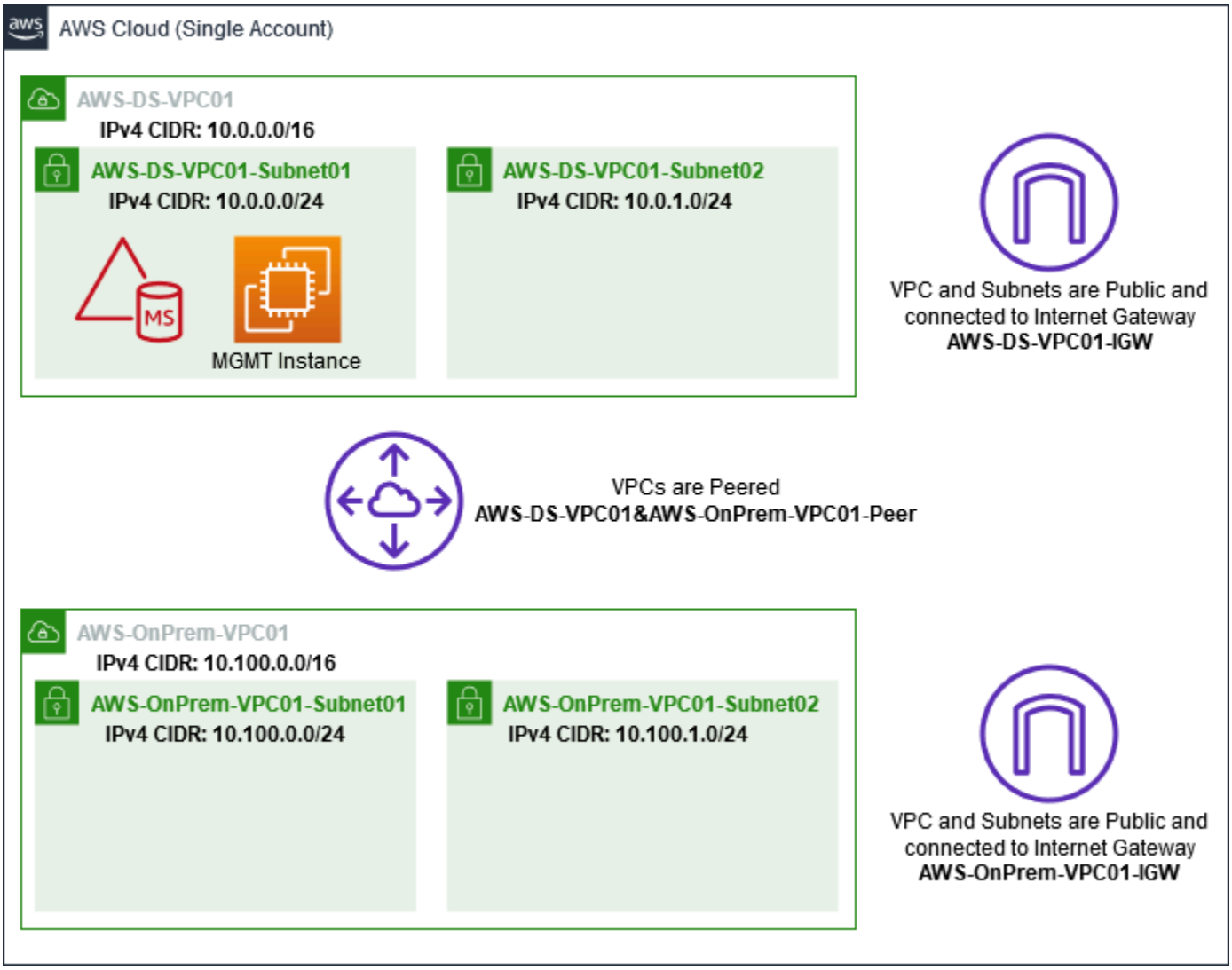
1. Connectez-vous à la console Amazon EC2 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sous Réseau et sécurité, choisissez Paires de clés, puis sélectionnez Créer une paire de clés.
3. Pour Key pair name (Nom de la paire de clés), saisissez **`AWS-DS-KP`**. Pour Key pair file format (Format de fichier de la paire de clés), sélectionnez pem, puis choisissez Create (Créer).
4. Le fichier de clé privée est automatiquement téléchargé dans votre navigateur. Le nom de fichier est le nom que vous avez spécifié lorsque vous avez créé votre paire de clés, suivi de l'extension `.pem`. Enregistrez le fichier de clé privée en lieu sûr.

> **Important**
>
> C'est votre seule occasion d'enregistrer le fichier de clé privée. Vous devez indiquer le nom de votre paire de clés quand vous lancez une instance, ainsi que la clé privée correspondante chaque fois que vous déchiffrez le mot de passe de l'instance.

Créez, configurez et associez deux Amazon VPC

Comme le montre l'illustration suivante, ce processus à plusieurs étapes permet de créer et de configurer deux VPC publics, deux sous-réseaux publics par VPC, une passerelle Internet par VPC et une connexion d'appairage de VPC entre les VPC. Nous avons choisi d'utiliser des VPC et des sous-réseaux publics pour des raisons de simplicité et de coût. Pour les charges de travail de production, nous vous recommandons d'utiliser des VPC privés. Pour de plus amples informations

sur l'amélioration de la sécurité VPC, veuillez consulter Security in Amazon Virtual Private Cloud (français non garanti).



Tous les AWS CLI PowerShell exemples utilisent les informations VPC ci-dessous et sont intégrés dans us-west-2. Vous pouvez choisir n'importe quelle région prise en charge pour créer votre environnement. Pour de plus amples informations, veuillez consulter What is Amazon VPC? (français non garanti).

Étape 1 : Créer deux VPC

Au cours de cette étape, vous devez créer deux VPC dans le même compte en utilisant les paramètres spécifiés dans le tableau suivant. AWS Managed Microsoft AD prend en charge l'utilisation de comptes distincts avec Partagez votre annuaire cette fonctionnalité. Le premier VPC sera utilisé pour Managed AWS Microsoft AD. Le deuxième VPC sera utilisé pour des ressources

qui pourront servir plus tard dans Tutoriel : Création d'une relation de confiance entre AWS Managed Microsoft AD et une installation Active Directory autogérée sur Amazon EC2.

Informations sur les VPC Active Directory gérés	Informations sur le VPC sur site
Nom du tag : AWS-DS-VPC01 Bloc d'adresse CIDR IPv4 : 10.0.0.0/16 Bloc d'adresse CIDR IPv6 : Pas de bloc d'adresse CIDR IPv6 Location : Par défaut	Balise de nom : AWS- OnPrem -VPC01 Bloc d'adresse CIDR IPv4 : 10.100.0.0/16 Bloc d'adresse CIDR IPv6 : Pas de bloc d'adresse CIDR IPv6 Location : Par défaut

Pour obtenir des instructions détaillées, veuillez consulter Creating a VPC (français non garanti).

Étape 2 : Créer deux sous-réseaux par VPC

Après avoir créé les VPC, vous devrez créer deux sous-réseaux par VPC en utilisant les paramètres spécifiés dans le tableau suivant. Pour ce laboratoire de test, chaque sous-réseau sera de type /24. Cela permet d'émettre jusqu'à 256 adresses par sous-réseau. Chaque sous-réseau doit être un dans une zone de disponibilité distincte. Mettre chaque sous-réseau dans une zone de disponibilité distincte est un des AWS Conditions préalables à la gestion de Microsoft AD.

Informations sur le sous-réseau AWS-DS-VPC01 :	AWS- Informations sur le OnPrem sous-réseau -VPC01
Balise de nom : AWS-DS-VPC01-subnet01 VPC : vpc-xxxxxxxxxxxxxxxxx-DS-VPC01 AWS Zone de disponibilité : us-west-2a Bloc d'adresse CIDR IPv4 : 10.0.0.0/24	Balise de nom : AWS- OnPrem -vPC01-subnet01 VPC : AWS vpc-xxxxxxxxxxxxxxxxx - -VPC01 OnPrem Zone de disponibilité : us-west-2a Bloc d'adresse CIDR IPv4 : 10.100.0.0/24
Balise de nom : AWS-DS-VPC01-subnet02 VPC : vpc-xxxxxxxxxxxxxxxxx-DS-VPC01 AWS	Tag de nom : AWS- OnPrem -vPC01-subnet02

Informations sur le sous-réseau AWS-DS-VPC01 :	AWS- Informations sur le OnPrem sous-réseau -VPC01
Zone de disponibilité : us-west-2b Bloc d'adresse CIDR IPv4 : 10.0.1.0/24	VPC : AWS vpc-xxxxxxxxxxxxxxxxx - -VPC01 OnPrem Zone de disponibilité : us-west-2b Bloc d'adresse CIDR IPv4 : 10.100.1.0/24

Pour obtenir des instructions détaillées, veuillez consulter Creating a subnet in your VPC (français non garanti).

Étape 3 : Créer et attacher une passerelle Internet à vos VPC

Puisque nous utilisons des VPC publics, vous devrez créer et attacher une passerelle Internet à vos VPC en utilisant les paramètres spécifiés dans le tableau suivant. Cela vous donnera la possibilité de vous connecter à vos instances EC2 et de les gérer.

Informations sur la passerelle Internet AWS-DS-VPC01	AWS- OnPrem -Informations sur la passerelle Internet Gateway VPC01
Nom du tag : AWS-DS-VPC01-IGW VPC : vpc-xxxxxxxxxxxxxxxxx-DS-VPC01 AWS	Balise de nom : AWS- OnPrem -VPC01-IGW VPC : AWS vpc-xxxxxxxxxxxxxxxxx - -VPC01 OnPrem

Pour obtenir des instructions détaillées, veuillez consulter Internet gateways (français non garanti).

Étape 4 : Configuration d'une connexion d'appairage VPC entre AWS-DS-VPC01 et -VPC01 AWS OnPrem

Étant donné que vous avez déjà créé deux VPC précédemment, vous devrez les mettre en réseau à l'aide de l'appairage de VPC en utilisant les paramètres spécifiés dans le tableau suivant. Bien qu'il existe de nombreuses manières de connecter vos VPC, ce didacticiel utilisera le peering VPC. AWS Managed Microsoft AD prend en charge de nombreuses solutions pour connecter vos VPC, notamment le peering VPC, Transit Gateway et VPN.

Étiquette nominative de connexion d'appairage : AWS-DS-VPC01& -AWS-VPC01-Peer OnPrem

VPC (demandeur) : vpc-xxxxxxxxxxxxxxxxx -DS-VPC01 AWS

Compte : Mon compte

Région : Cette région

VPC (Accepter) : vpc-xxxxxxxxxxxxxxxxx - -VPC01 AWS OnPrem

Pour obtenir des instructions sur la création d'une connexion d'appairage de VPC avec un autre VPC depuis votre compte, veuillez consulter Creating a VPC peering connection with another VPC in your account (français non garanti).

Étape 5 : Ajouter deux routes à la table de routage principale de chaque VPC

Pour que les passerelles Internet et la connexion d'appairage de VPC créées au cours des étapes précédentes soient fonctionnelles, vous devez mettre à jour la table de routage principale des deux VPC en utilisant les paramètres spécifiés dans le tableau suivant. Vous allez ajouter deux routes : 0.0.0.0/0, qui desservira toutes les destinations non explicitement connues de la table de routage et 10.0.0.0/16 ou 10.100.0.0/16, qui desservira chaque VPC via la connexion d'appairage de VPC établie ci-dessus.

Vous pouvez facilement trouver la bonne table de routage pour chaque VPC en filtrant sur le nom du VPC (AWS-DS-VPC01 ou - -VPC01). AWS OnPrem

Informations sur la route 1 AWS-DS-VPC01	Informations sur la route 2 AWS-DS-VPC01	AWS- Informations OnPrem sur la route 1 -VPC01	AWS- Informations OnPrem sur la route 2 -VPC01
Destination : 0.0.0.0/0 Cible : igw-xxxxx xxxxxxxxxxxx -DS-VPC01-IGW AWS	Destination : 10.100.0.0/16 Cible : pcx-xxxxx xxxxxxxxxxxxxxxx -DS-VPC01& - AWS-VPC01-peer AWS OnPrem	Destination : 0.0.0.0/0 Cible : AWS igw-xxxxxxxxxxxxxxxxx -OnPrem-VPC01	Destination : 10.0.0.0/16 Cible : pcx-xxxxx xxxxxxxxxxxxxxxx -DS-VPC01& - AWS-VPC01-peer AWS OnPrem

Pour obtenir des instructions sur l'ajout de routes à une table de routage de VPC, veuillez consulter Adding and removing routes from a route table (français non garanti).

Création de groupes de sécurité pour les instances Amazon EC2

Par défaut, AWS Managed Microsoft AD crée un groupe de sécurité pour gérer le trafic entre ses contrôleurs de domaine. Dans cette section, vous devrez créer 2 groupes de sécurité (un pour chaque VPC) qui seront utilisés pour gérer le trafic dans votre VPC pour vos instances EC2 à l'aide des paramètres spécifiés dans les tableaux suivants. Vous allez également ajouter une règle qui autorise le trafic entrant RDP (3389) entrant depuis n'importe où et pour tous les types de trafic entrant depuis le VPC local. Pour en savoir plus, veuillez consulter la section Amazon EC2 security groups for Windows instances (français non garanti).

Informations sur le groupe de sécuritéAWS-DS-VPC01 :
Nom du groupe de sécurité : AWS DS Test Lab Security Group
Description : Groupe de sécurité AWS DS Test Lab
VPC : vpc-xxxxxxxxxxxxxxxxx-DS-VPC01 AWS

Règles entrantes du groupe de sécurité pour AWS-DS-VPC01

Type	Protocole	Plage de ports	Source	Type de trafic
Destination	TCP	3389	Mon IP	Bureau à distance
Tout le trafic	Tous	Tous	10.0.0.0/16	Tout le trafic du VPC local

Règles de sortie du groupe de sécurité pour AWS-DS-VPC01

Type	Protocole	Plage de ports	Destination	Type de trafic
Tout le trafic	Tous	Tous	0.0.0.0/0	Tout le trafic

AWS- Informations OnPrem sur le groupe de sécurité -VPC01 :
Nom du groupe de sécurité : AWS OnPrem Test Lab Security Group.
Description : Groupe de sécurité du laboratoire de AWS OnPrem test.
VPC : AWS vpc-xxxxxxxxxxxxxxxxx - -VPC01 OnPrem

Règles entrantes du groupe de sécurité pour AWS- -VPC01 OnPrem

Type	Protocole	Plage de ports	Source	Type de trafic
Destination	TCP	3389	Mon IP	Bureau à distance
Destination	TCP	53	10.0.0.0/16	DNS
Destination	TCP	88	10.0.0.0/16	Kerberos
Destination	TCP	389	10.0.0.0/16	LDAP
Destination	TCP	464	10.0.0.0/16	Mot de passe Kerberos (modification/définition)
Destination	TCP	445	10.0.0.0/16	SMB / CIFS
Destination	TCP	135	10.0.0.0/16	Réplication
Destination	TCP	636	10.0.0.0/16	LDAP SSL
Destination	TCP	49152 - 65535	10.0.0.0/16	RPC
Destination	TCP	3268 - 3269	10.0.0.0/16	LDAP GC & LDAP GC SSL
Règle UDP personnalisée	UDP	53	10.0.0.0/16	DNS

Type	Protocole	Plage de ports	Source	Type de trafic
Règle UDP personnalisée	UDP	88	10.0.0.0/16	Kerberos
Règle UDP personnalisée	UDP	123	10.0.0.0/16	Heure Windows
Règle UDP personnalisée	UDP	389	10.0.0.0/16	LDAP
Règle UDP personnalisée	UDP	464	10.0.0.0/16	Mot de passe Kerberos (modification/définition)
Tout le trafic	Tous	Tous	10.100.0.0/16	Tout le trafic du VPC local

Règles sortantes du groupe de sécurité pour AWS- -VPC01 OnPrem

Type	Protocole	Plage de ports	Destination	Type de trafic
Tout le trafic	Tous	Tous	0.0.0.0/0	Tout le trafic

Pour obtenir des instructions détaillées sur la création et l'ajout de règles à vos groupes de sécurité, veuillez consulter Working with security groups (français non garanti).

Étape 2 : Création de votre répertoire Microsoft AD Active Directory AWS géré

Vous pouvez créer votre annuaire selon trois méthodes différentes. Vous pouvez utiliser la AWS Management Console procédure (recommandée pour ce didacticiel) ou vous pouvez utiliser les AWS Tools for Windows PowerShell procédures AWS CLI ou pour créer votre répertoire.

Méthode 1 : pour créer votre répertoire Microsoft AD AWS géré (AWS Management Console)

1. Dans le panneau de navigation de la console AWS Directory Service, choisissez Annuaires, puis Configurer un annuaire.

2. Sur la page Sélectionner un type d'annuaire, choisissez AWS Managed Microsoft AD, puis Suivant.
3. Sur la page Enter directory information (Saisir les détails de l'annuaire), indiquez les informations suivantes, puis choisissez Next (Suivant).

   - Pour Edition (Édition), choisissez Standard Edition (Édition standard) ou Enterprise Edition (Édition d'entreprise). Pour plus d'informations sur les éditions, veuillez consulter AWS Directory Service for Microsoft Active Directory Service (français non garanti).
   - Pour Directory DNS name (Nom DNS de l'annuaire), tapez **`corp.example.com`**.
   - Pour Directory NetBIOS name (Nom NetBIOS de l'annuaire), saisissez **`corp`**.
   - Pour Directory description (Description de l'annuaire), saisissez **`AWS DS Managed`**.
   - Pour Mot de passe administrateur, saisissez le mot de passe que vous souhaitez utiliser pour ce compte, puis saisissez de nouveau le mot de passe dans le champ Confirmer le mot de passe. Ce compte Admin est automatiquement créé pendant le processus de création de l'annuaire. Le mot de passe ne peut pas contenir le terme admin. Le mot de passe de l'administrateur de l'annuaire est sensible à la casse et doit comporter entre 8 et 64 caractères (inclus). Il doit également contenir au moins un caractère de trois des quatre catégories suivantes :
     - Lettres minuscules (a-z)
     - Lettres majuscules (A-Z)
     - Chiffres (0-9)
     - Caractères non alphanumériques (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
4. Sur la page Choose VPC and subnets (Choisir un VPC et des sous-réseaux), indiquez les informations suivantes, puis choisissez Next (Suivant).

   - Pour VPC, choisissez l'option qui commence par AWS-DS-VPC01 et qui se termine par (10.0.0.0/16).
   - Pour Subnets (Sous-réseaux), sélectionnez les sous-réseaux publics 10.0.0.0/24 et 10.0.1.0/24.
5. Sur la page Review & create (Vérifier et créer), vérifiez les informations concernant l'annuaire et effectuez les modifications nécessaires. Lorsque les informations sont correctes, choisissez Create directory (Créer l'annuaire). La création de l'annuaire prend entre 20 et 40 minutes. Une fois l'annuaire créé, le champ Statut prend la valeur Actif.

Méthode 2 : pour créer votre Microsoft AD AWS géré (Windows PowerShell) (facultatif)

1. Ouvrir Windows PowerShell.
2. Saisissez la commande suivante. Assurez-vous d'utiliser les valeurs fournies à l'étape 4 de la AWS Management Console procédure précédente.

```
New-DSMicrosoftAD -Name corp.example.com -ShortName corp -Password P@ssw0rd
 -Description “AWS DS Managed” - VpcSettings_VpcId vpc-xxxxxxxx -
VpcSettings_SubnetId subnet-xxxxxxxx, subnet-xxxxxxxx
```

Méthode 3 : pour créer votre Microsoft AD AWS géré (AWS CLI) (facultatif)

1. Ouvrez le AWS CLI.
2. Saisissez la commande suivante. Assurez-vous d'utiliser les valeurs fournies à l'étape 4 de la AWS Management Console procédure précédente.

```
aws ds create-microsoft-ad --name corp.example.com --short-name corp --
password P@ssw0rd --description "AWS DS Managed" --vpc-settings VpcId= vpc-
xxxxxxxx,SubnetIds= subnet-xxxxxxxx, subnet-xxxxxxxx
```

Étape 3 : Déployer une instance Amazon EC2 pour gérer votre annuaire AWS Microsoft AD Active Directory géré

Pour cet atelier, nous utilisons des instances Amazon EC2 dotées d'adresses IP publiques afin de faciliter l'accès à l'instance de gestion où que vous soyez. Dans un environnement de production, vous pouvez utiliser des instances situées dans un VPC privé qui ne sont accessibles que via un VPN ou AWS Direct Connect un lien. Il n'est pas nécessaire que l'instance possède une adresse IP publique.

Dans cette section, vous allez exécuter les différentes tâches post-déploiement nécessaires pour que les ordinateurs clients puissent se connecter à votre domaine à l'aide de Windows Server sur votre nouvelle instance EC2. Vous allez utiliser Windows Server dans l'étape suivante pour vérifier que votre atelier de test est opérationnel.

Facultatif : créez un ensemble d'options DHCP dans AWS-DS-VPC01 pour votre répertoire

Dans cette procédure facultative, vous configurez une étendue d'options DHCP afin que les instances EC2 de votre VPC utilisent automatiquement votre AWS Microsoft AD géré pour la résolution DNS. Pour plus d'informations, veuillez consulter DHCP options sets (français non garanti).

Pour créer un jeu d'options DHCP défini pour votre annuaire

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez DHCP Options Sets, puis sélectionnez Create DHCP options set.
3. Dans la page Créer un jeu d'options DHCP, entrez les valeurs suivantes pour votre annuaire :
   - Pour Name (Nom), tapez **`AWS DS DHCP`**.
   - Pour Domain name (Nom de domaine), tapez **`corp.example.com`**.
   - Pour Domain name servers (Serveurs de noms de domaine), tapez les adresses IP des serveurs DNS de votre annuaire fourni par AWS .

     > **Note**
     >
     > Pour trouver ces adresses, rendez-vous sur la page AWS Directory Service Répertoires, puis choisissez l'ID de répertoire applicable. Sur la page Détails, identifiez et utilisez les adresses IP affichées dans l'adresse DNS.
     > Pour trouver ces adresses, rendez-vous sur la page AWS Directory Service Annuaires, puis choisissez l'ID de répertoire applicable. Choisissez ensuite Mettre à l'échelle et partager. Sous Contrôleurs de domaine, identifiez et utilisez les adresses IP affichées dans Adresse IP.

   - Ne renseignez aucune valeur dans les champs Serveurs NTP, Serveurs de noms NetBIOS et Type de nœud NetBIOS.
4. Choisissez Créer un jeu d'options DHCP, puis choisissez Fermer. Le nouveau jeu d'options DHCP apparaît dans votre liste d'options DHCP.
5. Notez l'ID du nouveau jeu d'options DHCP (dopt-***xxxxxxxx***). Vous en aurez besoin à la fin de cette procédure lorsque vous associerez le nouveau jeu d'options à votre VPC.

> **Note**
>
> La jonction transparente de domaines fonctionne sans qu'il soit nécessaire de configurer un jeu d'options DHCP.

6. Dans le panneau de navigation, sélectionnez Your VPCs (Vos VPC).
7. Dans la liste des VPC, sélectionnez AWS DS VPC, choisissez Actions, puis sélectionnez Modifier le jeu d'options DHCP.
8. Sur la page Modifier le jeu d'options DHCP, sélectionnez les options que vous avez enregistrées à l'étape 5, puis choisissez Enregistrer.

Créez un rôle pour joindre des instances Windows à votre domaine Microsoft AD AWS géré

Utilisez cette procédure pour configurer un rôle qui joint une instance Windows Amazon EC2 à un domaine. Pour plus d'informations, consultez Associez facilement une instance Windows Amazon EC2 à votre compte AWS Microsoft AD géré Active Directory.

Pour configurer EC2 afin de relier les instances Windows à votre domaine

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation de la console IAM, choisissez Rôles, puis Créer un rôle.
3. Sous Select type of trusted entity (Sélectionner le type d'entité approuvée), choisissez service AWS .
4. Immédiatement sous Choisir le service qui utilisera ce rôle, choisissez EC2, puis Next: Permissions (Suivant : Autorisations).
5. Sur la page Stratégie d'autorisations attachée, procédez comme suit :

   - Cochez la case à côté de la politique ManagedInstanceCore gérée par AmazonSSM. Cette stratégie fournit les autorisations minimales nécessaires pour pouvoir utiliser le service Systems Manager.
   - Cochez la case à côté de la politique DirectoryServiceAccess gérée par AmazonSSM. La stratégie fournit les autorisations nécessaires pour joindre des instances à un domaine Active Directory géré par AWS Directory Service.

Pour plus d'informations sur ces politiques gérées et sur les autres politiques que vous pouvez attacher à un profil d'instance IAM pour Systems Manager consultez Création d'un profil d'instance IAM pour Systems Manager dans le Guide de l'utilisateur AWS Systems Manager . Pour plus d'informations sur les politiques gérées, veuillez consulter AWS Managed policies (français non garanti) dans le Guide de l'utilisateur IAM.

6. Sélectionnez Suivant : Étiquettes.
7. (Facultatif) Ajoutez une ou plusieurs paires clé-valeur de balise afin d'organiser, de suivre ou de contrôler l'accès pour ce rôle, puis sélectionnez Suivant : Vérifier.
8. Dans Nom du rôle, entrez un nom pour le rôle qui décrit qu'il est utilisé pour joindre des instances à un domaine, tel que EC2 DomainJoin.
9. (Facultatif) Pour Role description (Description du rôle), entrez une description.
10. Sélectionnez Créer un rôle. Le système vous renvoie à la page Rôles.

Créez une instance Amazon EC2 et rejoignez automatiquement le répertoire

Dans cette procédure, vous configurez un système Windows Server dans une instance EC2 qui pourra être utilisée ultérieurement pour administrer les utilisateurs, les groupes et les politiques dans Active Directory.

Pour créer une instance EC2 et rejoindre automatiquement l'annuaire

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Choisissez Launch Instances (Lancer les instances).
3. Sur la page Step 1 (Étape 1), en regard de Microsoft Windows Server 2019 Base - ami-***xxxxxxxxxxxxxxxx***, cliquez sur Select (Sélectionner).
4. Sur la page Step 2 (Étape 2), sélectionnez t3.micro (notez que vous pouvez choisir un type d'instance plus volumineux), puis cliquez sur Next: Configure Instance Details (Suivant : Configurer les détails de l'instance).
5. Sur la page Étape 3, procédez comme suit :

   - Pour Réseau, choisissez le VPC qui se termine par AWS-DS-VPC01 (par exemple, vpc-***xxxxxxxxxxxxxxxxx*** | AWS-DS-VPC01).

- Pour Sous-réseau sélectionnez Sous-réseau public 1, qui doit être préconfiguré pour la zone de disponibilité de votre choix (par exemple, subnet-***xxxxxxxxxxxxxxxxx*** | AWS-DS-VPC01-Subnet01 | ***us-west-2a***).
- Pour Attribuer automatiquement l'adresse IP publique, choisissez Activer (si le sous-réseau n'est pas défini sur Activer par défaut).
- Pour Répertoire de jonction de domaines, choisissez corp.example.com (d-***xxxxxxxxxx***).
- Pour le rôle IAM, choisissez le nom dans lequel vous avez attribué votre rôle d'instanceCréez un rôle pour joindre des instances Windows à votre domaine Microsoft AD AWS géré, par exemple DomainJoinEC2.
- Conservez les valeurs par défaut des autres paramètres.
- Choisissez Next: Add Storage (Suivant : Ajouter le stockage).

6. Sur la page Étape 4, conservez les paramètres par défaut, puis choisissez Next: Add Tags.
7. Sur la page Étape 5, choisissez Add Tag. Sous Key (Clé), saisissez **`corp.example.com-mgmt`**, puis choisissez Next: Configure Security Group (Suivant : Configurer le groupe de sécurité).
8. Sur la page Étape 6, choisissez Sélectionner un groupe de sécurité existant, sélectionnez AWS DS Test Lab Security Group (que vous avez précédemment défini dans le didacticiel de base), puis choisissez Vérifier et lancer pour vérifier votre instance.
9. Sur la page Étape 7, vérifiez la page, puis choisissez Lancer.
10. Dans la boîte de dialogue Sélectionner une paire de clés existante ou créer une nouvelle paire de clés, procédez comme suit :

    - Choisissez Choisir une paire de clés existante.
    - Sous Sélectionner une paire de clés, choisissez AWS-DS-KP.
    - Cochez la case I acknowledge....
    - Choisissez Launch Instances (Démarrer les instances).

11. Sélectionnez Afficher les instances pour revenir à la console Amazon EC2 et consulter l'état du déploiement.

Installation des outils Active Directory sur votre instance EC2

Vous avez le choix entre deux méthodes pour installer les outils de gestion de domaines Active Directory sur votre instance EC2. Vous pouvez utiliser l'interface utilisateur du gestionnaire de serveur (recommandée pour ce didacticiel) ouWindows PowerShell.

Pour installer les outils Active Directory sur votre instance EC2 (avec Server Manager)

1. Dans la console Amazon EC2, choisissez Instances, sélectionnez l'instance que vous venez de créer, puis sélectionnez Connecter.
2. Dans la boîte de dialogue Connectez-vous à votre instance, sélectionnez Obtenir le mot de passe pour récupérer votre mot de passe si vous ne l'avez pas déjà fait, puis choisissez Télécharger le fichier Bureau à distance.
3. Dans la boîte de dialogue Windows Security (Sécurité Windows) saisissez vos informations d'identification d'administrateur local pour que l'ordinateur Windows Server puisse se connecter (par exemple : **`administrator`**).
4. Dans le menu Démarrer, choisissez Server Manager.
5. Dans le Tableau de bord, choisissez Ajouter des rôles et des fonctionnalités.
6. Dans l'Assistant Ajouter des rôles et des fonctionnalités, choisissez Suivant.
7. Sur la page Sélectionner le type d'installation, choisissez Installation basée sur un rôle ou une fonctionnalité, puis choisissez Suivant.
8. Sur la page Sélectionner le serveur de destination, assurez-vous que le serveur local est sélectionné, puis choisissez Suivant.
9. Sur la page Sélectionner des rôles de serveur, cliquez sur Suivant.
10. Sur la page Sélectionner les fonctionnalités, procédez comme suit :
    - Cochez la case Gestion des stratégies de groupe.
    - Développez Outils d'administration de serveur distant, puis Outils d'administration de rôles.
    - Cochez la case Outils AD DS et AD LDS.
    - Cochez la case DNS Server Tools.
    - Choisissez Suivant.
11. Sur la page Confirmer les sélections d'installation, vérifiez les informations, puis cliquez sur Installer. Une fois l'installation des fonctionnalités terminée, les nouveaux outils ou composants suivants seront disponibles dans le dossier Outils d'administration Windows, via le menu Démarrer.

- Centre d'administration Active Directory
- Domaines et approbations Active Directory
- Module Active Directory pour Windows PowerShell
- Sites et services Active Directory
- Utilisateurs et ordinateurs Active Directory
- ADSI Edit
- DNS
- Gestion des stratégies de groupe

Pour installer les outils Active Directory sur votre instance EC2 (Windows PowerShell) (facultatif)

1. Démarrer Windows PowerShell.
2. Saisissez la commande suivante.

```
Install-WindowsFeature -Name GPMC,RSAT-AD-PowerShell,RSAT-AD-AdminCenter,RSAT-ADDS-
Tools,RSAT-DNS-Server
```

Étape 4 : vérifier que l'atelier de test de base est opérationnel

Utilisez la procédure suivante pour vérifier que l'atelier de test a bien été configuré avant d'ajouter d'autres modules de guide pour votre atelier de test. Cette procédure permet de vérifier que votre serveur Windows est correctement configuré, qu'il peut se connecter au domaine corp.example.com et qu'il est utilisé pour administrer votre forêt AWS Microsoft AD gérée.

Pour vérifier que l'atelier de test est opérationnel

1. Déconnectez-vous de l'instance EC2 à laquelle vous vous êtes connecté en tant qu'administrateur local.
2. Revenez dans le volet de navigation de la console Amazon EC2 et sélectionnez Instances. Sélectionnez ensuite l'instance que vous avez créée. Choisissez Se connecter.
3. Dans la boîte de dialogue Connectez-vous à votre instance, choisissez Télécharger le fichier Bureau à distance.

4. Dans la boîte de dialogue Windows Security (Sécurité Windows), saisissez vos informations d'identification d'administrateur local pour que le domaine CORP puisse se connecter (par exemple, **`corp\admin`**).
5. Une fois connecté, dans le menu Démarrer, sous Outils d'administration Windows, choisissez Utilisateurs et ordinateurs Active Directory.
6. corp.example.com doit normalement apparaître avec tous les comptes et unités d'organisation par défaut associés à un nouveau domaine. Sous Contrôleurs de domaine, notez les noms des contrôleurs de domaine qui ont été automatiquement créés lorsque vous avez créé votre AWS Managed Microsoft AD à l'étape 2 de ce didacticiel.

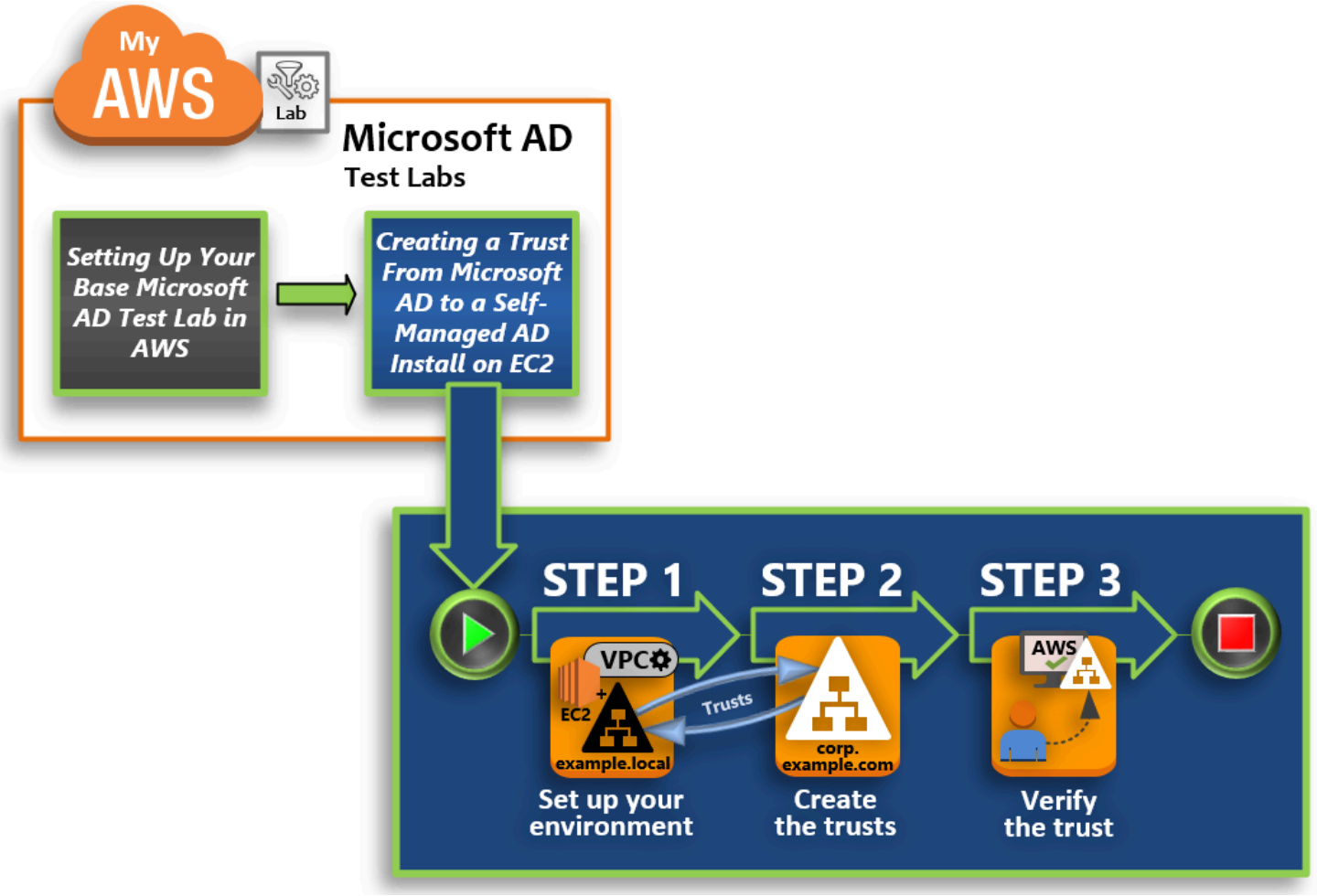
Félicitations ! Votre environnement de laboratoire de test de base Microsoft AD AWS géré est maintenant configuré. Vous pouvez commencer à ajouter le prochain atelier de test de la série.

Didacticiel suivant : Tutoriel : Création d'une relation de confiance entre AWS Managed Microsoft AD et une installation Active Directory autogérée sur Amazon EC2

Tutoriel : Création d'une relation de confiance entre AWS Managed Microsoft AD et une installation Active Directory autogérée sur Amazon EC2

Dans ce didacticiel, vous apprendrez à créer une relation de confiance entre la forêt AWS Directory Service for Microsoft Active Directory que vous avez créée dans le didacticiel de base. Vous apprendrez également à créer une nouvelle forêt Active Directory native sur un serveur Windows dans Amazon EC2. Comme le montre l'illustration suivante, le laboratoire que vous créez à partir de ce didacticiel est le deuxième élément de base nécessaire pour configurer un laboratoire de test Microsoft AD AWS géré complet. Vous pouvez utiliser le laboratoire de test pour tester vos solutions basées sur AWS le cloud pur ou hybride.

Vous ne devez créer ce didacticiel qu'une seule fois. Après cela, vous pourrez ajouter des didacticiels facultatifs, si nécessaire, pour acquérir davantage d'expérience.



Étape 1 : configurer votre environnement pour les approbations

Avant de pouvoir établir des approbations entre une nouvelle forêt Active Directory et la forêt AWS Managed Microsoft AD que vous avez créée dans le Didacticiel de base, vous devez préparer votre environnement Amazon EC2. Pour ce faire, vous devez d'abord créer un serveur Windows Server 2019, promouvoir ce serveur en contrôleur de domaine, puis configurer votre VPC en conséquence.

Étape 2 : création des approbations

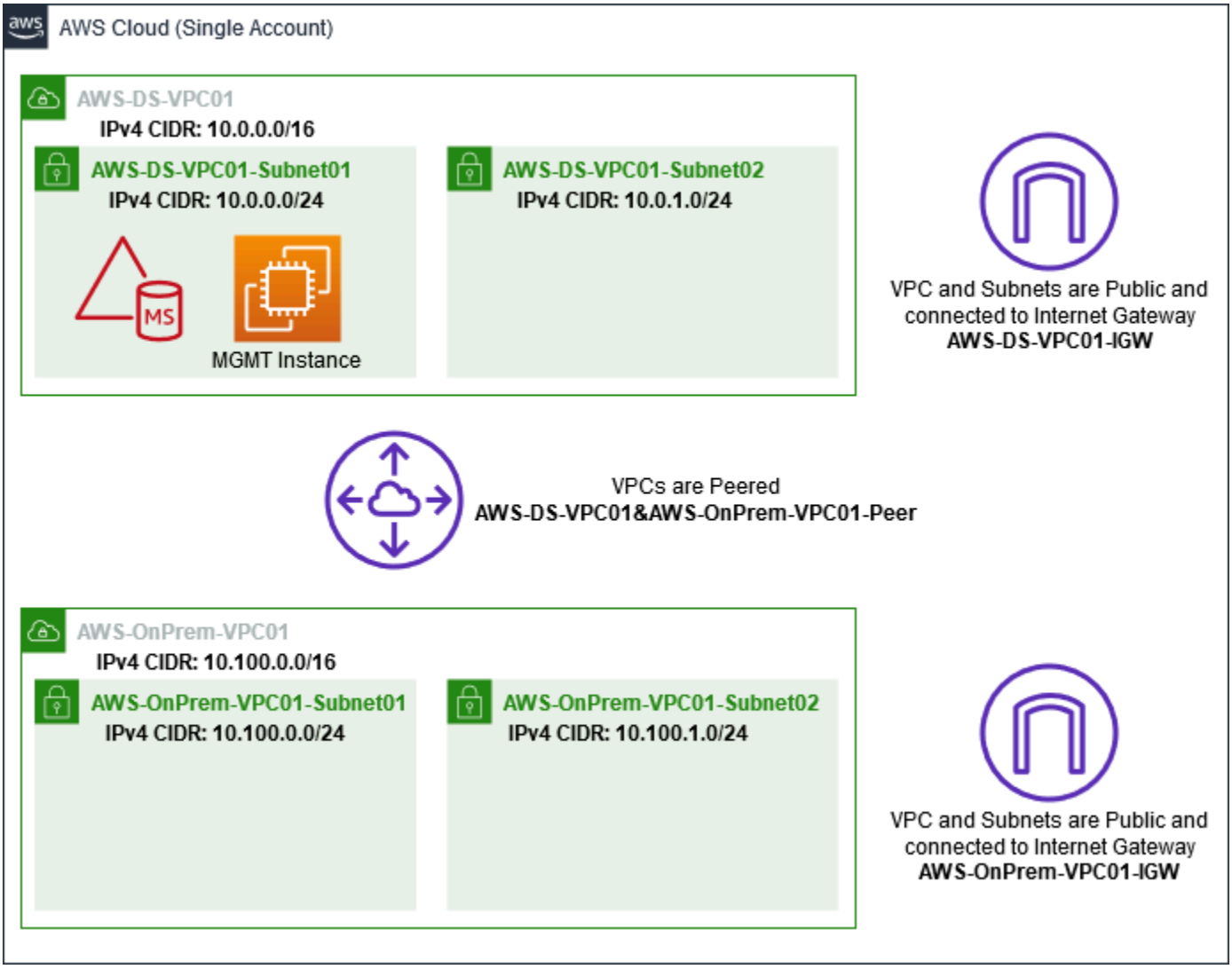
Au cours de cette étape, vous créez une relation d'approbation forestière bidirectionnelle entre votre forêt Active Directory nouvellement créée hébergée dans Amazon EC2 et votre forêt Microsoft AD AWS gérée dans. AWS

Étape 3 : vérification de l'approbation

Enfin, en tant qu'administrateur, vous utilisez la AWS Directory Service console pour vérifier que les nouvelles approbations sont opérationnelles.

Étape 1 : configurer votre environnement pour les approbations

Dans cette section, vous allez configurer votre environnement Amazon EC2, déployer votre nouvelle forêt et préparer votre VPC pour les approbations avec. AWS



Créer une instance EC2 Windows Server 2019

Utilisez la procédure suivante pour créer un serveur membre Windows Server 2019 dans Amazon EC2.

Pour créer une instance EC2 Windows Server 2019

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la console Amazon EC2, choisissez Lancer une instance.

3. Sur la page Step 1 (Étape 1), recherchez Microsoft Windows Server 2019 Base - ami-***xxxxxxxxxxxxxxxxx*** dans la liste. Puis choisissez Sélectionner.
4. Sur la page Étape 2, sélectionnez t2.large, puis choisissez Suivant : Configurer les détails de l'instance.
5. Sur la page Étape 3, procédez comme suit :
   - Pour Réseau, sélectionnez vpc- ***xxxxxxxxxxxxxxxxx*** AWS- OnPrem -VPC01 (que vous avez précédemment configuré dans le didacticiel de base).
   - Pour Sous-réseau, sélectionnez subnet - ***xxxxxxxxxxxxxxxxx*** | - -VPC01-Sous-réseau 01 | AWS - -VPC01. OnPrem AWS OnPrem
   - Dans la liste Attribuer automatiquement l'adresse IP publique, choisissez Activer (si le sous-réseau n'est pas défini sur Activer par défaut).
   - Conservez les valeurs par défaut des autres paramètres.
   - Choisissez Next: Add Storage (Suivant : Ajouter le stockage).
6. Sur la page Étape 4, conservez les paramètres par défaut, puis choisissez Next: Add Tags.
7. Sur la page Étape 5, choisissez Add Tag. SousUnder Key (Clé), saisissez **`example.local-DC01`**, puis choisissez Next: Configure Security Group (Suivant : Configurer le groupe de sécurité).
8. Sur la page Étape 6, choisissez Sélectionner un groupe de sécurité existant, sélectionnez AWS On-Prem Test Lab Security Group (que vous avez précédemment défini dans le didacticiel de base), puis choisissez Vérifier et lancer pour vérifier votre instance.
9. Sur la page Étape 7, vérifiez la page, puis choisissez Lancer.
10. Dans la boîte de dialogue Sélectionner une paire de clés existante ou créer une nouvelle paire de clés, procédez comme suit :
    - Choisissez Choisir une paire de clés existante.
    - Sous Sélectionner une paire de clés, choisissez AWS-DS-KP (que vous avez précédemment défini dans le didacticiel de base).
    - Cochez la case I acknowledge....
    - Choisissez Launch Instances (Démarrer les instances).
11. Sélectionnez Afficher les instances pour revenir à la console Amazon EC2 et consulter l'état du déploiement.

Promouvoir votre serveur en contrôleur de domaine

Avant de pouvoir créer des approbations, vous devez générer et déployer le premier contrôleur de domaine pour une nouvelle forêt. Au cours de ce processus, vous configurez une nouvelle forêt Active Directory, installez DNS et définissez ce serveur afin qu'il utilise le serveur DNS local pour la résolution des noms. Vous devez redémarrer le serveur à la fin de cette procédure.

> **Note**
>
> Si vous souhaitez créer un contrôleur de domaine AWS qui se réplique avec votre réseau local, vous devez d'abord joindre manuellement l'instance EC2 à votre domaine sur site. Après cela, vous pourrez promouvoir le serveur en contrôleur de domaine.

Pour promouvoir votre serveur en contrôleur de domaine

1. Dans la console Amazon EC2, choisissez Instances, sélectionnez l'instance que vous venez de créer, puis sélectionnez Connecter.
2. Dans la boîte de dialogue Connectez-vous à votre instance, choisissez Télécharger le fichier Bureau à distance.
3. Dans la boîte de dialogue Windows Security (Sécurity Windows) saisissez vos informations d'identification d'administrateur local pour que l'ordinateur Windows Server puisse se connecter (par exemple : **`administrator`**). Si vous ne possédez pas encore le mot de passe d'administrateur local, revenez à la console Amazon EC2, cliquez avec le bouton droit de la souris sur l'instance et choisissez Obtenir le mot de passe de Windows. Accédez à votre fichier `AWS DS KP.pem` ou votre clé `.pem` personnelle, puis choisissez Déchiffrer le mot de passe.
4. Dans le menu Démarrer, choisissez Server Manager.
5. Dans le Tableau de bord, choisissez Ajouter des rôles et des fonctionnalités.
6. Dans l'Assistant Ajouter des rôles et des fonctionnalités, choisissez Suivant.
7. Sur la page Sélectionner le type d'installation, choisissez Installation basée sur un rôle ou une fonctionnalité, puis choisissez Suivant.
8. Sur la page Sélectionner le serveur de destination, assurez-vous que le serveur local est sélectionné, puis choisissez Suivant.
9. Sur la page Sélectionner des rôles de serveurs, sélectionnez Services de domaine Active Directory. Dans la boîte de dialogue Assistant Ajouter des rôles et des fonctionnalités, vérifiez

que la case Inclure les outils de gestion (le cas échéant) est cochée. Cliquez sur Ajouter des fonctionnalités, puis sur Suivant.

10. Sur la page Sélectionner les fonctionnalités, choisissez Suivant.
11. Sur la page Services de domaine Active Directory, choisissez Suivant.
12. Sur la page Confirmer les sélections d'installation, choisissez Installer.
13. Une fois les fichiers binaires Active Directory installés, choisissez Fermer.
14. Lorsque le Gestionnaire de serveurs s'ouvre, recherchez un indicateur en haut de la page en regard de la mention Gérer. Lorsque cet indicateur devient jaune, le serveur est prêt à être promu.
15. Choisissez l'indicateur jaune, puis choisissez Promouvoir ce serveur en contrôleur de domaine.
16. Sur la page Configuration de déploiement, choisissez Ajouter une nouvelle forêt. Dans Root domain nam (Nom de domaine racine), saisissez **`example.local`**, puis choisissez Next (Suivant).
17. Sur la page Options du contrôleur de domaine, procédez comme suit :
    - Dans Niveau fonctionnel de la forêt et Niveau fonctionnel du domaine, choisissez Windows Server 2016.
    - Sous Spécifier les capacités du contrôleur de domaine, vérifiez que le serveur DNS et le catalogue global (GC) sont sélectionnés.
    - Saisissez et confirmez un mot de passe pour le mode de restauration des services d'annuaire (DSRM). Ensuite, sélectionnez Suivant.
18. Sur la page Options DNS, ignorez l'avertissement sur la délégation et choisissez Suivant.
19. Sur la page Options supplémentaires, assurez-vous que EXAMPLE est répertorié comme nom de NetBios domaine.
20. Sur la page Chemins, conservez les valeurs par défaut, puis choisissez Suivant.
21. Sur la page Vérifier les options, choisissez Suivant. Le serveur vérifie maintenant que toutes les conditions préalables requises pour le contrôleur de domaine sont remplies. Certains avertissements peuvent s'afficher, mais vous pouvez les ignorer sans risque.
22. Choisissez Installer. Une fois l'installation terminée, le serveur redémarre puis devient un contrôleur de domaine fonctionnel.

Configuration de votre VPC

Les trois procédures suivantes vous guident à travers les étapes de configuration de votre VPC pour établir une connectivité avec AWS.

Pour configurer vos règles sortantes VPC

1. Dans la AWS Directory Service console, notez l'ID de répertoire Microsoft AD AWS géré pour corp.example.com que vous avez créé précédemment dans le didacticiel de base.
2. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
3. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité).
4. Recherchez votre ID d'annuaire Microsoft AD AWS géré. Dans les résultats de recherche, sélectionnez l'élément avec la description AWS created security group for d-***xxxxxx*** directory controllers.

   > **Note**
   >
   > Ce groupe de sécurité a été automatiquement créé lorsque vous avez créé votre annuaire.

5. Choisissez l'onglet Règles sortantes de ce groupe de sécurité. Choisissez Modifier, Ajouter une autre règle, puis ajoutez les valeurs suivantes :
   - Pour Type, sélectionnez Tout le trafic.
   - Pour Destination, tapez **`0.0.0.0/0`**.
   - Conservez les valeurs par défaut des autres paramètres.
   - Sélectionnez Save.

Pour vérifier que l'authentification préalable Kerberos est activée

1. Sur le contrôleur de domaine example.local, ouvrez le Gestionnaire de serveurs.
2. Dans le menu Tools, choisissez Active Directory Users and Computers.
3. Accédez à l'annuaire Utilisateurs, cliquez avec le bouton droit sur n'importe quel utilisateur et sélectionnez Propriétés, puis choisissez l'onglet Compte. Faites défiler la liste Options de compte vers le bas pour vérifier que l'option La pré-authentification Kerberos n'est pas nécessaire n'est pas cochée.

4. Effectuez les mêmes étapes pour le domaine corp.example.com de l'instance corp.example.com-mgmt.

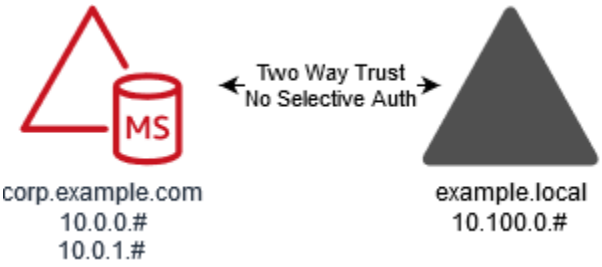
Pour configurer des redirecteurs conditionnels DNS

> **Note**
>
> Un redirecteur conditionnel est un serveur DNS sur un réseau qui est utilisé pour transférer des requêtes DNS en fonction du nom de domaine DNS dans la requête. Par exemple, un serveur DNS peut être configuré pour transférer toutes les requêtes qu'il reçoit pour des noms se terminant par widgets.example.com à l'adresse IP d'un serveur DNS spécifique ou aux adresses IP de plusieurs serveurs DNS.

1. Ouvrez la AWS Directory Service console.
2. Dans le volet de navigation, choisissez Directories (Annuaires).
3. Sélectionnez l'ID de répertoire de votre AWS Managed Microsoft AD.
4. Prenez note du nom de domaine complet (FQDN), corp.example.com, et des adresses DNS de votre annuaire.
5. À présent, retournez sur votre contrôleur de domaine example.local, puis ouvrez le Gestionnaire de serveurs.
6. Dans le menu Tools, choisissez DNS.
7. Dans l'arborescence de la console, développez le serveur DNS du domaine pour lequel vous configurez l'approbation et accédez à Redirecteurs conditionnels.
8. Cliquez avec le bouton droit de la souris sur Redirecteurs conditionnels, puis choisissez Nouveau redirecteur conditionnel.
9. Pour le domaine DNS, saisissez **`corp.example.com`**.
10. Sous Adresses IP des serveurs principaux, choisissez <Cliquez ici pour ajouter... >, tapez la première adresse DNS de votre annuaire Microsoft AD AWS géré (dont vous avez pris note dans la procédure précédente), puis appuyez sur Entrée. Répétez l'opération pour la seconde adresse DNS. Après avoir saisi les adresses DNS, il est possible que l'erreur « timeout » ou « Impossible à résoudre » s'affiche. Vous pouvez généralement ignorer ces erreurs.
11. Cochez la case Stocker ce redirecteur conditionnel dans Active Directory, et le répliquer comme suit. Dans le menu déroulant, choisissez Tous les serveurs DNS de cette forêt, puis cliquez sur OK.

Étape 2 : création des approbations

Dans cette section, vous créez deux approbations de forêts. Une approbation est créée à partir du domaine Active Directory de votre instance EC2 et l'autre à partir de votre AWS Managed Microsoft AD in AWS.



Pour créer un lien de confiance entre votre domaine EC2 et votre AWS Managed Microsoft AD

1. Connectez-vous à example.local.
2. Ouvrez le Gestionnaire de serveurs et choisissez DNS dans l'arborescence de la console. Prenez note de l'adresse IPv4 indiquée pour le serveur. Vous en aurez besoin au cours de la procédure suivante lors de la création d'un redirecteur conditionnel depuis corp.example.com vers l'annuaire example.local.
3. Dans le menu Outils, choisissez Domaines et approbations Active Directory.
4. Dans l'arborescence de la console, cliquez avec le bouton droit de la souris sur example.local, puis choisissez Propriétés.
5. Dans l'onglet Approbations, choisissez Nouvelle approbation, puis Suivant.
6. Sur la page Trust Name (Nom d'approbation), saisissez **`corp.example.com`**, puis choisissez Next (Suivant).
7. Sur la page Type d'approbation, choisissez Approbation de forêt, puis Suivant.

> **Note**
>
> AWS Managed Microsoft AD prend également en charge les approbations externes. Toutefois, dans le cadre de ce didacticiel, vous allez créer une approbation de forêt birectionnelle.

8. Sur la page Direction d'approbation, choisissez Bidirectionnelle, puis Suivant.

> **Note**
>
> Si vous décidez ultérieurement d'utiliser une approbation unidirectionnelle à la place, assurez-vous que les directions d'approbation sont correctement configurées (sortant sur le domaine d'approbation, entrant sur le domaine approuvé). Pour de plus amples informations générales, veuillez consulter Understanding trust direction (français non garanti) sur le site web de Microsoft.

9. Sur la page Sens d'approbation, choisissez Ce domaine uniquement, puis Suivant.
10. Sur la page Niveau d'authentification d'approbations sortantes, choisissez Authentification pour toutes les ressources de la forêt, puis Suivant.

> **Note**
>
> Bien que Selective authentication (Authentification sélective) soit une option, pour la simplicité de ce didacticiel, nous vous recommandons de ne pas l'activer ici. Lorsqu'elle est configurée, elle restreint l'accès sur une approbation externe ou de forêt aux seuls utilisateurs d'un domaine ou d'une forêt approuvé ayant reçu explicitement des autorisations d'authentification sur des objets informatiques (ordinateurs de ressources) résidant dans le domaine ou la forêt d'approbation. Pour de plus amples informations, veuillez consulter Configuring selective authentication settings (français non garanti).

11. Sur la page Mot de passe d'approbation, saisissez le mot de passe d'approbation deux fois, puis choisissez Suivant. Vous utiliserez ce mot de passe au cours de la procédure suivante.
12. Sur la page Fin de la sélection des approbations, passez en revue les résultats, puis choisissez Suivant.
13. Sur la page Fin de la création des approbations, passez en revue les résultats, puis choisissez Suivant.
14. Sur la page Confirmer l'approbation sortante, choisissez Non, ne pas confirmer l'approbation sortante. Ensuite, sélectionnez Next
15. Sur la pageConfirmer l'approbation entrante, choisissez Non, ne pas confirmer l'approbation entrante. Ensuite, sélectionnez Next
16. Sur la page Fin de l'Assistant Nouvelle approbation, choisissez Terminer.

> **Note**
>
> Les relations de confiance sont une fonctionnalité globale de AWS Managed Microsoft AD. Si vous utilisez Réplication multi-régions, les procédures suivantes doivent être effectuées dans Région principale. Les modifications seront appliquées automatiquement à toutes les régions répliquées. Pour plus d'informations, consultez Caractéristiques mondiales et régionales.

Pour créer un lien de confiance entre votre AWS Managed Microsoft AD et votre domaine EC2

1. Ouvrez la AWS Directory Service console.
2. Choisissez l'annuaire corp.example.com.
3. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :
   - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région principale, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour plus d'informations, consultez Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Réseau et sécurité.
4. Dans la section Trust relationships (Relations d'approbation), choisissez Actions, puis sélectionnez Add trust relationship (Ajouter une relation d'approbation).
5. Dans la boîte de dialogue Ajouter une relation d'approbation, procédez comme suit :
   - Sous Trust type (Type d'approbation) sélectionnez Forest trust (Approbation de forêt.

     > **Note**
     >
     > Assurez-vous que le type d'approbation que vous choisissez ici correspond au même type d'approbation configuré dans la procédure précédente (pour créer l'approbation de votre domaine EC2 vers votre Microsoft AD AWS géré).

   - Pour Existing or new remote domain name (Nom de domaine distant existant ou nouveau), tapez exemple.local.
   - Pour Mot de passe d'approbation, saisissez le même mot de passe que vous avez fourni au cours de la procédure précédente.
   - Dans Trust direction (Direction d'approbation), sélectionnez Two-Way (Bidirectionnelle).

> **Note**
>
> - Si vous décidez ultérieurement d'utiliser une approbation unidirectionnelle à la place, assurez-vous que les directions d'approbation sont correctement configurées (sortant sur le domaine d'approbation, entrant sur le domaine approuvé). Pour de plus amples informations générales, veuillez consulter Understanding trust direction (français non garanti) sur le site web de Microsoft.
> - Bien que Selective authentication (Authentification sélective) soit une option, pour la simplicité de ce didacticiel, nous vous recommandons de ne pas l'activer ici. Lorsqu'elle est configurée, elle restreint l'accès sur une approbation externe ou de forêt aux seuls utilisateurs d'un domaine ou d'une forêt approuvé ayant reçu explicitement des autorisations d'authentification sur des objets informatiques (ordinateurs de ressources) résidant dans le domaine ou la forêt d'approbation. Pour de plus amples informations, veuillez consulter Configuring selective authentication settings (français non garanti).

- Dans Conditional forwarder (Redirecteur conditionnel), saisissez l'adresse IP de votre serveur DNS dans la forêt example.local (dont vous avez pris note au cours de la procédure précédente).

> **Note**
>
> Un redirecteur conditionnel est un serveur DNS sur un réseau qui est utilisé pour transférer des requêtes DNS en fonction du nom de domaine DNS dans la requête. Par exemple, un serveur DNS peut être configuré pour transférer toutes les requêtes qu'il reçoit pour des noms se terminant par widgets.example.com à l'adresse IP d'un serveur DNS spécifique ou aux adresses IP de plusieurs serveurs DNS.

6. Choisissez Ajouter.

Étape 3 : vérification de l'approbation

Dans cette section, vous allez tester si les approbations ont été configurées avec succès entre AWS et Active Directory sur Amazon EC2.

Pour vérifier l'approbation

1. Ouvrez la AWS Directory Service console.
2. Choisissez l'annuaire corp.example.com.
3. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :
   - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région principale, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour plus d'informations, consultez Régions principales et régions supplémentaires.
   - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Réseau et sécurité.
4. Dans la section Relations d'approbation, sélectionnez la relation d'approbation que vous venez de créer.
5. Choisissez Actions, puis Vérifier la relation d'approbation.

Une fois la vérification terminée, la mention Vérifié devrait s'afficher dans la colonne Statut.

Félicitations, vous avez terminé ce didacticiel ! Vous disposez à présent d'un environnement Active Directory multi-forêts entièrement fonctionnel à partir duquel vous pouvez commencer à tester différents scénarios. Des didacticiels d'atelier de test supplémentaires sont planifiés en 2018. Revenez sur cette page occasionnellement pour découvrir les nouveautés.

Résolution des problèmes liés AWS à Managed Microsoft AD

Les sections suivantes peuvent vous aider à résoudre certains problèmes courants que vous pourriez rencontrer lors de la création ou de l'utilisation de votre annuaire.

Problèmes liés à votre Microsoft AD AWS géré

Certaines tâches de dépannage ne peuvent être effectuées que par AWS Support. Voici certaines des tâches à accomplir :

- Redémarrer les contrôleurs de domaine que vous AWS Directory Service avez fournis.
- Mettez à niveau votre Microsoft AD AWS géré.

Pour créer un dossier d'assistance, consultez les sections Création de dossiers d'assistance et gestion des dossiers.

Problèmes liés à Netlogon et aux communications par canal sécurisé

Pour réduire la vulnérabilité CVE-2020-1472, Microsoft a publié un correctif qui modifie la façon dont les communications par canal sécurisé Netlogon sont traitées par les contrôleurs de domaine. Depuis l'introduction de ces modifications relatives à la sécurité Netlogon, certaines connexions Netlogon (serveurs, postes de travail et validations de confiance) peuvent ne pas être acceptées par votre Managed Microsoft AD. AWS

Pour vérifier si votre problème est lié à Netlogon ou aux communications par canal sécurisé, recherchez dans Amazon CloudWatch Logs les identifiants d'événement 5827 (pour les problèmes liés à l'authentification des appareils) ou 5828 (pour les problèmes liés à la validation AD Trust). Pour plus d'informations sur CloudWatch AWS Managed Microsoft AD, consultezActiver le transfert de journaux.

Pour plus d'informations sur les mesures d'atténuation contre CVE-2020-1472, veuillez consulter How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472 (français non garanti) sur le site web de Microsoft.

Récupération d'un mot de passe

Si un utilisateur oublie un mot de passe ou rencontre des difficultés pour se connecter à votre annuaire Simple AD ou AWS Managed Microsoft AD, vous pouvez réinitialiser son mot de passe à l'aide du AWS Management Console, Windows PowerShell ou du AWS CLI.

Pour plus d'informations, consultez Réinitialiser un mot de passe utilisateur.

Ressources supplémentaires

Les ressources suivantes peuvent vous aider à résoudre les problèmes pendant que vous travaillez avec AWS.

- AWS Centre de connaissances : trouvez des FAQ et des liens vers d'autres ressources pour vous aider à résoudre les problèmes.
- AWS Centre de support : bénéficiez d'une assistance technique.
- AWS Premium Support Center : bénéficiez d'un support technique haut de gamme.

Les ressources suivantes peuvent vous aider à résoudre les Active Directory problèmes courants.

- Documentation Active Directory

- AD DS Résolutions des problèmes
- Résolution des problèmes liés aux données du répertoire

Rubriques

- Surveillance du serveur DNS avec Microsoft Event Viewer
- Erreurs de jonction du domaine Linux
- Espace de stockage disponible bientôt saturé dans Active Directory
- Erreurs d'extension de schéma
- Raisons liées aux statuts de création d'une relation d'approbation

Surveillance du serveur DNS avec Microsoft Event Viewer

Vous pouvez vérifier vos événements DNS AWS Managed Microsoft AD, ce qui vous permet d'identifier et de résoudre les problèmes de DNS. Par exemple, si un enregistrement DNS est manquant, vous pouvez utiliser le journal des événements d'audit DNS pour vous aider à identifier la cause première et résoudre le problème. Vous pouvez également utiliser les journaux des événements d'audit DNS pour améliorer la sécurité en détectant et en bloquant les demandes en provenance d'adresses IP suspectes.

Pour ce faire, vous devez être connecté avec le compte Admin ou avec un compte qui est un membre du groupe AWSAdministrateurs des systèmes de noms de domaine . Pour en savoir plus sur ce groupe, consultez Qu'est-ce qui est créé avec votre annuaire Microsoft AD Active Directory AWS géré.

Pour accéder à Event Viewer pour votre DNS AWS Managed Microsoft AD

1. Ouvrez la console Amazon EC2 sur https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation de gauche, sélectionnez instances.
3. Localisez une instance Amazon EC2 qui est jointe à votre annuaire AWS Managed Microsoft AD. Sélectionnez l'instance, puis choisissez Connecter.
4. Une fois connecté à l'instance Amazon EC2, ouvrez le menu Start (Démarrer) et sélectionnez le dossier Windows Administrative Tools (Outils d'administration Windows). Dans le dossier Administrative Tools (Outils d'administration), sélectionnez Event Viewer.
5. Dans la fenêtre Observateur d'événements, choisissez Action, puis choisissez Connecter à un autre ordinateur.

6. Sélectionnez Another computer (Autre ordinateur), tapez le nom ou l'adresse IP de l'un de vos serveurs DNS AWS Managed Microsoft AD et choisissez OK.
7. Dans le volet de gauche, accédez à Journaux d'applications et de services>Microsoft>WindowsServeur DNS, puis sélectionnez Audit.

Erreurs de jonction du domaine Linux

Les informations suivantes peuvent vous aider à résoudre les problèmes générant certains messages d'erreur que vous pouvez rencontrer lors de la jonction d'une instance EC2 Linux à votre annuaire AWS Managed Microsoft AD.

Impossible d'effectuer la jonction de domaine ou l'authentification d'instances Linux

Les instances Ubuntu 14.04, 16.04 et 18.04 doivent pouvoir être résolues à l'envers dans le DNS pour qu'un domaine puisse fonctionner avec Microsoft Active Directory. Sinon, vous risquez de rencontrer l'un des deux scénarios suivants :

Scénario 1 : Instances Ubuntu qui ne sont pas encore jointes à un domaine

Pour les instances Ubuntu qui tentent de joindre un domaine, la commande `sudo realm join` peut ne pas fournir les autorisations requises pour joindre le domaine et afficher l'erreur suivante :

! Couldn't authenticate to active directory: SASL(-1): generic failure: GSSAPI Error: An invalid name was supplied (Success) adcli: couldn't connect to EXEMPLE.COM domain: Couldn't authenticate to active directory: SASL(-1): generic failure: GSSAPI Error: An invalid name was supplied (Success) ! Insufficient permissions to join the domain realm: Couldn't join realm: Insufficient permissions to join the domain

Scénario 2 : Instances Ubuntu qui sont jointes à un domaine

Pour les instances Ubuntu déjà jointes à un domaine Microsoft Active Directory, les tentatives de connexion SSH à l'instance à l'aide des informations d'identification du domaine peuvent échouer avec les erreurs suivantes :

$ ssh admin@EXEMPLE.COM@198.51.100

no such identity: /Users/username/.ssh/id_ed25519: No such file or directory

admin@EXEMPLE.COM@198.51.100's password:

Permission denied, please try again.

admin@EXEMPLE.COM@198.51.100's password:

Si vous vous connectez à l'instance avec une clé publique et que vous vérifiez `/var/log/auth.log`, vous risquez de voir les erreurs suivantes d'utilisateur introuvable :

May 12 01:02:12 ip-192-0-2-0 sshd[2251]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=203.0.113.0

May 12 01:02:12 ip-192-0-2-0 sshd[2251]: pam_sss(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=203.0.113.0 user=admin@EXEMPLE.COM

May 12 01:02:12 ip-192-0-2-0 sshd[2251]: pam_sss(sshd:auth): received for user admin@EXEMPLE.COM: 10 (User not known to the underlying authentication module)

May 12 01:02:14 ip-192-0-2-0 sshd[2251]: Failed password for invalid user admin@EXEMPLE.COM from 203.0.113.0 port 13344 ssh2

May 12 01:02:15 ip-192-0-2-0 sshd[2251]: Connection closed by 203.0.113.0 [preauth]

Par contre, `kinit` pour l'utilisateur continue de fonctionner. Veuillez consulter cet exemple :

ubuntu@ip-192-0-2-0:~$ kinit admin@EXEMPLE.COM Password for admin@EXEMPLE.COM: ubuntu@ip-192-0-2-0:~$ klist Ticket cache: FILE:/tmp/krb5cc_1000 Default principal: admin@EXEMPLE.COM

Solution

La solution recommandée actuelle pour ces deux scénarios consiste à désactiver DNS inverse dans `/etc/krb5.conf` dans la section [libdefaults], comme illustré ci-dessous :

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

Problème d'authentification d'approbation unidirectionnelle associé à une jonction de domaine fluide

Si une approbation sortante unidirectionnelle est établie entre votre Microsoft AD AWS géré et votre Active Directory local, vous pouvez rencontrer un problème d'authentification lorsque vous

tentez de vous authentifier auprès de l'instance Linux jointe au domaine à l'aide de vos informations d'identification Active Directory fiables avec Winbind.

Erreurs

Jul 31 00:00:00 EC2AMAZ-LSMWqT sshd[23832]: Failed password for user@corp.example.com from xxx.xxx.xxx.xxx port 18309 ssh2

Jul 31 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): getting password (0x00000390)

Jul 31 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): pam_get_item returned a password)

31 juillet 00:05:00 Ec2Amaz-LSMWqt sshd [23832] : pam_winbind (sshd:auth) : wbcLogonUser échec de la demande : WBC_ERR_AUTH_ERROR, erreur PAM : PAM_SYSTEM_ERR (4), NTSTATUS_OBJECT_NAME_NOT_FOUND**, le message d'erreur était le suivant : Le nom de l'objet est introuvable.

Jul 31 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): internal module error (retval = PAM_SYSTEM_ERR(4), user = 'CORP\user')

Solution

Pour résoudre ce problème, vous devez exclure ou supprimer une directive du fichier de configuration du module PAM (`/etc/security/pam_winbind.conf`) en procédant comme suit.

1. Ouvrez le fichier `/etc/security/pam_winbind.conf` dans un éditeur de texte.

```
sudo vim /etc/security/pam_winbind.conf
```

2. Excluez ou supprimez la directive suivante krb5_auth = yes.

```
[global]

cached_login = yes
krb5_ccache_type = FILE
#krb5_auth = yes
```

3. Arrêtez le service Winbind, puis redémarrez-le.

```
service winbind stop or systemctl stop winbind
```

```
net cache flush
service winbind start or systemctl start winbind
```

Espace de stockage disponible bientôt saturé dans Active Directory

Si votre AWS Managed Microsoft AD est altéré, car l'espace de stockage disponible d'Active Directory est bientôt saturé, agissez immédiatement afin que l'annuaire soit de nouveau actif. Pour connaître les deux causes les plus fréquentes de cette déficience, consultez les sections suivantes :

1. Le dossier SYSVOL stocke des objets de politique de groupe plus qu'essentiels
2. La base de données Active Directory a atteint sa capacité maximale

Pour obtenir des informations sur les tarifs relatifs au stockage AWS Managed Microsoft AD, consultez la section Tarification AWS Directory Service.

Le dossier SYSVOL stocke des objets de politique de groupe plus qu'essentiels

Cette déficience est souvent causée par le stockage de fichiers non essentiels dans le dossier SYSVOL dédiés au traitement de la stratégie de groupe. Ils peuvent se présenter sous forme de fichiers EXE, MSI ou autre qui ne sont pas essentiels au traitement de la stratégie de groupe. Les éléments de stratégie de groupe essentiels devant être traités sont les objets de stratégie de groupe, les scripts de connexion et de déconnexion, ainsi que le magasin central des objets de stratégie de groupe. Tous les fichiers non essentiels doivent être stockés sur un ou plusieurs serveurs de fichiers autres que vos contrôleurs de domaine AWS Managed Microsoft AD.

Si vous avez besoin de fichiers pour l'installation du logiciel de stratégie de groupe, stockez-les sur un serveur de fichiers. Si vous préférez ne pas vous occuper de la gestion du serveur de fichiers, AWS propose une option permettant de le faire à votre place : Amazon FSx.

Pour supprimer des fichiers inutiles, accédez au dossier partagé SYSVOL via le chemin UNC (Universal Naming Convention). Par exemple, si le nom complet de votre domaine est example.com, le chemin UNC de SYSVOL serait « \\example.local\SYSVOL\example.local\ ». Une fois ces objets non essentiels au traitement de l'annuaire par la stratégie de groupe localisés et supprimés, l'annuaire doit redevenir actif sous 30 minutes. Si l'annuaire n'est pas actif après 30 minutes, contactez AWS Support.

En stockant seulement les fichiers de stratégie de groupe essentiels dans le dossier partagé SYSVOL, vous permettez à votre annuaire de ne pas être affecté par la distension de SYSVOL.

La base de données Active Directory a atteint sa capacité maximale

Cette déficience est souvent causée par le fait que la base de données Active Directory a atteint sa capacité maximale. Pour vérifier cela, consultez le nombre total d'objets dans votre annuaire. Nous mettons en gras le mot total pour que vous compreniez que les objets supprimés sont toujours comptabilisés dans le nombre total d'objets d'un annuaire.

AWS Managed Microsoft AD conserve par défaut les éléments dans la corbeille pendant 180 jours avant qu'ils ne soient définitivement recyclés. Une fois un objet recyclé (désactivé), il est conservé pendant 180 jours avant d'être finalement supprimé de l'annuaire. Ainsi, un objet supprimé demeure dans la base de données de l'annuaire pendant 360 jours avant d'être définitivement supprimé. C'est pourquoi vous devez évaluer le nombre total d'objets.

Pour plus de détails sur le nombre d'objets pris en charge par AWS Managed Microsoft AD, consultez la section Tarification AWS Directory Service.

Pour calculer le nombre total d'objets dans un annuaire, éléments supprimés inclus, exécutez la commande PowerShell suivante à partir d'une instance Windows avec liaison de domaine. Pour apprendre à configurer une instance de gestion, reportez-vous à la section Gérer des utilisateurs et des groupes dans AWS Managed Microsoft AD.

```
Get-ADObject -Filter * -IncludeDeletedObjects | Measure-Object -Property 'Count' |
 Select-Object -Property 'Count'
```

Voici un exemple de sortie de la commande ci-dessus :

```
Count
10000
```

Si le nombre total est supérieur au nombre d'objets pouvant être pris en charge par votre annuaire comme indiqué dans la note ci-dessus, cela veut dire que votre annuaire a atteint sa capacité de stockage maximale.

Voici des options permettant de résoudre cette déficience :

1. Nettoyez AD
   a. Supprimez tous les objets AD indésirables.
   b. Supprimez tous les objets indésirables de la corbeille AD. Veuillez noter que cette action est irréversible et que vous ne pourrez récupérer ces objets supprimés qu'en restaurant l'annuaire.

c. La commande suivante supprimera définitivement tous les objets se trouvant dans la corbeille AD.

> **Important**
>
> Procédez avec prudence, car cette action est irréversible, et vous ne pourrez récupérer ces objets supprimés qu'en restaurant l'annuaire.

```
$DomainInfo = Get-ADDomain
$BaseDn = $DomainInfo.DistinguishedName
$NetBios = $DomainInfo.NetBIOSName
$ObjectsToRemove = Get-ADObject -Filter { isDeleted -eq $true } -
IncludeDeletedObjects -SearchBase "CN=Deleted Objects,$BaseDn" -Properties
 'LastKnownParent','DistinguishedName','msDS-LastKnownRDN' | Where-Object
 { ($_.LastKnownParent -Like "*OU=$NetBios,$BaseDn") -or ($_.LastKnownParent -Like
 '*\0ADEL:*') }
ForEach ($ObjectToRemove in $ObjectsToRemove) { Remove-ADObject -Identity
 $ObjectToRemove.DistinguishedName -IncludeDeletedObjects }
```

d. Envoyez une demande à AWS Support afin de récupérer plus d'espace sur AWS Directory Service.

2. Si votre annuaire est de type Standard Edition, demandez à AWS Support de mettre à niveau votre annuaire vers Enterprise Edition. Cela augmentera également le coût de votre annuaire. Pour de plus amples informations sur la tarification, veuillez consulter Tarification de AWS Directory Service.

Dans AWS Managed Microsoft AD, les administrateurs AWS de cycle de vie d'objet supprimé délégués ont la possibilité de modifier l'attribut `msDS-DeletedObjectLifetime` qui définit le nombre de jours pendant lesquels les objets supprimés sont conservés dans la corbeille AD avant d'être recyclés.

> **Note**
>
> Il s'agit d'un sujet avancé. Si la configuration n'est pas correctement effectuée, elle peut entraîner une perte de données. Pour mieux comprendre ce procédé, nous vous invitons à

passer en revue Corbeille AD : compréhension, application, meilleures pratiques et résolution de problèmes.

Réduire le `msDS-DeletedObjectLifetime`nombre d'objets pris en charge peut vous aider à ne pas dépasser le niveau de capacité maximale. La valeur de ce nombre ne peut être inférieure à 2 jours. Une fois cette limite dépassée, vous ne pourrez plus récupérer l'objet supprimé via la corbeille AD. Pour récupérer le(s) objet(s) en question, vous devrez restaurer votre annuaire à partir d'un instantané. Pour de plus amples informations, veuillez consulter Création d'un instantané ou d'une restauration de votre annuaire. Toute restauration à partir d'un instantané peut entraîner une perte de données, car les instantanés correspondent à un moment donné.

Pour modifier le cycle de vie de l'objet supprimé de votre annuaire, exécutez la commande suivante :

Note

Si vous exécutez la commande telle quelle, le cycle de vie de l'objet supprimé sera défini sur 30 jours. Si vous souhaitez rallonger ou raccourcir cette durée, remplacez « 30 » par le nombre correspondant. Cependant, nous vous recommandons de ne pas dépasser 180, le nombre par défaut.

```
$DeletedObjectLifetime = 30
$DomainInfo = Get-ADDomain
$BaseDn = $DomainInfo.DistinguishedName
Set-ADObject -Identity "CN=Directory Service,CN=Windows
 NT,CN=Services,CN=Configuration,$BaseDn" -Partition "CN=Configuration,$BaseDn" -
Replace:@{"msDS-DeletedObjectLifetime" = $DeletedObjectLifetime}
```

Erreurs d'extension de schéma

Les informations suivantes peuvent vous aider à résoudre certains messages d'erreur que vous pouvez rencontrer lorsque vous étendez le schéma pour votre annuaire AWS Managed Microsoft AD.

Référence

Erreur

> Erreur d'ajout sur l'entrée commençant à la ligne 1 : Référence L'erreur côté serveur est : 0x202b Une référence a été renvoyée à partir du serveur. L'erreur de serveur étendue est : 0000202B: RefErr: DSID-0310082F, data 0, 1 access points \tref 1: 'example.com' Number of Objects Modified: 0

Résolution des problèmes

> Veillez à ce que tous les champs de nom uniques disposent d'un nom de domaine correct. Dans l'exemple ci-dessus, `DC=example,dc=com` doit être remplacé par le code `DistinguishedName` affiché par l'applet de commande `Get-ADDomain`.

Impossible de lire le fichier d'importation

Erreur

> Impossible de lire le fichier d'importation. Nombre d'objets modifiés : 0

Résolution des problèmes

> Le fichier LDIF importé est vide (0 octet). Vérifiez que le bon fichier a été chargé.

Erreur de syntaxe

Erreur

> Le fichier d'entrée Failed contient une erreur de syntaxe à la ligne 21. Le dernier jeton commence par « q ». Nombre d'objets modifiés : 0

Résolution des problèmes

> Le texte sur la ligne 21 n'a pas été formaté correctement. La première lettre du texte non valide est `A`. Mettez à jour la ligne 21 avec une syntaxe LDIF valide. Pour plus d'informations sur le formatage d'un fichier LDIF, consultez Étape 1 : créer votre fichier LDIF.

L'attribut ou la valeur existe

Erreur

> Erreur d'ajout sur l'entrée commençant à la ligne 1 : L'attribut ou la valeur existe L'erreur côté serveur est : 0x2083 Une valeur spécifique existe déjà. L'erreur de serveur étendue est : 00002083: AtrErr: DSID-03151830, #1: \t0: 00002083: DSID-03151830, problem 1006 (ATT_OR_VALUE_EXISTS), data 0, Att 20019 (mayContain):len 4 Number of Objects Modified: 0

Résolution des problèmes

> La modification du schéma a déjà été appliquée.

Aucun attribut de ce type

Erreur

> Erreur d'ajout sur l'entrée commençant à la ligne 1 : Aucun attribut de ce type L'erreur côté serveur est : 0x2085 La valeur de l'attribut ne peut pas être supprimée car elle n'existe pas pour l'objet. L'erreur de serveur étendue est : 00002085: AtrErr: DSID-03152367, #1: \t0: 00002085: DSID-03152367, problem 1001 (NO_ATTRIBUTE_OR_VAL), data 0, Att 20019 (mayContain):len 4 Number of Objects Modified: 0

Résolution des problèmes

> Le fichier LDIF essaie de supprimer un attribut d'une classe, mais cet attribut n'est actuellement pas attaché à la classe. La modification du schéma a probablement déjà été appliquée.

Erreur

> Erreur d'ajout sur l'entrée commençant à la ligne 41 : Aucun attribut de ce type 0x57 Le paramètre est incorrect. L'erreur de serveur étendue est : 0x208d Objet de l'annuaire introuvable. L'erreur de serveur étendue est : "00000057: LdapErr: DSID-0C090D8A, comment: Error in attribute conversion operation, data 0, v2580" Number of Objects Modified: 0

Résolution des problèmes

> L'attribut répertorié à la ligne 41 est incorrect. Revérifiez l'orthographe.

Aucun objet de ce type

Erreur

> Erreur d'ajout sur l'entrée commençant à la ligne 1 : Aucun attribut de ce type L'erreur côté serveur est : 0x208d Objet de l'annuaire introuvable. L'erreur de serveur étendu est : 0000208D: NameErr: DSID-03100238, problem 2001 (NO_OBJECT), data 0, best match of: 'CN=Schema,CN=Configuration,DC=example,DC=com' Number of Objects Modified: 0

Résolution des problèmes

> L'objet référencé par le nom unique (DN) n'existe pas.

Raisons liées aux statuts de création d'une relation d'approbation

Si la création d'une relation d'approbation échoue, le message de statut contient des informations supplémentaires. Voici comment interpréter ces messages.

L'accès est refusé

Accès refusé lorsque vous essayez de créer la relation d'approbation. Le mot de passe de la relation d'approbation est incorrect ou les paramètres de sécurité du domaine distant n'autorisent pas la configuration d'une relation d'approbation. Pour résoudre ce problème, essayez ce qui suit :

- Le Microsoft AD AWS géré Active Directory et le site autogéré avec lesquels Active Directory vous souhaitez créer une relation de confiance doivent porter le même nom de First Site. Le nom du premier site est défini sur`Default-First-Site-Name`. Une erreur de refus d'accès se produit si ces noms varient d'un domaine à l'autre.
- Vérifiez que vous utilisez le même mot de passe de relation d'approbation que celui que vous avez utilisé lors de la création de la relation d'approbation correspondante sur le domaine distant.
- Vérifiez que les paramètres de sécurité de votre domaine permettent la création de la relation d'approbation.
- Vérifiez que votre stratégie de sécurité locale est définie correctement. En particulier, vérifiez `Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously` et assurez-vous que ce paramètre contient au moins les trois canaux nommés suivants :
  - netlogon
  - samr

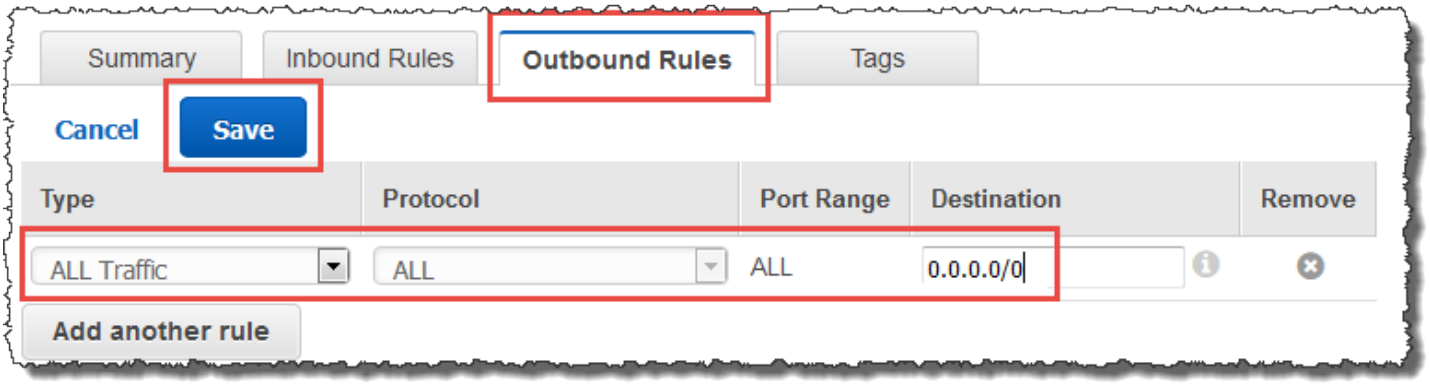
  - lsarpc
- Vérifiez que les canaux nommés ci-dessus existent en tant que valeur de la clé de NullSessionPipesregistre qui se trouve dans le chemin de registre HKLM \ SYSTEM \ \ services \ CurrentControlSet LanmanServer \ Parameters. Ces valeurs doivent être insérées sur des lignes séparées.

  > **Note**
  >
  > Par défaut, `Network access: Named Pipes that can be accessed anonymously` n'est pas défini et affiche `Not Defined`. Ceci est normal, car les paramètres par défaut effectifs du contrôleur de domaine pour `Network access: Named Pipes that can be accessed anonymously` sont `netlogon`, `samr`, `lsarpc`.

- Vérifiez le paramètre de signature SMB (Server Message Block) suivant dans la politique des contrôleurs de domaine par défaut. Ces paramètres se trouvent sous Configuration de l'ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies locales/Options de sécurité. Ils doivent correspondre aux paramètres suivants :
  - Microsoftclient réseau : communications signées numériquement (toujours) : Par défaut : Activé
  - Microsoftclient réseau : communications signées numériquement (si le serveur est d'accord) : par défaut : activé
  - Microsoftserveur réseau : communications signées numériquement (toujours) : Activé
  - Microsoftserveur réseau : Signer numériquement les communications (si le client est d'accord) : Par défaut : Activé

Le nom de domaine spécifié n'existe pas ou n'a pas pu être contacté

Pour résoudre ce problème, vérifiez que les paramètres du groupe de sécurité de votre nom de domaine, ainsi que la liste de contrôle d'accès (ACL) de votre VPC sont corrects, et que vous avez fourni avec précision les informations relatives à votre redirecteur conditionnel. AWS configure le groupe de sécurité pour ouvrir uniquement les ports nécessaires aux communications Active Directory. Dans la configuration par défaut, le groupe de sécurité accepte le trafic vers ces ports à partir de n'importe quelle adresse IP. Le trafic sortant est limité au groupe de sécurité. Vous devez mettre à jour la règle sortante du groupe de sécurité pour autoriser le trafic vers votre réseau sur site. Pour plus d'informations sur les exigences de sécurité, veuillez consulter Étape 2 : préparer votre AWS Managed Microsoft AD.



Si les serveurs DNS des réseaux des autres annuaires utilisent des adresses IP publiques (non conformes à la norme RFC 1918), vous devrez ajouter une route IP sur l'annuaire depuis la console Directory Services vers les serveurs DNS. Pour plus d'informations, veuillez consulter Création, vérification ou suppression d'une relation d'approbation et Prérequis.

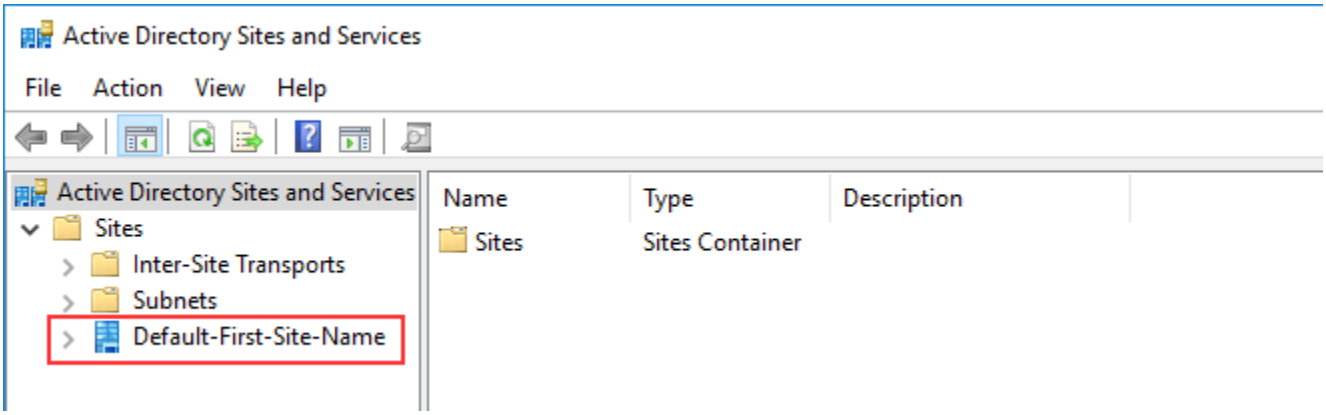
L'Internet Assigned Numbers Authority (IANA) a réservé les trois blocs suivants de l'espace d'adresse IP aux Internets privés :

- 10.0.0.0 - 10.255.255.255 (préfixe 10/8)
- 172.16.0.0 - 172.31.255.255 (préfixe 172.16/12)
- 192.168.0.0 - 192.168.255.255 (préfixe 192.168/16)

Pour plus d'informations, veuillez consulter https://tools.ietf.org/html/rfc1918.

Vérifiez que le nom du site AD par défaut de votre Microsoft AD AWS géré correspond au nom du site AD par défaut de votre infrastructure locale. L'ordinateur détermine le nom du site en utilisant un domaine dont l'ordinateur est membre, et non le domaine de l'utilisateur. Le fait de renommer le site pour qu'il corresponde au site le plus proche garantit que le localisateur de contrôleurs de domaine utilisera un contrôleur de domaine du site le plus proche. Si le problème n'est pas résolu, il est possible que les informations fournies d'un redirecteur conditionnel créé précédemment soient mises en cache et empêchent la création d'une nouvelle approbation. Patientez plusieurs minutes et essayez à nouveau de créer la confiance et un redirecteur conditionnel.

Pour plus d'informations sur son fonctionnement, consultez Domain Locator Across a Forest Trust sur le Microsoft site Web.



L'opération n'a pas pu être effectuée sur ce domaine

Pour résoudre ce problème, assurez-vous que les noms NETBIOS des deux domaines/annuaires sont différents. Si les noms NETBIOS des domaines/annuaires sont identiques, créez à nouveau l'un d'entre eux avec un nom NETBIOS différent, puis réessayez.

La création d'une relation d'approbation échoue en raison de l'erreur « Required and valid domain name » (Nom de domaine obligatoire et valide)

Les noms DNS peuvent uniquement contenir des caractères alphabétiques (A à Z), des caractères numériques (0 à 9), le signe moins (-) et un point (.). Les points ne sont autorisés que lorsqu'ils sont utilisés pour délimiter les composants des noms de style de domaine. Éléments à prendre également en compte :

- AWS Managed Microsoft AD ne prend pas en charge les approbations avec des domaines à étiquette unique. Pour plus d'informations, consultez la section Microsoftprise en charge des domaines à étiquette unique.
- Selon la norme RFC 1123 (https://tools.ietf.org/html/rfc1123), les seuls caractères pouvant être utilisés dans les étiquettes DNS sont « A » à « Z », « a » à « z », « 0 » à « 9 » et un trait d'union (« - »). Un point (.) est également utilisé dans les noms DNS, mais uniquement entre les étiquettes DNS et à la fin d'un FQDN.
- Selon la norme RFC 952 (https://tools.ietf.org/html/rfc952), un « nom » (un nom de réseau, d'hôte, de passerelle ou de domaine) est une chaîne de texte comportant jusqu'à 24 caractères issus de l'alphabet (A-Z), des chiffres (0-9), du signe moins (-) et du point (.). Notez que les points ne sont autorisés que lorsqu'ils servent à délimiter les composants des « noms de style de domaine ».

Pour plus d'informations, consultez la section Respect des restrictions de noms pour les hôtes et les domaines sur le Microsoft site Web.

Outils généraux utilisés pour tester les approbations

Les outils suivants peuvent être utilisés pour résoudre divers problèmes liés aux approbations.

AWS Outil de dépannage de Systems Manager Automation

Support Automation Workflows (SAW) tire parti de AWS Systems Manager Automation pour vous fournir un runbook prédéfini pour AWS Directory Service. L'outil AWSSupport-TroubleshootDirectoryTrust runbook vous aide à diagnostiquer les problèmes courants de création de confiance entre AWS Managed Microsoft AD et un site sur site. Microsoft Active Directory

DirectoryServicePortTest outil

L'outil de DirectoryServicePortTesttest peut être utile pour résoudre les problèmes de création de confiance entre AWS Managed Microsoft AD et Active Directory sur site. Pour obtenir un exemple de la manière dont l'outil peut être utilisé, veuillez consulter Test de votre connecteur AD Connector.

Outils NETDOM et NLTEST

Les administrateurs peuvent utiliser les outils de ligne de commande Netdom et Nltest pour rechercher, afficher, créer, supprimer et gérer les approbations. Ces outils communiquent directement avec l'autorité LSA d'un contrôleur de domaine. Pour un exemple d'utilisation de ces outils, consultez Netdom et NLTEST sur le Microsoft site Web.

Outil de capture de paquets

Vous pouvez utiliser l'utilitaire intégré de capture de paquets Windows pour étudier et résoudre un problème de réseau potentiel. Pour plus d'informations, veuillez consulter Capture a Network Trace without installing anything (français non garanti).

AD Connector

AD Connector est une passerelle d'annuaire grâce à laquelle vous pouvez rediriger les demandes d'annuaire vers votre site Microsoft Active Directory sans mettre en cache aucune information dans le cloud. AD Connector est disponible en deux tailles, petite et grande. Un AD Connector petit est conçu pour les petites organisations et est destiné à gérer un faible nombre d'opérations par seconde. Un grand AD Connector est conçu pour les grandes organisations et est destiné à gérer un nombre moyen à élevé d'opérations par seconde. Vous pouvez répartir les charges d'application sur plusieurs connecteurs AD Connector en fonction de vos besoins en matière de performances. Aucune limite de connexions ou d'utilisateurs n'est appliquée.

AD Connector ne prend pas en charge les approbations transitives Active Directory. Les connecteurs AD et vos domaines Active Directory locaux entretiennent une relation 1 à 1. C'est-à-dire que pour chaque domaine local, y compris les domaines enfants d'une forêt Active Directory auprès desquels vous souhaitez vous authentifier, vous devez créer un AD Connector unique.

> **Note**
>
> AD Connector ne peut pas être partagé avec d'autres AWS comptes. Si cela s'avère nécessaire, pensez à utiliser AWS Managed Microsoft AD pourPartagez votre annuaire. AD Connector n'est pas non plus compatible avec le multi-VPC, ce qui signifie que AWS les applications de ce type WorkSpacesdoivent être provisionnées dans le même VPC que votre AD Connector.

Une fois configuré, AD Connector offre les avantages suivants :

- Vos utilisateurs finaux et administrateurs informatiques peuvent utiliser leurs identifiants d'entreprise existants pour se connecter à AWS des applications telles qu' WorkSpacesAmazon WorkDocs ou Amazon WorkMail.
- Vous pouvez gérer AWS des ressources telles que les instances Amazon EC2 ou les compartiments Amazon S3 via un accès basé sur les rôles IAM au. AWS Management Console
- Vous pouvez appliquer de manière cohérente les politiques de sécurité existantes (telles que l'expiration des mots de passe, l'historique des mots de passe et le verrouillage des comptes), que les utilisateurs ou les administrateurs informatiques accèdent aux ressources de votre infrastructure sur site ou dans le AWS cloud.

- Vous pouvez utiliser AD Connector pour activer l'authentification multifactorielle en l'intégrant à votre infrastructure MFA existante basée sur Radius afin de fournir un niveau de sécurité supplémentaire lorsque les utilisateurs accèdent aux applications. AWS

Poursuivez la lecture des rubriques de cette section pour savoir comment vous connecter à un annuaire et utiliser au mieux les fonctionnalités d'AD Connector.

Rubriques

Démarrer avec AD Connector

Avec AD Connector, vous pouvez vous connecter AWS Directory Service à votre entreprise existanteActive Directory. Lorsque vous êtes connecté à votre annuaire existant, toutes les données de celui-ci restent sur vos contrôleurs de domaine. AWS Directory Service ne réplique aucune des données de votre répertoire.

Rubriques

Conditions préalables requises pour AD Connector

Pour vous connecter à votre annuaire existant avec AD Connector, les éléments suivants sont requis :

Amazon VPC

Configurez un VPC avec les éléments suivants :

- Au moins deux sous-réseaux. Chaque sous-réseau doit disposer d'une zone de disponibilité différente.
- Le VPC doit être connecté à votre réseau existant via une connexion réseau privé virtuel (VPN) ou AWS Direct Connect.
- Le VPC doit avoir la location matérielle par défaut.

AWS Directory Service utilise une structure à deux VPC. Les instances EC2 qui constituent votre répertoire s'exécutent en dehors de votre AWS compte et sont gérées par AWS. Elles ont deux cartes réseau, `ETH0` et `ETH1`. `ETH0` est la carte de gestion et existe en dehors de votre compte. `ETH1` est créé au sein de votre compte.

La plage d'adresses IP de gestion du réseau `ETH0` de votre annuaire est choisie par programmation afin de garantir qu'elle n'entre pas en conflit avec le VPC sur lequel votre annuaire est déployé. Cette plage d'adresses IP peut être comprise dans l'une des paires suivantes (car les annuaires s'exécutent dans deux sous-réseaux) :

- 10.0.1.0/24 et 10.0.2.0/24
- 169,254,0,0/16
- 192.168.1.0/24 et 192.168.2.0/24

Nous évitons les conflits en vérifiant le premier octet du CIDR `ETH1`. S'il commence par un 10, nous choisissons un VPC 192.168.0.0/16 avec des sous-réseaux 192.168.1.0/24 et 192.168.2.0/24. Si le premier octet est différent de 10, nous choisissons un VPC 10.0.0.0/16 avec des sous-réseaux 10.0.1.0/24 et 10.0.2.0/24.

L'algorithme de sélection n'inclut pas de routages dans votre VPC. Il est donc possible qu'un conflit de routage IP résulte de ce scénario.

Pour plus d'informations, veuillez consulter les rubriques suivantes dans le Amazon VPC Guide de l'utilisateur :

- Qu'est-ce qu'Amazon VPC ?
- Sous-réseaux dans votre VPC
- Ajout d'une passerelle réseau privé virtuel Hardware à votre VPC

Pour plus d'informations AWS Direct Connect, consultez le guide de AWS Direct Connect l'utilisateur.

Existant Active Directory

Vous devez vous connecter à un réseau existant avec un Active Directory domaine.

> **Note**
>
> AD Connector ne prend pas en charge les domaines à étiquette unique.

Le niveau fonctionnel de ce Active Directory domaine doit être `Windows Server 2003` ou supérieur. AD Connector prend également en charge la connexion à un domaine hébergé sur une instance Amazon EC2.

> **Note**
>
> AD Connector ne prend pas en charge les contrôleurs de domaine en lecture seule (RODC) en association avec la fonctionnalité de jonction de domaine Amazon EC2.

Compte de service

Vous devez disposer des informations d'identification d'un compte de service dans l'annuaire existant auquel les privilèges suivants ont été délégués :

- Utilisateurs et groupes en lecture - Obligatoire
- Joindre des ordinateurs au domaine : obligatoire uniquement lors de l'utilisation de Seamless Domain Join et WorkSpaces
- Création d'objets informatiques : obligatoire uniquement lors de l'utilisation de Seamless Domain Join et WorkSpaces
- Le mot de passe du compte de service doit être conforme aux exigences en matière AWS de mot de passe. AWS les mots de passe doivent être :
  - Entre 8 et 128 caractères inclus.
  - Contient au moins un caractère appartenant à trois des quatre catégories suivantes :
    - Lettres minuscules (a-z)
    - Lettres majuscules (A-Z)
    - Chiffres (0-9)
    - Caractères non alphanumériques (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Pour plus d'informations, consultez Délégation de privilèges à votre compte de service.

> **Note**
>
> AD Connector utilise Kerberos pour l'authentification et l'autorisation des applications AWS . LDAP est uniquement utilisé pour les recherches d'objets par des utilisateurs et des groupes (opérations de lecture). Avec les transactions LDAP, rien n'est mutable et les informations d'identification ne sont pas transmises en texte clair. L'authentification est gérée par un service AWS interne qui utilise des tickets Kerberos pour effectuer des opérations LDAP en tant qu'utilisateur.

Autorisations des utilisateurs

Tous les utilisateurs Active Directory doivent disposer des autorisations nécessaires pour lire leurs propres attributs. Il s'agit plus précisément des attributs suivants :

- GivenName
- SurName
- Mail
- SamAccountName
- UserPrincipalName
- UserAccountControl
- MemberOf

Par défaut, les utilisateurs Active Directory ont l'autorisation de lire ces attributs. Toutefois, les administrateurs peuvent modifier ces autorisations au fil du temps. Pensez donc peut-être à vérifier si vos utilisateurs disposent des autorisations en lecture avant de configurer AD Connector pour la première fois.

Adresses IP

Obtenez les adresses IP de deux contrôleurs de domaine ou serveurs DNS dans votre annuaire existant.

AD Connector obtient le `_ldap._tcp.<DnsDomainName>` et les enregistrements SRV `_kerberos._tcp.<DnsDomainName>` de ces serveurs lors de la connexion à votre annuaire, donc ces serveurs doivent comporter ces enregistrements SRV. L'AD Connector tente de trouver un contrôleur de domaine commun qui fournira à la fois les services LDAP et les services Kerberos. Ces enregistrements SRV doivent donc inclure au moins un contrôleur de domaine

commun. Pour plus d'informations sur les enregistrements SRV, consultez SRV Resource Records sur Microsoft. TechNet

Ports pour les sous-réseaux

Pour qu'AD Connector redirige les demandes d'annuaire vers vos contrôleurs de Active Directory domaine existants, le pare-feu de votre réseau existant doit disposer des ports suivants ouverts aux CIDR pour les deux sous-réseaux de votre Amazon VPC.

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Authentification Kerberos
- TCP/UDP 389 - LDAP

Il s'agit des ports minimum requis pour qu'AD Connector puisse se connecter à votre annuaire. Votre configuration spécifique peut nécessiter l'ouverture de ports supplémentaires.

Si vous souhaitez utiliser AD Connector et Amazon WorkSpaces, l'attribut DisableVLVSupportLDAP doit être défini sur 0 pour vos contrôleurs de domaine. Il s'agit du paramètre par défaut pour les contrôleurs de domaine. AD Connector ne pourra pas interroger les utilisateurs de l'annuaire si l'attribut DisableVLVSupportLDAP est activé. Cela empêche AD Connector de fonctionner avec Amazon WorkSpaces.

> **Note**
>
> Si les serveurs DNS ou les serveurs de contrôleur de domaine de votre Active Directory domaine existant se trouvent dans le VPC, les ports des groupes de sécurité associés à ces serveurs doivent être ouverts aux CIDR pour les deux sous-réseaux du VPC.

Pour connaître les exigences de port supplémentaires, consultez la section Exigences relatives aux ports AD et AD DS dans la Microsoft documentation.

Pré-authentification Kerberos

Vos comptes d'utilisateur doivent avoir une pré-authentification Kerberos activée. Pour obtenir des instructions détaillées sur la façon d'activer ce paramètre, veuillez consulter Vérification de l'activation de l'authentification préalable Kerberos. Pour obtenir des informations générales sur ce paramètre, consultez la section Préauthentification activée Microsoft TechNet.

Types de chiffrement

AD Connector prend en charge les types de chiffrement suivants lors de l'authentification à vos contrôleurs de domaine Active Directory via Kerberos :

- AES-256-HMAC
- AES-128-HMAC
- RC4-HMAC

AWS IAM Identity Center prérequis

Si vous envisagez d'utiliser l'IAM Identity Center avec AD Connector, vous devez vous assurer que ce qui suit est vrai :

- Votre AD Connector est configuré dans le compte de gestion de votre AWS organisation.
- Votre instance d'IAM Identity Center se trouve dans la même région que celle où votre AD Connector est configuré.

Pour plus d'informations, consultez les conditions requises pour IAM Identity Center dans le guide de l' AWS IAM Identity Center utilisateur.

Prérequis pour l'authentification multifactorielle

Pour prendre en charge l'authentification multifactorielle avec votre annuaire AD Connector, les éléments suivants sont requis :

- Un serveur Remote Authentication Dial In User Service (RADIUS) sur votre réseau existant disposant de deux points de terminaison client. Les points de terminaison client RADIUS ont les critères suivants :
  - Pour créer les points de terminaison, les adresses IP des serveurs AWS Directory Service sont requises. Ces adresses IP peuvent être obtenues à partir du champ Directory IP Address figurant dans les détails de votre annuaire.
  - Les deux points de terminaison RADIUS doivent utiliser le même code secret partagé.
- Votre réseau existant doit autoriser le trafic entrant via le port du serveur RADIUS par défaut (1812) en provenance des AWS Directory Service serveurs.
- Les noms d'utilisateur entre votre serveur RADIUS et votre annuaire existant doivent être identiques.

Pour en savoir plus sur l'utilisation d'AD Connector avec MFA, veuillez consulter Activer l'authentification multifactorielle pour AD Connector.

Délégation de privilèges à votre compte de service

Pour vous connecter à votre annuaire existant, vous devez disposer des informations d'identification pour votre compte de service AD Connector dans l'annuaire existant, auquel certains privilèges ont été délégués. Alors que les membres du groupe Administrateurs du domaine doivent avoir des privilèges suffisants pour se connecter à l'annuaire, en tant que bonne pratique, vous devez utiliser un compte de service disposant uniquement des privilèges minimum nécessaires pour la connexion à l'annuaire. La procédure suivante explique comment créer un nouveau groupe appelé`Connectors`, déléguer les privilèges nécessaires pour se connecter AWS Directory Service à ce groupe, puis ajouter un nouveau compte de service à ce groupe.

Cette procédure doit être effectuée sur un ordinateur qui est joint à votre annuaire et qui dispose du composant logiciel enfichable Utilisateurs et ordinateurs Active Directory. Vous devez également être connecté en tant qu'administrateur de domaine.

Pour déléguer des privilèges à votre compte de service

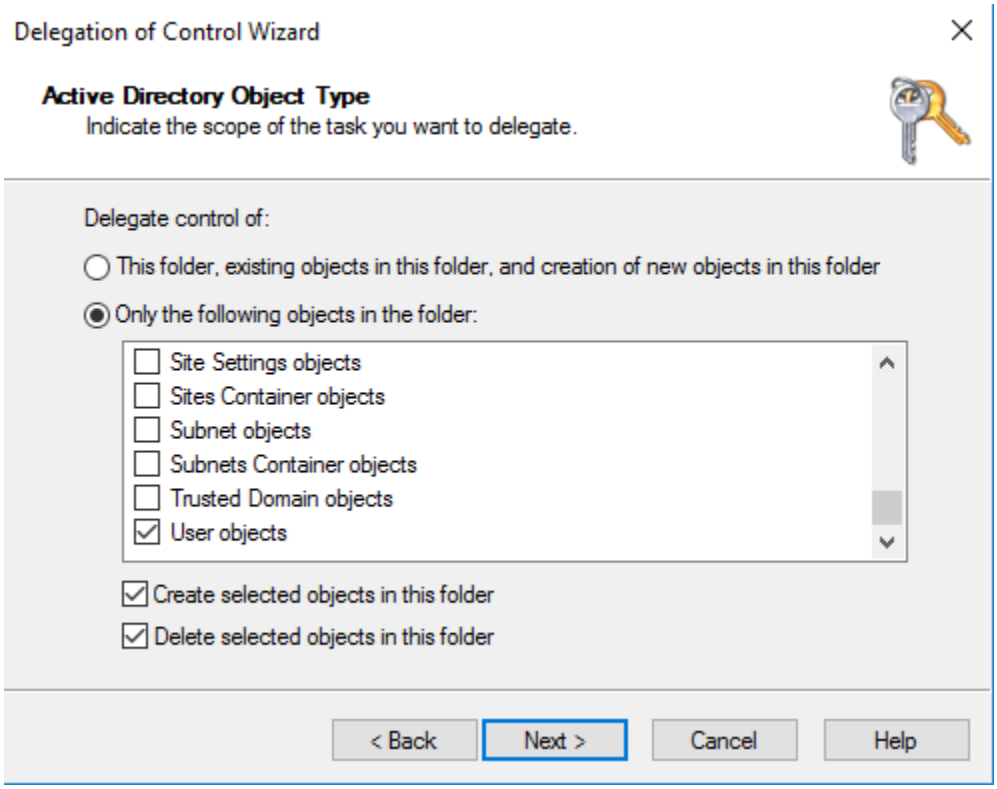
1. Ouvrez Utilisateurs et ordinateurs Active Directory, puis sélectionnez votre domaine dans l'arborescence de navigation.
2. Dans la liste du volet de gauche, effectuez un clic droit sur Utilisateurs, sélectionnez Nouveau, puis Groupe.
3. Dans la boîte de dialogue Nouvel objet - groupe, entrez la commande suivante, puis cliquez sur OK.

Champ	Valeur/sélection
Nom du groupe	`Connectors`
Étendue du groupe	Solution internationale
Type de groupe	Sécurité

4. Dans l'arborescence de navigation Utilisateurs et ordinateurs Active Directory, sélectionnez la racine de votre domaine. Dans le menu, sélectionnez Action, puis Déléguer le contrôle. Si votre AD Connector est connecté à AWS Managed Microsoft AD, vous n'aurez pas accès au contrôle

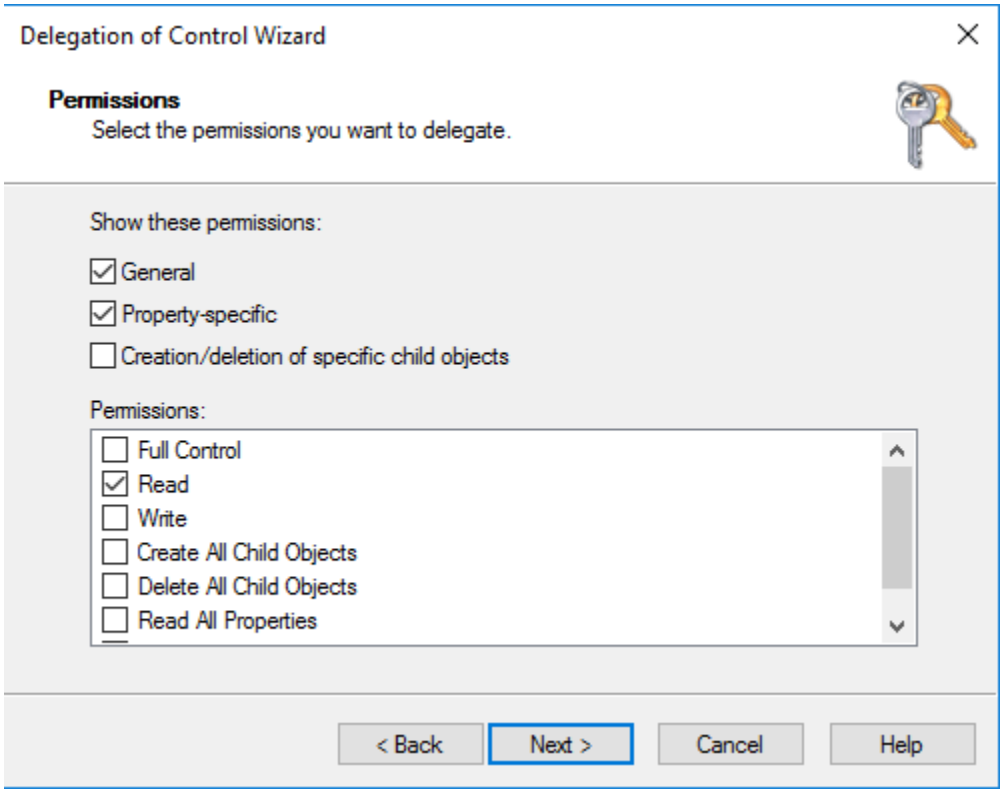
délégué au niveau de la racine du domaine. Dans ce cas, pour déléguer le contrôle, sélectionnez l'unité d'organisation (UO) sous l'UO de votre annuaire où les objets ordinateur seront créés.

5. Sur la page Assistant Délégation de contrôle, cliquez sur Suivant, puis cliquez sur Ajouter.
6. Dans la boîte de dialogue Sélectionner les utilisateurs, ordinateurs ou groupes, entrez `Connectors`, puis cliquez sur OK. Si vous trouvez plusieurs objets, sélectionnez le groupe `Connectors` créé précédemment. Cliquez sur Next (Suivant).
7. Sur la page Tâches à déléguer, sélectionnez Créer une tâche personnalisée à déléguer, puis choisissez Suivant.
8. Sélectionnez Seulement des objets suivants dans le dossier, puis sélectionnez Objets ordinateur et Objets utilisateur.
9. Sélectionnez Créer les objets sélectionnés dans ce dossier et Supprimer les objets sélectionnés dans ce dossier. Ensuite, sélectionnez Suivant.



10. Sélectionnez Lecture, puis choisissez Suivant.

> **Note**
>
> Si vous comptez utiliser Seamless Domain WorkSpaces Join or, vous devez également activer les autorisations d'écriture afin qu'Active Directory puisse créer des objets informatiques.



11. Vérifiez les informations de la page Fin de l'Assistant Délégation de contrôle, puis cliquez sur Terminer.
12. Créez un compte utilisateur avec un mot de passe fort et ajoutez-le au groupe `Connectors`. Cet utilisateur sera connu sous le nom de compte de service AD Connector et, comme il est désormais membre du `Connectors` groupe, il dispose désormais de privilèges suffisants pour se connecter AWS Directory Service à l'annuaire.

Test de votre connecteur AD Connector

Pour qu'AD Connector se connecte à votre annuaire existant, le pare-feu de votre réseau existant doit avoir certains ports ouverts vers les CIDR des deux sous-réseaux du VPC Pour vérifier si ces conditions sont satisfaites, exécutez les étapes suivantes :

Pour tester la connexion

1. Lancez une instance Windows dans le VPC et connectez-vous à celle-ci via RDP. L'instance doit être un membre de votre domaine existant. Les étapes restantes sont exécutées sur cette instance VPC.
2. Téléchargez et décompressez l'application de DirectoryServicePortTesttest. Le code source et les fichiers de projet Visual Studio sont inclus. Vous pouvez donc modifier l'application de test si vous le souhaitez.

   > **Note**
   >
   > Ce script n'est pas pris en charge sur Windows Server 2003 ni les systèmes d'exploitation de version antérieure.

3. À partir d'une invite de commande Windows, exécutez l'application de test DirectoryServicePortTest avec les options suivantes :

   > **Note**
   >
   > L'application de DirectoryServicePortTest test ne peut être utilisée que lorsque les niveaux fonctionnels du domaine et de la forêt sont définis sur Windows Server 2012 R2 ou version inférieure.

   ```
   DirectoryServicePortTest.exe -d <domain_name> -ip <server_IP_address> -tcp
    "53,88,389" -udp "53,88,389"
   ```

   <domain_name>

   Nom de domaine entièrement qualifié. Il permet de tester les niveaux fonctionnels des forêts et des domaines. Si vous excluez le nom de domaine, les niveaux fonctionnels ne seront pas testés.

   <server_IP_address>

   Adresse IP d'un contrôleur de domaine dans votre domaine existant. Les ports seront testés sur cette adresse IP. Si vous excluez l'adresse IP, les ports ne seront pas testés.

Cette application de test détermine si les ports nécessaires sont disponibles sur le VPC de votre domaine, et vérifie également les niveaux fonctionnels minimum des forêts et des domaines.

La sortie est similaire à ce qui suit :

```
Testing forest functional level.
Forest Functional Level = Windows2008R2Forest : PASSED

Testing domain functional level.
Domain Functional Level = Windows2008R2Domain : PASSED

Testing required TCP ports to <server_IP_address>:
Checking TCP port 53: PASSED
Checking TCP port 88: PASSED
Checking TCP port 389: PASSED

Testing required UDP ports to <server_IP_address>:
Checking UDP port 53: PASSED
Checking UDP port 88: PASSED
Checking UDP port 389: PASSED
```

Utilisez le code d'application suivant pour l'application DirectoryServicePortTest.

```
using System;
using System.Collections.Generic;
using System.IO;
using System.Linq;
using System.Net;
using System.Net.Sockets;
using System.Text;
using System.Threading.Tasks;
using System.DirectoryServices.ActiveDirectory;
using System.Threading;
using System.DirectoryServices.AccountManagement;
using System.DirectoryServices;
using System.Security.Authentication;
using System.Security.AccessControl;
using System.Security.Principal;

namespace DirectoryServicePortTest
```

```
{
    class Program
    {
        private static List<int> _tcpPorts;
        private static List<int> _udpPorts;

        private static string _domain = "";
        private static IPAddress _ipAddr = null;

        static void Main(string[] args)
        {
            if (ParseArgs(args))
            {
                try
                {
                    if (_domain.Length > 0)
                    {
                        try
                        {
                            TestForestFunctionalLevel();

                            TestDomainFunctionalLevel();
                        }
                        catch (ActiveDirectoryObjectNotFoundException)
                        {
                            Console.WriteLine("The domain {0} could not be found.\n",
 _domain);
                        }
                    }

                    if (null != _ipAddr)
                    {
                        if (_tcpPorts.Count > 0)
                        {
                            TestTcpPorts(_tcpPorts);
                        }

                        if (_udpPorts.Count > 0)
                        {
                            TestUdpPorts(_udpPorts);
                        }
                    }
                }
                catch (AuthenticationException ex)
```

```
                {
                    Console.WriteLine(ex.Message);
                }
            }
            else
            {
                PrintUsage();
            }

            Console.Write("Press <enter> to continue.");
            Console.ReadLine();
        }

        static void PrintUsage()
        {
            string currentApp =
Path.GetFileName(System.Reflection.Assembly.GetExecutingAssembly().Location);
            Console.WriteLine("Usage: {0} \n-d <domain> \n-ip \"<server IP address>\"
\n[-tcp \"<tcp_port1>,<tcp_port2>,etc\"] \n[-udp \"<udp_port1>,<udp_port2>,etc\"]",
currentApp);
        }

        static bool ParseArgs(string[] args)
        {
            bool fReturn = false;
            string ipAddress = "";

            try
            {
                _tcpPorts = new List<int>();
                _udpPorts = new List<int>();

                for (int i = 0; i < args.Length; i++)
                {
                    string arg = args[i];

                    if ("-tcp" == arg | "/tcp" == arg)
                    {
                        i++;
                        string portList = args[i];
                        _tcpPorts = ParsePortList(portList);
                    }

                    if ("-udp" == arg | "/udp" == arg)
```

```
                {
                    i++;
                    string portList = args[i];
                    _udpPorts = ParsePortList(portList);
                }

                if ("-d" == arg | "/d" == arg)
                {
                    i++;
                    _domain = args[i];
                }

                if ("-ip" == arg | "/ip" == arg)
                {
                    i++;
                    ipAddress = args[i];
                }
            }
        }
        catch (ArgumentOutOfRangeException)
        {
            return false;
        }

        if (_domain.Length > 0 || ipAddress.Length > 0)
        {
            fReturn = true;
        }

        if (ipAddress.Length > 0)
        {
            _ipAddr = IPAddress.Parse(ipAddress);
        }

        return fReturn;
    }

    static List<int> ParsePortList(string portList)
    {
        List<int> ports = new List<int>();

        char[] separators = {',', ';', ':'};

        string[] portStrings = portList.Split(separators);
```

```
            foreach (string portString in portStrings)
            {
                try
                {
                    ports.Add(Convert.ToInt32(portString));
                }
                catch (FormatException)
                {
                }
            }

            return ports;
        }

        static void TestForestFunctionalLevel()
        {
            Console.WriteLine("Testing forest functional level.");

            DirectoryContext dirContext = new
DirectoryContext(DirectoryContextType.Forest, _domain, null, null);
            Forest forestContext = Forest.GetForest(dirContext);

            Console.Write("Forest Functional Level = {0} : ",
forestContext.ForestMode);

            if (forestContext.ForestMode >= ForestMode.Windows2003Forest)
            {
                Console.WriteLine("PASSED");
            }
            else
            {
                Console.WriteLine("FAILED");
            }

            Console.WriteLine();
        }

        static void TestDomainFunctionalLevel()
        {
            Console.WriteLine("Testing domain functional level.");

            DirectoryContext dirContext = new
DirectoryContext(DirectoryContextType.Domain, _domain, null, null);
            Domain domainObject = Domain.GetDomain(dirContext);
```

```
            Console.Write("Domain Functional Level = {0} : ", domainObject.DomainMode);

            if (domainObject.DomainMode >= DomainMode.Windows2003Domain)
            {
                Console.WriteLine("PASSED");
            }
            else
            {
                Console.WriteLine("FAILED");
            }

            Console.WriteLine();
        }

        static List<int> TestTcpPorts(List<int> portList)
        {
            Console.WriteLine("Testing TCP ports to {0}:", _ipAddr.ToString());

            List<int> failedPorts = new List<int>();

            foreach (int port in portList)
            {
                Console.Write("Checking TCP port {0}: ", port);

                TcpClient tcpClient = new TcpClient();

                try
                {
                    tcpClient.Connect(_ipAddr, port);

                    tcpClient.Close();
                    Console.WriteLine("PASSED");
                }
                catch (SocketException)
                {
                    failedPorts.Add(port);
                    Console.WriteLine("FAILED");
                }
            }

            Console.WriteLine();

            return failedPorts;
```

```
        }

        static List<int> TestUdpPorts(List<int> portList)
        {
            Console.WriteLine("Testing UDP ports to {0}:", _ipAddr.ToString());

            List<int> failedPorts = new List<int>();

            foreach (int port in portList)
            {
                Console.Write("Checking UDP port {0}: ", port);

                UdpClient udpClient = new UdpClient();

                try
                {
                    udpClient.Connect(_ipAddr, port);
                    udpClient.Close();
                    Console.WriteLine("PASSED");
                }
                catch (SocketException)
                {
                    failedPorts.Add(port);
                    Console.WriteLine("FAILED");
                }
            }

            Console.WriteLine();

            return failedPorts;
        }
    }
}
```

Création d'un AD Connector

Pour vous connecter à votre annuaire existant avec AD Connector, procédez comme suit. Avant de commencer cette procédure, assurez-vous que vous avez terminé les prérequis identifiés dans Conditions préalables requises pour AD Connector.

> **Note**
>
> Vous ne pouvez pas créer un AD Connector avec un modèle CloudFormation.

Pour vous connecter à AD Connector

1. Dans le panneau de navigation de la console AWS Directory Service, choisissez Directories (Annuaires), puis Set up directory (Configurer l'annuaire).
2. Sur la page Select directory type (Sélectionner un type d'annuaire), choisissez AD Connector, puis Next (Suivant).
3. Sur la page Enter AD Connector information (Saisir les informations AD Connector), renseignez les informations suivantes :

   Taille de l'annuaire

   Faites votre choix parmi les options de taille Petit ou Large. Pour en savoir plus sur les tailles, veuillez consulter AD Connector.

   Description de l'annuaire

   Description facultative de l'annuaire.
4. Sur la page Choose VPC and subnets (Choisir un VPC et des sous-réseaux), indiquez les informations suivantes, puis choisissez Next (Suivant).

   VPC

   VPC de l'annuaire.

   Sous-réseaux

   Choisissez les sous-réseaux pour les contrôleurs de domaine. Les deux sous-réseaux doivent être dans des zones de disponibilité différentes.
5. Sur la page Connect to AD (Connecter à AD), fournissez les informations suivantes :

   Nom de DNS de l'annuaire

   Nom complet de votre annuaire existant, par exemple `corp.example.com`.

   Nom NetBIOS de l'annuaire

   Nom court de votre annuaire existant, tel que `CORP`.

DNS IP addresses (Adresses IP DNS)

Adresse IP d'au moins un serveur DNS dans votre annuaire existant. Ces serveurs doivent être accessibles à partir de chaque sous-réseau spécifié dans l'étape 4. Ces serveurs peuvent être situés à l'extérieur AWS, à condition qu'il existe une connectivité réseau entre les sous-réseaux spécifiés et les adresses IP du serveur DNS.

Nom d'utilisateur du compte de service

Nom d'utilisateur d'un utilisateur figurant dans l'annuaire existant. Pour plus d'informations sur ce compte, veuillez consulter le Conditions préalables requises pour AD Connector.

Mot de passe du compte de service

Mot de passe du compte utilisateur existant. Le mot de passe est sensible à la casse et doit comporter entre 8 et 128 caractères inclus. Il doit également contenir au moins un caractère de trois des quatre catégories suivantes :

- Lettres minuscules (a-z)
- Lettres majuscules (A-Z)
- Chiffres (0-9)
- Caractères non alphanumériques (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirmer le mot de passe

Saisissez à nouveau le mot de passe du compte utilisateur existant.

6. Sur la page Review & create (Vérifier et créer), vérifiez les informations concernant l'annuaire et effectuez les modifications nécessaires. Lorsque les informations sont correctes, choisissez Create directory (Créer l'annuaire). La création de l'annuaire prend plusieurs minutes. Une fois l'annuaire créé, le champ Statut prend la valeur Actif.

Qu'est-ce qui est créé avec votre AD Connector

Lorsque vous créez un AD Connector, il crée et associe AWS Directory Service automatiquement une Elastic Network Interface (ENI) à chacune de vos instances AD Connector. Chacun de ces ENI est essentiel à la connectivité entre votre VPC et AD AWS Directory Service Connector et ne doit jamais être supprimé. Vous pouvez identifier toutes les interfaces réseau réservées à l'utilisation AWS Directory Service par la description : « interface réseau AWS créée pour le répertoire directory-id ». Pour plus d'informations, veuillez consulter la section Elastic Network Interfaces (français non garanti) dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.

> **Note**
>
> Les instances AD Connector sont déployées par défaut dans deux zones de disponibilité d'une région et connectées à votre cloud privé virtuel (VPC) Amazon. Les instances AD Connector qui échouent sont automatiquement remplacées dans la même zone de disponibilité en utilisant la même adresse IP.

Lorsque vous vous connectez à une AWS application ou à un service intégré à un AD Connector (AWS IAM Identity Center inclus), l'application ou le service transmet votre demande d'authentification à AD Connector, qui la transmet ensuite à un contrôleur de domaine dans votre Active Directory autogéré pour authentification. Si vous êtes authentifié avec succès auprès de votre Active Directory autogéré, AD Connector renvoie un jeton d'authentification à l'application ou au service (similaire à un jeton Kerberos). À ce stade, vous pouvez désormais accéder à l' AWS application ou au service.

Comment administrer AD Connector ?

Cette section répertorie toutes les procédures de fonctionnement et de maintenance d'un environnement AD Connector.

Rubriques

Sécurisation de votre annuaire AD Connector

Cette section décrit les éléments à prendre en compte pour sécuriser votre environnement AD Connector.

Rubriques

- Mettre à jour les informations d'identification de votre compte de service AD Connector dans AWS Directory Service
- Activer l'authentification multifactorielle pour AD Connector
- Activation de LDAPS côté client à l'aide d'AD Connector
- Activer l'authentification mTLS dans AD Connector pour une utilisation avec des cartes à puce
- Configurer le AWS Private CA connecteur pour AD

Mettre à jour les informations d'identification de votre compte de service AD Connector dans AWS Directory Service

Les informations d'identification AD Connector que vous fournissez dans AWS Directory Service représentent le compte de service utilisé pour accéder à votre annuaire sur site existant. Vous pouvez modifier les informations d'identification du compte de service dans AWS Directory Service en effectuant les opérations suivantes.

> **Note**
>
> Si AWS IAM Identity Center est activée pour l'annuaire, AWS Directory Service doit transférer le nom principal du service (SPN) à partir du compte de service actuel vers le nouveau compte de service. Si le compte de service actuel n'a pas l'autorisation de supprimer le SPN ou que le nouveau compte de service n'a pas l'autorisation d'ajouter le SPN, vous serez invité à fournir les informations d'identification d'un compte d'annuaire disposant de l'autorisation d'effectuer les deux actions. Ces informations d'identification ne sont pas utilisées pour transférer le SPN et ne sont pas stockées par le service.

Pour mettre à jour les informations d'identification de votre compte de service AD Connector dans AWS Directory Service

1. Dans le volet de navigation de la console AWS Directory Service, sous Active Directory, sélectionnez Directories (Annuaires).
2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), faites défiler la page vers le bas jusqu'à la section Service account credentials (Informations d'identification du compte de service).
4. Dans la section Informations d'identification du compte de service choisissez Mettre à jour.

5. Dans la boîte de dialogue Update service account credentials (Mettre à jour les informations d'identification du compte de service), tapez le nom d'utilisateur et le mot de passe du compte de service. Saisissez à nouveau le mot de passe pour le confirmer, puis cliquez sur Update (Mettre à jour).

Activer l'authentification multifactorielle pour AD Connector

Vous pouvez activer l'authentification multifactorielle pour AD Connector lorsqu'Active Directory s'exécute sur site ou dans des instances EC2. Pour plus d'informations sur l'utilisation de l'authentification multifactorielle avec AWS Directory Service, veuillez consulter Conditions préalables requises pour AD Connector.

> **Note**
>
> L'authentification multifactorielle n'est pas disponible pour Simple AD. Toutefois, MFA peut être activé pour votre annuaire AWS Managed Microsoft AD. Pour en savoir plus, consultez Activer l'authentification multifactorielle pour AWS Managed Microsoft AD.

Pour activer l'authentification multifactorielle pour AD Connector

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).
2. Choisissez le lien de l'ID correspondant à votre annuaire AD Connector.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Networking & security (Mise en réseau et sécurité).
4. Dans la section Authentification multifactorielle, choisissez Actions, puis sélectionnez Activer.
5. Dans la page Activer l'authentification multifactorielle (MFA), indiquez les valeurs suivantes :

   Afficher l'étiquette

   Indiquez un nom d'étiquette.

   Nom DNS ou adresses IP du serveur RADIUS

   Adresses IP des points de terminaison de votre serveur RADIUS ou adresse IP de l'équilibreur de charge de votre serveur RADIUS. Vous pouvez entrer plusieurs adresses IP en les séparant par une virgule (par exemple, `192.0.0.0,192.0.0.12`).

> **Note**
>
> La MFA RADIUS s'applique uniquement pour authentifier l'AWS Management Consoleaccès aux applications et services Amazon Enterprise tels qu'Amazon ou WorkSpaces Amazon QuickSight Chime. Il ne fournit pas la fonction MFA aux charges de travail Windows s'exécutant sur des instances EC2 ou pour la connexion à une instance EC2. AWS Directory Service ne prend pas en charge l'authentification par simulation/réponse RADIUS.
> Les utilisateurs doivent disposer de leur code MFA au moment d'entrer leur nom d'utilisateur et leur mot de passe. Vous devez également utiliser une solution qui effectue une MFA, out-of-band telle que la vérification du texte par SMS pour l'utilisateur. Dans les solutions out-of-band MFA, vous devez vous assurer de définir la valeur du délai d'expiration RADIUS de manière appropriée pour votre solution. Lorsque vous utilisez une solution out-of-band MFA, la page de connexion invite l'utilisateur à saisir un code MFA. Dans ce cas, la bonne pratique consiste à entrer son mot de passe dans la zone de mot de passe et dans la zone MFA.

Port

Port que votre serveur RADIUS utilise pour les communications. Votre réseau sur site doit autoriser le trafic entrant par le port serveur RADIUS par défaut (UDP : 1812) depuis vos serveurs AWS Directory Service.

Shared secret code

Code secret partagé qui a été spécifié lorsque vos points de terminaison RADIUS ont été créés.

Confirmer le code secret partagé

Confirmez le code secret partagé pour vos points de terminaison RADIUS.

Protocole

Sélectionnez le protocole qui a été spécifié lorsque vos points de terminaison RADIUS ont été créés.

Délai d'attente du serveur (en secondes)

Durée, en secondes, d'attente de la réponse du serveur RADIUS. La valeur doit être comprise entre 1 et 50.

Nombre maximal de tentatives RADIUS

Nombre de tentatives de communication avec le serveur RADIUS. La valeur doit être comprise entre 0 et 10.

L'authentification multifactorielle est disponible lorsque le paramètre RADIUS Status passe à l'état Enabled.

6. Sélectionnez Activer.

Activation de LDAPS côté client à l'aide d'AD Connector

La prise en charge de LDAPS côté client dans AD Connector chiffre les communications entre les applications AWS et Microsoft Active Directory (AD). WorkSpaces, AWS IAM Identity Center, Amazon QuickSight et Amazon Chime sont des exemples de telles applications. Ce chiffrement vous aide à mieux protéger les données d'identité de votre organisation et répondre à vos exigences de sécurité.

Rubriques

- Prérequis
- Activation de LDAPS côté client
- Gestion de LDAPS côté client

Prérequis

Avant d'activer LDAPS côté client, vous devez satisfaire les exigences suivantes.

Rubriques

- Déploiement des certificats de serveur dans Active Directory
- Exigences relatives aux certificats de CA
- Exigences liées à la mise en réseau

Déploiement des certificats de serveur dans Active Directory

Afin d'activer LDAPS côté client, vous devez obtenir et installer des certificats de serveur pour chaque contrôleur de domaine dans Active Directory. Ces certificats seront utilisés par le service LDAP pour écouter et accepter automatiquement les connexions SSL provenant de clients LDAP. Vous pouvez utiliser des certificats SSL émis par un déploiement ADCS (services de certificat Active Directory) interne ou achetés auprès d'un émetteur commercial. Pour plus d'informations sur les exigences relatives aux certificats de serveur Active Directory, consultez LDAP over SSL (LDAPS) Certificate sur le site web de Microsoft.

Exigences relatives aux certificats de CA

Un certificat d'autorité de certification (CA), qui représente l'émetteur de vos certificats de serveur, est requis pour le fonctionnement de LDAPS côté client. Les certificats d'une autorité de certification sont mis en correspondance avec les certificats de serveur présentés par vos contrôleurs de domaine Active Directory pour chiffrer les communications LDAP. Notez les exigences suivantes relatives aux certificats d'autorité de certification :

- Pour que vous puissiez enregistrer un certificat, celui-ci doit expirer dans plus de 90 jours.
- Les certificats doivent être au format PEM (Privacy-Enhanced Mail). Si vous exportez des certificats d'autorité de certification à partir d'Active Directory, choisissez X.509 codé en base64 (.CER) comme format de fichier d'exportation.
- Cinq (5) certificats d'une autorité de certification au maximum peuvent être stockés par l'annuaire AD Connector.
- Les certificats utilisant l'algorithme de signature RSASSA-PSS ne sont pas pris en charge.

Exigences liées à la mise en réseau

Le trafic LDAP d'application AWS doit s'exécuter exclusivement sur le port TCP 636, sans basculement sur le port LDAP 389. Toutefois, les communications LDAP Windows prenant en charge la réplication, les approbations, etc. continueront d'utiliser le port LDAP 389 avec une sécurité native Windows. Configurez des pare-feu et des groupes de sécurité AWS pour autoriser les communications TCP sur le port 636 dans AD Connector (en sortie) et Active Directory autogérées (en entrée).

Activation de LDAPS côté client

Pour activer LDAPS côté client, vous importez votre certificat d'une autorité de certification dans AD Connector, puis vous activez LDAPS sur votre annuaire. Lors de l'activation, tout le trafic LDAP entre

les applications AWS et votre Active Directory autogéré est transmis avec le chiffrement de canal Secure Sockets Layer (SSL).

Vous pouvez utiliser deux méthodes différentes pour activer LDAPS côté client pour votre annuaire. Vous pouvez utiliser la méthode AWS Management Console ou la méthode AWS CLI.

Rubriques

Étape 1 : Enregistrer le certificat dans AWS Directory Service

Utilisez l'une des méthodes suivantes pour enregistrer un certificat dans AWS Directory Service.

Méthode 1 : Pour enregistrer votre certificat dans AWS Directory Service (AWS Management Console)

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).
2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Détails de l'annuaire, choisissez l'onglet Mise en réseau et sécurité.
4. Dans la section LDAPS côté client sélectionnez le menu Actions, puis Enregistrer le certificat.
5. Dans la boîte de dialogue Enregistrer un certificat d'une autorité de certification, sélectionnez Parcourir, puis le certificat et choisissez Ouvrir.
6. Choisissez Enregistrer le certificat.

Méthode 2 : Pour enregistrer votre certificat dans AWS Directory Service (AWS CLI)

- Exécutez la commande suivante. Pour les données de certificat, pointez vers l'emplacement de votre fichier de certificat de CA. Un ID de certificat sera fourni dans la réponse.

```
aws ds register-certificate --directory-id your_directory_id --certificate-data
 file://your_file_path
```

Étape 2 : Vérifier l'état d'enregistrement

Pour afficher l'état d'un enregistrement de certificat ou d'une liste de certificats enregistrés, utilisez l'une des méthodes suivantes.

Méthode 1 : Pour vérifier l'état d'un enregistrement de certificat dans AWS Directory Service (AWS Management Console)

1. Accédez à la section LDAPS côté client sur la page Détails de l'annuaire.
2. Vérifiez l'état de l'enregistrement de certificat actuel qui s'affiche sous la colonne État de l'enregistrement. Lorsque la valeur de l'état de l'enregistrement passe à Registered (Enregistré), cela signifie que votre certificat a été enregistré avec succès.

Méthode 2 : Pour vérifier l'état d'un enregistrement de certificat dans AWS Directory Service (AWS CLI)

- Exécutez la commande suivante. Si la valeur de l'état renvoie `Registered`, cela signifie que votre certificat a été enregistré avec succès.

```
aws ds list-certificates --directory-id your_directory_id
```

Étape 3 : Activer LDAPS côté client

Utilisez l'une des méthodes suivantes pour activer LDAPS côté client dans AWS Directory Service.

> **Note**
>
> Avant de pouvoir activer LDAPS côté client, vous devez avoir enregistré avec succès au moins un certificat.

Méthode 1 : Pour activer LDAPS côté client dans AWS Directory Service (AWS Management Console)

1. Accédez à la section LDAPS côté client sur la page Détails de l'annuaire.
2. Sélectionnez Enable (Activer). Si cette option n'est pas disponible, vérifiez qu'un certificat valide a bien été enregistré, puis réessayez.
3. Dans la boîte de dialogue Activer LDAPS côté client choisissez Activer.

Méthode 2 : Pour activer LDAPS côté client dans AWS Directory Service (AWS CLI)

- Exécutez la commande suivante.

```
aws ds enable-ldaps --directory-id your_directory_id --type Client
```

Étape 4 : Vérifier le statut LDAPS

Utilisez l'une des méthodes suivantes pour vérifier le statut LDAPS dans AWS Directory Service.

Méthode 1 : Pour vérifier le statut LDAPS dans AWS Directory Service (AWS Management Console)

1. Accédez à la section LDAPS côté client sur la page Détails de l'annuaire.
2. Si la valeur d'état est affichée en tant que Enabled (Activé), cela signifie que LDAPS a été configuré avec succès.

Méthode 2 : Pour vérifier le statut LDAPS dans AWS Directory Service (AWS CLI)

- Exécutez la commande suivante. Si la valeur d'état renvoie `Enabled`, cela signifie que LDAPS a été configuré avec succès.

```
aws ds describe-ldaps-settings -directory-id your_directory_id
```

Gestion de LDAPS côté client

Utilisez ces commandes pour gérer votre configuration LDAPS.

Vous pouvez utiliser deux méthodes différentes pour gérer les paramètres LDAPS côté client. Vous pouvez utiliser la méthode AWS Management Console ou la méthode AWS CLI.

Afficher les détails du certificat

Utilisez l'une des méthodes suivantes pour voir lorsqu'un certificat est défini pour expirer.

Méthode 1 : Pour afficher les détails du certificat dans AWS Directory Service (AWS Management Console)

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).

2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Détails de l'annuaire, choisissez l'onglet Mise en réseau et sécurité.
4. Les informations relatives au certificat sont affichées dans la section LDAPS côté client sous Certificats d'une autorité de certification.

Méthode 2 : Pour afficher les détails du certificat dans AWS Directory Service (AWS CLI)

- Exécutez la commande suivante. Pour l'ID de certificat, utilisez l'identifiant renvoyé par `register-certificate` ou `list-certificates`.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Annuler l'enregistrement d'un certificat

Utilisez l'une des méthodes suivantes pour annuler l'enregistrement d'un certificat.

> **Note**
>
> Si un seul certificat est enregistré, vous devez d'abord désactiver LDAPS avant de pouvoir annuler l'enregistrement d'un certificat.

Méthode 1 : Pour annuler l'enregistrement d'un certificat dans AWS Directory Service (AWS Management Console)

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).
2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Détails de l'annuaire, choisissez l'onglet Mise en réseau et sécurité.
4. Dans la section LDAPS côté client choisissez Actions, puis Annuler l'enregistrement du certificat.
5. Dans la boîte de dialogue Annuler l'enregistrement d'un certificat d'une autorité de certification, choisissez Annuler l'enregistrement.

Méthode 2 : Pour annuler l'enregistrement d'un certificat dans AWS Directory Service (AWS CLI)

- Exécutez la commande suivante. Pour l'ID de certificat, utilisez l'identifiant renvoyé par `register-certificate` ou `list-certificates`.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Désactivation de LDAPS côté client

Utilisez l'une des méthodes suivantes pour désactiver LDAPS côté client.

Méthode 1 : Pour désactiver LDAPS côté client dans AWS Directory Service (AWS Management Console)

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).
2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Détails de l'annuaire, choisissez l'onglet Mise en réseau et sécurité.
4. Dans la section LDAPS côté client choisissez Désactiver.
5. Dans la boîte de dialogue Désactiver LDAPS côté client, choisissez Désactiver.

Méthode 2 : Pour désactiver LDAPS côté client dans AWS Directory Service (AWS CLI)

- Exécutez la commande suivante.

```
aws ds disable-ldaps --directory-id your_directory_id --type Client
```

Activer l'authentification mTLS dans AD Connector pour une utilisation avec des cartes à puce

Vous pouvez utiliser l'authentification mTLS (Mutual Transport Layer Security) basée sur des certificats avec des cartes à puce pour authentifier les utilisateurs sur Amazon WorkSpaces par le biais de votre Active Directory (AD) et de votre AD Connector autogérés. Lorsque cette option est activée, les utilisateurs sélectionnent leur carte à puce sur l'écran de WorkSpaces connexion et saisissent un code PIN pour s'authentifier, au lieu d'utiliser un nom d'utilisateur et un mot de passe. À

partir de là, le bureau virtuel Windows ou Linux utilise la carte à puce pour s'authentifier auprès d'AD à partir du système d'exploitation de bureau natif.

> **Note**
>
> L'authentification par carte à puce dans AD Connector n'est disponible que dans les Régions AWS versions suivantes, et uniquement avec WorkSpaces. Les autres AWS applications ne sont pas prises en charge pour le moment.
>
> - USA Est (Virginie du Nord)
> - USA Ouest (Oregon)
> - Asie-Pacifique (Sydney)
> - Asia Pacific (Tokyo)
> - Europe (Ireland)
> - AWS GovCloud (US-Ouest)

Rubriques

Prérequis

Pour activer l'authentification mTLS (Mutual Transport Layer Security) basée sur des certificats à l'aide de cartes à puce pour le WorkSpaces client Amazon, vous avez besoin d'une infrastructure de cartes à puce opérationnelle intégrée à votre infrastructure autogérée. Active Directory Pour plus d'informations sur la configuration de l'authentification par carte à puce auprès WorkSpaces d'AmazonActive Directory, consultez le guide d' WorkSpaces administration Amazon.

Avant d'activer l'authentification par carte à puce pour WorkSpaces, veuillez prendre en compte les points suivants :

- Exigences relatives aux certificats de CA
- Exigences relatives aux certificats utilisateur
- Processus de vérification de la révocation des certificats

- Autres considérations

Exigences relatives aux certificats de CA

AD Connector nécessite un certificat d'autorité de certification (CA), qui représente l'émetteur de vos certificats utilisateur, pour l'authentification par carte à puce. AD Connector associe les certificats CA aux certificats présentés par vos utilisateurs avec leurs cartes à puce. Notez les exigences suivantes relatives aux certificats d'autorité de certification :

- Avant de pouvoir enregistrer un certificat CA, celui-ci doit expirer dans plus de 90 jours.
- Les certificats CA doivent être au format PEM (Privacy-Enhanced Mail). Si vous exportez des certificats CA à partir d'Active Directory, choisissez X.509 codé en base64 (.CER) comme format de fichier d'exportation.
- Pour que l'authentification par carte à puce réussisse, tous les certificats CA racine et intermédiaire qui relient une CA émettrice aux certificats utilisateur doivent être téléchargés.
- Cent (100) certificats CA au maximum peuvent être stockés par l'annuaire AD Connector.
- AD Connector ne prend pas en charge l'algorithme de signature RSASSA-PSS pour les certificats CA.
- Vérifiez que le service de propagation des certificats est défini sur Automatique et qu'il est en cours d'exécution.

Exigences relatives aux certificats utilisateur

Voici certaines des exigences relatives au certificat utilisateur :

- Le certificat de carte à puce de l'utilisateur possède un nom alternatif d'objet (SAN) correspondant à celui de l'utilisateur userPrincipalName (UPN).
- Le certificat de carte à puce de l'utilisateur comporte une utilisation améliorée des clés en tant que connexion par carte à puce (1.3.6.1.4.1.311.20.2.2) Authentification du client (1.3.6.1.5.5.7.3.2).
- Les informations du protocole OCSP (Online Certificate Status Protocol) pour le certificat de carte à puce de l'utilisateur doivent être Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) dans le champ Authority Information Access.

Pour plus d'informations sur les exigences relatives à l'AD Connector et à l'authentification par carte à puce, consultez la section Exigences du guide d' WorkSpaces administration Amazon. Pour obtenir de l'aide pour résoudre WorkSpaces les problèmes liés à Amazon, tels que la connexion

WorkSpaces, la réinitialisation du mot de passe ou la connexion à Amazon WorkSpaces, consultez la section Résoudre les problèmes liés aux WorkSpaces clients dans le guide de WorkSpaces l'utilisateur Amazon.

Processus de vérification de la révocation des certificats

Pour effectuer l'authentification par carte à puce, AD Connector doit vérifier l'état de révocation des certificats utilisateur à l'aide du protocole OCSP (Online Certificate Status Protocol). Pour vérifier la révocation des certificats, l'URL d'un répondeur OCSP doit être accessible par Internet. Si vous utilisez un nom DNS, l'URL d'un répondeur OCSP doit utiliser un domaine de premier niveau figurant dans la Base de données de la zone racine de l'Internet Assigned Numbers Authority (IANA).

La vérification de la révocation des certificats AD Connector se déroule de la manière suivante :

- AD Connector doit vérifier que l'extension Authority Information Access (AIA) du certificat utilisateur contient une URL de répondeur OCSP, puis AD Connector utilise l'URL pour vérifier la révocation.
- Si AD Connector ne parvient pas à résoudre l'URL trouvée dans l'extension AIA du certificat utilisateur ou à trouver une URL de répondeur OCSP dans le certificat utilisateur, AD Connector utilise alors l'URL OCSP optionnelle fournie lors de l'enregistrement du certificat CA racine.

  Si l'URL de l'extension AIA du certificat utilisateur est résolue, mais ne répond pas, l'authentification de l'utilisateur échoue.
- Si l'URL du répondeur OCSP fournie lors de l'enregistrement du certificat CA racine ne peut pas être résolue, ne répond pas ou si aucune URL du répondeur OCSP n'a été fournie, l'authentification de l'utilisateur échoue.
- Le serveur OCSP doit être conforme à la norme RFC 6960. En outre, le serveur OCSP doit prendre en charge les demandes utilisant la méthode GET pour les demandes dont la valeur totale est inférieure ou égale à 255 octets.

> **Note**
>
> AD Connector nécessite une URL HTTP pour l'URL du répondeur OCSP.

Autres considérations

Avant d'activer l'authentification par carte à puce dans AD Connector, tenez compte des points suivants :

- AD Connector utilise l'authentification mutuelle basée sur des certificats (protocole TLS mutuel) pour authentifier les utilisateurs auprès d'Active Directory à l'aide de certificats de carte à puce matériels ou logiciels. Seules les cartes d'accès communes (CAC) et les cartes de vérification d'identité personnelle (PIV) sont prises en charge pour le moment. D'autres types de cartes à puce matérielles ou logicielles peuvent fonctionner mais leur utilisation avec le protocole de WorkSpaces streaming n'a pas été testée.
- L'authentification par carte à puce remplace l'authentification par nom d'utilisateur et mot de passe par WorkSpaces.

  Si d'autres AWS applications sont configurées sur votre annuaire AD Connector avec l'authentification par carte à puce activée, ces applications présentent toujours l'écran de saisie du nom d'utilisateur et du mot de passe.
- L'activation de l'authentification par carte à puce limite la durée de session utilisateur à la durée de vie maximale des tickets de service Kerberos. Vous pouvez configurer ce paramètre à l'aide d'une politique de groupe, qui est fixé par défaut à 10 heures. Pour plus d'informations sur ce paramètre, veuillez consulter la documentation Microsoft.
- Le type de chiffrement Kerberos pris en charge par le compte de service AD Connector doit correspondre à chacun des types de chiffrement Kerberos pris en charge par le contrôleur de domaine.

Activer l'authentification par carte à puce

Pour activer l'authentification par carte à puce WorkSpaces sur votre AD Connector, vous devez d'abord importer vos certificats d'autorité de certification (CA) dans AD Connector. Vous pouvez importer vos certificats CA dans AD Connector à l'aide de AWS Directory Service la console, de l'API ou de la CLI. Suivez les étapes ci-dessous pour importer vos certificats CA et activer ensuite l'authentification par carte à puce.

Rubriques

- Étape 1 : activer la délégation contrainte Kerberos pour le compte de service AD Connector
- Étape 2 : enregistrer le certificat CA dans AD Connector
- Étape 3 : activer l'authentification par carte à puce pour les applications et services AWS pris en charge

Étape 1 : activer la délégation contrainte Kerberos pour le compte de service AD Connector

Pour utiliser l'authentification par carte à puce avec AD Connector, vous devez activer la délégation Kerberos contrainte (KCD) pour le compte service AD Connector vers le service LDAP dans l'annuaire AD autogéré.

La délégation Kerberos contrainte est une fonctionnalité de Windows Server. Cette fonctionnalité permet aux administrateurs de services de spécifier et d'appliquer des limites d'approbation d'applications en limitant l'étendue d'intervention des services applicatifs qui agissent au nom d'un utilisateur. Pour plus d'informations, veuillez consulter la section Kerberos constrained delegation (français non garanti).

> **Note**
>
> Kerberos Constrained Delegation (KCD) nécessite que la partie nom d'utilisateur du compte de service AD Connector corresponde au sAM AccountName du même utilisateur. Le sAM AccountName est limité à 20 caractères. sAM AccountName est un attribut Microsoft Active Directory utilisé comme nom de connexion pour les versions antérieures des clients et serveurs Windows.

1. Utilisez la commande `SetSpn` pour définir un nom principal du service (SPN) pour le compte de service AD Connector dans l'AD autogéré. Cela active le compte de service pour la configuration de la délégation.

   Le SPN peut être n'importe quelle combinaison de service ou de noms, mais ne peut pas être une copie d'un SPN existant. Le `-s` vérifie la présence de doublons.

   ```
   setspn -s my/spn service_account
   ```

2. Dans AD Users and Computers (Utilisateurs et ordinateurs AD), ouvrez le menu contextuel (clic droit) et choisissez le compte de service AD Connector, puis Properties (Propriétés).
3. Choisissez l'onglet Delegation (Délégation).
4. Choisissez les options Trust this user for delegation to specified service only (Approuver cet utilisateur pour la délégation au service spécifié uniquement) et Use any authentication protocol (Utiliser n'importe quel protocole d'authentification).
5. Choisissez Add (Ajouter), puis Users or Computers (Utilisateurs ou ordinateurs) pour localiser le contrôleur de domaine.

6. Cliquez sur OK pour afficher une liste des services disponibles utilisés pour la délégation.
7. Choisissez le type de service LDAP et cliquez sur OK.
8. Cliquez à nouveau sur OK pour enregistrer la configuration.
9. Répétez ce processus pour les autres contrôleurs de domaine dans Active Directory. Vous pouvez également automatiser le processus en utilisant PowerShell.

Étape 2 : enregistrer le certificat CA dans AD Connector

Utilisez l'une des méthodes suivantes pour enregistrer un certificat CA pour votre annuaire AD Connector.

Méthode 1 : pour enregistrer votre certificat CA dans AD Connector (AWS Management Console)

1. Dans le volet de navigation de la AWS Directory Service console, sélectionnez Annuaires.
2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Détails de l'annuaire, choisissez l'onglet Mise en réseau et sécurité.
4. Dans la section Smart card authentication (Authentification par carte à puce), choisissez Actions, puis sélectionnez Register certificate (Enregistrer le certificat).
5. Dans la boîte de dialogue Register a certificate (Enregistrer un certificat), sélectionnez Choose file (Choisir un fichier), puis un certificat et cliquez sur Open (Ouvrir). Vous pouvez éventuellement choisir d'effectuer une vérification de révocation pour ce certificat en fournissant une URL du répondeur OCSP (Online Certificate Status Protocol). Pour plus d'informations sur le protocole OCSP, veuillez consulter Processus de vérification de la révocation des certificats.
6. Choisissez Register certificate (Enregistrer le certificat). Lorsque le statut du certificat passe à Registered (Enregistré), cela signifie que le processus d'enregistrement s'est terminé avec succès.

Méthode 2 : pour enregistrer votre certificat CA dans AD Connector (AWS CLI)

- Exécutez la commande suivante. Pour les données de certificat, pointez vers l'emplacement de votre fichier de certificat de CA. Pour fournir une adresse de répondeur OCSP secondaire, utilisez l'objet `ClientCertAuthSettings` facultatif.

```
aws ds register-certificate --directory-id your_directory_id --certificate-
data file://your_file_path --type ClientCertAuth --client-cert-auth-settings
 OCSPUrl=http://your_OCSP_address
```

En cas de succès, la réponse fournit un identifiant de certificat. Vous pouvez également vérifier que votre certificat CA a bien été enregistré en exécutant la commande CLI suivante :

```
aws ds list-certificates --directory-id your_directory_id
```

Si la valeur du statut renvoie `Registered`, cela signifie que votre certificat a été enregistré avec succès.

Étape 3 : activer l'authentification par carte à puce pour les applications et services AWS pris en charge

Utilisez l'une des méthodes suivantes pour enregistrer un certificat CA pour votre annuaire AD Connector.

Méthode 1 : pour activer l'authentification par carte à puce dans AD Connector (AWS Management Console)

1. Accédez à la section Smart card authentication (Authentification par carte à puce) sur la page Directory details (Détails de l'annuaire), puis choisissez Enable (Activer). Si cette option n'est pas disponible, vérifiez qu'un certificat valide a bien été enregistré, puis réessayez.
2. Dans la boîte de dialogue Enable smart card authentication (Activer l'authentification par carte à puce), sélectionnez Enable (Activer).

Méthode 2 : pour activer l'authentification par carte à puce dans AD Connector (AWS CLI)

- Exécutez la commande suivante.

```
aws ds enable-client-authentication --directory-id your_directory_id --type
 SmartCard
```

En cas de succès, AD Connector renvoie une réponse `HTTP 200` avec un corps HTTP vide.

Gérer les paramètres d'authentification par carte à puce

Vous pouvez utiliser deux méthodes différentes pour gérer les paramètres des cartes à puce. Vous pouvez utiliser la AWS Management Console méthode ou la AWS CLI méthode.

Rubriques

Afficher les détails du certificat

Utilisez l'une des méthodes suivantes pour voir lorsqu'un certificat est défini pour expirer.

Méthode 1 : pour afficher les détails du certificat dans AWS Directory Service (AWS Management Console)

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).
2. Choisissez le lien de l'ID correspondant à votre annuaire AD Connector.
3. Sur la page Détails de l'annuaire, choisissez l'onglet Mise en réseau et sécurité.
4. Dans la section Smart card authentication (Authentification par carte à puce), sous CA certificates (Certificats CA), choisissez l'ID du certificat pour en afficher les détails.

Méthode 2 : pour afficher les détails du certificat dans AWS Directory Service (AWS CLI)

- Exécutez la commande suivante. Pour l'ID de certificat, utilisez l'identifiant renvoyé par `register-certificate` ou `list-certificates`.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Annuler l'enregistrement d'un certificat

Utilisez l'une des méthodes suivantes pour annuler l'enregistrement d'un certificat.

> **Note**
>
> Si un seul certificat est enregistré, vous devez d'abord désactiver l'authentification par carte à puce avant de pouvoir annuler l'enregistrement d'un certificat.

Méthode 1 : pour annuler l'enregistrement d'un certificat dans AWS Directory Service ()AWS Management Console

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).
2. Choisissez le lien de l'ID correspondant à votre annuaire AD Connector.
3. Sur la page Détails de l'annuaire, choisissez l'onglet Mise en réseau et sécurité.
4. Dans la section Smart card authentication (Authentification par carte à puce), sous CA certificates (Certificats CA), sélectionnez le certificat dont vous souhaitez annuler l'enregistrement, cliquez sur Actions, puis sur Deregister certificate (Annuler l'enregistrement du certificat).

   > **Important**
   >
   > Assurez-vous que le certificat dont vous vous apprêtez à annuler l'enregistrement n'est pas actif ou qu'il est actuellement utilisé dans le cadre d'une chaîne de certificats CA pour l'authentification par carte à puce.

5. Dans la boîte de dialogue Annuler l'enregistrement d'un certificat d'une autorité de certification, choisissez Annuler l'enregistrement.

Méthode 2 : pour annuler l'enregistrement d'un certificat dans AWS Directory Service ()AWS CLI

- Exécutez la commande suivante. Pour l'ID de certificat, utilisez l'identifiant renvoyé par `register-certificate` ou `list-certificates`.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Désactiver l'authentification par carte à puce

Utilisez l'une des méthodes suivantes pour désactiver l'authentification par carte à puce.

Méthode 1 : pour désactiver l'authentification par carte à puce dans AWS Directory Service (AWS Management Console)

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).
2. Choisissez le lien de l'ID correspondant à votre annuaire AD Connector.
3. Sur la page Détails de l'annuaire, choisissez l'onglet Mise en réseau et sécurité.
4. Dans la section Smart card authentication (Authentification par carte à puce), choisissez Disable (Désactiver).
5. Dans la section Disable smart card authentication (Désactiver l'authentification par carte à puce), choisissez Disable (Désactiver).

Méthode 2 : pour désactiver l'authentification par carte à puce dans AWS Directory Service (AWS CLI)

- Exécutez la commande suivante.

```
aws ds disable-client-authentication --directory-id your_directory_id --type
 SmartCard
```

Configurer le AWS Private CA connecteur pour AD

Vous pouvez intégrer votre Active Directory (AD) autogéré à AWS Private Certificate Authority (CA) à AD Connector pour émettre et gérer des certificats pour les utilisateurs, groupes et machines associés à votre domaine AD. AWS Private CA Connector for AD vous permet d'utiliser une solution de remplacement entièrement gérée pour AWS Private CA les autorités de certification autogérées de votre entreprise sans qu'il soit nécessaire de déployer, de patcher ou de mettre à jour des agents locaux ou des serveurs proxy.

Vous pouvez configurer AWS Private CA l'intégration à votre annuaire via la console Directory Service, la console AWS Private CA Connector for AD ou en appelant l'`CreateTemplate`API. Pour configurer l'intégration de Private CA via la console AWS Private CA Connector for Active Directory, consultez AWS Private CA Connector for Active Directory. Vous trouverez ci-dessous les étapes à suivre pour configurer cette intégration depuis la AWS Directory Service console.

Prérequis

Lorsque vous utilisez AD Connector, vous devez déléguer des autorisations supplémentaires au compte de service. Définissez la liste de contrôle d'accès (ACL) sur votre compte de service pour pouvoir effectuer les opérations suivantes.

- Ajoutez et supprimez un nom principal de service (SPN) à lui-même.
- Créez et mettez à jour les autorités de certification dans les conteneurs suivants :

```
#containers
CN=Public Key Services,CN=Services,CN=Configuration
CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration
CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration
```

- Créez et mettez à jour un objet d'autorité de AuthCertificates certification NT comme dans l'exemple ci-dessous. Si l'objet Autorité de AuthCertificates certification NT existe, vous devez lui déléguer des autorisations. Si l'objet n'existe pas, vous devez déléguer la possibilité de créer des objets enfants dans le conteneur Public Key Services.

```
#objects
CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration
```

> **Note**
>
> Si vous utilisez AWS Managed Microsoft AD, les autorisations supplémentaires seront déléguées automatiquement lorsque vous autorisez le service AWS Private CA Connector for AD à accéder à votre annuaire.

Vous pouvez utiliser le PowerShell script suivant pour déléguer les autorisations supplémentaires et créer l'objet d'autorité de AuthCertifiates certification NT. Remplacez « myconnectoraccount » par le nom du compte de service.

```
$AccountName = 'myconnectoraccount'

# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module -Name 'ActiveDirectory'
$RootDSE = Get-ADRootDSE
```

```
# Getting AD Connector service account Information
$AccountProperties = Get-ADUser -Identity $AccountName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'servicePrincipalName' } -
Properties 'schemaIDGUID').schemaIDGUID
$AccountAclPath = $AccountProperties.DistinguishedName

# Getting ACL settings for AD Connector service account.
$AccountAcl = Get-ACL -Path "AD:\$AccountAclPath"

# Setting ACL allowing the AD Connector service account the ability to add and remove a
 Service Principal Name (SPN) to itself
$AccountAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
 'Allow', $ServicePrincipalNameGuid, 'None'
$AccountAcl.AddAccessRule($AccountAccessRule)
Set-ACL -AclObject $AccountAcl -Path "AD:\$AccountAclPath"

# Add ACLs allowing AD Connector service account the ability to create certification
 authorities
[System.GUID]$CertificationAuthorityGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'certificationAuthority' }
 -Properties 'schemaIDGUID').schemaIDGUID
$CAAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid,
 'ReadProperty,WriteProperty,CreateChild,DeleteChild', 'Allow',
 $CertificationAuthorityGuid, 'None'
$PKSDN = "CN=Public Key Services,CN=Services,CN=Configuration,
$($RootDSE.rootDomainNamingContext)"
$PKSACL = Get-ACL -Path "AD:\$PKSDN"
$PKSACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $PKSACL -Path "AD:\$PKSDN"

$AIADN = "CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,
$($RootDSE.rootDomainNamingContext)"
$AIAACL = Get-ACL -Path "AD:\$AIADN"
$AIAACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $AIAACL -Path "AD:\$AIADN"

$CertificationAuthoritiesDN = "CN=Certification Authorities,CN=Public Key
 Services,CN=Services,CN=Configuration,$($RootDSE.rootDomainNamingContext)"
```

```
$CertificationAuthoritiesACL = Get-ACL -Path "AD:\$CertificationAuthoritiesDN"
$CertificationAuthoritiesACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $CertificationAuthoritiesACL -Path "AD:\$CertificationAuthoritiesDN"

$NTAuthCertificatesDN = "CN=NTAuthCertificates,CN=Public Key
 Services,CN=Services,CN=Configuration,$($RootDSE.rootDomainNamingContext)"
If (-Not (Test-Path -Path "AD:\$NTAuthCertificatesDN")) {
New-ADObject -Name 'NTAuthCertificates' -Type 'certificationAuthority' -OtherAttributes
 @{certificateRevocationList=[byte[]]'00';authorityRevocationList=[byte[]]'00';cACertificate=[b
 -Path "CN=Public Key Services,CN=Services,CN=Configuration,
$($RootDSE.rootDomainNamingContext)"
}

$NTAuthCertificatesACL = Get-ACL -Path "AD:\$NTAuthCertificatesDN"
$NullGuid = [System.GUID]'00000000-0000-0000-0000-000000000000'
$NTAuthAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid,
 'ReadProperty,WriteProperty', 'Allow', $NullGuid, 'None'
$NTAuthCertificatesACL.AddAccessRule($NTAuthAccessRule)
Set-ACL -AclObject $NTAuthCertificatesACL -Path "AD:\$NTAuthCertificatesDN"
```

Pour configurer AWS Private CA Connector pour AD

1. Connectez-vous à la AWS Directory Service console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/directoryservicev2/.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sous l'onglet Réseau et sécurité, sous AWS Private CA Connecteur pour AD, choisissez Configurer le AWS Private CA connecteur pour AD. La page Créer un certificat CA privé pour Active Directory apparaît. Suivez les étapes indiquées sur la console pour créer votre autorité de certification privée pour le Active Directory connecteur afin de vous inscrire auprès de votre autorité de certification privée. Pour de plus amples informations, veuillez consulter Creating a connector (français non garanti).
4. Après avoir créé votre connecteur, suivez les étapes ci-dessous pour afficher les détails, notamment le statut du connecteur et le statut de l'autorité de certification privée associée.

Pour afficher AWS Private CA Connector for AD

1. Connectez-vous à la AWS Directory Service console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/directoryservicev2/.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sous Réseau et sécurité, sous AWS Private CA Connecteur pour AD, vous pouvez afficher vos connecteurs d'autorité de certification privée et votre autorité de certification privée associée. Par défaut, les champs suivants s'affichent :

    a. AWS Private CA ID du connecteur : identifiant unique d'un AWS Private CA connecteur. Cliquez dessus pour accéder à la page de détails de ce AWS Private CA connecteur.

    b. AWS Private CA objet — Informations sur le nom distinctif de l'autorité de certification. Cliquez dessus pour accéder à la page de détails de cet élément AWS Private CA.

    c. État — Sur la base d'une vérification de l'état du AWS Private CA connecteur et du AWS Private CA. Si les deux contrôles sont réussis, Actif s'affiche. Si l'une des vérifications échoue, la mention 1/2 checks failed (1 vérifications sur 2 a échoué) s'affiche. Si les deux vérifications échouent, la mention Failed (Échec) s'affiche. Pour plus d'informations sur un état d'échec, passez le pointeur de la souris sur le lien hypertexte pour savoir quelle vérification a échoué. Suivez les instructions de la console pour résoudre le problème.

    d. Date de création — Le jour où le AWS Private CA connecteur a été créé.

Pour plus d'informations, veuillez consulter View connector details (français non garanti).

Surveillance de votre annuaire AD Connector

Vous pouvez surveiller votre annuaire AD Connector en procédant comme suit :

Rubriques

- Comprendre le statut de votre annuaire
- Configurer les notifications d'état de l'annuaire avec Amazon SNS

Comprendre le statut de votre annuaire

Voici les différents statuts possibles pour un annuaire.

Actif

L'annuaire fonctionne normalement. Aucun problème n'a été détecté par AWS Directory Service pour votre annuaire.

Création

L'annuaire est en cours de création. La création de l'annuaire prend généralement entre 20 et 45 minutes, mais peut varier selon la charge du système.

Supprimé

L'annuaire a été supprimé. Toutes les ressources de l'annuaire ont été libérées. Une fois qu'un annuaire se trouve dans cet état, il ne peut pas être récupéré.

Suppression en cours

L'annuaire est en cours de suppression. L'annuaire restera dans cet état jusqu'à ce qu'il soit totalement supprimé. Une fois qu'un annuaire se trouve dans cet état, l'opération de suppression ne peut pas être annulée, et l'annuaire ne peut pas être récupéré.

Échec

L'annuaire n'a pas pu être créé. Veuillez supprimer cet annuaire. Si le problème persiste, veuillez contacter le centre AWS Support.

Dégradé

L'annuaire est en cours d'exécution dans un état dégradé. Un ou plusieurs problèmes ont été détectés. Il se peut que toutes les opérations liées à l'annuaire ne puissent pas être totalement opérationnelles. Il existe de nombreuses raisons pouvant expliquer que l'annuaire se trouve dans cet état. Parmi ces raisons, citons une opération de maintenance d'exploitation normale comme une application de correctif ou une rotation d'instance EC2, la création temporaire d'un point chaud par une application sur l'un de vos contrôleurs de domaine ou des modifications que vous avez apportées à votre réseau et qui ont interrompu les communications de l'annuaire. Pour plus d'informations, veuillez consulter Résolution des problèmes liés AWS à Managed Microsoft AD, Résolution des problèmes liés à AD Connector, Résolution des problèmes de Simple AD. Pour les problèmes normaux liés à la maintenance, AWS les problèmes sont résolus dans les 40 minutes. Si, après avoir consulté la rubrique de dépannage, votre annuaire reste à l'état Dégradé pendant plus de 40 minutes, nous vous recommandons de contacter le centre AWS Support.

> **Important**
>
> Ne restaurez pas un instantané lorsqu'un annuaire est dans un état dégradé. Il est rare qu'une restauration d'instantané soit nécessaire pour résoudre les problèmes d'état dégradé. Pour plus d'informations, consultez Création d'un instantané ou d'une restauration de votre annuaire.

Inopérable

L'annuaire n'est pas fonctionnel. Tous les points de terminaison de l'annuaire ont signalé des problèmes.

Demandé

La demande de création de votre annuaire est actuellement en attente.

Configurer les notifications d'état de l'annuaire avec Amazon SNS

Avec Amazon Simple Notification Service (Amazon SNS), vous pouvez recevoir des e-mails ou des messages texte (SMS) lorsque le statut de votre annuaire change. Vous êtes averti lorsque votre annuaire passe du statut Active (Actif) au statut Impaired (Défaillant) ou Inoperable (Inutilisable). Vous recevez également une notification lorsque l'annuaire renvoie un statut Active (Actif).

Comment ça marche

Amazon SNS utilise des « rubriques » pour collecter et diffuser des messages. Chaque rubrique compte un ou plusieurs abonnés qui reçoivent les messages qui ont été publiés dans cette rubrique. En suivant les étapes ci-dessous, vous pouvez ajouter un article AWS Directory Service en tant qu'éditeur à une rubrique Amazon SNS. Lorsqu'il AWS Directory Service détecte un changement dans le statut de votre annuaire, il publie un message sur ce sujet, qui est ensuite envoyé aux abonnés du sujet.

Vous pouvez associer plusieurs annuaires en tant que diffuseurs de publication à une même rubrique. Vous pouvez également ajouter des messages de statut de l'annuaire aux rubriques que vous avez créées précédemment dans Amazon SNS. Vous avez un contrôle détaillé sur les personnes autorisées à publier et à s'abonner à une rubrique. Pour obtenir des informations détaillées sur Amazon SNS, veuillez consulter Qu'est-ce qu'Amazon SNS ?

Pour activer la messagerie SNS pour votre annuaire

1. Connectez-vous à la AWS Directory Service console AWS Management Console et ouvrez-la.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sélectionnez l'onglet Maintenance.
4. Dans la section Surveillance de l'annuaire, choisissez Actions, puis sélectionnez Créer une notification.
5. Sur la page Créer une notification, sélectionnez Choisir un type de notification, puis choisissez Créer une notification. Si vous avez déjà une rubrique SNS existante, vous pouvez également choisir Associer une rubrique SNS existante pour envoyer des messages de statut de cet annuaire à cette rubrique.

   > **Note**
   >
   > Si vous choisissez Créer une nouvelle notification, mais que vous utilisez le même nom de rubrique pour une rubrique SNS qui existe déjà, Amazon SNS ne crée pas de rubrique, mais ajoute simplement les nouvelles informations d'abonnement à la rubrique existante.
   > Si vous choisissez Associer une rubrique SNS existante, vous ne pourrez choisir qu'une rubrique SNS située dans la même région que l'annuaire.

6. Choisissez le type de destinataire et saisissez les coordonnées du destinataire. Si vous saisissez un numéro de téléphone pour les SMS, utilisez uniquement des chiffres. N'incluez pas de tirets, d'espaces, ni de parenthèses.
7. (Facultatif) Donnez un nom à votre rubrique et un nom d'affichage SNS. Le nom d'affichage est un nom court de 10 caractères maximum inclus dans tous les messages SMS de cette rubrique. Lorsque vous utilisez l'option SMS, le nom d'affichage est obligatoire.

   > **Note**
   >
   > Si vous êtes connecté à l'aide d'un utilisateur ou d'un rôle IAM doté uniquement de la politique DirectoryServiceFullAccessgérée, le nom de votre rubrique doit commencer par « DirectoryMonitoring ». Si vous souhaitez personnaliser davantage le nom de votre rubrique, vous aurez besoin de privilèges supplémentaires pour SNS.

8. Sélectionnez Create (Créer).

Si vous souhaitez désigner des abonnés SNS supplémentaires, tels qu'une adresse e-mail supplémentaire, des files d'attente Amazon SQS AWS Lambdaou, vous pouvez le faire depuis la console Amazon SNS.

Pour supprimer les messages de statut de l'annuaire d'une rubrique

1. Connectez-vous à la AWS Directory Service console AWS Management Console et ouvrez-la.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sélectionnez l'onglet Maintenance.
4. Dans la section Surveillance de l'annuaire, sélectionnez le nom d'une rubrique SNS dans la liste, choisissez Actions, puis sélectionnez Supprimer.
5. Sélectionnez Remove (Supprimer).

Cela supprime votre annuaire en tant que diffuseur de publication pour la rubrique SNS sélectionnée. Si vous souhaitez supprimer le sujet dans son intégralité, vous pouvez le faire depuis la console Amazon SNS.

> **Note**
>
> Avant de supprimer une rubrique Amazon SNS à l'aide de la console SNS, vous devez vous assurer qu'aucun annuaire n'envoie de messages de statut à cette rubrique.
> Si vous supprimez une rubrique Amazon SNS à l'aide de la console SNS, cette modification ne sera pas immédiatement reflétée dans la console Directory Services. Vous ne serez averti que la prochaine fois qu'un annuaire publiera une notification concernant la rubrique supprimée, auquel cas vous verrez un statut mis à jour dans l'onglet Surveillance de l'annuaire indiquant que la rubrique est introuvable.
> Par conséquent, pour éviter de manquer des messages importants sur le statut du répertoire, avant de supprimer toute rubrique recevant des messages AWS Directory Service, associez votre annuaire à une autre rubrique Amazon SNS.

Joignez une instance Amazon EC2 à votre Active Directory

AD Connector est une passerelle d'annuaire grâce à laquelle vous pouvez rediriger les demandes d'annuaire vers votre site Microsoft Active Directory sans mettre en cache aucune information dans le cloud. Voici plus d'informations sur la façon dont vous pouvez joindre une Amazon EC2 à un domaine Active Directory :

- Vous pouvez facilement joindre une instance Amazon EC2 à votre Active Directory domaine lorsque l'instance est lancée. Pour plus d'informations, consultez Associez facilement une Windows instance Amazon EC2 à votre compte AWS Microsoft AD géré avec AD Connector.
- Si vous devez joindre manuellement une instance EC2 à votre Active Directory domaine, vous devez lancer l'instance dans le groupe de sécurité ou le sous-réseau approprié Région AWS , puis joindre l'instance au Active Directory domaine.
- Pour pouvoir vous connecter à distance à ces instances, vous devez disposer d'une connectivité IP aux instances depuis le réseau à partir duquel vous vous connectez. Dans la plupart des cas, cela nécessite qu'une passerelle Internet soit attachée à votre Amazon VPC et que l'instance possède une adresse IP publique. Pour obtenir plus d'informations sur la connexion à Internet à l'aide d'une passerelle Internet, veuillez consulter la section Connect to the internet using an internet gateway (français non garanti).

> **Note**
>
> Une fois que vous avez joint une instance à votre instance autogérée Active Directory (sur site), elle communique directement avec vous Active Directory et contourne AD Connector.

Rubriques

- Associez facilement une Windows instance Amazon EC2 à votre compte AWS Microsoft AD géré avec AD Connector
- Associez facilement une instance Linux Amazon EC2 à votre Managed AWS Microsoft AD with AD Connector

Associez facilement une Windows instance Amazon EC2 à votre compte AWS Microsoft AD géré avec AD Connector

Cette procédure permet de joindre facilement une Windows instance Amazon EC2 à votre Managed AWS Microsoft AD. Active Directory

Pour rejoindre facilement une instance EC2 Windows

1. Connectez-vous à la console Amazon EC2 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.

2. Dans la barre de navigation, choisissez le même répertoire Région AWS que le répertoire existant.
3. Sur le EC2 Dashboard (tableau de bord EC2), dans la section Launch instance (Lancer une instance), choisissez Launch instance (Lancer une instance).
4. Sur la page Launch an instance (Lancer une instance), dans la section Name and Tags (Nom et balises), saisissez le nom que vous souhaitez utiliser pour votre instance Windows EC2.
5. (Facultatif) Sélectionnez Add additional tags (Ajouter des balises supplémentaires) pour ajouter une ou plusieurs paires clé-valeur d'identification afin d'organiser, de suivre ou de contrôler l'accès pour cette instance EC2.
6. Dans la section Application and OS Image (Amazon Machine Image) [Image de l'application et du système d'exploitation (Amazon Machine Image)], sélectionnez Windows dans le volet Quick Start (Démarrage rapide). Vous pouvez modifier Windows Amazon Machine Image (AMI) dans la liste déroulante Amazon Machine Image (AMI).
7. Dans la section Type d'instance, choisissez le type d'instance que vous souhaitez utiliser dans la liste déroulante Type d'instance.
8. Dans la section Paire de clés (connexion), vous pouvez choisir de créer une nouvelle paire de clés ou choisir une paire de clés existante.

    a. Pour créer une nouvelle paire de clés, choisissez Créer une paire de clés.

    b. Entrez le nom de la paire de clés et sélectionnez une option pour le type de paire de clés et le format de fichier de clé privée.

    c. 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.

    d. Choisissez Créer une paire de clés.

    e. Le fichier de clé privée est automatiquement téléchargé dans votre navigateur. Enregistrez le fichier de clé privée en lieu sûr.

    > **Important**
    >
    > C'est votre seule occasion d'enregistrer le fichier de clé privée.

9. Sur la page Lancer une instance, dans la section Paramètres réseau, choisissez Modifier. Choisissez le VPC dans lequel votre répertoire a été créé dans la liste déroulante VPC obligatoire.

10. Choisissez l'un des sous-réseaux publics de votre VPC dans la liste déroulante Sous-réseau. Tout le trafic externe du sous-réseau que vous choisissez doit être acheminé vers une passerelle Internet. Sinon, vous ne pourrez pas vous connecter à l'instance à distance.

    Pour obtenir plus d'informations sur la manière de se connecter à une passerelle Internet, veuillez consulter la section Connect to the internet using an internet gateway (français non garanti) dans le Guide de l'utilisateur Amazon VPC.

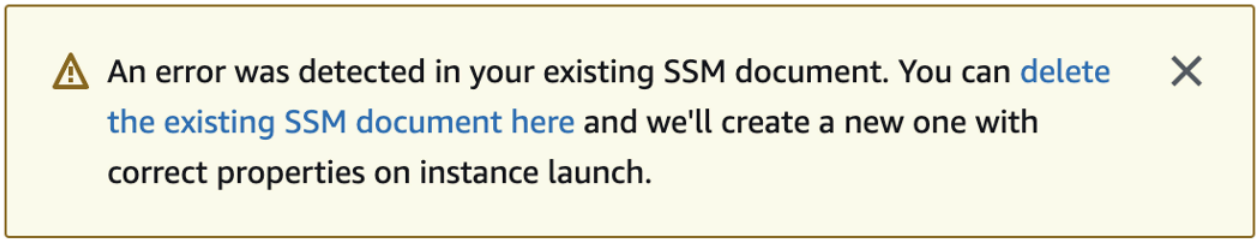
11. Sous Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique), choisissez Enable (Activer).

    Pour plus d'informations sur les adresses IP publiques et privées, veuillez consulter la section Amazon EC2 instance IP addressing (français non garanti) dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.

12. Pour les paramètres Firewall (security groups) [Pare-feu (groupes de sécurité)], vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.

13. Pour les paramètres Configure storage (Configurer le stockage), vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.

14. Choisissez la section Advanced details (Détails avancés), puis sélectionnez votre domaine dans la liste déroulante Domain join directory (Annuaire de jonction de domaines).

> **Note**
>
> Après avoir choisi le répertoire de jointure du domaine, vous pouvez voir :
>
> 
>
>
> Cette erreur se produit si l'assistant de lancement EC2 identifie un document SSM existant présentant des propriétés inattendues. Vous pouvez effectuer l'une des actions suivantes :
>
> - Si vous avez déjà modifié le document SSM et que les propriétés sont attendues, choisissez Fermer et lancez l'instance EC2 sans aucune modification.
> - Cliquez sur le lien Supprimer le document SSM existant ici pour supprimer le document SSM. Cela permettra de créer un document SSM avec les propriétés

correctes. Le document SSM est automatiquement créé lorsque vous lancez l'instance EC2.

15. Pour l'IAM instance profile (profil d'instance IAM), vous pouvez sélectionner un profil d'instance IAM existant ou en créer un nouveau. Sélectionnez un profil d'instance IAM DirectoryServiceAccess auquel sont associées les politiques AWS gérées AmazonSSM ManagedInstanceCore et AmazonSSM dans la liste déroulante des profils d'instance IAM. Pour en créer un nouveau, choisissez Créer un nouveau lien de profil IAM, puis procédez comme suit :

    1. Sélectionnez Créer un rôle.
    2. Sous Select trusted entity (Sélectionner une entité approuvée), choisissez service AWS .
    3. Sous Use case (Cas d'utilisation), choisissez EC2.
    4. Sous Ajouter des autorisations, dans la liste des politiques, sélectionnez les politiques AmazonSSM ManagedInstanceCore et DirectoryServiceAccessAmazonSSM. Pour filtrer la liste, tapez **`SSM`** dans la zone de recherche. Choisissez Suivant.

    > **Note**
    >
    > AmazonSSM DirectoryServiceAccess fournit les autorisations nécessaires pour joindre des instances à une instance Active Directory gérée par. AWS Directory ServiceAmazonSSM ManagedInstanceCore fournit les autorisations minimales nécessaires pour utiliser le AWS Systems Manager service. Pour plus d'informations sur la création d'un rôle doté de ces autorisations, ainsi que sur les autres autorisations et politiques que vous pouvez attribuer à votre rôle IAM, veuillez consulter la section Create an IAM instance profile for Systems Manager (français non garanti) dans le Guide de l'utilisateur AWS Systems Manager .

    5. Sur la page Name, review, and create (Nommer, vérifier et créer), saisissez un Role name (Nom du rôle). Vous aurez besoin de ce nom de rôle pour l'attacher à l'instance EC2.
    6. (Facultatif) Vous pouvez fournir une description du profil d'instance IAM dans le champ Description.
    7. Sélectionnez Créer un rôle.
    8. Revenez à la page Launch an instance (Lancer une instance) et choisissez l'icône d'actualisation à côté du profil d'instance IAM. Votre nouveau profil d'instance IAM doit être

visible dans la liste déroulante des IAM instance profile (profil d'instance IAM). Choisissez le nouveau profil et laissez le reste de paramètres avec leurs valeurs par défaut.

16. Choisissez Launch instance (Lancer une instance).

Associez facilement une instance Linux Amazon EC2 à votre Managed AWS Microsoft AD with AD Connector

Cette procédure permet de joindre facilement une instance Linux Amazon EC2 à votre répertoire AWS Managed Microsoft AD.

Les distributions et les versions d'instance Linux suivantes sont prises en charge :

- AMI Amazon Linux 2018.03.0
- Amazon Linux 2 (64 bits x86)
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS et Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Les distributions antérieures à Ubuntu 14 et Red Hat Enterprise Linux 7 ne prennent pas en charge la fonctionnalité de jonction de domaine transparente.

Prérequis

Avant de pouvoir configurer une jonction de domaine fluide à une instance Linux EC2, vous devez suivre les procédures décrites dans cette section.

Sélectionnez votre compte de service de jonction transparente à un domaine

Vous pouvez facilement associer des ordinateurs Linux à votre Active Directory domaine local via AD Connector. Pour ce faire, vous devez créer un compte utilisateur autorisé à créer un compte d'ordinateur pour joindre les ordinateurs au domaine. Vous pouvez utiliser votre compte de service AD Connector si vous le souhaitez. Vous pouvez également utiliser n'importe quel autre

compte disposant de privilèges suffisants pour joindre des ordinateurs au domaine. Bien que les Administrateurs de domaine ou les membres d'autres groupes puissent disposer de privilèges suffisants pour joindre des ordinateurs au domaine, nous vous le déconseillons. À titre de bonne pratique, nous vous recommandons d'utiliser un compte de service disposant des privilèges minimaux nécessaires pour joindre des ordinateurs au domaine.

Pour déléguer un compte doté des privilèges minimaux nécessaires pour associer des ordinateurs au domaine, vous pouvez exécuter les PowerShell commandes suivantes. Vous devez exécuter ces commandes à partir d'un Windows ordinateur joint au domaine sur lequel le Installation des outils d'administration Active Directory pour Microsoft AD AWS géré est installé. En outre, vous devez utiliser un compte autorisé à modifier les autorisations sur l'unité d'organisation ou le conteneur de votre ordinateur. La PowerShell commande définit les autorisations qui permettent au compte de service de créer des objets informatiques dans le conteneur d'ordinateurs par défaut de votre domaine. Si vous préférez utiliser une interface utilisateur graphique (GUI), vous pouvez utiliser le processus manuel décrit dans Délégation de privilèges à votre compte de service.

```
$AccountName = 'awsSeamlessDomain'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$Domain = Get-ADDomain -ErrorAction Stop
$BaseDn = $Domain.DistinguishedName
$ComputersContainer = $Domain.ComputersContainer
$SchemaNamingContext = Get-ADRootDSE | Select-Object -ExpandProperty
 'schemaNamingContext'
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase $SchemaNamingContext
 -Filter { lDAPDisplayName -eq 'Computer' } -Properties 'schemaIDGUID').schemaIDGUID
# Getting Service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for the Computers container.
$ObjectAcl = Get-ACL -Path "AD:\$ComputersContainer"
# Setting ACL allowing the service account the ability to create child computer objects
 in the Computers container.
$AddAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'CreateChild',
 'Allow', $ServicePrincipalNameGUID, 'All'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$ComputersContainer"
```

Si vous préférez utiliser une interface utilisateur graphique (GUI), vous pouvez utiliser le processus manuel décrit dans Délégation de privilèges à votre compte de service.

Créer les secrets pour stocker le compte de service de domaine

Vous pouvez l'utiliser AWS Secrets Manager pour stocker le compte de service de domaine.

Pour créer des secrets et stocker les informations du compte de service de domaine

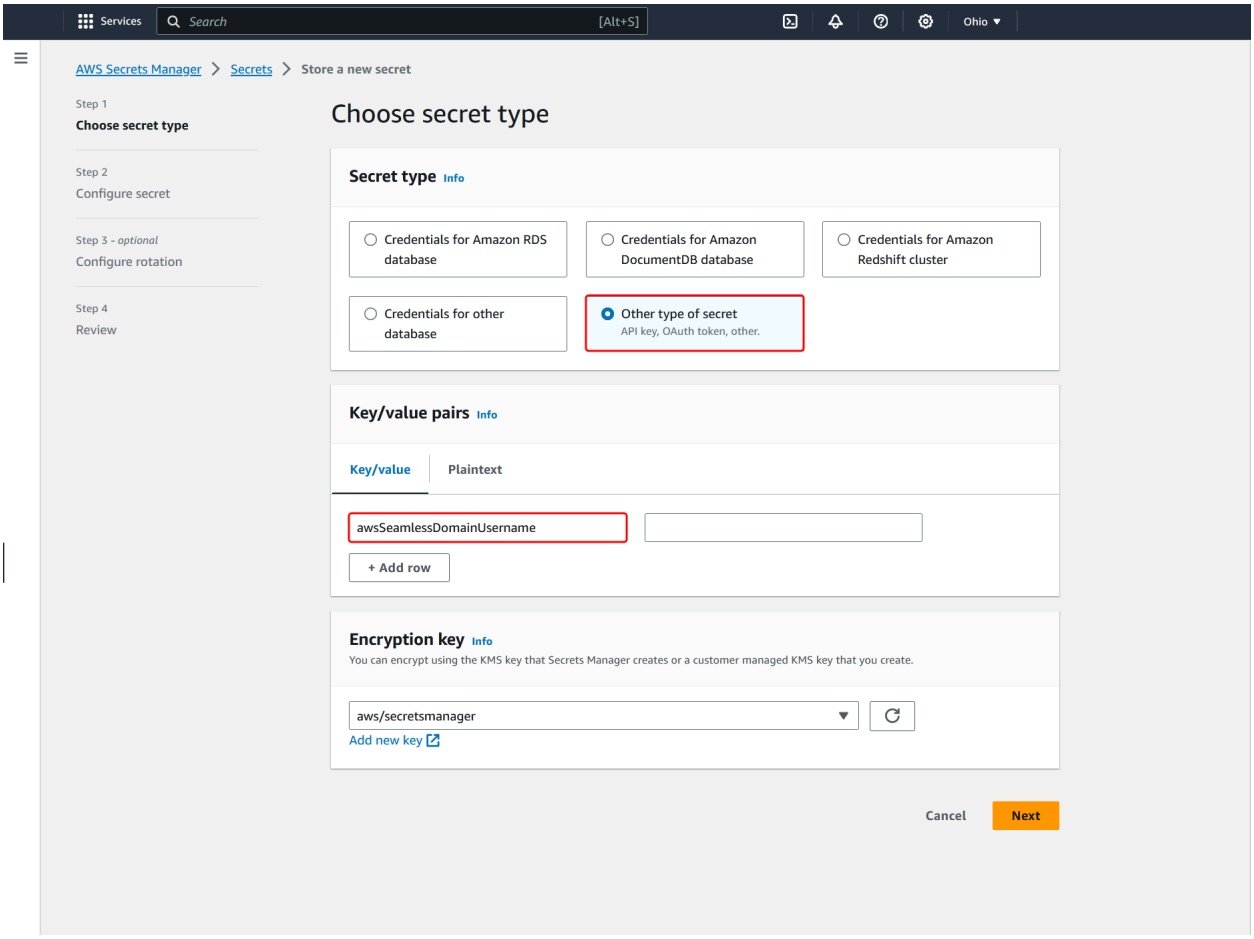
1. Connectez-vous à la AWS Secrets Manager console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/secretsmanager/.
2. Choisissez Store a new secret (Stocker un nouveau secret).
3. Sur la page Store a new secret (Stocker un nouveau secret), procédez comme suit :

    a. Sous Type de secret, sélectionnez Autre type de secret.

    b. Sous Paires clé/valeur, procédez comme suit :

        i. Dans la première case, saisissez **`awsSeamlessDomainUsername`**. Sur la même ligne, dans la case suivante, entrez le nom d'utilisateur de votre compte de service. Par exemple, si vous avez déjà utilisé la PowerShell commande, le nom du compte de service serait**`awsSeamlessDomain`**.

> **Note**
>
> Vous devez saisir **`awsSeamlessDomainUsername`** exactement tel quel. Assurez-vous qu'il n'y a pas d'espaces au début ni à la fin. Sinon, la jonction de domaine échouera.



ii. Choisissez Add row (Ajouter une ligne).

iii. Sur la nouvelle ligne, dans la première case, saisissez **`awsSeamlessDomainPassword`**. Sur la même ligne, dans la case suivante, saisissez le mot de passe de votre compte de service.

> **Note**
>
> Vous devez saisir **`awsSeamlessDomainPassword`** exactement tel quel. Assurez-vous qu'il n'y a pas d'espaces au début ni à la fin. Sinon, la jonction de domaine échouera.

iv. Sous Clé de chiffrement, laissez la valeur par défaut`aws/secretsmanager`. AWS Secrets Manager chiffre toujours le secret lorsque vous choisissez cette option. Vous pouvez également choisir une clé que vous avez créée.

> **Note**
>
> Des frais sont associés AWS Secrets Manager, selon le secret que vous utilisez. Pour obtenir la liste de prix actuelle complète, consultez Tarification AWS Secrets Manager.
> Vous pouvez utiliser la clé AWS `aws/secretsmanager` gérée créée par Secrets Manager pour chiffrer vos secrets gratuitement. Si vous créez vos propres clés KMS pour chiffrer vos secrets, cela vous AWS sera facturé au AWS KMS tarif en vigueur. Pour plus d'informations, consultez Tarification d'AWS Key Management Service.

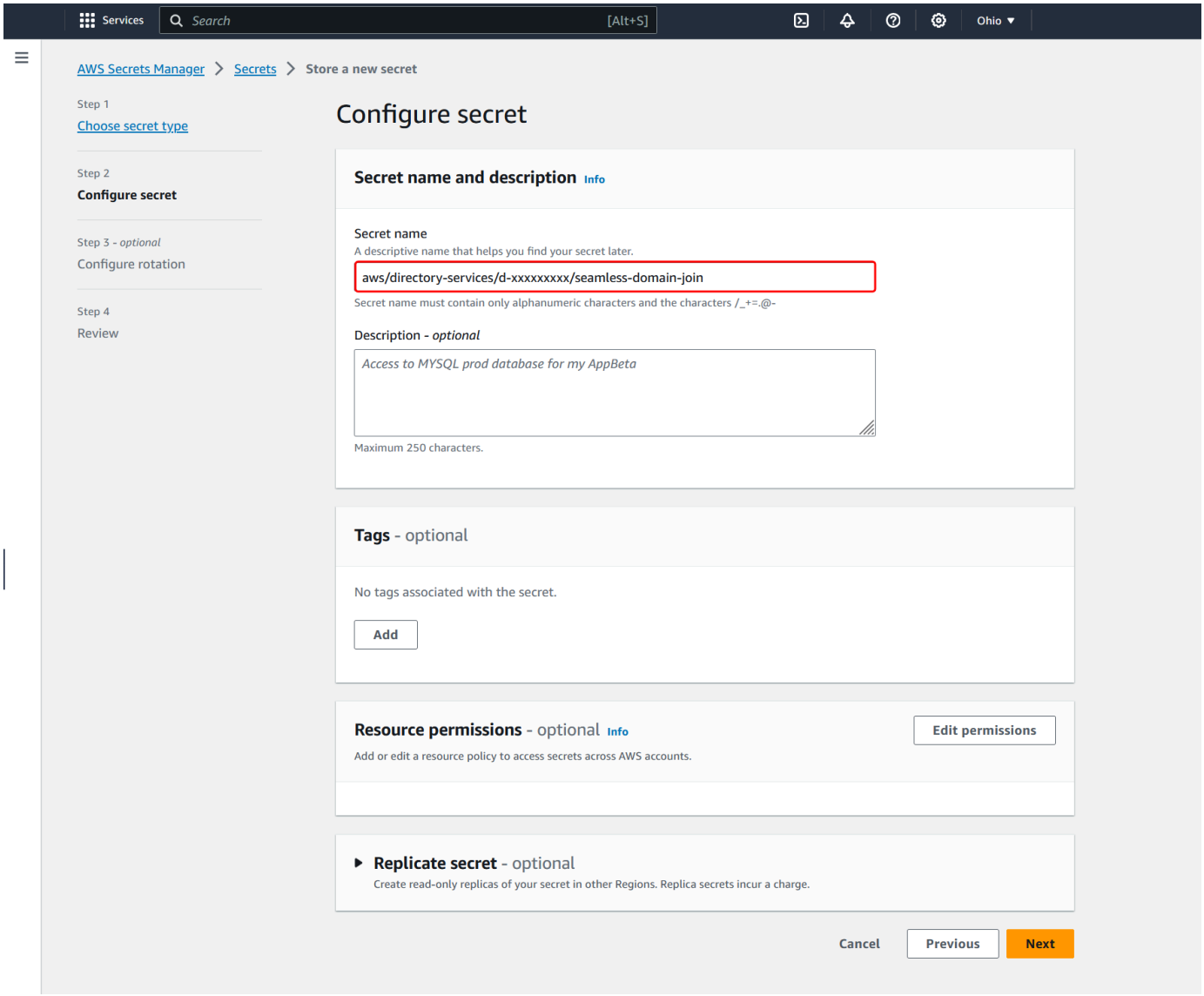
v. Choisissez Suivant.

4. Sous Nom secret, entrez un nom secret qui inclut votre identifiant de répertoire en utilisant le format suivant, en remplaçant *d-xxxxxxxxx* par votre identifiant de répertoire :

```
aws/directory-services/d-xxxxxxxxx/seamless-domain-join
```

Cela servira à récupérer des secrets dans l'application.

> **Note**
>
> Vous devez saisir **aws/directory-services/*d-xxxxxxxxx*/seamless-domain-join** exactement tel quel, mais remplacez *d-xxxxxxxxx* par votre ID d'annuaire. Assurez-vous qu'il n'y a pas d'espaces au début ni à la fin. Sinon, la jonction de domaine échouera.



5. Laissez le reste des paramètres définis par défaut, puis choisissez Next (Suivant).
6. Sous Configure automatic rotation (Configurer la rotation automatique), choisissez Disable automatic rotation (Désactiver la rotation automatique), puis cliquez sur Next (Suivant).

   Vous pouvez activer la rotation pour ce secret après l'avoir enregistré.
7. Vérifiez les paramètres, puis choisissez Store (Stocker) pour enregistrer vos modifications. La console Secrets Manager vous redirige à la liste des secrets de votre compte, où votre nouveau secret est désormais inclus.
8. Choisissez le nom du secret que vous venez de créer dans la liste et prenez note de la valeur de l'ARN secret. Vous en aurez besoin pour la section suivante.

Activer la rotation pour le secret du compte de service de domaine

Nous vous recommandons d'alterner régulièrement les secrets afin d'améliorer votre niveau de sécurité.

Pour activer la rotation pour le secret du compte de service de domaine

- Suivez les instructions de la section Configurer la rotation automatique pour les AWS Secrets Manager secrets dans le Guide de AWS Secrets Manager l'utilisateur.

  Pour l'étape 5, utilisez le modèle de rotation des informations d'identification Microsoft Active Directory dans le guide de AWS Secrets Manager l'utilisateur.

  Pour obtenir de l'aide, consultez la section Résolution des problèmes AWS Secrets Manager de rotation dans le Guide de AWS Secrets Manager l'utilisateur.

Créez le rôle et la politique IAM requis

Suivez les étapes préalables suivantes pour créer une politique personnalisée qui autorise un accès en lecture seule à votre secret de jonction de domaine transparent Secrets Manager (que vous avez créé précédemment) et pour créer un nouveau rôle IAM DomainJoin LinuxEC2.

Créer la politique de lecture IAM Secrets Manager

Utilisez la console IAM pour créer une politique qui accorde un accès en lecture seule à votre secret Secrets Manager.

Pour créer la politique de lecture IAM Secrets Manager

1. Connectez-vous au en AWS Management Console tant qu'utilisateur autorisé à créer des politiques IAM. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, Gestion des accès, sélectionnez Policies.
3. Choisissez Créer une politique.
4. Choisissez l'onglet JSON et copiez le texte du document de politique JSON suivant. Collez-le ensuite dans la zone de texte JSON.

> **Note**
>
> Assurez-vous de remplacer l'ARN de la région et de la ressource par la région et l'ARN réels du secret que vous avez créé précédemment.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:xxxxxxxxx:secret:aws/directory-
services/d-xxxxxxxxx/seamless-domain-join"
            ]
        }
    ]
}
```

5. Lorsque vous avez terminé, choisissez Next. Le programme de validation des politiques signale les éventuelles erreurs de syntaxe. Pour plus d'informations, veuillez consulter la section Validating IAM policies (français non garanti).
6. Sur la page Review policy (Réviser la politique), saisissez un nom pour la politique, tel que **`SM-Secret-Linux-DJ-d-xxxxxxxxxx-Read`**. Vérifiez la section Summary (Récapitulatif) pour voir les autorisations accordées par votre politique. Sélectionnez Create Policy (Créer une politique) pour enregistrer vos changements. La nouvelle politique s'affiche dans la liste des politiques gérées et est prête à être attachée à une identité.

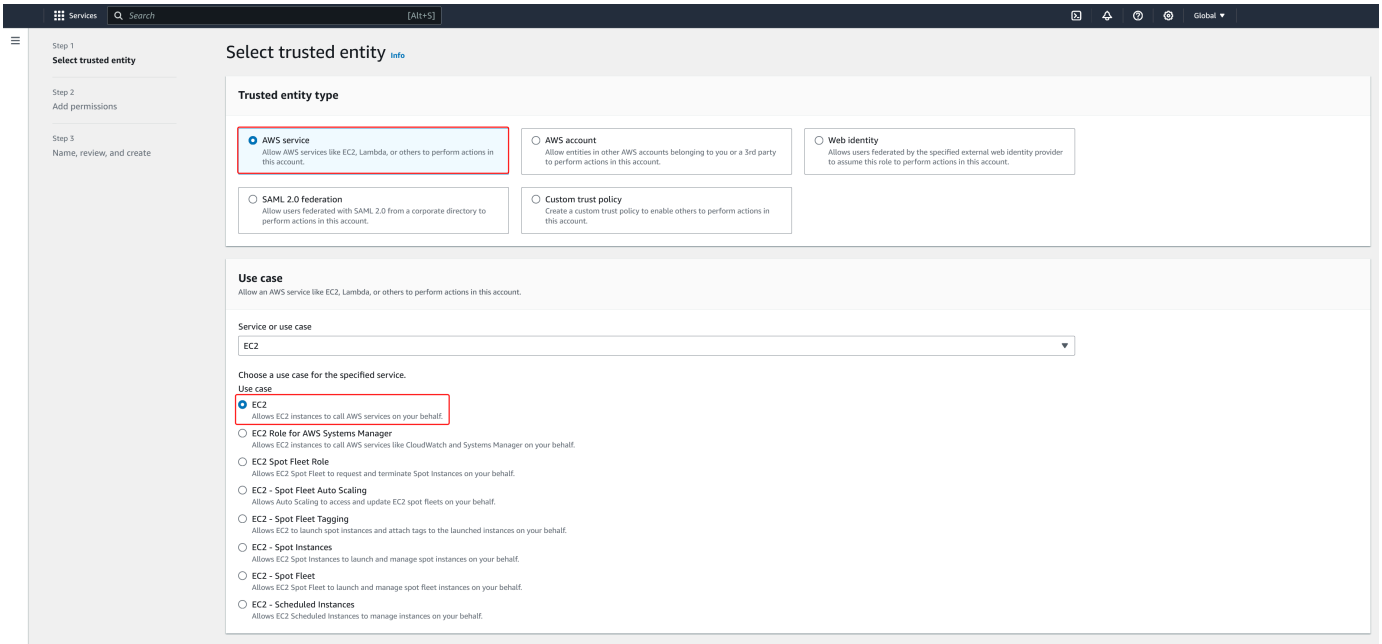
> **Note**
>
> Nous vous recommandons de créer une politique par secret. Cela garantit que les instances n'ont accès qu'au secret approprié et minimise les répercussions si une instance est compromise.

Création du rôle LinuxEC2 DomainJoin

Utilisez la console IAM pour créer le rôle que vous utiliserez pour joindre un domaine à votre instance Linux EC2.

Pour créer le rôle LinuxEC2 DomainJoin

1. Connectez-vous au en AWS Management Console tant qu'utilisateur autorisé à créer des politiques IAM. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, sous Gestion des accès, sélectionnez Rôles.
3. Dans le panneau de contenu, sélectionnez Create role (Créer un rôle).
4. Sous Select type of trusted entity (Sélectionner le type d'entité approuvée), choisissez service AWS .
5. Sous Cas d'utilisation, choisissez EC2, puis Next.



6. Pour Filter policies (Filtrer les politiques), procédez comme suit :

   a. Saisissez **`AmazonSSMManagedInstanceCore`**. Cochez ensuite la case correspondant à cet élément de la liste.

   b. Saisissez **`AmazonSSMDirectoryServiceAccess`**. Cochez ensuite la case correspondant à cet élément de la liste.

   c. Saisissez **`SM-Secret-Linux-DJ-`*`d-xxxxxxxxxx`*`-Read`** (ou le nom de la politique que vous avez créée dans la procédure précédente). Cochez ensuite la case correspondant à cet élément de la liste.

d. Après avoir ajouté les trois politiques répertoriées ci-dessus, sélectionnez Créer un rôle.

> **Note**
>
> AmazonSSM DirectoryServiceAccess fournit les autorisations nécessaires pour joindre des instances à une instance Active Directory gérée par. AWS Directory Service AmazonSSM ManagedInstanceCore fournit les autorisations minimales nécessaires pour utiliser le AWS Systems Manager service. Pour plus d'informations sur la création d'un rôle doté de ces autorisations, ainsi que sur les autres autorisations et politiques que vous pouvez attribuer à votre rôle IAM, veuillez consulter la section Create an IAM instance profile for Systems Manager (français non garanti) dans le Guide de l'utilisateur AWS Systems Manager .

7. Entrez un nom pour votre nouveau rôle, par exemple un autre nom que vous préférez dans le champ Nom du rôle. **`LinuxEC2DomainJoin`**
8. (Facultatif) Pour Role description (Description du rôle), entrez une description.
9. (Facultatif) Choisissez Ajouter une nouvelle balise à l'étape 3 : Ajouter des balises pour ajouter des balises. Les paires clé-valeur de balise sont utilisées pour organiser, suivre ou contrôler l'accès pour ce rôle.
10. Sélectionnez Créer un rôle.

Associez facilement votre instance Linux Amazon EC2 à votre Managed AWS Microsoft AD Active Directory

Maintenant que vous avez configuré toutes les tâches prérequises, vous pouvez utiliser la procédure suivante pour rejoindre facilement votre instance EC2 Linux.

Pour rejoindre facilement votre instance Linux

1. Connectez-vous à la console Amazon EC2 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le sélecteur de région de la barre de navigation, choisissez le même répertoire Région AWS que le répertoire existant.
3. Sur le EC2 Dashboard (tableau de bord EC2), dans la section Launch instance (Lancer une instance), choisissez Launch instance (Lancer une instance).

4. Sur la page Lancer une instance, dans la section Nom et balises, entrez le nom que vous souhaitez utiliser pour votre instance Linux EC2.
5. (Facultatif) Sélectionnez Add additional tags (Ajouter des balises supplémentaires) pour ajouter une ou plusieurs paires clé-valeur d'identification afin d'organiser, de suivre ou de contrôler l'accès pour cette instance EC2.
6. Dans la section Image de l'application et du système d'exploitation (Amazon Machine Image), choisissez l'AMI Linux que vous souhaitez lancer.

> **Note**
>
> L'AMI utilisée doit avoir la version 2.3.1644.0 ou supérieure AWS Systems Manager (agent SSM). Pour vérifier la version de l'agent SSM installée dans votre AMI en lançant une instance à partir de cette AMI, veuillez consulter Getting the currently installed SSM Agent version (français non garanti). Si vous devez mettre à niveau l'agent SSM, veuillez consulter Installing and configuring SSM Agent on EC2 instances for Linux (français non garanti).
> SSM utilise le `aws:domainJoin` plugin pour joindre une instance Linux à un Active Directory domaine. *`Le plugin remplace le nom d'hôte des instances Linux par le format EC2AMAZ-XXXXXXX.`* Pour plus d'informations à ce sujet`aws:domainJoin`, consultez AWS Systems Manager la référence du plug-in du document de commande dans le guide de AWS Systems Manager l'utilisateur.

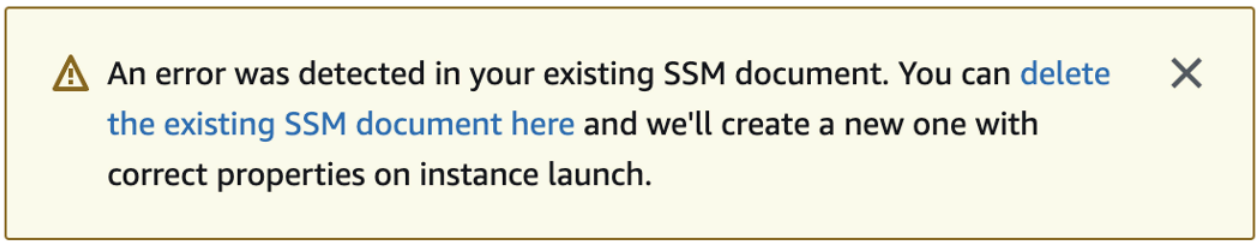
7. Dans la section Type d'instance, choisissez le type d'instance que vous souhaitez utiliser dans la liste déroulante Type d'instance.
8. Dans la section Paire de clés (connexion), vous pouvez choisir de créer une nouvelle paire de clés ou choisir une paire de clés existante. Pour créer une nouvelle paire de clés, choisissez Créer une paire de clés. Entrez le nom de la paire de clés et sélectionnez une option pour le type de paire de clés et le format de fichier de 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. Choisissez Créer une paire de clés. Le fichier de clé privée est automatiquement téléchargé dans votre navigateur. Enregistrez le fichier de clé privée en lieu sûr.

> **Important**
>
> C'est votre seule occasion d'enregistrer le fichier de clé privée.

9. Sur la page Lancer une instance, dans la section Paramètres réseau, choisissez Modifier. Choisissez le VPC dans lequel votre répertoire a été créé dans la liste déroulante VPC obligatoire.
10. Choisissez l'un des sous-réseaux publics de votre VPC dans la liste déroulante Sous-réseau. Tout le trafic externe du sous-réseau que vous choisissez doit être acheminé vers une passerelle Internet. Sinon, vous ne pourrez pas vous connecter à l'instance à distance.

    Pour obtenir plus d'informations sur la manière de se connecter à une passerelle Internet, veuillez consulter la section Connect to the internet using an internet gateway (français non garanti) dans le Guide de l'utilisateur Amazon VPC.
11. Sous Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique), choisissez Enable (Activer).

    Pour plus d'informations sur les adresses IP publiques et privées, veuillez consulter la section Amazon EC2 instance IP addressing (français non garanti) dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.
12. Pour les paramètres Firewall (security groups) [Pare-feu (groupes de sécurité)], vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
13. Pour les paramètres Configure storage (Configurer le stockage), vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
14. Choisissez la section Advanced details (Détails avancés), puis sélectionnez votre domaine dans la liste déroulante Domain join directory (Annuaire de jonction de domaines).

> **Note**
>
> Après avoir choisi le répertoire de jointure du domaine, vous pouvez voir :
>
> 
>
>
> Cette erreur se produit si l'assistant de lancement EC2 identifie un document SSM existant présentant des propriétés inattendues. Vous pouvez effectuer l'une des actions suivantes :

- Si vous avez déjà modifié le document SSM et que les propriétés sont attendues, choisissez Fermer et lancez l'instance EC2 sans aucune modification.
- Cliquez sur le lien Supprimer le document SSM existant ici pour supprimer le document SSM. Cela permettra de créer un document SSM avec les propriétés correctes. Le document SSM est automatiquement créé lorsque vous lancez l'instance EC2.

15. Pour le profil d'instance IAM, choisissez le rôle IAM que vous avez créé précédemment dans la section des prérequis Étape 2 : Création du rôle LinuxEC2. DomainJoin
16. Choisissez Launch instance (Lancer une instance).

> **Note**
>
> Si vous effectuez une jonction de domaine transparente avec SUSE Linux, un redémarrage est nécessaire pour que les authentifications fonctionnent. Pour redémarrer SUSE depuis le terminal Linux, tapez sudo reboot.

Maintenance de votre annuaire AD Connector

Cette section décrit comment assurer la gestion des tâches administratives courantes pour votre environnement AD Connector.

Rubriques

- Supprimer votre AD Connector
- Affichage des informations d'annuaire

Supprimer votre AD Connector

Lorsqu'un connecteur AD Connector est supprimé, votre annuaire sur site reste intact. Toutes les instances qui sont jointes à l'annuaire restent également intactes et jointes à votre annuaire sur site. Vous pouvez toutefois utiliser les informations d'identification de votre annuaire pour vous connecter à ces instances.

Pour supprimer AD Connector

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires). Assurez-vous que vous vous trouvez Région AWS là où votre AD Connector est déployé. Pour plus d'informations, voir Choisir une région.
2. Assurez-vous qu'aucune AWS application n'est activée pour l'AD Connector que vous souhaitez supprimer. AWS Les applications activées vous empêcheront de supprimer votre AD Connector.

   a. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.

   b. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications). Dans la section AWS Applications et services, vous pouvez voir quelles AWS applications sont activées pour votre AD Connector.

      - Désactivez AWS Management Console l'accès. Pour plus d'informations, consultez Désactiver l'accès à AWS Management Console.
      - Pour désactiver Amazon WorkSpaces, vous devez désenregistrer le service depuis le répertoire de la WorkSpaces console. Pour plus d'informations, consultez la section Désenregistrement d'un annuaire dans le guide d'administration Amazon WorkSpaces .
      - Pour désactiver Amazon WorkDocs, vous devez supprimer le WorkDocs site Amazon dans la WorkDocs console Amazon. Pour plus d'informations, consultez Supprimer un site dans le guide d' WorkDocs administration Amazon.
      - Pour désactiver Amazon WorkMail, vous devez supprimer l' WorkMail organisation Amazon dans la WorkMail console Amazon. Pour plus d'informations, consultez Supprimer une organisation dans le manuel Amazon WorkMail Administrator Guide.
      - Pour désactiver Amazon FSx for Windows File Server, vous devez supprimer le système de fichiers Amazon FSx du domaine. Pour plus d'informations, consultez la section Travailler avec un Active Directory serveur de fichiers FSx for Windows dans le guide de l'utilisateur d'Amazon FSx for Windows File Server.
      - Pour désactiver Amazon Relational Database Service, vous devez supprimer l'instance Amazon RDS du domaine. Pour plus d'informations, veuillez consulter la section Managing a DB instance in a domain (français non garanti) dans le Guide de l'utilisateur Amazon RDS.
      - Pour désactiver le AWS Client VPN service, vous devez supprimer le service d'annuaire du point de terminaison VPN du Client. Pour plus d'informations, consultez la section Active DirectoryAuthentification dans le guide de AWS Client VPN l'administrateur.

- Pour désactiver Amazon Connect, vous devez supprimer l'instance Amazon Connect. Pour plus d'informations, veuillez consulter Deleting an Amazon Connect instance (français non garanti) dans le Guide d'administration Amazon Connect.
- Pour désactiver Amazon QuickSight, vous devez vous désabonner d'Amazon QuickSight. Pour plus d'informations, consultez la section Fermeture de votre Amazon QuickSight compte dans le guide de QuickSight l'utilisateur Amazon.

> **Note**
>
> Si vous l'utilisez AWS IAM Identity Center et que vous l'avez déjà connecté au répertoire AWS Managed Microsoft AD que vous souhaitez supprimer, vous devez d'abord modifier la source d'identité avant de pouvoir la supprimer. Pour plus d'informations, veuillez consulter la section Change your identity source (français non garanti) dans le Guide de l'utilisateur IAM Identity Center.

3. Dans le volet de navigation, choisissez Directories (Annuaires).
4. Sélectionnez uniquement l'AD Connector à supprimer, puis cliquez sur Delete (Supprimer). La suppression de l'AD Connector prend plusieurs minutes. Lorsque l'AD Connector a été supprimé, il est retiré de votre liste d'annuaires.

Affichage des informations d'annuaire

Vous pouvez afficher des informations détaillées sur un annuaire.

Pour afficher les informations détaillées de l'annuaire

1. Dans le volet de navigation de la AWS Directory Service console, sous Active Directory, sélectionnez Répertoires.
2. Cliquez sur le lien de l'ID correspondant à votre annuaire. Les informations relatives à l'annuaire sont affichées sur la page Détails de l'annuaire.

Pour de plus amples informations sur le champ Status (Statut), veuillez consulter Comprendre le statut de votre annuaire.

Permettre l'accès aux AWS applications et aux services

Les utilisateurs peuvent autoriser AD Connector à autoriser AWS des applications et des services, tels qu'Amazon WorkSpaces, à accéder à votreActive Directory. Les AWS applications et services suivants peuvent être activés ou désactivés pour fonctionner avec AD Connector.

AWS application/service	En savoir plus...
Amazon Chime	Pour plus d'informations, veuillez consulter le Guide d'administration Amazon Chime.
Amazon Connect	Pour plus d'informations, veuillez consulter le Guide d'administration Amazon Connect.
Amazon WorkDocs	Pour plus d'informations, consultez le guide d' WorkDocs administration Amazon.
Amazon WorkMail	Pour plus d'informations, consultez le guide de WorkMail l'administrateur Amazon.
Amazon WorkSpaces	Vous pouvez créer un Simple AD, AWS Managed Microsoft AD ou AD Connector directement à partir de WorkSpaces. Il vous suffit de lancer la configuration avancée lors de la création de votre Workspace. Pour plus d'informations, consultez le guide d' WorkSpaces administration Amazon.
AWS Client VPN	Pour plus d'informations, veuillez consulter le Guide de l'utilisateurAWS Client VPN.
AWS IAM Identity Center	Pour de plus amples informations, veuillez consulter le Guide de l'utilisateurAWS IAM Identity Center.
AWS Management Console	Pour de plus amples informations, veuillez consulter Activation de l'accès à AWS

AWS application/service	En savoir plus...
	Management Console avec les informations d'identification AD.
AWS Transfer Family	Pour de plus amples informations, veuillez consulter le Guide de l'utilisateurAWS Transfer Family.

Une fois activé, vous gérez l'accès à vos annuaires dans la console de l'application ou du service auquel vous souhaitez donner accès à votre répertoire. Pour rechercher les liens vers AWS les applications et les services décrits ci-dessus dans la AWS Directory Service console, effectuez les opérations suivantes.

Pour afficher les applications et les services d'un annuaire

1. Dans le panneau de navigation de la consoleAWS Directory Service, choisissez Annuaires.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications).
4. Consultez la liste dans la section Applications et servicesAWS .

Pour plus d'informations sur la manière d'autoriser ou d'annuler l'autorisation d' AWS applications et de services utilisant AWS Directory Service, consultezAutorisation pour AWS les applications et les services utilisant AWS Directory Service.

Mise à jour de l'adresse DNS pour votre AD Connector

Utilisez les étapes suivantes pour mettre à jour les adresses DNS vers lesquelles votre AD Connector pointe.

> **Note**
>
> Si vous avez une mise à jour en cours, vous devez attendre la fin de son exécution avant de soumettre une nouvelle mise à jour.
> Si vous utilisez WorkSpaces avec votre AD Connector, assurez-vous que les adresses DNS de WorkSpace sont également mises à jour. Pour de plus amples informations,

consultez la section Update DNS servers for WorkSpaces (Mise à jour des serveurs DNS pour WorkSpaces).

Pour mettre à jour vos paramètres DNS pour AD Connector

1. Dans le volet de navigation de la console AWS Directory Service, sous Active Directory, sélectionnez Directories (Annuaires).
2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), choisissez l'onglet Network & Security (Réseau et sécurité).
4. Faites défiler l'écran jusqu'à la section Existing DNS settings (Paramètres DNS existants) et choisissez Update (Mettre à jour).
5. Dans la boîte de dialogue Update existing DNS addresses (Mettre à jour les adresses DNS existantes) saisissez les adresses IP DNS mises à jour, puis sélectionnez Update (Mettre à jour).

Pour plus d'informations sur la résolution des problèmes liés à AD Connector, consultez la section Troubleshooting AD Connector (Résolution des problèmes liés à AD Connector).

Bonnes pratiques pour AD Connector

Voici quelques suggestions et directives que vous devez prendre en compte pour éviter de rencontrer des problèmes et tirer le meilleur parti d'AD Connector.

Configuration : prérequis

Pensez à utiliser ces consignes avant de créer votre annuaire.

Vérifiez que vous avez le type d'annuaire approprié

AWS Directory Service propose plusieurs méthodes d'utilisation Microsoft Active Directory avec d'autres AWS services. Vous pouvez choisir le service d'annuaire doté des fonctionnalités dont vous avez besoin à un prix adapté à votre budget :

- AWS Directory Service pour Microsoft Active Directory est un service géré riche en fonctionnalités Microsoft Active Directory hébergé sur le AWS cloud. AWS Managed Microsoft AD est votre meilleur choix si vous avez plus de 5 000 utilisateurs et que vous avez besoin d'établir une relation de confiance entre un annuaire AWS hébergé et vos annuaires locaux.

- AD Connector connecte simplement votre site existant Active Directory à AWS. AD Connector est votre meilleur allié si vous souhaitez utiliser votre annuaire sur site existant avec les services AWS .
- Simple AD est un annuaire à petite échelle et à faible coût doté d'une Active Directory compatibilité de base. Il prend en charge jusqu'à 5 000 utilisateurs, des applications compatibles avec Samba 4 et une compatibilité LDAP pour les applications LDAP.

Pour une comparaison plus détaillée des AWS Directory Service options, voirQue choisir ?.

Assurez-vous que vos VPC et instances sont correctement configurés

Pour vous connecter à vos annuaires, les gérer et les utiliser, vous devez configurer correctement les VPC auxquels les annuaires sont associés. Consultez AWS Conditions préalables à la gestion de Microsoft AD, Conditions préalables requises pour AD Connector ou Prérequis pour Simple AD pour obtenir plus d'informations sur les exigences de sécurité et de mise en réseau des VPC.

Si vous ajoutez une instance à votre domaine, assurez-vous de disposer d'une connectivité et d'un accès à distance à votre instance, comme décrit dans Joindre une instance Amazon EC2 à votre compte AWS Microsoft AD géré Active Directory.

Tenez compte des limites

Découvrez les différentes limites applicables à votre type d'annuaire spécifique. Le stockage disponible et la taille globale de vos objets sont les seules limites quant au nombre d'objets que vous pouvez stocker dans votre annuaire. Consultez AWS Quotas Managed Microsoft AD, Quotas AD Connector ou Quotas Simple AD pour plus d'informations sur l'annuaire que vous avez choisi.

Comprenez la configuration et l'utilisation AWS des groupes de sécurité de votre annuaire

AWS crée un groupe de sécurité et l'attache aux interfaces réseau élastiques de votre annuaire accessibles depuis vos VPC pairs ou redimensionnés. AWS configure le groupe de sécurité pour bloquer le trafic inutile vers le répertoire et autorise le trafic nécessaire.

Modification du groupe de sécurité de l'annuaire

Si vous souhaitez modifier la sécurité des groupes de sécurité des annuaires, vous pouvez le faire. Effectuez ces modifications uniquement si vous avez entièrement compris le fonctionnement du

filtrage des groupes de sécurité. Pour plus d'informations, veuillez consulter la section Amazon EC2 security groups for Linux instances (français non garanti) dans le Guide de l'utilisateur Amazon EC2. Des modifications inappropriées peuvent entraîner une perte de communication avec les ordinateurs et les instances concernés. AWS recommande de ne pas essayer d'ouvrir des ports supplémentaires vers votre répertoire car cela réduit la sécurité de votre répertoire. Veuillez lire attentivement le modèle de responsabilité partagée AWS.

> **Warning**
>
> Vous êtes techniquement en mesure d'associer le groupe de sécurité de l'annuaire à d'autres instances EC2 que vous créez. Il AWS déconseille toutefois cette pratique. AWS peut avoir des raisons de modifier le groupe de sécurité sans préavis pour répondre aux besoins fonctionnels ou de sécurité du répertoire géré. Ces modifications affectent toutes les instances auxquelles vous associez le groupe de sécurité d'annuaire et peuvent interrompre le fonctionnement des instances associées. De plus, l'association du groupe de sécurité de l'annuaire avec vos instances EC2 peut créer un risque de sécurité potentiel pour vos instances EC2.

Configuration appropriée des sites locaux et des sous-réseaux dans le cadre de l'utilisation d'AD Connector

Si votre réseau sur site comporte des sites Active Directory définis, vous devez vous assurer que les sous-réseaux du VPC sur lesquels votre AD Connector réside sont définis dans un site Active Directory, et qu'il n'y a pas de conflits entre les sous-réseaux de votre VPC et les sous-réseaux de vos autres sites.

Pour découvrir les contrôleurs de domaine, AD Connector utilise le site Active Directory dont les plages d'adresses IP de sous-réseau sont proches de celles du VPC contenant l'AD Connector. Si vous avez un site comportant des sous-réseaux avec les mêmes plages d'adresses IP que votre VPC, l'AD Connector découvre les contrôleurs de domaine présents sur ce site, qui ne sont peut-être pas physiquement proches de votre région.

Comprendre les restrictions relatives aux noms d'utilisateur pour AWS les applications

AWS Directory Service prend en charge la plupart des formats de caractères pouvant être utilisés dans la construction des noms d'utilisateur. Cependant, certaines restrictions de caractères sont appliquées aux noms d'utilisateur qui seront utilisés pour se connecter à AWS des applications, telles

qu'Amazon WorkSpaces WorkDocs WorkMail, Amazon ou Amazon QuickSight. Ces restrictions empêchent l'utilisation des caractères suivants :

- Espaces
- Caractères multioctets
- !"#$%&'()*+,/:;<=>?@[\]^`{|}~

> **Note**
>
> Le symbole @ est autorisé s'il précède un suffixe UPN.

Programmation de vos applications

Avant de programmer vos applications, prenez en compte les éléments suivants :

Testez la charge avant de lancer la production

Assurez-vous de procéder à des tests avec des applications et des requêtes représentatifs de votre charge de travail de production afin de confirmer que l'annuaire s'adapte à la charge de travail de votre application. Si vous avez besoin de capacité supplémentaire, répartissez votre charge parmi plusieurs annuaires du connecteur AD.

Utilisation de votre annuaire

Voici quelques suggestions à garder à l'esprit lorsque vous utilisez votre annuaire.

Effectuez une rotation régulière des informations d'identification administrateur

Modifiez régulièrement votre mot de passe administrateur de compte de service AD Connector et assurez-vous que celui-ci est conforme à vos stratégies de gestion des mots de passe Active Directory existantes. Pour obtenir des instructions sur la façon de modifier le mot de passe du compte de service, veuillez consulter Mettre à jour les informations d'identification de votre compte de service AD Connector dans AWS Directory Service.

Utilisez des connecteurs AD uniques pour chaque domaine

Les AD Connector et vos domaines AD sur site ont une relation 1-à-1. En d'autres termes, pour chaque domaine sur site, y compris les domaines enfants dans une forêt AD par rapport à laquelle

vous souhaitez vous authentifier, vous devez créer un AD Connector unique. Chaque AD Connector que vous créez doit utiliser un compte de service différent, même s'ils sont connectés dans le même annuaire.

Vérifiez la compatibilité

Lorsque vous utilisez AD Connector, vous devez vous assurer que votre annuaire local est et reste compatible avec AWS Directory Service s. Pour plus d'informations sur vos responsabilités, veuillez consulter notre modèle de responsabilité partagée.

Quotas AD Connector

Voici les quotas par défaut pour AD Connector. Sauf indication contraire, chaque quota est spécifique à une région.

Quotas AD Connector

Ressource	Quota par défaut
Annuaires AD Connector	10
Nombre maximal de certificats d'autorité de certification enregistrés par annuaire	5

Politique de compatibilité des applications pour AD Connector

Solution alternative à AWS Directory Service for Microsoft Active Directory (AWS Microsoft AD géré), AD Connector est un proxy Active Directory dédié exclusivement aux applications et aux services crées par AWS. Vous configurez le proxy de manière à ce qu'il utilise un domaine Active Directory spécifié. Lorsque l'application doit rechercher un utilisateur ou un groupe dans Active Directory, AD Connector relaie la demande à l'annuaire. De même, lorsqu'un utilisateur se connecte à l'application, AD Connector relaie la demande d'authentification à l'annuaire. Aucune application tierce ne fonctionne avec AD Connector.

Voici une liste des applications et des services AWS compatibles :

- Amazon Chime : pour obtenir des instructions détaillées, veuillez consulter la section Connect to your Active Directory (français non garanti).

- Amazon Connect : pour plus d'informations, veuillez consulter la section How Amazon Connect works (français non garanti).
- Amazon EC2 pour Windows ou Linux : vous pouvez utiliser la fonctionnalité de jonction de domaine Active Directory fluide d'Amazon EC2 Windows ou Linux pour joindre votre instance à votre Active Directory autogéré (sur site). Une fois jointe, l'instance communique directement avec votre Active Directory et contourne AD Connector. Pour en savoir plus, consultez Joignez une instance Amazon EC2 à votre Active Directory.
- AWS Management Console – Vous pouvez utiliser AD Connector pour authentifier les utilisateurs AWS Management Console au moyen de leurs informations d'identification Active Directory sans avoir à configurer l'infrastructure SAML. Pour en savoir plus, consultez Activation de l'accès à AWS Management Console avec les informations d'identification AD.
- Amazon QuickSight - Pour plus d'informations, consultez la section Gestion des comptes utilisateurs dans Amazon QuickSight Enterprise Edition.
- AWS IAM Identity Center : pour obtenir des instructions détaillées, veuillez consulter la section Connect IAM Identity Center to an on-premises Active Directory (français non garanti).
- AWS Transfer Family : pour obtenir des instructions détaillées, veuillez consulter la section Working with AWS Directory Service for Microsoft Active Directory (français non garanti).
- AWS Client VPN : pour obtenir des instructions détaillées, veuillez consulter la section Client authentication and authorization (français non garanti).
- Amazon WorkDocs - Pour obtenir des instructions détaillées, consultez Connexion à votre annuaire local avec AD Connector.
- Amazon WorkMail - Pour des instructions détaillées, consultez Intégrer Amazon WorkMail à un annuaire existant (configuration standard).
- WorkSpaces - Pour obtenir des instructions détaillées, voir Lancer un connecteur WorkSpace à l'aide d'AD Connector.

> **Note**
>
> Amazon RDS est compatible avec AWS Managed Microsoft AD uniquement et n'est pas compatible avec AD Connector. Pour plus d'informations, consultez la section AWS Managed Microsoft AD de la page AWS Directory ServiceFAQ.

Résolution des problèmes liés à AD Connector

Les informations suivantes peuvent vous aider à résoudre certains problèmes courants que vous pouvez rencontrer lors de la création ou de l'utilisation de votre AD Connector.

Rubriques

Problèmes liés à la création

Les problèmes de création suivants sont courants pour AD Connector

L'erreur « AZ Constrained » s'affiche lorsque je crée un annuaire

Certains AWS comptes créés avant 2012 peuvent avoir accès aux zones de disponibilité des régions de l'est des États-Unis (Virginie du Nord), de l'ouest des États-Unis (Californie du Nord) ou de l'Asie-Pacifique (Tokyo) qui ne prennent pas en charge les AWS Directory Service annuaires. Si vous recevez une telle erreur lors de la création d'unActive Directory, choisissez un sous-réseau dans une autre zone de disponibilité et réessayez de créer le répertoire.

Je reçois le message d'erreur « Problèmes de connectivité détectés » lorsque j'essaie de créer un AD Connector

Si vous recevez le message d'erreur « Problème de connectivité détecté » lorsque vous essayez de créer un AD Connector, cela peut être dû à la disponibilité du port ou à la complexité du mot de passe AD Connector. Vous pouvez tester la connexion de votre connecteur AD pour vérifier si les ports suivants sont disponibles :

- 53 (DNS)

- 88 (Kerberos)
- 389 (LDAP)

Pour tester votre connexion, consultezTest de votre connecteur AD Connector. Le test de connexion doit être effectué sur l'instance jointe aux deux sous-réseaux auxquels les adresses IP du connecteur AD sont associées.

Si le test de connexion est réussi et que l'instance rejoint le domaine, vérifiez le mot de passe de votre connecteur AD. AD Connector doit répondre aux exigences AWS de complexité des mots de passe. Pour plus d'informations, consultez la section Compte de service dansConditions préalables requises pour AD Connector.

Si votre AD Connector ne répond pas à ces exigences, recréez-le avec un mot de passe conforme à ces exigences.

Problèmes de connectivité

Les problèmes de connectivité courants liés à AD Connector sont les suivants :

- L'erreur « Connectivity issues detected » s'affiche lorsque je tente de me connecter à mon annuaire sur site
- L'erreur « DNS unavailable » s'affiche lorsque j'essaie de me connecter à mon annuaire sur site
- L'erreur « SRV record » s'affiche lorsque je tente de me connecter à mon annuaire sur site

L'erreur « Connectivity issues detected » s'affiche lorsque je tente de me connecter à mon annuaire sur site

Un message d'erreur similaire à ce qui suit s'affiche lors de la connexion à votre annuaire sur site :

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: <IP address>
 Kerberos/authentication unavailable (TCP port 88) for IP: <IP address> Please ensure
 that the listed ports are available and retry the operation.
```

AD Connector doit être capable de communiquer avec vos contrôleurs de domaine sur site via les protocoles TCP et UDP sur les ports suivants. Vérifiez que vos groupes de sécurité et pare-feu sur site autorisent la communication TCP et UDP sur ces ports. Pour plus d'informations, consultez Conditions préalables requises pour AD Connector.

- 88 (Kerberos)
- 389 (LDAP)

Vous aurez peut-être besoin de ports TCP/UDP supplémentaires en fonction de vos besoins. Consultez la liste suivante pour certains de ces ports. Pour plus d'informations sur les ports utilisés parActive Directory, consultez la section Comment configurer un pare-feu pour les Active Directory domaines et les approbations dans Microsoft la documentation.

- 135 (mappeur de points de terminaison RPC)
- 646 (LDAP SSL)
- 3268 (LDAP GC)
- 3269 (LDAP GC SSL)

L'erreur « DNS unavailable » s'affiche lorsque j'essaie de me connecter à mon annuaire sur site

Un message d'erreur similaire à ce qui suit s'affiche lors de la connexion à votre annuaire sur site :

```
DNS unavailable (TCP port 53) for IP: <DNS IP address>
```

AD Connector doit être capable de communiquer avec vos serveurs DNS sur site via les protocoles TCP et UDP sur le port 53. Vérifiez que vos groupes de sécurité et pare-feu sur site autorisent la communication TCP et UDP sur ce port. Pour plus d'informations, consultez Conditions préalables requises pour AD Connector.

L'erreur « SRV record » s'affiche lorsque je tente de me connecter à mon annuaire sur site

Un message d'erreur similaire à un ou plusieurs des messages suivants s'affiche lors de la connexion à votre annuaire sur site :

```
SRV record for LDAP does not exist for IP: <DNS IP address> SRV record for Kerberos
 does not exist for IP: <DNS IP address>
```

AD Connector doit obtenir les enregistrements SRV `_ldap._tcp.`*`<DnsDomainName>`* et `_kerberos._tcp.`*`<DnsDomainName>`* lors de la connexion à votre annuaire. Cette erreur s'affiche

si le service ne peut pas obtenir ces enregistrements auprès des serveurs DNS que vous avez spécifiés lors de la connexion à votre annuaire. Pour plus d'informations sur ces enregistrements SRV, veuillez consulter SRV record requirements.

Problèmes d'authentification

Voici quelques problèmes d'authentification courants liés à AD Connector :

- Je reçois un message d'erreur « Échec de la validation du certificat » lorsque j'essaie de me connecter à l' Amazon WorkSpaces aide d'une carte à puce
- L'erreur « Invalid Credentials » s'affiche lorsque le compte de service utilisé par AD Connector tente une authentification
- Je reçois un message d'erreur « Impossible de m'authentifier » lorsque j'utilise AWS des applications pour rechercher des utilisateurs ou des groupes
- Je reçois un message d'erreur concernant mes informations d'identification d'annuaire lorsque j'essaie de mettre à jour le compte du service AD Connector
- Certains de mes utilisateurs ne peuvent pas s'authentifier avec mon annuaire

Je reçois un message d'erreur « Échec de la validation du certificat » lorsque j'essaie de me connecter à l' Amazon WorkSpaces aide d'une carte à puce

Vous recevez un message d'erreur similaire au suivant lorsque vous essayez de vous connecter à l' WorkSpaces aide d'une carte à puce :

```
ERROR: Certificate Validation failed. Please try again by restarting your browser or
 application and make sure you select the correct certificate.
```

L'erreur se produit si le certificat de la carte à puce n'est pas correctement stocké sur le client qui utilise les certificats. Pour plus d'informations sur les exigences relatives à l'AD Connector et aux cartes à puce, consultezPrérequis.

Utilisez les procédures suivantes pour résoudre les problèmes liés à la capacité de la carte à puce à stocker des certificats dans le magasin de certificats de l'utilisateur :

1. Sur l'appareil qui rencontre des difficultés pour accéder aux certificats, accédez au Microsoft Management Console (MMC).

> **Important**
>
> Avant de poursuivre, créez une copie du certificat de la carte à puce.

2. Accédez au magasin de certificats dans la MMC. Supprimez le certificat de carte à puce de l'utilisateur du magasin de certificats. Pour plus d'informations sur l'affichage du magasin de certificats dans la MMC, voir Comment : afficher les certificats avec le composant logiciel enfichable MMC dans la documentation. Microsoft
3. Retirez la carte à puce.
4. Réinsérez la carte à puce afin qu'elle puisse remplir à nouveau le certificat de carte à puce dans le magasin de certificats de l'utilisateur.

> **Warning**
>
> Si la carte à puce ne recharge pas le certificat dans le magasin de l'utilisateur, elle ne peut pas être utilisée pour l'authentification par carte à WorkSpaces puce.

Le compte de service du connecteur AD doit comporter les éléments suivants :

- `my/spn`ajouté au nom du principe de service
- Délégué pour le service LDAP

Une fois le certificat rechargé sur la carte à puce, le contrôleur de domaine sur site doit être vérifié pour déterminer s'il est bloqué lors du mappage du nom d'utilisateur principal (UPN) pour le nom alternatif du sujet. Pour plus d'informations sur cette modification, consultez Comment désactiver le nom alternatif du sujet pour le mappage UPN dans Microsoft la documentation.

Pour vérifier la clé de registre de votre contrôleur de domaine, procédez comme suit :

1. Dans l'éditeur de registre, accédez à la clé de ruche suivante

   HKEY_LOCAL_MACHINE \ SYSTÈME \ \ Services \ Kdc \ CurrentControlSet
   UseSubjectAltName
2. Sélectionnez UseSubjectAltName. Assurez-vous que la valeur est définie sur 0.

> **Note**
>
> Si la clé de registre est définie sur les contrôleurs de domaine locaux, l'AD Connector ne sera pas en mesure de localiser les utilisateurs Active Directory et le message d'erreur ci-dessus s'affichera.

Les certificats de l'autorité de certification (CA) doivent être téléchargés sur le certificat de carte à puce AD Connector. Le certificat doit contenir des informations OCSP. La liste suivante répertorie les exigences supplémentaires pour l'autorité de certification :

- Le certificat doit se trouver dans l'autorité racine sécurisée du contrôleur de domaine, du serveur de l'autorité de certification et du WorkSpaces.
- Les certificats hors ligne et Root CA ne contiendront pas les informations OSCP. Ces certificats contiennent des informations relatives à leur révocation.
- Si vous utilisez un certificat d'autorité de certification tiers pour l'authentification par carte à puce, l'autorité de certification et les certificats intermédiaires doivent être publiés dans le magasin Active Directory NTAuth. Ils doivent être installés dans l'autorité racine approuvée pour tous les contrôleurs de domaine, serveurs d'autorités de certification et WorkSpaces.
  - Vous pouvez utiliser la commande suivante pour publier des certificats dans le magasin Active Directory NTAuth :

```
certutil -dspublish -f Third_Party_CA.cer NTAuthCA
```

Pour plus d'informations sur la publication de certificats dans le magasin NTAuth, voir Importer le certificat CA émetteur dans le magasin Enterprise NTAuth dans le guide d'installation d'Access Amazon WorkSpaces with Common Access Cards.

Vous pouvez vérifier si le certificat utilisateur ou les certificats de chaîne CA sont vérifiés par OCSP en suivant cette procédure :

1. Exportez le certificat de carte à puce vers un emplacement sur la machine locale, tel que le lecteur C :.
2. Ouvrez une invite de ligne de commande et naviguez jusqu'à l'emplacement où le certificat de carte à puce exporté est stocké.

3. Entrez la commande suivante :

```
certutil -URL Certficate_name.cer
```

4. Une fenêtre contextuelle devrait apparaître à la suite de la commande. Sélectionnez l'option OCSP dans le coin droit, puis sélectionnez Récupérer. Le statut devrait revenir tel que vérifié.

Pour plus d'informations sur la commande certutil, consultez certutil dans la documentation Microsoft

L'erreur « Invalid Credentials » s'affiche lorsque le compte de service utilisé par AD Connector tente une authentification

Cela peut se produire si le disque dur de votre contrôleur de domaine manque d'espace libre. Assurez-vous que les disques durs de votre contrôleur de domaine ne sont pas pleins.

Je reçois un message d'erreur « Impossible de m'authentifier » lorsque j'utilise AWS des applications pour rechercher des utilisateurs ou des groupes

Vous pouvez rencontrer des erreurs lors de la recherche d'utilisateurs lors de l'utilisation d' AWS applications, telles qu' WorkSpaces Amazon QuickSight, même lorsque le statut AD Connector était actif. Les informations d'identification ayant expiré peuvent empêcher AD Connector d'exécuter des requêtes sur les objets dans votre Active Directory. Mettez à jour le mot de passe du compte de service en suivant les étapes indiquées dansLa jointure de domaine fluide pour les instances Amazon EC2 a cessé de fonctionner.

Je reçois un message d'erreur concernant mes informations d'identification d'annuaire lorsque j'essaie de mettre à jour le compte du service AD Connector

Vous recevez un message d'erreur similaire à l'un ou plusieurs des suivants lorsque vous essayez de mettre à jour le compte de service AD Connector :

```
Message:An Error Has Occurred
Your directory needs a credential update. Please update the directory credentials.
```

```
An Error Has Occurred
Your directory needs a credential update. Please update the directory credentials
following Update your AD Connector Service Account Credentials
```

```
Message:
```

```
An Error Has Occurred
Your request has a problem. Please see the following details.
There was an error with the service account/password combination
```

Il se peut qu'il y ait un problème avec la synchronisation de l'heure et Kerberos. AD Connector envoie des demandes d'authentification Kerberos à. Active Directory Ces demandes sont urgentes et, si elles sont retardées, elles échoueront. Pour résoudre ce problème, consultez la section Recommandation - Configurer le PDC racine avec une source de temps officielle et éviter un décalage temporel généralisé dans la documentation. Microsoft Pour plus d'informations sur le service horaire et la synchronisation, voir ci-dessous :

- Comment fonctionne le Windows Time Service
- Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur
- WindowsOutils et paramètres du service de gestion du temps

Certains de mes utilisateurs ne peuvent pas s'authentifier avec mon annuaire

Vos comptes d'utilisateur doivent avoir une pré-authentification Kerberos activée. Il s'agit du paramètre par défaut pour les nouveaux comptes d'utilisateur, mais il ne doit pas être modifié. Pour plus d'informations sur ce paramètre, consultez la section Préauthentification activée Microsoft TechNet.

Problèmes de maintenance

Les problèmes de maintenance courants liés à AD Connector sont les suivants :

- Mon annuaire est bloqué à l'état « Demandé »
- La jointure de domaine fluide pour les instances Amazon EC2 a cessé de fonctionner

Mon annuaire est bloqué à l'état « Demandé »

Si vous avez un annuaire qui se trouve à l'état « Demandé » depuis plus de cinq minutes, essayez de supprimer l'annuaire et de le recréer. Si le problème persiste, contactez AWS Support.

La jointure de domaine fluide pour les instances Amazon EC2 a cessé de fonctionner

Si une liaison de domaine transparente pour les instances EC2 était en cours puis a été interrompue pendant que l'AD Connector était actif, cela peut indiquer que les informations d'identification de

votre compte de service AD Connector ont expiré. Les informations d'identification expirées peuvent empêcher AD Connector de créer des objets informatiques dans votreActive Directory.

Pour résoudre ce problème, mettez à jour le mot de passe du compte de service dans l'ordre suivant afin que les mots de passe soient identiques :

1. Mettez à jour le mot de passe du compte de service dans votreActive Directory.
2. Mettez à jour le mot de passe du compte de service dans votre AD Connector dans AWS Directory Service. Pour plus d'informations, consultez Mettre à jour les informations d'identification de votre compte de service AD Connector dans AWS Directory Service.

> **Important**
>
> La mise à jour du mot de passe uniquement dans AWS Directory Service n'entraîne pas le changement de mot de passe sur votre site existant. Il est Active Directory donc important de le faire dans l'ordre indiqué dans la procédure précédente.

Je ne parviens pas à supprimer mon AD Connector

Si votre AD Connector passe à un statut inutilisable, vous n'avez plus accès à vos contrôleurs de domaine. Nous bloquons la suppression d'un AD Connector lorsque des applications y sont encore liées, car l'une de ces applications utilise peut-être encore l'annuaire. Pour obtenir la liste des applications que vous devez désactiver afin de supprimer votre AD Connector, consultezSupprimer votre AD Connector. Si vous ne parvenez toujours pas à supprimer votre AD Connector, vous pouvez demander de l'aide via AWS Support.

Simple AD

Simple AD est un annuaire géré et autonome alimenté par un serveur compatible Active Directory avec Samba 4. Il est disponible en deux formats.

- Small : prend en charge 500 utilisateurs maximum (environ 2 000 objets parmi lesquels des utilisateurs, des groupes et des ordinateurs).
- Large : prend en charge 5 000 utilisateurs maximum (environ 20 000 objets parmi lesquels des utilisateurs, des groupes et des ordinateurs).

Simple AD fournit un sous-ensemble des fonctionnalités proposées par AWS Managed Microsoft AD, notamment la possibilité de gérer les comptes utilisateurs et les appartenances à des groupes, de créer et d'appliquer des politiques de groupe, de se connecter en toute sécurité aux instances Amazon EC2 et de fournir une authentification unique (SSO) basée sur Kerberos. Notez toutefois que Simple AD ne prend pas en charge les fonctionnalités telles que l'authentification multifactorielle (MFA), les relations de confiance avec d'autres domaines, le centre d'administration Active Directory, le support PowerShell , la corbeille Active Directory, les comptes de services gérés par des groupes et les extensions de schéma pour les applications POSIX et Microsoft.

Simple AD offre de nombreux avantages :

- Simple AD facilite la gestion des instances Amazon EC2 exécutant Linux et Windows et le déploiement d'applications Windows dans le AWS cloud.
- Un grand nombre des applications et outils utilisés aujourd'hui et qui requièrent la prise en charge de Microsoft Active Directory peuvent être utilisés avec Simple AD.
- Les comptes utilisateurs de Simple AD permettent d'accéder à AWS des applications telles qu' WorkSpacesAmazon WorkDocs ou Amazon WorkMail.
- Vous pouvez gérer les AWS ressources via un accès basé sur les rôles IAM au. AWS Management Console
- Des instantanés automatisés quotidiens permettent la point-in-time restauration.

Simple AD ne prend en charge aucun des éléments suivants :

- Amazon AppStream 2.0
- Amazon Chime

- Amazon RDS for SQL Server
- Amazon RDS for Oracle
- AWS IAM Identity Center
- Relations d'approbation avec d'autres domaines
- Centre d'administration Active Directory
- PowerShell
- Corbeille Active Directory
- Comptes de service gérés de groupe
- Extensions de schéma pour les applications POSIX et Microsoft

Poursuivez la lecture des rubriques de cette section pour savoir comment créer votre propre Simple AD.

Rubriques

Mise en route avec Simple AD

Simple AD crée un annuaire entièrement géré basé sur Samba dans le AWS cloud. Lorsque vous créez un annuaire avec Simple AD, il AWS Directory Service crée deux contrôleurs de domaine et deux serveurs DNS en votre nom. Les contrôleurs de domaine sont créés dans différents sous-réseaux d'un Amazon VPC. Cette redondance permet de garantir que votre répertoire reste accessible même en cas de panne.

Rubriques

- Qu'est-ce qui est créé avec votre Simple AD Active Directory
- Configuration du DNS pour Simple AD

Prérequis pour Simple AD

Pour créer un Simple ADActive Directory, vous avez besoin d'un Amazon VPC avec les éléments suivants :

- Le VPC doit avoir la location matérielle par défaut.
- Le VPC ne doit pas être configuré avec le ou les points de terminaison de VPC suivants :
  - Points de terminaison VPC Route53 qui incluent des remplacements conditionnels du DNS pour*.amazonaws.com qui sont résolus en adresses IP non publiques AWS
  - CloudWatch Point de terminaison d'un VPC
  - Point de terminaison d'un VPC Systems Manager
  - Point de terminaison d'un VPC du service de jetons de sécurité
- Au moins deux sous-réseaux dans deux zones de disponibilité différentes. Les sous-réseaux doivent se trouver dans la même plage de routage interdomaine sans classe (CIDR). Si vous souhaitez étendre ou redimensionner le VPC pour votre annuaire, assurez-vous de sélectionner les deux sous-réseaux de contrôleur de domaine pour la plage d'adresses CIDR de VPC étendu. Lorsque vous créez un Simple AD, vous AWS Directory Service créez deux contrôleurs de domaine et deux serveurs DNS en votre nom.
  - Pour plus d'informations sur la plage d'adresses CIDR, consultez la section Adressage IP pour vos VPC et sous-réseaux dans le guide de l'utilisateur Amazon VPC.
- Si vous avez besoin du support LDAPS avec Simple AD, nous vous recommandons de le configurer à l'aide d'un Network Load Balancer connecté au port 389. Ce modèle vous permet d'utiliser un certificat fort pour la connexion LDAPS, de simplifier l'accès à LDAPS par le biais d'une seule adresse IP NLB et de définir un basculement automatique avec NLB. Simple AD ne prend pas en charge l'utilisation de certificats auto-signés sur le port 636. Pour plus d'informations sur la configuration de LDAPS avec Simple AD, reportez-vous à la section How to Configure an LDAPS Endpoint for Simple AD (Comment configurer un point de terminaison LDAPS pour Simple AD) dans le blog sur la sécuritéAWS .
- Les types de chiffrement suivants doivent être activés dans l'annuaire :
  - RC4_HMAC_MD5
  - AES128_HMAC_SHA1

- AES256_HMAC_SHA1
- Futurs types de chiffrement

> **Note**
>
> Si vous désactivez ces types de chiffrement, cela risque d'engendrer des problèmes de communication avec les outils d'administration de serveur distant (RSAT) et de nuire à la disponibilité ou à votre annuaire.

- Pour de plus amples informations, veuillez consulter Qu'est-ce qu'Amazon VPC ? dans le Guide de l'utilisateur Amazon VPC.

AWS Directory Service utilise une structure à deux VPC. Les instances EC2 qui constituent votre répertoire s'exécutent en dehors de votre AWS compte et sont gérées par AWS. Elles ont deux cartes réseau, `ETH0` et `ETH1`. `ETH0` est la carte de gestion et existe en dehors de votre compte. `ETH1` est créé au sein de votre compte.

La plage d'adresses IP de gestion du réseau `ETH0` de votre annuaire est choisie par programmation afin de garantir qu'elle n'entre pas en conflit avec le VPC sur lequel votre annuaire est déployé. Cette plage d'adresses IP peut être comprise dans l'une des paires suivantes (car les annuaires s'exécutent dans deux sous-réseaux) :

- 10.0.1.0/24 et 10.0.2.0/24
- 169,254,0,0/16
- 192.168.1.0/24 et 192.168.2.0/24

Nous évitons les conflits en vérifiant le premier octet du CIDR `ETH1`. S'il commence par un 10, nous choisissons un VPC 192.168.0.0/16 avec des sous-réseaux 192.168.1.0/24 et 192.168.2.0/24. Si le premier octet est différent de 10, nous choisissons un VPC 10.0.0.0/16 avec des sous-réseaux 10.0.1.0/24 et 10.0.2.0/24.

L'algorithme de sélection n'inclut pas de routages dans votre VPC. Il est donc possible qu'un conflit de routage IP résulte de ce scénario.

Créez votre Simple AD Active Directory

Pour créer un nouveau Simple ADActive Directory, effectuez les étapes suivantes. Avant de commencer cette procédure, assurez-vous que vous avez terminé les prérequis identifiés dans Prérequis pour Simple AD.

Pour créer un Simple AD Active Directory

1. Dans le panneau de navigation de la console AWS Directory Service, choisissez Annuaires, puis Configurer un annuaire.
2. Sur la page Sélectionner un type d'annuaire, choisissez Simple AD, puis Suivant.
3. Sur la page Enter directory information (Saisir les détails de l'annuaire), renseignez les informations suivantes :

   Taille de l'annuaire

   Faites votre choix parmi les options de taille Petit ou Large. Pour en savoir plus sur les tailles, veuillez consulter Simple AD.

   Nom de l'organisation

   Nom d'organisation unique pour votre répertoire qui sera utilisé pour enregistrer les appareils clients.

   Ce champ n'est disponible que si vous créez votre répertoire dans le cadre du lancement WorkSpaces.

   Nom de DNS de l'annuaire

   Nom complet de l'annuaire, par exemple `corp.example.com`.

   Nom NetBIOS de l'annuaire

   Nom court de l'annuaire, par exemple `CORP`.

   Mot de passe administrateur

   Mot de passe de l'administrateur de l'annuaire. Le processus de création d'un annuaire crée un compte d'administrateur avec le nom utilisateur `Administrator` et ce mot de passe.

   Le mot de passe de l'administrateur de l'annuaire est sensible à la casse et doit comporter entre 8 et 64 caractères (inclus). Il doit également contenir au moins un caractère de trois des quatre catégories suivantes :

- Lettres minuscules (a-z)
- Lettres majuscules (A-Z)
- Chiffres (0-9)
- Caractères non alphanumériques (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirmer le mot de passe

Saisissez à nouveau le mot de passe de l'administrateur.

Description de l'annuaire

Description facultative de l'annuaire.

4. Sur la page Choose VPC and subnets (Choisir un VPC et des sous-réseaux), indiquez les informations suivantes, puis choisissez Next (Suivant).

   VPC

   VPC de l'annuaire.

   Sous-réseaux

   Choisissez les sous-réseaux pour les contrôleurs de domaine. Les deux sous-réseaux doivent être dans des zones de disponibilité différentes.

5. Sur la page Review & create (Vérifier et créer), vérifiez les informations concernant l'annuaire et effectuez les modifications nécessaires. Lorsque les informations sont correctes, choisissez Create directory (Créer l'annuaire). La création de l'annuaire prend plusieurs minutes. Une fois l'annuaire créé, le champ Statut prend la valeur Actif.

Qu'est-ce qui est créé avec votre Simple AD Active Directory

Lorsque vous créez un Active Directory avec Simple AD, il AWS Directory Service exécute les tâches suivantes en votre nom :

- Configure un annuaire basé sur Samba dans le VPC.
- Création d'un compte d'administrateur d'annuaire avec le nom d'utilisateur `Administrator` et le mot de passe spécifié. Ce compte est utilisé pour gérer votre annuaire.

> **Important**
>
> N'oubliez pas d'enregistrer ce mot de passe. AWS Directory Service ne stocke pas ce mot de passe et il ne peut pas être récupéré. Vous pouvez toutefois réinitialiser un mot de passe depuis la AWS Directory Service console ou à l'aide de l'ResetUserPasswordAPI.

- Création d'un groupe de sécurité pour les contrôleurs de l'annuaire.
- Crée un compte avec le nom `AWSAdminD-xxxxxxxx` qui dispose des privilèges d'administration de domaine. Ce compte est utilisé pour effectuer des opérations automatisées pour les opérations de maintenance des annuaires, telles que la prise de clichés d'annuaires et les transferts de rôles FSMO. AWS Directory Service Les informations d'identification pour ce compte sont stockées en toute sécurité par AWS Directory Service.
- Crée et associe automatiquement une interface réseau Elastic (ENI) à chacun de vos contrôleurs de domaine. Chacun de ces ENI est essentiel à la connectivité entre votre VPC AWS Directory Service et les contrôleurs de domaine et ne doit jamais être supprimé. Vous pouvez identifier toutes les interfaces réseau réservées à l'utilisation AWS Directory Service par la description : « interface réseau AWS créée pour le répertoire directory-id ». Pour plus d'informations, consultez Elastic Network Interfaces dans le guide de l'utilisateur Amazon EC2 pour les instances Windows. Le serveur DNS par défaut de AWS Managed Microsoft AD Active Directory est le serveur DNS VPC avec Classless Inter-Domain Routing (CIDR) +2. Pour plus d'informations, consultez le serveur Amazon DNS dans le guide de l'utilisateur Amazon VPC.

> **Note**
>
> Les contrôleurs de domaine sont déployés par défaut dans deux zones de disponibilité d'une région et connectés à votre cloud privé virtuel (VPC) Amazon. Les sauvegardes sont effectuées automatiquement une fois par jour, et les volumes Amazon Elastic Block Store (EBS) sont chiffrés pour garantir la sécurité des données au repos. Les contrôleurs de domaine qui échouent sont automatiquement remplacés dans la même zone de disponibilité à l'aide de la même adresse IP, et une reprise après sinistre complète peut être effectuée avec la dernière sauvegarde.

Configuration du DNS pour Simple AD

Simple AD transfère les demandes DNS à l'adresse IP des serveurs DNS fournis par Amazon pour votre VPC Amazon. Ces serveurs DNS résolvent les noms configurés dans vos zones hébergées privées Amazon Route 53. En pointant vos ordinateurs sur site vers votre Simple AD, vous pouvez désormais résoudre les demandes DNS dans la zone hébergée privée. Pour plus d'informations sur Route 53, veuillez consulter What is Route 53 (français non garanti).

Notez que pour activer votre Simple AD pour répondre aux requêtes DNS externes, la liste de contrôle d'accès (ACL) réseau pour le VPC contenant votre Simple AD doit être configurée pour autoriser le trafic depuis l'extérieur du VPC.

- Si vous n'utilisez pas les zones hébergées privées Route 53, vos demandes DNS seront transmises aux serveurs DNS publics.
- Si vous utilisez des serveurs DNS personnalisés situés en dehors de votre VPC et si vous souhaitez utiliser un DNS privé, vous devez procéder à une nouvelle configuration pour utiliser des serveurs DNS personnalisés sur des instances EC2 au sein de votre VPC. Pour plus d'informations, veuillez onsulter Utilisation des zones hébergées privées.
- Si vous voulez que votre Simple AD résolve les noms à l'aide des serveurs DNS au sein de votre VPC et des serveurs DNS privés en dehors de votre VPC, vous pouvez le faire à l'aide d'un jeu d'options DHCP. Pour obtenir un exemple détaillé, veuillez consulter cet article.

> **Note**
>
> Les mises à jour dynamiques DNS ne sont pas prises en charge dans les domaines Simple AD. En revanche, vous pouvez effectuer les modifications directement en connectant votre annuaire à l'aide du Gestionnaire DNS sur une instance qui est jointe à votre domaine.

Comment administrer Simple AD

Cette section répertorie toutes les procédures de fonctionnement et de maintenance d'un environnement Simple AD.

Rubriques

- Gérer des utilisateurs et des groupes dans Simple AD

- Surveillance de votre annuaire Simple AD
- Joindre une instance Amazon EC2 à votre répertoire Simple AD Active Directory
- Maintenance de votre annuaire Simple AD
- Permettre l'accès aux AWS applications et aux services
- Activation de l'accès à AWS Management Console avec les informations d'identification AD

Gérer des utilisateurs et des groupes dans Simple AD

Les utilisateurs représentent des individus ou des entités individuelles qui ont accès à votre annuaire. Les groupes sont très utiles pour octroyer ou refuser des privilèges à des groupes d'utilisateurs, plutôt que d'appliquer ces privilèges à chaque utilisateur. Si un utilisateur change d'organisation, déplacez-le dans un autre groupe. Il reçoit alors automatiquement les privilèges nécessaires pour la nouvelle organisation.

Pour créer des utilisateurs et des groupes dans un annuaire AWS Directory Service, vous devez utiliser une instance (soit sur site, soit EC2) associée à votre annuaire AWS Directory Service, et être connecté en tant qu'utilisateur disposant des privilèges requis pour créer des utilisateurs et des groupes. Vous devrez également installer les outils Active Directory sur votre instance EC2 afin de pouvoir ajouter vos utilisateurs et vos groupes avec le composant logiciel enfichable Active Directory Users and Computers. Pour plus d'informations sur la configuration d'une instance EC2 et l'installation des outils nécessaires, veuillez consulter Joindre une instance Amazon EC2 à votre répertoire Simple AD Active Directory.

> **Note**
>
> Vos comptes d'utilisateur doivent avoir une pré-authentification Kerberos activée. Il s'agit du paramètre par défaut pour les nouveaux comptes d'utilisateur, mais il ne doit pas être modifié. Pour plus d'informations sur ce paramètre, consultez la section Préauthentification sur Microsoft TechNet.

Les rubriques suivantes expliquent comment créer et gérer des utilisateurs et des groupes.

Rubriques

- Installation des outils d'administration Active Directory pour Simple AD
- Créez un utilisateur

- Suppression d'un utilisateur
- Réinitialiser un mot de passe utilisateur
- Créez un groupe
- Ajouter un utilisateur à un groupe

Installation des outils d'administration Active Directory pour Simple AD

Pour gérer votre Active Directory à partir d'une instance Amazon EC2 Windows Server, vous devez installer les outils Active Directory Domain Services et Active Directory Lightweight Directory Services sur l'instance. Utilisez la procédure suivante pour installer ces outils sur une instance Windows Server EC2.

Prérequis

Avant de commencer cette procédure, effectuez les opérations suivantes :

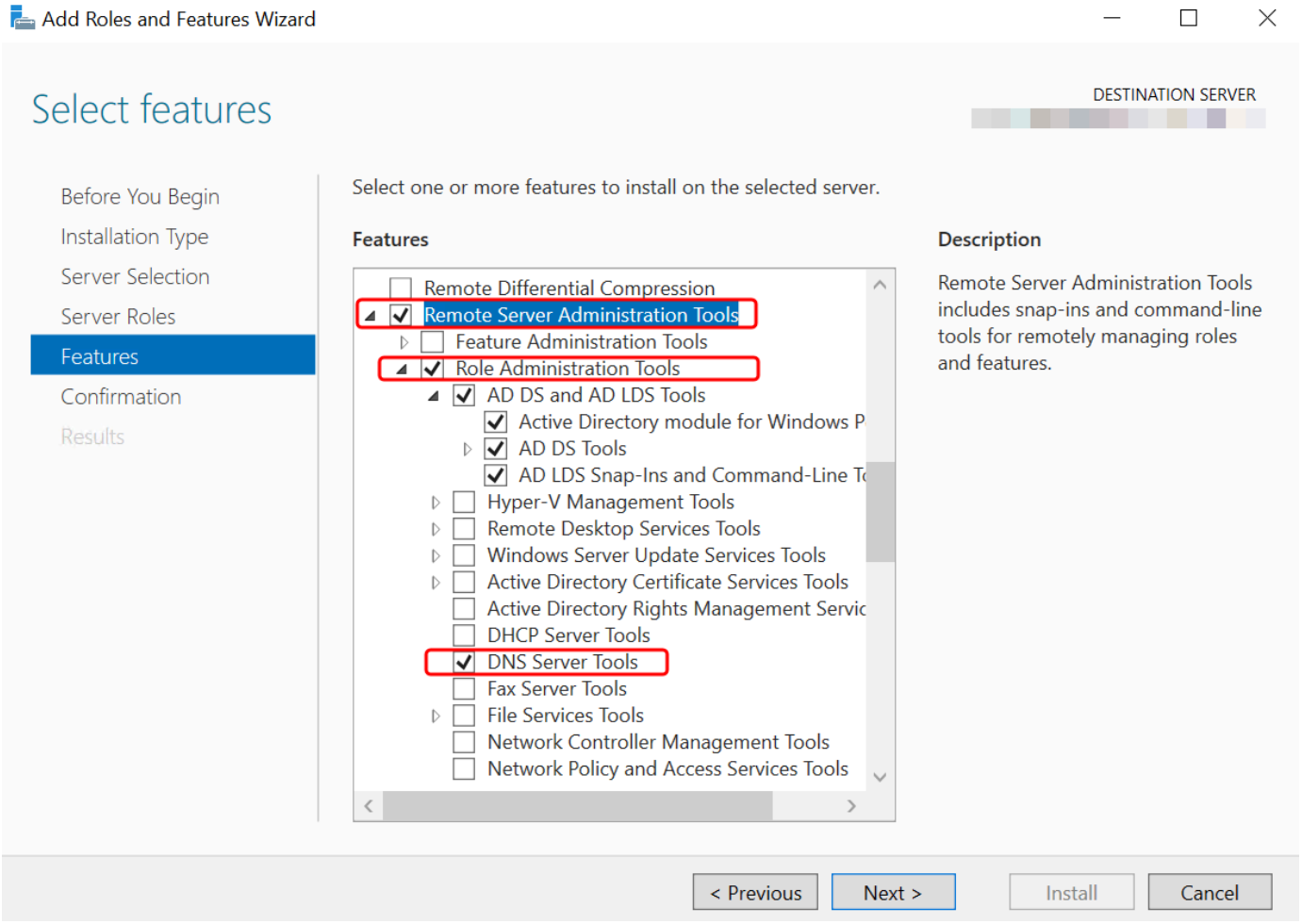
1. Créez un répertoire Active Directory Simple AD. Pour plus d'informations, consultez Créez votre Simple AD Active Directory.
2. Lancez une instance Windows Server EC2 et joignez-la à votre répertoire Simple AD Active Directory. L'instance EC2 a besoin des politiques suivantes pour créer des utilisateurs et des groupes : **`AWSSSMManagedInstanceCore`** et**`AmazonSSMDirectoryServiceAccess`**. Pour plus d'informations, consultez Joignez facilement une instance Windows Amazon EC2 à votre répertoire Simple AD Active Directory.
3. Vous aurez besoin des informations d'identification de votre administrateur de domaine Active Directory. Ces informations d'identification ont été créées lors de la création du Simple AD. Si vous avez suivi la procédure décrite dansCréez votre Simple AD Active Directory, votre nom d'utilisateur d'administrateur inclut votre nom NetBIOS,. **`corp\administrator`**

Installation des outils d'administration Active Directory sur une instance Windows Server EC2

Pour installer les outils d'administration Active Directory sur une instance Windows Server EC2

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la console Amazon EC2, choisissez Instances, sélectionnez l'instance Windows Server, puis sélectionnez Se connecter.
3. Dans la page Se connecter à l'instance, sélectionnez Client RDP.

4. Dans l'onglet Client RDP, sélectionnez Télécharger le fichier Bureau à distance, puis choisissez Obtenir le mot de passe pour récupérer votre mot de passe.
5. Dans le champ Obtenir le mot de passe Windows, sélectionnez Chargement du fichier de clé privée. Choisissez le fichier de clé privée .pem associé à l'instance Windows Server. Après avoir chargé le fichier de clé privée, sélectionnez Déchiffrer le mot de passe.
6. Dans la boîte de dialogue de sécurité Windows, copiez vos informations d'identification d'administrateur local pour que l'ordinateur Windows Server puisse se connecter. Le nom d'utilisateur peut être dans les formats suivants : ***NetBIOS-Name*****\administrator** ou***DNS-Name*****\administrator**. Par exemple, **corp\administrator** ce serait le nom d'utilisateur si vous avez suivi la procédure dansCréez votre Simple AD Active Directory.
7. Une fois connecté à l'instance Windows Server, ouvrez le Gestionnaire de serveur dans le menu Démarrer en choisissant Gestionnaire de serveur.
8. Dans le tableau de bord du Gestionnaire de serveur, choisissez Ajouter des rôles et des fonctionnalités.
9. Dans l'Assistant Ajout de rôles et de fonctionnalités, choisissez Type d'installation, sélectionnez Installation basée sur un rôle ou une fonctionnalité, puis choisissez Suivant.
10. Sous Sélection de serveur, vérifiez que le serveur local est sélectionné, puis choisissez Fonctionnalités dans le volet de navigation de gauche.
11. Dans l'arborescence Fonctionnalités, sélectionnez et ouvrez Outils d'administration de serveur distant, Outils d'administration de rôles et Outils AD DS et AD LDS. Lorsque les outils AD DS et AD LDS sont sélectionnés, le Active Directorymodule pour, les outils AD DSWindows PowerShell, les composants logiciels enfichables et les outils de ligne de commande AD LDS sont sélectionnés. Faites défiler la page vers le bas et sélectionnez Outils du serveur DNS, puis cliquez sur Suivant.



12. Passez en revue les informations, puis choisissez Installer. Lorsque l'installation des fonctionnalités est terminée, les outils Active Directory Domain Services et Active Directory Lightweight Directory Services sont disponibles sur l'écran Démarrer dans le dossier Outils d'administration.

Méthode alternative pour installer les outils d'administration Active Directory sur une instance Windows Server EC2

- Voici une autre méthode pour installer les outils d'administration Active Directory :
  - Vous pouvez éventuellement choisir d'installer les outils d'administration Active Directory à l'aide deWindows PowerShell. Par exemple, vous pouvez installer les outils d'administration à distance Active Directory à partir d'une PowerShell invite en utilisant`Install-WindowsFeature RSAT-ADDS`. Pour plus d'informations, consultez Install- WindowsFeature sur le site Web de Microsoft.

Créez un utilisateur

Utilisez la procédure suivante pour créer un utilisateur avec une instance EC2 qui est jointe à votre annuaire Simple AD. Avant de créer des utilisateurs, vous devez suivre les procédures décrites dans la section Installation des outils d'administration Active Directory.

> **Note**
>
> Lors de l'utilisation de Simple AD, si vous créez un compte d'utilisateur sur une instance Linux avec l'option « Force user to change password at first login », cet utilisateur ne pourra pas modifier initialement son mot de passe à l'aide de la commande kpasswd. Pour modifier le mot de passe la première fois, un administrateur de domaine doit mettre à jour le mot de passe utilisateur à l'aide des outils de gestion Active Directory.

Vous pouvez utiliser l'une des méthodes suivantes pour créer un utilisateur :

- Active DirectoryOutils d'administration
- Windows PowerShell

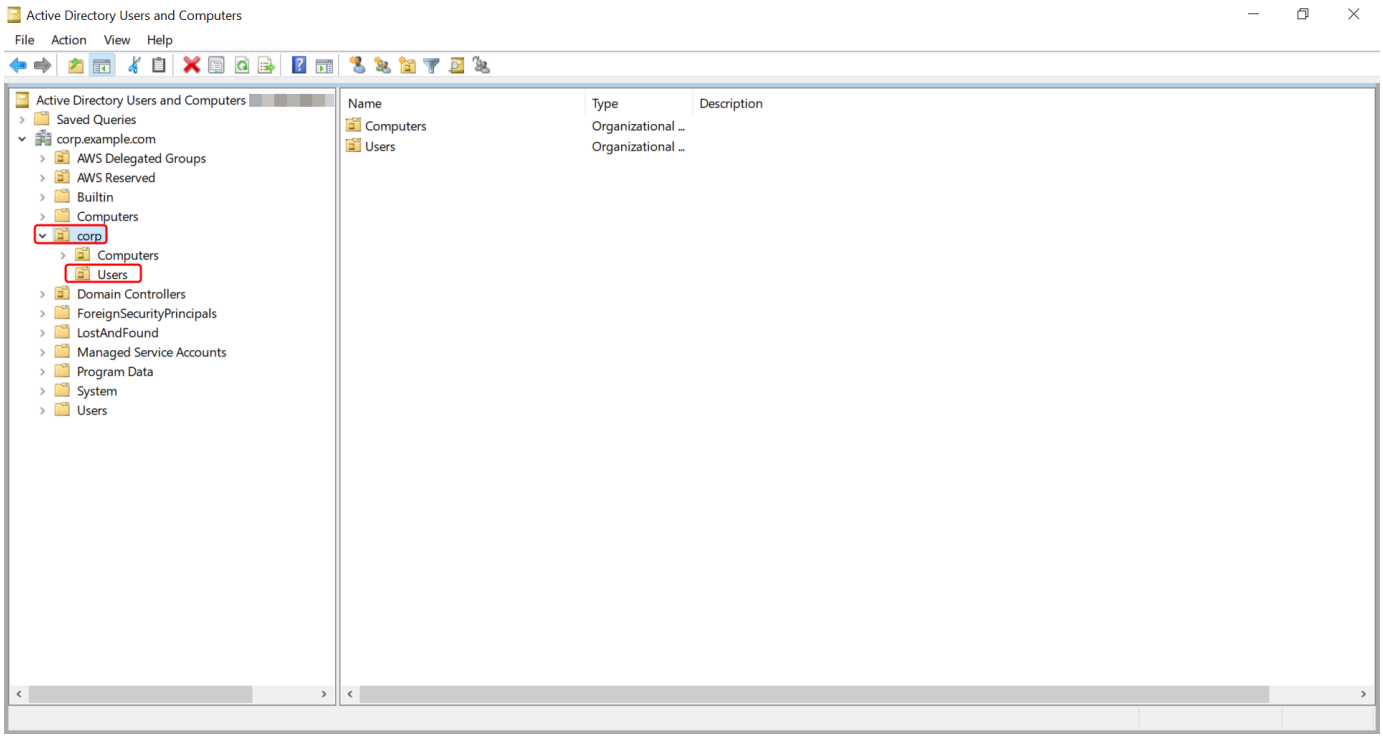
Création d'un utilisateur à l'aide des outils d'Active Directoryadministration

1. Connectez-vous à l'instance où les outils d'administration Active Directory ont été installés.
2. Ouvrez l'outil Utilisateurs et ordinateurs Active Directory dans le menu Démarrer de Windows. Un raccourci vers cet outil se trouve dans le dossier Outils d'administration de Windows.

   > **Tip**
   >
   > Vous pouvez exécuter ce qui suit à partir d'une invite de commande sur l'instance pour ouvrir directement la boîte à outils Utilisateurs et ordinateurs Active Directory.
   >
   > ```
   > %SystemRoot%\system32\dsa.msc
   > ```

3. Dans l'arborescence du répertoire, sélectionnez une unité d'organisation sous le nom NetBIOS de votre répertoire ou dans laquelle vous souhaitez enregistrer votre utilisateur (par exemple,**`corp\Users`**). Pour plus d'informations sur la structure de l'UO utilisée par les

annuaires dans AWS, consultezQu'est-ce qui est créé avec votre annuaire Microsoft AD Active Directory AWS géré.



4. Dans le menu Action, choisissez Nouveau, puis sélectionnez Utilisateur pour ouvrir l'assistant de création d'utilisateurs.
5. Sur la première page de l'assistant, entrez les valeurs des champs suivants, puis sélectionnez Suivant.
   - Prénom
   - Nom
   - Nom de connexion de l'utilisateur
6. Sur la deuxième page de l'assistant, entrez un mot de passe temporaire dans Mot de passe et Confirmer le mot de passe. Assurez-vous que l'utilisateur doit modifier le mot de passe lors de sa prochaine connexion. Aucune autre option ne doit être sélectionnée. Choisissez Suivant.
7. Sur la troisième page de l'assistant Nouvel utilisateur, vérifiez que les informations du nouvel utilisateur sont correctes, puis choisissez Terminer. Le nouvel utilisateur s'affiche dans le dossier Utilisateurs.

Créez un utilisateur dans Windows PowerShell

1. Connectez-vous à l'instance jointe à votre Active Directory domaine en tant qu'Active Directoryadministrateur.
2. Ouvrir Windows PowerShell.
3. Tapez la commande suivante en remplaçant le nom **`jane.doe`** d'utilisateur par le nom d'utilisateur de l'utilisateur que vous souhaitez créer. Vous serez invité Windows PowerShell à fournir un mot de passe pour le nouvel utilisateur. Pour plus d'informations sur les exigences relatives à la complexité des mots de Active Directory passe, consultez Microsoftla documentation. Pour plus d'informations sur la commande New-ADUser, consultez Microsoft la documentation.

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -AsSecureString
 'Password')
```

Suppression d'un utilisateur

Utilisez la procédure suivante pour supprimer un utilisateur avec une instance Windows EC2 jointe à votre annuaire Simple AD.

Vous pouvez utiliser l'une des méthodes suivantes pour supprimer un utilisateur :

- Active DirectoryOutils d'administration
- Windows PowerShell

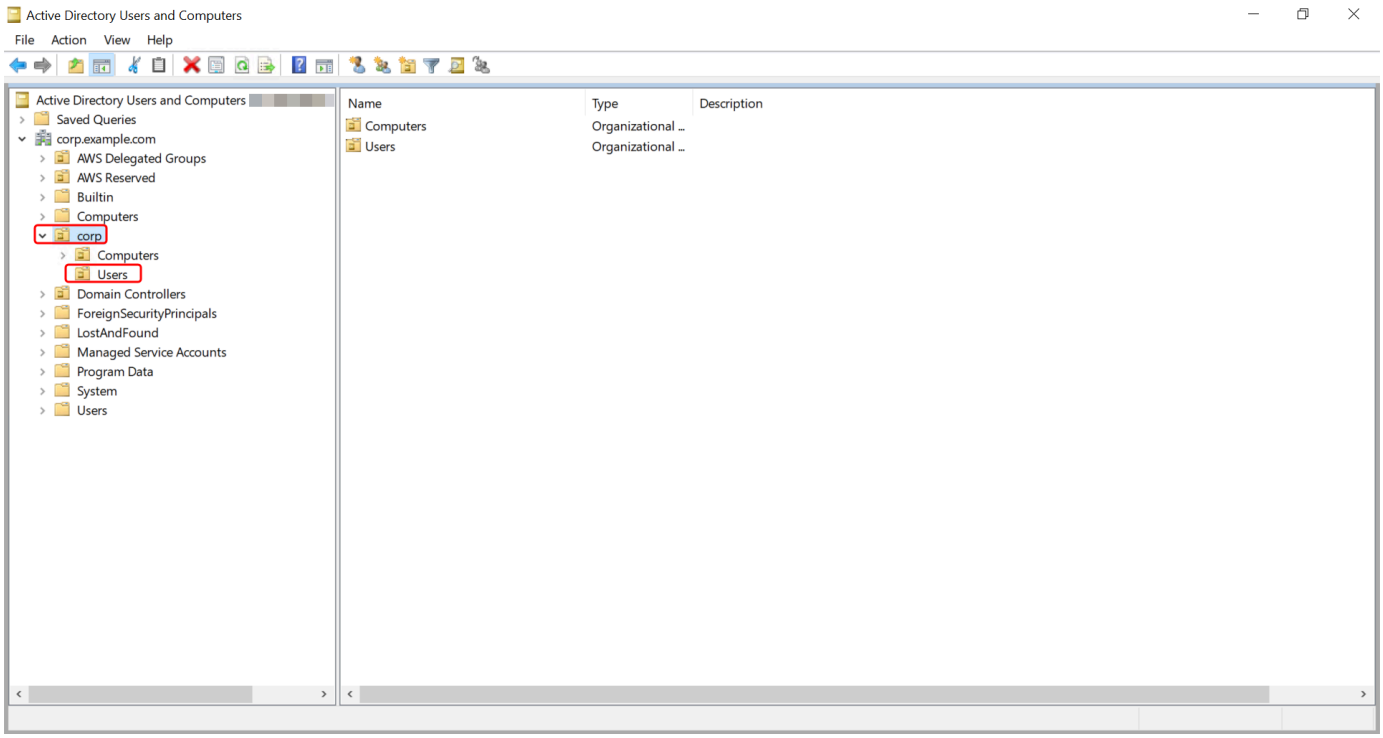
Supprimer un utilisateur à l'aide des outils d'Active Directoryadministration

1. Connectez-vous à l'instance où les outils d'administration Active Directory ont été installés.
2. Ouvrez l'outil Utilisateurs et ordinateurs Active Directory dans le menu Démarrer de Windows. Un raccourci vers cet outil se trouve dans le dossier Outils d'administration de Windows.

> **Tip**
>
> Vous pouvez exécuter ce qui suit à partir d'une invite de commande sur l'instance pour ouvrir directement la boîte à outils Utilisateurs et ordinateurs Active Directory.

```
%SystemRoot%\system32\dsa.msc
```

3. Dans l'arborescence du répertoire, sélectionnez l'unité d'organisation contenant l'utilisateur que vous souhaitez supprimer (par exemple,**`corp\Users`**).



4. Sélectionnez l'utilisateur que vous souhaitez supprimer. Dans le menu Action, sélectionnez Supprimer.
5. Une boîte de dialogue vous demande de confirmer que vous souhaitez supprimer l'utilisateur. Choisissez Oui pour supprimer l'utilisateur. Cette action supprime définitivement l'utilisateur sélectionné.

Supprimer un utilisateur dans Windows PowerShell

1. Connectez-vous à l'instance jointe à votre Active Directory domaine en tant qu'Active Directoryadministrateur.
2. Ouvrir Windows PowerShell.
3. Tapez la commande suivante en remplaçant le nom **`jane.doe`** d'utilisateur par le nom d'utilisateur de l'utilisateur que vous souhaitez supprimer. Pour plus d'informations sur la commande Remove-ADUser, consultez la documentation. Microsoft

```
Remove-ADUser -Identity "jane.doe"
```

Réinitialiser un mot de passe utilisateur

Les utilisateurs doivent respecter les politiques relatives aux mots de passe définies dans leActive Directory. Parfois, cela peut prendre le dessus sur les utilisateurs, y compris l'Active Directoryadministrateur, et ils oublient leur mot de passe. Dans ce cas, vous pouvez rapidement réinitialiser le mot de passe de l'utilisateur en indiquant AWS Directory Service s'il réside dans Simple AD.

Vous devez être connecté en tant qu'utilisateur avec les autorisations nécessaires pour réinitialiser les mots de passe. Pour plus d'informations sur les autorisations, consultez Vue d'ensemble de la gestion des autorisations d'accès à vos AWS Directory Service ressources.

Vous pouvez réinitialiser le mot de passe de n'importe quel utilisateur, à l'Active Directoryexception des exceptions suivantes :

- Vous pouvez réinitialiser le mot de passe de n'importe quel utilisateur de l'unité organisationnelle (UO) en fonction du nom NetBIOS que vous avez utilisé lors de la création de votre. Active Directory Par exemple, si vous avez suivi la procédure décrite dansCréez votre Simple AD Active Directory, votre nom NetBIOS serait CORP et les mots de passe des utilisateurs que vous pourriez réinitialiser seraient membres de Corp/Users OU.
- Vous ne pouvez pas réinitialiser le mot de passe d'un utilisateur en dehors de l'unité d'organisation en fonction du nom NetBIOS que vous avez utilisé lors de la création de votre. Active Directory Pour plus d'informations sur la structure de l'UO de Simple AD, consultezQu'est-ce qui est créé avec votre Simple AD Active Directory.
- Vous ne pouvez pas réinitialiser le mot de passe d'un utilisateur membre de deux domaines. Vous ne pouvez pas non plus réinitialiser le mot de passe d'un utilisateur membre du groupe Administrateurs du domaine ou du groupe Administrateurs d'entreprise, à l'exception de l'utilisateur administrateur.

Vous pouvez utiliser l'une des méthodes suivantes pour réinitialiser le mot de passe d'un utilisateur :

- AWS Management Console
- AWS CLI
- Windows PowerShell

Réinitialisez un mot de passe utilisateur dans AWS Management Console

1. Dans le volet de navigation de la AWS Directory Service console Active Directory, sous, choisissez Répertoires, puis sélectionnez le répertoire Active Directory dans lequel vous souhaitez réinitialiser un mot de passe utilisateur.
2. Sur la page des détails de l'annuaire, choisissez Actions, puis Réinitialiser le mot de passe utilisateur.
3. Dans la boîte de dialogue Réinitialiser le mot de passe utilisateur, dans Nom d'utilisateur, tapez le nom d'utilisateur de l'utilisateur dont le mot de passe doit être modifié.
4. Entrez un mot de passe dans Nouveau mot de passe et Confirmer le mot de passe, puis choisissez Réinitialiser le mot de passe.

Réinitialiser un mot de passe utilisateur dans AWS CLI

1. Pour installer le AWS CLI, voir Installer ou mettre à jour la dernière version du AWS CLI.
2. Ouvrez le AWS CLI.
3. Tapez la commande suivante et remplacez l'ID de répertoire, le nom d'utilisateur **`jane.doe`** et le mot de passe **`P@ssw0rd`** par votre ID de Active Directory répertoire et les informations d'identification souhaitées. Consultez reset-user-passwordle manuel de référence des AWS CLI commandes pour plus d'informations.

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-
password "P@ssw0rd"
```

Réinitialiser un mot de passe utilisateur dans Windows PowerShell

1. Connectez-vous à l'instance jointe à votre Active Directory domaine en tant qu'Active Directoryadministrateur.
2. Ouvrir Windows PowerShell.
3. Tapez la commande suivante en remplaçant le nom d'utilisateur**`jane.doe`**, l'ID de répertoire et le mot de passe **`P@ssw0rd`** par votre ID de Active Directory répertoire et les informations d'identification souhaitées. Consultez l'UserPassword applet de commande Reset-DS pour plus d'informations.

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword
 "P@ssw0rd"
```

Créez un groupe

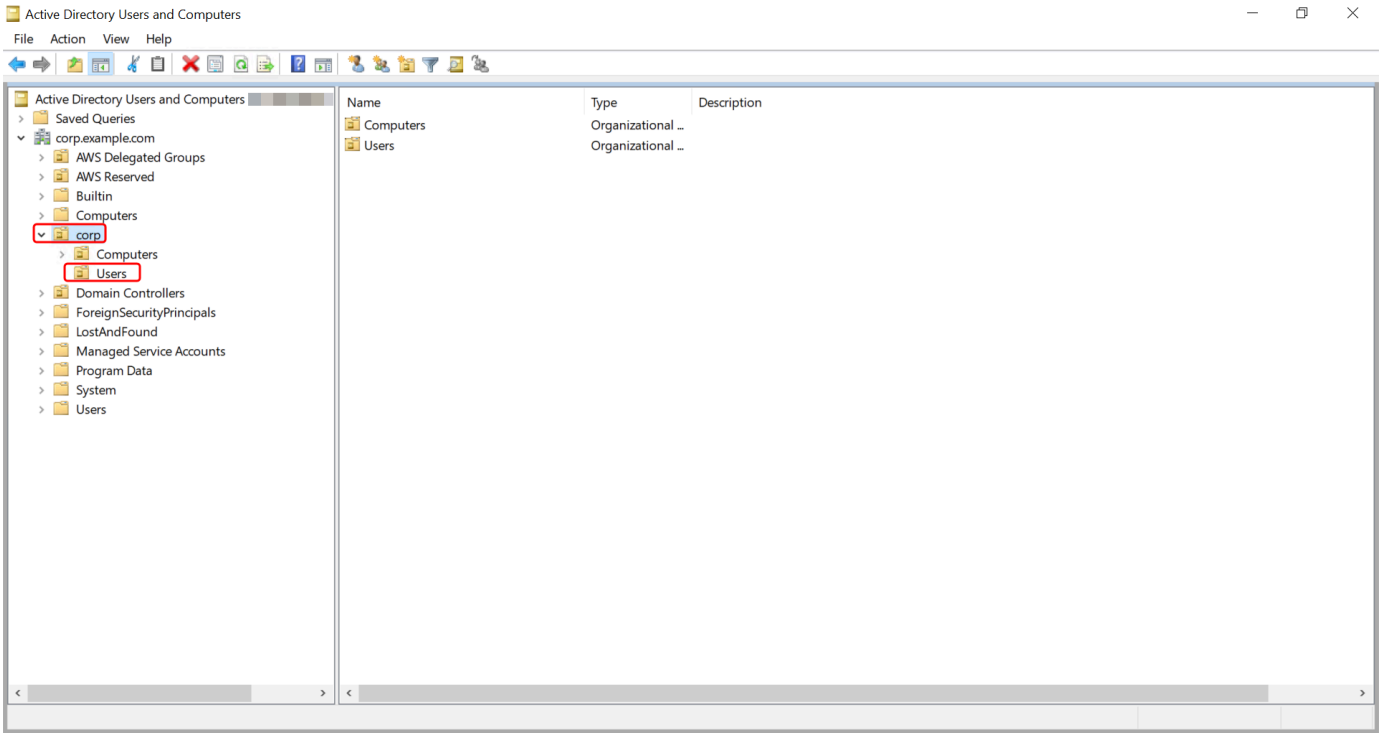
Utilisez la procédure suivante pour créer un groupe de sécurité avec une instance EC2 qui est jointe à votre annuaire . Avant de créer des groupes de sécurité, vous devez suivre les procédures décrites dans la section Installation des outils d'administration Active Directory.

Pour créer un groupe

1. Connectez-vous à l'instance où les outils d'administration Active Directory ont été installés.
2. Ouvrez l'outil Utilisateurs et ordinateurs Active Directory. Il existe un raccourci vers cet outil dans le dossier Outils d'administration.

   > **Tip**
   >
   > Vous pouvez exécuter ce qui suit à partir d'une invite de commande sur l'instance pour ouvrir directement la boîte à outils Utilisateurs et ordinateurs Active Directory.
   >
   > ```
   > %SystemRoot%\system32\dsa.msc
   > ```

3. Dans l'arborescence du répertoire, sélectionnez une unité d'organisation sous l'unité d'organisation du nom NetBIOS de votre annuaire dans laquelle vous souhaitez stocker votre groupe (par exemple, Corp\Users). Pour plus d'informations sur la structure de l'UO utilisée par les annuaires dans AWS, veuillez consulter Qu'est-ce qui est créé avec votre annuaire Microsoft AD Active Directory AWS géré.



4. Dans le menu Action, cliquez sur Nouveau, puis sur Groupe pour ouvrir l'assistant de création de nouveaux groupes.
5. Tapez le nom du groupe dans Nom du groupe, sélectionnez une étendue de groupe qui répond à vos besoins, puis sélectionnez Sécurité pour le type de groupe. Pour plus d'informations sur l'étendue des groupes Active Directory et les groupes de sécurité, veuillez consulter la section Groupes de sécurité Active Directory dans la documentation de Microsoft Windows Server.
6. Cliquez sur OK. Le nouveau groupe de sécurité apparaîtra dans le dossier Utilisateurs.

Ajouter un utilisateur à un groupe

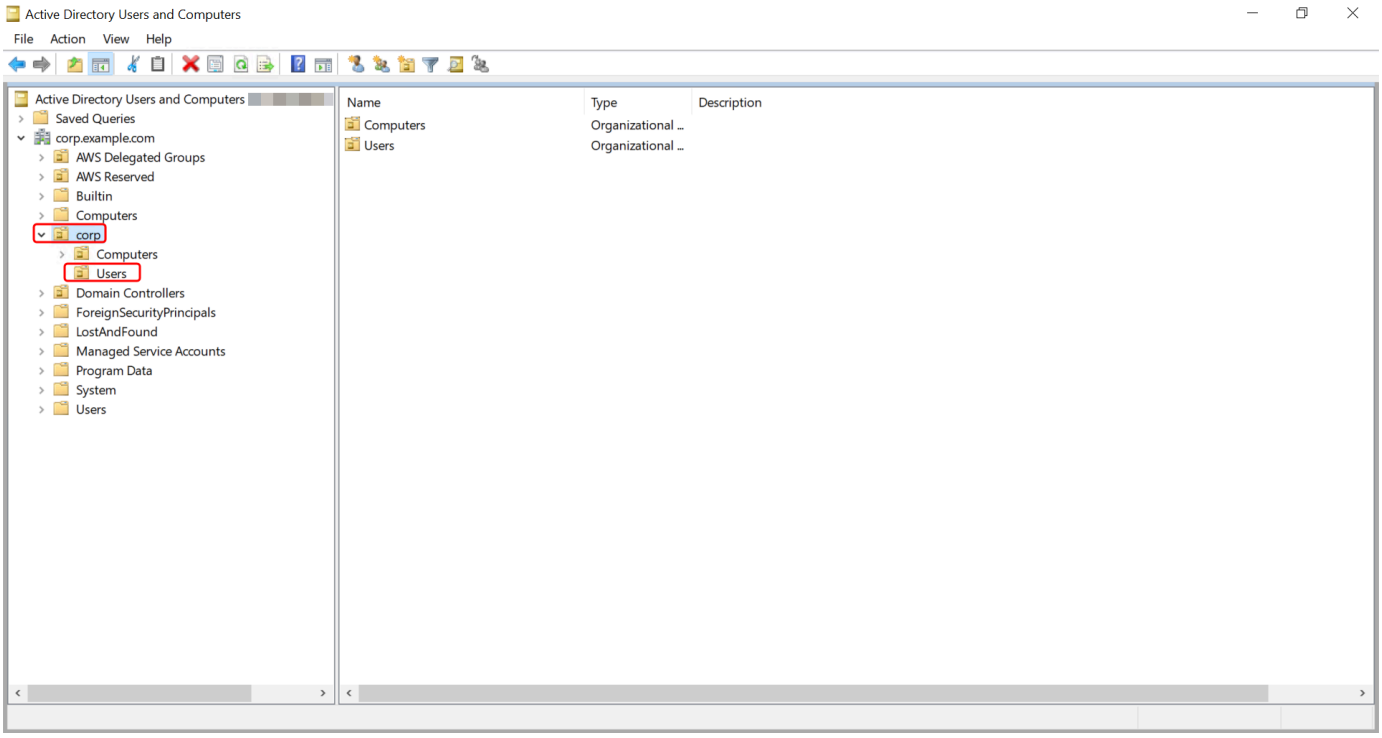
Utilisez la procédure suivante pour ajouter un utilisateur à un groupe de sécurité avec une instance EC2 qui est jointe à votre annuaire Simple AD.

Pour ajouter un utilisateur à un groupe

1. Connectez-vous à l'instance où les outils d'administration Active Directory ont été installés.
2. Ouvrez l'outil Utilisateurs et ordinateurs Active Directory. Il existe un raccourci vers cet outil dans le dossier Outils d'administration.

> **Tip**
>
> Vous pouvez exécuter ce qui suit à partir d'une invite de commande sur l'instance pour ouvrir directement la boîte à outils Utilisateurs et ordinateurs Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Dans l'arborescence de l'annuaire, sélectionnez l'unité d'organisation sous l'unité d'organisation du nom NetBIOS de votre annuaire dans laquelle vous avez enregistré votre groupe, puis sélectionnez le groupe auquel vous souhaitez ajouter un utilisateur en tant que membre.



4. Dans le menu Action, cliquez sur Propriétés pour ouvrir la boîte de dialogue des propriétés du groupe.
5. Sélectionnez l'onglet Membres, puis cliquez sur Ajouter.
6. Pour Entrez les noms des objets à sélectionner, tapez le nom d'utilisateur que vous souhaitez ajouter et cliquez sur OK. Le nom sera affiché dans la liste Membres. Cliquez à nouveau sur OK pour mettre à jour les membres du groupe.
7. Vérifiez que l'utilisateur est désormais membre du groupe en le sélectionnant dans le dossier Utilisateurs et en cliquant sur Propriétés dans le menu Action pour ouvrir la boîte de dialogue des

propriétés. Sélectionnez l'onglet Membre de. Le nom du groupe doit apparaître dans la liste des groupes auxquels appartient l'utilisateur.

Surveillance de votre annuaire Simple AD

Vous pouvez surveiller votre annuaire Simple AD en procédant comme suit :

Rubriques

- Comprendre le statut de votre annuaire
- Configurer les notifications d'état de l'annuaire avec Amazon SNS

Comprendre le statut de votre annuaire

Voici les différents statuts possibles pour un annuaire.

Actif

L'annuaire fonctionne normalement. Aucun problème n'a été détecté par AWS Directory Service pour votre annuaire.

Création

L'annuaire est en cours de création. La création de l'annuaire prend généralement entre 20 et 45 minutes, mais peut varier selon la charge du système.

Supprimé

L'annuaire a été supprimé. Toutes les ressources de l'annuaire ont été libérées. Une fois qu'un annuaire se trouve dans cet état, il ne peut pas être récupéré.

Suppression en cours

L'annuaire est en cours de suppression. L'annuaire restera dans cet état jusqu'à ce qu'il soit totalement supprimé. Une fois qu'un annuaire se trouve dans cet état, l'opération de suppression ne peut pas être annulée, et l'annuaire ne peut pas être récupéré.

Échec

L'annuaire n'a pas pu être créé. Veuillez supprimer cet annuaire. Si le problème persiste, veuillez contacter le centre AWS Support.

Dégradé

L'annuaire est en cours d'exécution dans un état dégradé. Un ou plusieurs problèmes ont été détectés. Il se peut que toutes les opérations liées à l'annuaire ne puissent pas être totalement opérationnelles. Il existe de nombreuses raisons pouvant expliquer que l'annuaire se trouve dans cet état. Parmi ces raisons, citons une opération de maintenance d'exploitation normale comme une application de correctif ou une rotation d'instance EC2, la création temporaire d'un point chaud par une application sur l'un de vos contrôleurs de domaine ou des modifications que vous avez apportées à votre réseau et qui ont interrompu les communications de l'annuaire. Pour plus d'informations, veuillez consulter Résolution des problèmes liés AWS à Managed Microsoft AD, Résolution des problèmes liés à AD Connector, Résolution des problèmes de Simple AD. Pour les problèmes normaux liés à la maintenance, AWS les problèmes sont résolus dans les 40 minutes. Si, après avoir consulté la rubrique de dépannage, votre annuaire reste à l'état Dégradé pendant plus de 40 minutes, nous vous recommandons de contacter le centre AWS Support.

> **Important**
>
> Ne restaurez pas un instantané lorsqu'un annuaire est dans un état dégradé. Il est rare qu'une restauration d'instantané soit nécessaire pour résoudre les problèmes d'état dégradé. Pour plus d'informations, consultez Création d'un instantané ou d'une restauration de votre annuaire.

Inopérable

L'annuaire n'est pas fonctionnel. Tous les points de terminaison de l'annuaire ont signalé des problèmes.

Demandé

La demande de création de votre annuaire est actuellement en attente.

RestoreFailed

Échec de la restauration de l'annuaire à partir d'un instantané. Renouvelez l'opération de restauration. Si le problème persiste, utilisez un autre instantané ou contactez le centre AWS Support.

Restauration en cours

L'annuaire est en cours de restauration à partir d'un instantané automatique ou manuel. La restauration à partir d'un instantané prend généralement plusieurs minutes, selon la taille des données de l'annuaire dans l'instantané.

Pour plus d'informations, voir Motifs de statut d'annuaire Simple AD.

Configurer les notifications d'état de l'annuaire avec Amazon SNS

Avec Amazon Simple Notification Service (Amazon SNS), vous pouvez recevoir des e-mails ou des messages texte (SMS) lorsque le statut de votre annuaire change. Vous êtes averti lorsque votre annuaire passe du statut Active (Actif) au statut Impaired (Défaillant) ou Inoperable (Inutilisable). Vous recevez également une notification lorsque l'annuaire renvoie un statut Active (Actif).

Comment ça marche

Amazon SNS utilise des « rubriques » pour collecter et diffuser des messages. Chaque rubrique compte un ou plusieurs abonnés qui reçoivent les messages qui ont été publiés dans cette rubrique. En suivant les étapes ci-dessous, vous pouvez ajouter un article AWS Directory Service en tant qu'éditeur à une rubrique Amazon SNS. Lorsqu'il AWS Directory Service détecte un changement dans le statut de votre annuaire, il publie un message sur ce sujet, qui est ensuite envoyé aux abonnés du sujet.

Vous pouvez associer plusieurs annuaires en tant que diffuseurs de publication à une même rubrique. Vous pouvez également ajouter des messages de statut de l'annuaire aux rubriques que vous avez créées précédemment dans Amazon SNS. Vous avez un contrôle détaillé sur les personnes autorisées à publier et à s'abonner à une rubrique. Pour obtenir des informations détaillées sur Amazon SNS, veuillez consulter Qu'est-ce qu'Amazon SNS ?

Pour activer la messagerie SNS pour votre annuaire

1. Connectez-vous à la AWS Directory Service console AWS Management Console et ouvrez-la.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sélectionnez l'onglet Maintenance.
4. Dans la section Surveillance de l'annuaire, choisissez Actions, puis sélectionnez Créer une notification.
5. Sur la page Créer une notification, sélectionnez Choisir un type de notification, puis choisissez Créer une notification. Si vous avez déjà une rubrique SNS existante, vous pouvez également

choisir Associer une rubrique SNS existante pour envoyer des messages de statut de cet annuaire à cette rubrique.

> **Note**
>
> Si vous choisissez Créer une nouvelle notification, mais que vous utilisez le même nom de rubrique pour une rubrique SNS qui existe déjà, Amazon SNS ne crée pas de rubrique, mais ajoute simplement les nouvelles informations d'abonnement à la rubrique existante.
> Si vous choisissez Associer une rubrique SNS existante, vous ne pourrez choisir qu'une rubrique SNS située dans la même région que l'annuaire.

6. Choisissez le type de destinataire et saisissez les coordonnées du destinataire. Si vous saisissez un numéro de téléphone pour les SMS, utilisez uniquement des chiffres. N'incluez pas de tirets, d'espaces, ni de parenthèses.
7. (Facultatif) Donnez un nom à votre rubrique et un nom d'affichage SNS. Le nom d'affichage est un nom court de 10 caractères maximum inclus dans tous les messages SMS de cette rubrique. Lorsque vous utilisez l'option SMS, le nom d'affichage est obligatoire.

> **Note**
>
> Si vous êtes connecté à l'aide d'un utilisateur ou d'un rôle IAM doté uniquement de la politique DirectoryServiceFullAccessgérée, le nom de votre rubrique doit commencer par « DirectoryMonitoring ». Si vous souhaitez personnaliser davantage le nom de votre rubrique, vous aurez besoin de privilèges supplémentaires pour SNS.

8. Sélectionnez Create (Créer).

Si vous souhaitez désigner des abonnés SNS supplémentaires, tels qu'une adresse e-mail supplémentaire, des files d'attente Amazon SQS AWS Lambdaou, vous pouvez le faire depuis la console Amazon SNS.

Pour supprimer les messages de statut de l'annuaire d'une rubrique

1. Connectez-vous à la AWS Directory Service console AWS Management Console et ouvrez-la.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sélectionnez l'onglet Maintenance.

4. Dans la section Surveillance de l'annuaire, sélectionnez le nom d'une rubrique SNS dans la liste, choisissez Actions, puis sélectionnez Supprimer.
5. Sélectionnez Remove (Supprimer).

Cela supprime votre annuaire en tant que diffuseur de publication pour la rubrique SNS sélectionnée. Si vous souhaitez supprimer le sujet dans son intégralité, vous pouvez le faire depuis la console Amazon SNS.

> **Note**
>
> Avant de supprimer une rubrique Amazon SNS à l'aide de la console SNS, vous devez vous assurer qu'aucun annuaire n'envoie de messages de statut à cette rubrique.
> Si vous supprimez une rubrique Amazon SNS à l'aide de la console SNS, cette modification ne sera pas immédiatement reflétée dans la console Directory Services. Vous ne serez averti que la prochaine fois qu'un annuaire publiera une notification concernant la rubrique supprimée, auquel cas vous verrez un statut mis à jour dans l'onglet Surveillance de l'annuaire indiquant que la rubrique est introuvable.
> Par conséquent, pour éviter de manquer des messages importants sur le statut du répertoire, avant de supprimer toute rubrique recevant des messages AWS Directory Service, associez votre annuaire à une autre rubrique Amazon SNS.

Joindre une instance Amazon EC2 à votre répertoire Simple AD Active Directory

Vous pouvez facilement joindre une instance Amazon EC2 à votre Active Directory domaine lorsque l'instance est lancée. Pour plus d'informations, consultez Associez facilement une instance Windows Amazon EC2 à votre compte AWS Microsoft AD géré Active Directory. Vous pouvez également lancer une instance EC2 et la joindre à un Active Directory domaine directement depuis la AWS Directory Service console avec AWS Systems Manager Automation.

Si vous devez joindre manuellement une instance EC2 à votre Active Directory domaine, vous devez lancer l'instance dans la région et le groupe de sécurité ou le sous-réseau appropriés, puis joindre l'instance au domaine.

Pour pouvoir vous connecter à distance à ces instances, vous devez disposer d'une connectivité IP aux instances depuis le réseau à partir duquel vous vous connectez. Dans la plupart des cas, cela

nécessite qu'une passerelle Internet soit attachée à votre VPC et que l'instance possède une adresse IP publique.

Rubriques

- Joignez facilement une instance Windows Amazon EC2 à votre répertoire Simple AD Active Directory
- Joindre manuellement une instance Windows Amazon EC2 à votre répertoire Simple AD Active Directory
- Joignez facilement une instance Linux Amazon EC2 à votre répertoire Simple AD Active Directory
- Joindre manuellement une instance Linux Amazon EC2 à votre répertoire Simple AD Active Directory
- Délégation des privilèges de jonction d'annuaire pour Simple AD
- Créer un jeu d'options DHCP

Joignez facilement une instance Windows Amazon EC2 à votre répertoire Simple AD Active Directory

Cette procédure permet de joindre facilement une instance Windows Amazon EC2 à votre répertoire Simple AD Active Directory.

Pour rejoindre facilement une instance Windows EC2

1. Connectez-vous à la console Amazon EC2 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation, choisissez le même répertoire Région AWS que le répertoire existant.
3. Sur le EC2 Dashboard (tableau de bord EC2), dans la section Launch instance (Lancer une instance), choisissez Launch instance (Lancer une instance).
4. Sur la page Launch an instance (Lancer une instance), dans la section Name and Tags (Nom et balises), saisissez le nom que vous souhaitez utiliser pour votre instance Windows EC2.
5. (Facultatif) Sélectionnez Add additional tags (Ajouter des balises supplémentaires) pour ajouter une ou plusieurs paires clé-valeur d'identification afin d'organiser, de suivre ou de contrôler l'accès pour cette instance EC2.
6. Dans la section Application and OS Image (Amazon Machine Image) [Image de l'application et du système d'exploitation (Amazon Machine Image)], sélectionnez Windows dans le volet Quick

Start (Démarrage rapide). Vous pouvez modifier Windows Amazon Machine Image (AMI) dans la liste déroulante Amazon Machine Image (AMI).

7. Dans la section Type d'instance, choisissez le type d'instance que vous souhaitez utiliser dans la liste déroulante Type d'instance.
8. Dans la section Paire de clés (connexion), vous pouvez choisir de créer une nouvelle paire de clés ou choisir une paire de clés existante.

   a. Pour créer une nouvelle paire de clés, choisissez Créer une paire de clés.

   b. Entrez le nom de la paire de clés et sélectionnez une option pour le type de paire de clés et le format de fichier de clé privée.

   c. 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.

   d. Choisissez Créer une paire de clés.

   e. Le fichier de clé privée est automatiquement téléchargé dans votre navigateur. Enregistrez le fichier de clé privée en lieu sûr.

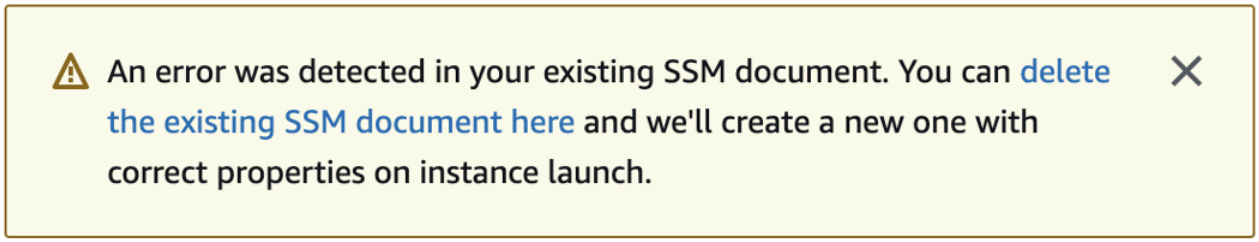
   > **Important**
   >
   > C'est votre seule occasion d'enregistrer le fichier de clé privée.

9. Sur la page Lancer une instance, dans la section Paramètres réseau, choisissez Modifier. Choisissez le VPC dans lequel votre répertoire a été créé dans la liste déroulante VPC obligatoire.
10. Choisissez l'un des sous-réseaux publics de votre VPC dans la liste déroulante Sous-réseau. Tout le trafic externe du sous-réseau que vous choisissez doit être acheminé vers une passerelle Internet. Sinon, vous ne pourrez pas vous connecter à l'instance à distance.

    Pour obtenir plus d'informations sur la manière de se connecter à une passerelle Internet, veuillez consulter la section Connect to the internet using an internet gateway (français non garanti) dans le Guide de l'utilisateur Amazon VPC.
11. Sous Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique), choisissez Enable (Activer).

Pour plus d'informations sur les adresses IP publiques et privées, veuillez consulter la section Amazon EC2 instance IP addressing (français non garanti) dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.

12. Pour les paramètres Firewall (security groups) [Pare-feu (groupes de sécurité)], vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
13. Pour les paramètres Configure storage (Configurer le stockage), vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
14. Choisissez la section Advanced details (Détails avancés), puis sélectionnez votre domaine dans la liste déroulante Domain join directory (Annuaire de jonction de domaines).

> **Note**
>
> Après avoir choisi le répertoire de jointure du domaine, vous pouvez voir :
>
> 
>
>
> Cette erreur se produit si l'assistant de lancement EC2 identifie un document SSM existant présentant des propriétés inattendues. Vous pouvez effectuer l'une des actions suivantes :
>
> - Si vous avez déjà modifié le document SSM et que les propriétés sont attendues, choisissez Fermer et lancez l'instance EC2 sans aucune modification.
> - Cliquez sur le lien Supprimer le document SSM existant ici pour supprimer le document SSM. Cela permettra de créer un document SSM avec les propriétés correctes. Le document SSM sera automatiquement créé lorsque vous lancerez l'instance EC2.

15. Pour l'IAM instance profile (profil d'instance IAM), vous pouvez sélectionner un profil d'instance IAM existant ou en créer un nouveau. Sélectionnez un profil d'instance IAM DirectoryServiceAccess auquel sont associées les politiques AWS gérées AmazonSSM ManagedInstanceCore et AmazonSSM dans la liste déroulante des profils d'instance IAM. Pour en créer un nouveau, choisissez Créer un nouveau lien de profil IAM, puis procédez comme suit :

1. Sélectionnez Créer un rôle.
2. Sous Select trusted entity (Sélectionner une entité approuvée), choisissez service AWS .
3. Sous Use case (Cas d'utilisation), choisissez EC2.
4. Sous Ajouter des autorisations, dans la liste des politiques, sélectionnez les politiques AmazonSSM ManagedInstanceCore et DirectoryServiceAccessAmazonSSM. Pour filtrer la liste, tapez **`SSM`** dans la zone de recherche. Choisissez Suivant.

   > **Note**
   >
   > AmazonSSM DirectoryServiceAccess fournit les autorisations nécessaires pour joindre des instances à une instance Active Directory gérée par. AWS Directory ServiceAmazonSSM ManagedInstanceCore fournit les autorisations minimales nécessaires pour utiliser le AWS Systems Manager service. Pour plus d'informations sur la création d'un rôle doté de ces autorisations, ainsi que sur les autres autorisations et politiques que vous pouvez attribuer à votre rôle IAM, veuillez consulter la section Create an IAM instance profile for Systems Manager (français non garanti) dans le Guide de l'utilisateur AWS Systems Manager .

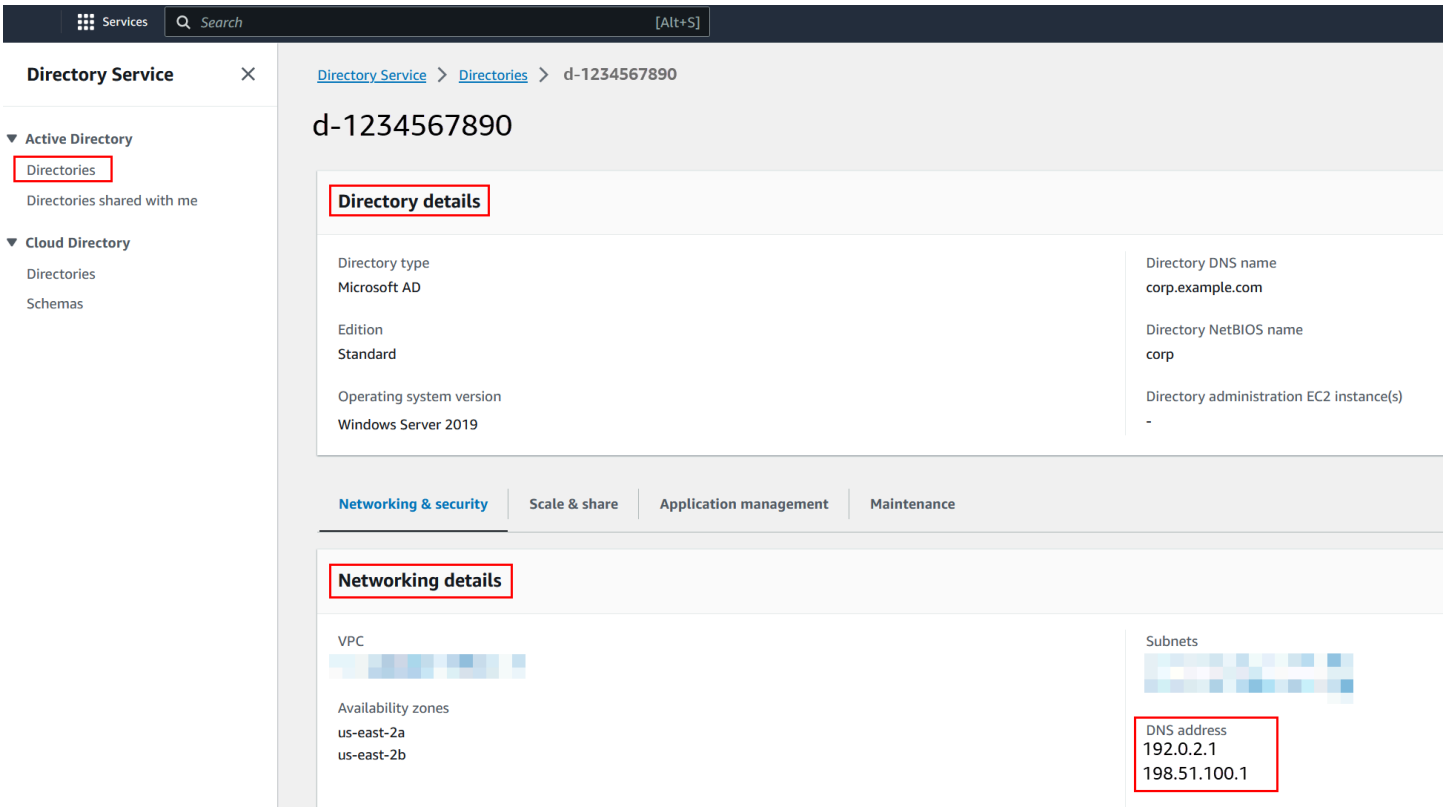
5. Sur la page Name, review, and create (Nommer, vérifier et créer), saisissez un Role name (Nom du rôle). Vous aurez besoin de ce nom de rôle pour l'attacher à l'instance EC2.
6. (Facultatif) Vous pouvez fournir une description du profil d'instance IAM dans le champ Description.
7. Sélectionnez Créer un rôle.
8. Revenez à la page Launch an instance (Lancer une instance) et choisissez l'icône d'actualisation à côté du profil d'instance IAM. Votre nouveau profil d'instance IAM doit être visible dans la liste déroulante des IAM instance profile (profil d'instance IAM). Choisissez le nouveau profil et laissez le reste de paramètres avec leurs valeurs par défaut.

16. Choisissez Launch instance (Lancer une instance).

Joindre manuellement une instance Windows Amazon EC2 à votre répertoire Simple AD Active Directory

Pour joindre manuellement une instance Windows Amazon EC2 existante à un répertoire Simple AD Active Directory, l'instance doit être lancée à l'aide des paramètres spécifiés dans. Joignez facilement une instance Windows Amazon EC2 à votre répertoire Simple AD Active Directory

Vous aurez besoin des adresses IP des serveurs DNS Simple AD. Ces informations se trouvent sous Directory Services (Services d'annuaire) > Directories (Annuaires) > le lien Directory ID (ID de l'annuaire) de votre annuaire > Directory details (Détails de l'annuaire) puis les sections Networking & Security Réseau et sécurité.



Pour joindre une instance Windows à un répertoire Simple AD Active Directory

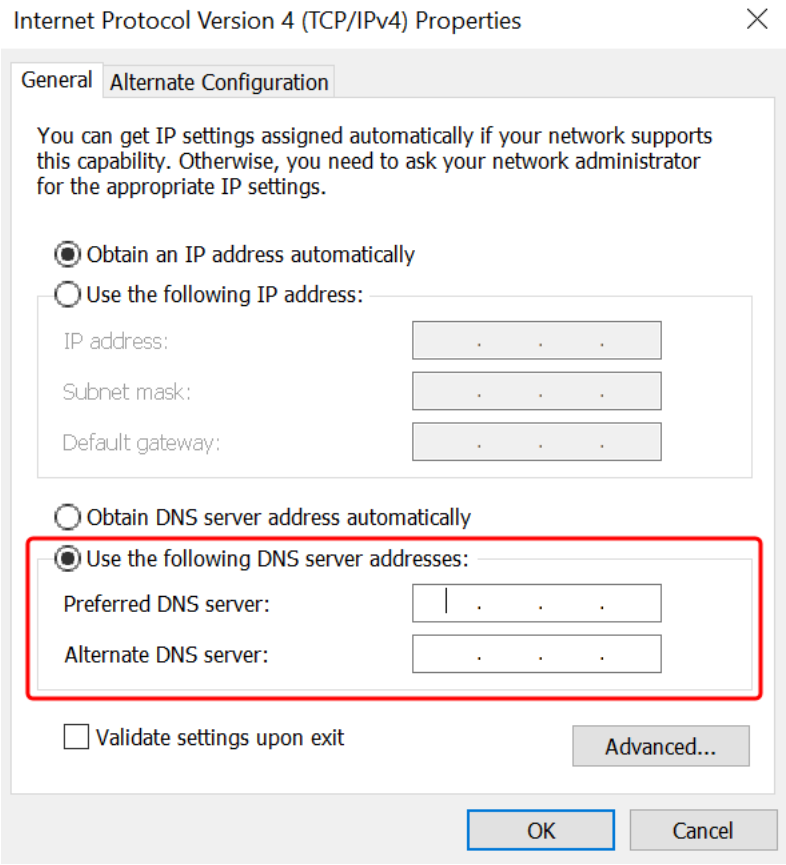
1. Connectez-vous à l'instance à l'aide d'un client RDP (Remote Desktop Protocol).
2. Ouvrez la boîte de dialogue des propriétés TCP/IPv4 sur l'instance.
   a. Ouvrez Network Connections (Connexions réseau).

> **Tip**
>
> Vous pouvez ouvrir Network Connections (Connexions réseau) directement en exécutant ce qui suit à partir d'une invite de commande sur l'instance.
>
> ```
> %SystemRoot%\system32\control.exe ncpa.cpl
> ```

b. Ouvrez le menu contextuel (clic droit) pour toute connexion de réseau active, puis choisissez Properties (Propriétés).

c. Dans la boîte de dialogue des propriétés de connexion, ouvrez (double-cliquez) Internet Protocol version 4.

3. Sélectionnez Utiliser les adresses de serveur DNS suivantes, remplacez les adresses du serveur DNS préféré et du serveur DNS alternatif par les adresses IP de vos serveurs DNS fournis par Simple AD, puis cliquez sur OK.



4. Ouvrez la boîte de dialogue System Properties (Propriétés système) de l'instance, sélectionnez l'onglet Computer Name (Nom de l'ordinateur), puis choisissez Change (Modifier).

> **Tip**
>
> Vous pouvez ouvrir la boîte de dialogue System Properties (Propriétés du système) directement en exécutant ce qui suit à partir d'une invite de commande sur l'instance.
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. Dans le champ Membre de, sélectionnez Domaine, entrez le nom complet de votre Simple AD Active Directory, puis cliquez sur OK.
6. Lorsque vous êtes invité à saisir le nom et le mot de passe de l'administrateur du domaine, entrez le nom d'utilisateur et le mot de passe d'un compte doté de privilèges de connexion au domaine. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter Délégation des privilèges de jonction d'annuaire pour Simple AD.

   > **Note**
   >
   > Vous pouvez saisir le nom complet de votre domaine ou le nom NetBIOS, suivi d'une barre oblique inverse (\), puis du nom d'utilisateur. Le nom d'utilisateur serait Administrator. Par exemple, **`corp.example.com\administrator`** ou **`corp\administrator`**.

7. Après avoir reçu le message de bienvenue dans le domaine, redémarrez l'instance pour que les modifications prennent effet.

Maintenant que votre instance a été jointe au domaine Simple AD Active Directory, vous pouvez vous connecter à distance à cette instance et installer des utilitaires pour gérer l'annuaire, tels que l'ajout d'utilisateurs et de groupes. Les outils d'administration Active Directory peuvent être utilisés pour créer des utilisateurs et des groupes. Pour plus d'informations, consultez Installation des outils d'administration Active Directory pour Simple AD.

Joignez facilement une instance Linux Amazon EC2 à votre répertoire Simple AD Active Directory

Cette procédure permet de joindre facilement une instance Linux Amazon EC2 à votre répertoire Simple AD Active Directory.

Les distributions et les versions d'instance Linux suivantes sont prises en charge :

- AMI Amazon Linux 2018.03.0
- Amazon Linux 2 (64 bits x86)
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS et Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Les distributions antérieures à Ubuntu 14 et Red Hat Enterprise Linux 7 ne prennent pas en charge la fonctionnalité de jonction de domaine transparente.

Prérequis

Avant de pouvoir configurer une jointure de domaine fluide à une instance Linux, vous devez suivre les procédures décrites dans cette section.

Sélectionnez votre compte de service de jonction transparente à un domaine

Vous pouvez joindre de manière transparente des ordinateurs Linux à votre domaine Simple AD. Pour ce faire, vous devez créer un compte utilisateur autorisé à créer un compte d'ordinateur pour joindre les ordinateurs au domaine. Bien que les Administrateurs de domaine ou les membres d'autres groupes puissent disposer de privilèges suffisants pour joindre des ordinateurs au domaine, nous vous le déconseillons. À titre de bonne pratique, nous vous recommandons d'utiliser un compte de service disposant des privilèges minimum nécessaires pour joindre les ordinateurs au domaine.

Pour plus d'informations sur le traitement et la délégation des autorisations à votre compte de service pour la création de comptes d'ordinateur, veuillez consulter Délégation de privilèges à votre compte de service.

Créer les secrets pour stocker le compte de service de domaine

Vous pouvez l'utiliser AWS Secrets Manager pour stocker le compte de service de domaine.

Pour créer des secrets et stocker les informations du compte de service de domaine

1. Connectez-vous à la AWS Secrets Manager console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/secretsmanager/.
2. Choisissez Store a new secret (Stocker un nouveau secret).
3. Sur la page Store a new secret (Stocker un nouveau secret), procédez comme suit :

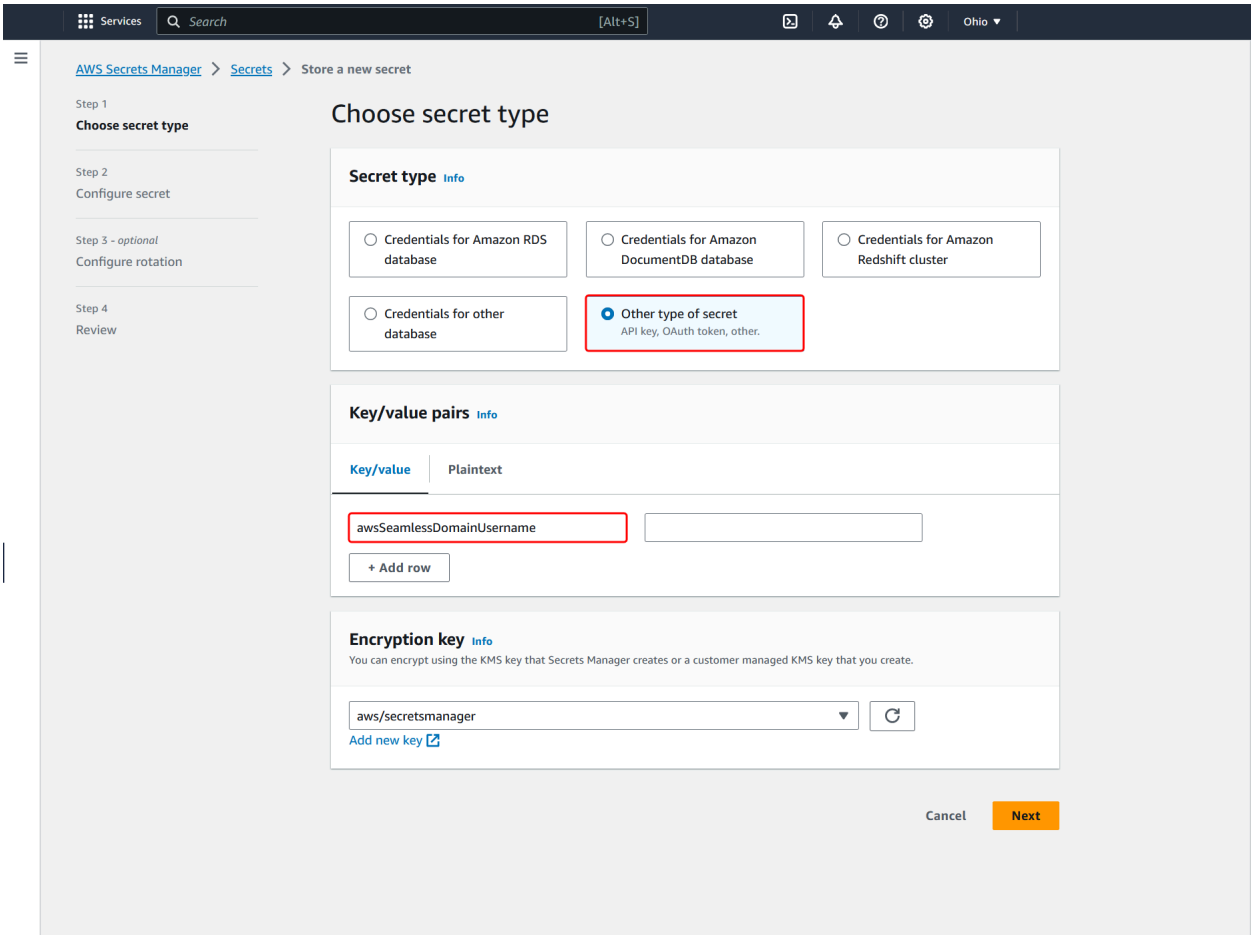
    a. Sous Type de secret, sélectionnez Autre type de secret.

    b. Sous Paires clé/valeur, procédez comme suit :

        i. Dans la première case, saisissez **`awsSeamlessDomainUsername`**. Sur la même ligne, dans la case suivante, entrez le nom d'utilisateur de votre compte de service.

Par exemple, si vous avez déjà utilisé la PowerShell commande, le nom du compte de service serait**`awsSeamlessDomain`**.

> **Note**
>
> Vous devez saisir **`awsSeamlessDomainUsername`** exactement tel quel. Assurez-vous qu'il n'y a pas d'espaces au début ni à la fin. Sinon, la jonction de domaine échouera.



ii. Choisissez Add row (Ajouter une ligne).

iii. Sur la nouvelle ligne, dans la première case, saisissez **`awsSeamlessDomainPassword`**. Sur la même ligne, dans la case suivante, saisissez le mot de passe de votre compte de service.

> **Note**
>
> Vous devez saisir **awsSeamlessDomainPassword** exactement tel quel. Assurez-vous qu'il n'y a pas d'espaces au début ni à la fin. Sinon, la jonction de domaine échouera.

iv. Sous Clé de chiffrement, laissez la valeur par défaut`aws/secretsmanager`. AWS Secrets Manager chiffre toujours le secret lorsque vous choisissez cette option. Vous pouvez également choisir une clé que vous avez créée.

> **Note**
>
> Des frais sont associés AWS Secrets Manager, selon le secret que vous utilisez. Pour obtenir la liste de prix actuelle complète, consultez Tarification AWS Secrets Manager.
> Vous pouvez utiliser la clé AWS `aws/secretsmanager` gérée créée par Secrets Manager pour chiffrer vos secrets gratuitement. Si vous créez vos propres clés KMS pour chiffrer vos secrets, cela vous AWS sera facturé au AWS KMS tarif en vigueur. Pour plus d'informations, consultez Tarification d'AWS Key Management Service.

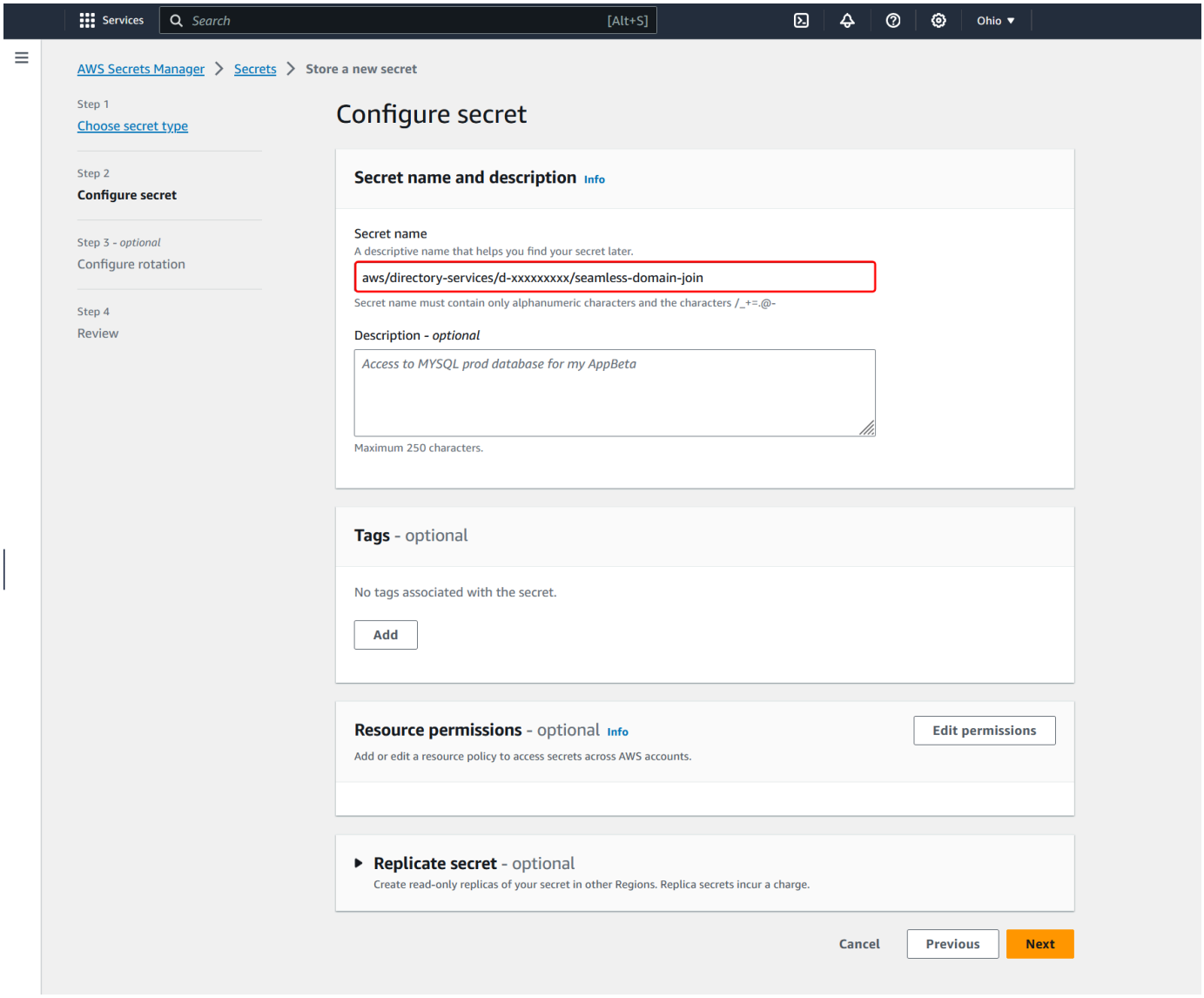
v. Choisissez Suivant.

4. Sous Nom secret, entrez un nom secret qui inclut votre identifiant de répertoire au format suivant, en remplaçant *d-xxxxxxxxx* par votre identifiant de répertoire :

```
aws/directory-services/d-xxxxxxxxx/seamless-domain-join
```

Cela servira à récupérer des secrets dans l'application.

> **Note**
>
> Vous devez saisir **aws/directory-services/*d-xxxxxxxxx*/seamless-domain-join** exactement tel quel, mais remplacez *d-xxxxxxxxx* par votre ID d'annuaire. Assurez-vous qu'il n'y a pas d'espaces au début ni à la fin. Sinon, la jonction de domaine échouera.



5. Laissez le reste des paramètres définis par défaut, puis choisissez Next (Suivant).
6. Sous Configure automatic rotation (Configurer la rotation automatique), choisissez Disable automatic rotation (Désactiver la rotation automatique), puis cliquez sur Next (Suivant).

   Vous pouvez activer la rotation pour ce secret une fois que vous l'avez enregistré.
7. Vérifiez les paramètres, puis choisissez Store (Stocker) pour enregistrer vos modifications. La console Secrets Manager vous redirige à la liste des secrets de votre compte, où votre nouveau secret est désormais inclus.
8. Choisissez le nom du secret que vous venez de créer dans la liste et prenez note de la valeur de l'ARN secret. Vous en aurez besoin pour la section suivante.

Activer la rotation pour le secret du compte de service de domaine

Nous vous recommandons d'alterner régulièrement les secrets afin d'améliorer votre niveau de sécurité.

Pour activer la rotation pour le secret du compte de service de domaine

- Suivez les instructions de la section Configurer la rotation automatique pour les AWS Secrets Manager secrets dans le Guide de AWS Secrets Manager l'utilisateur.

  Pour l'étape 5, utilisez le modèle de rotation des informations d'identification Microsoft Active Directory dans le guide de AWS Secrets Manager l'utilisateur.

  Pour obtenir de l'aide, consultez la section Résolution des problèmes AWS Secrets Manager de rotation dans le Guide de AWS Secrets Manager l'utilisateur.

Créez le rôle et la politique IAM requis

Suivez les étapes préalables suivantes pour créer une politique personnalisée qui autorise un accès en lecture seule à votre secret de jonction de domaine transparent Secrets Manager (que vous avez créé précédemment) et pour créer un nouveau rôle IAM DomainJoin LinuxEC2.

Créer la politique de lecture IAM Secrets Manager

Utilisez la console IAM pour créer une politique qui accorde un accès en lecture seule à votre secret Secrets Manager.

Pour créer la politique de lecture IAM Secrets Manager

1. Connectez-vous au en AWS Management Console tant qu'utilisateur autorisé à créer des politiques IAM. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, Gestion des accès, sélectionnez Policies.
3. Choisissez Créer une politique.
4. Choisissez l'onglet JSON et copiez le texte du document de politique JSON suivant. Collez-le ensuite dans la zone de texte JSON.

> **Note**
>
> Assurez-vous de remplacer l'ARN de la région et de la ressource par la région et l'ARN réels du secret que vous avez créé précédemment.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:xxxxxxxxx:secret:aws/directory-
services/d-xxxxxxxxx/seamless-domain-join"
            ]
        }
    ]
}
```

5. Lorsque vous avez terminé, choisissez Next. Le programme de validation des politiques signale les éventuelles erreurs de syntaxe. Pour plus d'informations, veuillez consulter la section Validating IAM policies (français non garanti).
6. Sur la page Review policy (Réviser la politique), saisissez un nom pour la politique, tel que **`SM-Secret-Linux-DJ-d-xxxxxxxxxx-Read`**. Vérifiez la section Summary (Récapitulatif) pour voir les autorisations accordées par votre politique. Sélectionnez Create Policy (Créer une politique) pour enregistrer vos changements. La nouvelle politique s'affiche dans la liste des politiques gérées et est prête à être attachée à une identité.

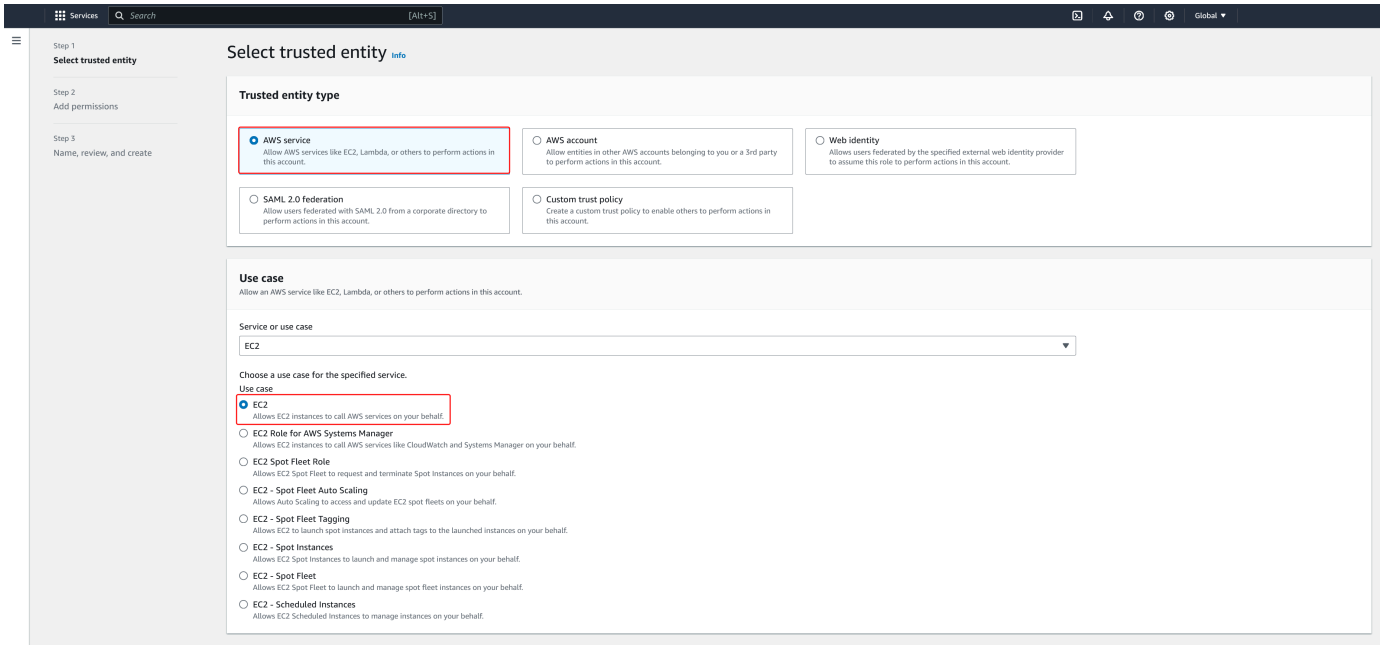
> **Note**
>
> Nous vous recommandons de créer une politique par secret. Cela garantit que les instances n'ont accès qu'au secret approprié et minimise les répercussions si une instance est compromise.

Création du rôle LinuxEC2 DomainJoin

Utilisez la console IAM pour créer le rôle que vous utiliserez pour joindre un domaine à votre instance Linux EC2.

Pour créer le rôle LinuxEC2 DomainJoin

1. Connectez-vous au en AWS Management Console tant qu'utilisateur autorisé à créer des politiques IAM. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, sous Gestion des accès, sélectionnez Rôles.
3. Dans le panneau de contenu, sélectionnez Create role (Créer un rôle).
4. Sous Select type of trusted entity (Sélectionner le type d'entité approuvée), choisissez service AWS .
5. Sous Cas d'utilisation, choisissez EC2, puis Next.



6. Pour Filter policies (Filtrer les politiques), procédez comme suit :

   a. Saisissez **`AmazonSSMManagedInstanceCore`**. Cochez ensuite la case correspondant à cet élément de la liste.

   b. Saisissez **`AmazonSSMDirectoryServiceAccess`**. Cochez ensuite la case correspondant à cet élément de la liste.

   c. Saisissez **`SM-Secret-Linux-DJ-`*`d-xxxxxxxxxx`*`-Read`** (ou le nom de la politique que vous avez créée dans la procédure précédente). Cochez ensuite la case correspondant à cet élément de la liste.

d. Après avoir ajouté les trois politiques répertoriées ci-dessus, sélectionnez Créer un rôle.

> **Note**
>
> AmazonSSM DirectoryServiceAccess fournit les autorisations nécessaires pour joindre des instances à une instance Active Directory gérée par. AWS Directory Service AmazonSSM ManagedInstanceCore fournit les autorisations minimales nécessaires pour utiliser le AWS Systems Manager service. Pour plus d'informations sur la création d'un rôle doté de ces autorisations, ainsi que sur les autres autorisations et politiques que vous pouvez attribuer à votre rôle IAM, veuillez consulter la section Create an IAM instance profile for Systems Manager (français non garanti) dans le Guide de l'utilisateur AWS Systems Manager .

7. Entrez un nom pour votre nouveau rôle, par exemple un autre nom que vous préférez dans le champ Nom du rôle. **`LinuxEC2DomainJoin`**
8. (Facultatif) Pour Role description (Description du rôle), entrez une description.
9. (Facultatif) Choisissez Ajouter une nouvelle balise à l'étape 3 : Ajouter des balises pour ajouter des balises. Les paires clé-valeur de balise sont utilisées pour organiser, suivre ou contrôler l'accès pour ce rôle.
10. Sélectionnez Créer un rôle.

Associez facilement une instance Linux à votre répertoire Simple AD Active Directory

Maintenant que vous avez configuré toutes les tâches prérequises, vous pouvez utiliser la procédure suivante pour rejoindre facilement votre instance EC2 Linux.

Pour rejoindre facilement votre instance Linux

1. Connectez-vous à la console Amazon EC2 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le sélecteur de région de la barre de navigation, choisissez le même répertoire Région AWS que le répertoire existant.
3. Sur le EC2 Dashboard (tableau de bord EC2), dans la section Launch instance (Lancer une instance), choisissez Launch instance (Lancer une instance).
4. Sur la page Lancer une instance, dans la section Nom et balises, entrez le nom que vous souhaitez utiliser pour votre instance Linux EC2.

5. (Facultatif) Sélectionnez Add additional tags (Ajouter des balises supplémentaires) pour ajouter une ou plusieurs paires clé-valeur d'identification afin d'organiser, de suivre ou de contrôler l'accès pour cette instance EC2.
6. Dans la section Image de l'application et du système d'exploitation (Amazon Machine Image), choisissez l'AMI Linux que vous souhaitez lancer.

> **Note**
>
> L'AMI utilisée doit avoir la version 2.3.1644.0 ou supérieure AWS Systems Manager (agent SSM). Pour vérifier la version de l'agent SSM installée dans votre AMI en lançant une instance à partir de cette AMI, veuillez consulter Getting the currently installed SSM Agent version (français non garanti). Si vous devez mettre à niveau l'agent SSM, veuillez consulter Installing and configuring SSM Agent on EC2 instances for Linux (français non garanti).
> SSM utilise le `aws:domainJoin` plugin pour joindre une instance Linux à un Active Directory domaine. *`Le plugin remplace le nom d'hôte des instances Linux par le format EC2AMAZ-XXXXXXX.`* Pour plus d'informations`aws:domainJoin`, consultez la référence du plug-in du document de AWS Systems Manager commande dans le guide de AWS Systems Manager l'utilisateur.

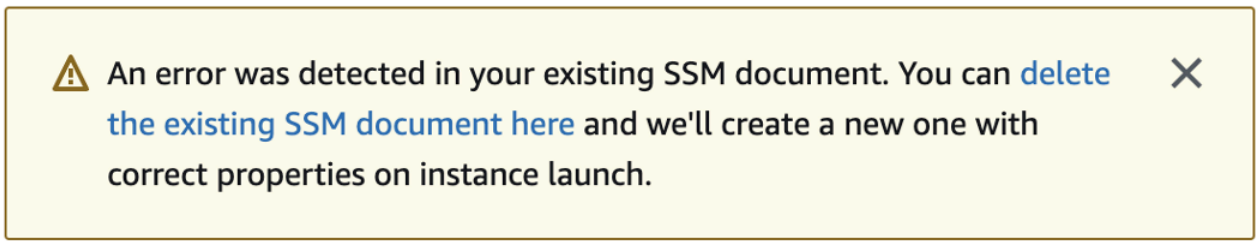
7. Dans la section Type d'instance, choisissez le type d'instance que vous souhaitez utiliser dans la liste déroulante Type d'instance.
8. Dans la section Paire de clés (connexion), vous pouvez choisir de créer une nouvelle paire de clés ou choisir une paire de clés existante. Pour créer une nouvelle paire de clés, choisissez Créer une paire de clés. Entrez le nom de la paire de clés et sélectionnez une option pour le type de paire de clés et le format de fichier de 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. Choisissez Créer une paire de clés. Le fichier de clé privée est automatiquement téléchargé dans votre navigateur. Enregistrez le fichier de clé privée en lieu sûr.

> **Important**
>
> C'est votre seule occasion d'enregistrer le fichier de clé privée.

9. Sur la page Lancer une instance, dans la section Paramètres réseau, choisissez Modifier. Choisissez le VPC dans lequel votre répertoire a été créé dans la liste déroulante VPC obligatoire.
10. Choisissez l'un des sous-réseaux publics de votre VPC dans la liste déroulante Sous-réseau. Tout le trafic externe du sous-réseau que vous choisissez doit être acheminé vers une passerelle Internet. Sinon, vous ne pourrez pas vous connecter à l'instance à distance.

    Pour obtenir plus d'informations sur la manière de se connecter à une passerelle Internet, veuillez consulter la section Connect to the internet using an internet gateway (français non garanti) dans le Guide de l'utilisateur Amazon VPC.
11. Sous Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique), choisissez Enable (Activer).

    Pour plus d'informations sur les adresses IP publiques et privées, veuillez consulter la section Amazon EC2 instance IP addressing (français non garanti) dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.
12. Pour les paramètres Firewall (security groups) [Pare-feu (groupes de sécurité)], vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
13. Pour les paramètres Configure storage (Configurer le stockage), vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
14. Choisissez la section Advanced details (Détails avancés), puis sélectionnez votre domaine dans la liste déroulante Domain join directory (Annuaire de jonction de domaines).

> **Note**
>
> Après avoir choisi le répertoire de jointure du domaine, vous pouvez voir :
>
> 
>
>
> Cette erreur se produit si l'assistant de lancement EC2 identifie un document SSM existant présentant des propriétés inattendues. Vous pouvez effectuer l'une des actions suivantes :

- Si vous avez déjà modifié le document SSM et que les propriétés sont attendues, choisissez Fermer et lancez l'instance EC2 sans aucune modification.
- Cliquez sur le lien Supprimer le document SSM existant ici pour supprimer le document SSM. Cela permettra de créer un document SSM avec les propriétés correctes. Le document SSM sera automatiquement créé lorsque vous lancerez l'instance EC2.

15. Pour le profil d'instance IAM, choisissez le rôle IAM que vous avez créé précédemment dans la section des prérequis Étape 2 : Création du rôle LinuxEC2. DomainJoin
16. Choisissez Launch instance (Lancer une instance).

> **Note**
>
> Si vous effectuez une jonction de domaine transparente avec SUSE Linux, un redémarrage est nécessaire pour que les authentifications fonctionnent. Pour redémarrer SUSE depuis le terminal Linux, tapez sudo reboot.

Joindre manuellement une instance Linux Amazon EC2 à votre répertoire Simple AD Active Directory

Outre les instances Windows Amazon EC2, vous pouvez également joindre certaines instances Amazon EC2 Linux à votre répertoire Simple AD Active Directory. Les distributions et les versions d'instance Linux suivantes sont prises en charge :

- AMI Amazon Linux 2018.03.0
- Amazon Linux 2 (64 bits x86)
- AMI Amazon Linux 2023
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS et Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> D'autres distributions et versions Linux peuvent fonctionner, mais n'ont pas été testées.

Prérequis

Avant de pouvoir joindre une instance Amazon Linux, CentOS, Red Hat ou Ubuntu à votre annuaire, l'instance doit d'abord être lancée comme indiqué dans Joignez facilement une instance Linux Amazon EC2 à votre répertoire Simple AD Active Directory.

> **Important**
>
> Certaines des procédures suivantes peuvent rendre votre instance inaccessible ou non utilisable si elles ne sont pas effectuées correctement. Par conséquent, nous vous conseillons vivement de faire une sauvegarde ou de prendre un instantané de votre instance avant d'exécuter ces procédures.

Pour joindre une instance Linux à votre annuaire

Suivez les étapes pour votre instance Linux spécifique à l'aide de l'un des onglets suivants :

Amazon Linux

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP des serveurs DNS AWS Directory Service fournis. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez la définir manuellement, veuillez consulter How do I assign a static DNS server to a private Amazon EC2 instance (français non garanti) dans le Centre de connaissances AWS pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version particulières de Linux.
3. Assurez-vous que votre instance Amazon Linux - 64 bits est à jour.

   ```
   sudo yum -y update
   ```

4. Installez les paquets Amazon Linux requis sur votre instance Linux.

> **Note**
>
> Certains de ces packages peuvent être déjà installés.
> Au fur et à mesure que vous installez les packages, plusieurs fenêtres de configuration contextuelles peuvent apparaître. Vous pouvez généralement laisser les champs de ces écrans vides.

Amazon Linux

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli
 krb5-workstation
```

> **Note**
>
> Pour vous aider à déterminer la version d'Amazon Linux que vous utilisez, veuillez consulter la section Identifying Amazon Linux images (français non garanti) dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.

5. Joignez l'instance à l'annuaire avec la commande suivante.

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

Un compte dans le domaine *example.com* qui dispose de privilèges de jointure de domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter Délégation des privilèges de jonction d'annuaire pour AWS Managed Microsoft AD.

example.com

Nom DNS complet de votre annuaire.

```
...
 * Successfully enrolled machine in realm
```

6. Définissez le service SSH pour permettre l'authentification du mot de passe.

a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

```
sudo vi /etc/ssh/sshd_config
```

b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

```
PasswordAuthentication yes
```

c. Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

Autrement :

```
sudo service sshd restart
```

7. Une fois que l'instance a redémarré, connectez-vous y avec un client SSH et ajoutez le groupe d'administrateurs du domaine à la liste sudoers en effectuant les étapes suivantes :

a. Ouvrez le fichier `sudoers` avec la commande suivante :

```
sudo visudo
```

b. Ajoutez les éléments suivants en bas du fichier `sudoers` et enregistrez-le.

```
## Add the "Domain Admins" group from the example.com domain.
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

CentOS

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP des serveurs DNS AWS Directory Service fournis. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez la définir manuellement, veuillez consulter How do I assign a static DNS server to a private Amazon EC2 instance (français non

garanti) dans le Centre de connaissances AWS pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version particulières de Linux.

3. Assurez-vous que votre instance CentOS 7 est à jour.

```
sudo yum -y update
```

4. Installez les paquets CentOS 7 obligatoires sur votre instance Linux.

> **Note**
>
> Certains de ces packages peuvent être déjà installés.
> Au fur et à mesure que vous installez les packages, plusieurs fenêtres de configuration contextuelles peuvent apparaître. Vous pouvez généralement laisser les champs de ces écrans vides.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Joignez l'instance à l'annuaire avec la commande suivante.

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

Un compte dans le domaine *example.com* qui dispose de privilèges de jointure de domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter Délégation des privilèges de jonction d'annuaire pour AWS Managed Microsoft AD.

example.com

Nom DNS complet de votre annuaire.

```
...
 * Successfully enrolled machine in realm
```

6. Définissez le service SSH pour permettre l'authentification du mot de passe.

   a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

```
sudo vi /etc/ssh/sshd_config
```

b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

```
PasswordAuthentication yes
```

c. Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

Autrement :

```
sudo service sshd restart
```

7. Une fois que l'instance a redémarré, connectez-vous y avec un client SSH et ajoutez le groupe d'administrateurs du domaine à la liste sudoers en effectuant les étapes suivantes :

a. Ouvrez le fichier `sudoers` avec la commande suivante :

```
sudo visudo
```

b. Ajoutez les éléments suivants en bas du fichier `sudoers` et enregistrez-le.

```
## Add the "Domain Admins" group from the example.com domain.
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

Red hat

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP des serveurs DNS AWS Directory Service fournis. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez la définir manuellement, veuillez consulter How do I assign a static DNS server to a private Amazon EC2 instance (français non

garanti) dans le Centre de connaissances AWS pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version particulières de Linux.

3. Assurez-vous que l'instance Red Hat - 64 bits est à jour.

```
sudo yum -y update
```

4. Installez les packages Red Hat obligatoires sur votre instance Linux.

> **Note**
>
> Certains de ces packages peuvent être déjà installés.
> Au fur et à mesure que vous installez les packages, plusieurs fenêtres de configuration contextuelles peuvent apparaître. Vous pouvez généralement laisser les champs de ces écrans vides.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Joignez l'instance à l'annuaire avec la commande suivante.

```
sudo realm join -v -U join_account example.com --install=/
```

join_account

Le SAM AccountName pour un compte du domaine *exemple.com* doté de privilèges de connexion à un domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter Délégation des privilèges de jonction d'annuaire pour AWS Managed Microsoft AD.

example.com

Nom DNS complet de votre annuaire.

```
...
 * Successfully enrolled machine in realm
```

6. Définissez le service SSH pour permettre l'authentification du mot de passe.

   a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

```
sudo vi /etc/ssh/sshd_config
```

b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

```
PasswordAuthentication yes
```

c. Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

Autrement :

```
sudo service sshd restart
```

7. Une fois que l'instance a redémarré, connectez-vous y avec un client SSH et ajoutez le groupe d'administrateurs du domaine à la liste sudoers en effectuant les étapes suivantes :

a. Ouvrez le fichier `sudoers` avec la commande suivante :

```
sudo visudo
```

b. Ajoutez les éléments suivants en bas du fichier `sudoers` et enregistrez-le.

```
## Add the "Domain Admins" group from the example.com domain.
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

Ubuntu

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP des serveurs DNS AWS Directory Service fournis. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez la définir manuellement, veuillez consulter How do I assign a static DNS server to a private Amazon EC2 instance (français non

garanti) dans le Centre de connaissances AWS pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version particulières de Linux.

3. Assurez-vous que l'instance Ubuntu - 64 bits est à jour.

```
sudo apt-get update
sudo apt-get -y upgrade
```

4. Installez les packages Ubuntu obligatoires sur votre instance Linux.

> **Note**
>
> Certains de ces packages peuvent être déjà installés.
> Au fur et à mesure que vous installez les packages, plusieurs fenêtres de configuration contextuelles peuvent apparaître. Vous pouvez généralement laisser les champs de ces écrans vides.

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. Désactivez la résolution DNS inversée et définissez le domaine par défaut sur le nom de domaine complet de votre domaine. Les instances Ubuntu doivent pouvoir faire l'objet d'une résolution inverse dans le DNS pour qu'un domaine puisse fonctionner. Sinon, vous devez désactiver la résolution DNS inverse dans /etc/krb5.conf de la façon suivante :

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. Joignez l'instance à l'annuaire avec la commande suivante.

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

Le SAM AccountName pour un compte du domaine *exemple.com* doté de privilèges de connexion à un domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir

plus d'informations sur la délégation de ces privilèges, veuillez consulter [Délégation des privilèges de jonction d'annuaire pour AWS Managed Microsoft AD](#).

example.com

Nom DNS complet de votre annuaire.

```
...
 * Successfully enrolled machine in realm
```

7. Définissez le service SSH pour permettre l'authentification du mot de passe.
   a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

```
sudo vi /etc/ssh/sshd_config
```

   b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

```
PasswordAuthentication yes
```

   c. Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

   Autrement :

```
sudo service sshd restart
```

8. Une fois que l'instance a redémarré, connectez-vous y avec un client SSH et ajoutez le groupe d'administrateurs du domaine à la liste sudoers en effectuant les étapes suivantes :
   a. Ouvrez le fichier `sudoers` avec la commande suivante :

```
sudo visudo
```

   b. Ajoutez les éléments suivants en bas du fichier `sudoers` et enregistrez-le.

```
## Add the "Domain Admins" group from the example.com domain.
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

> **Note**
>
> Lors de l'utilisation de Simple AD, si vous créez un compte d'utilisateur sur une instance Linux avec l'option « Force user to change password at first login », cet utilisateur ne pourra pas modifier initialement son mot de passe à l'aide de la commande kpasswd. Pour modifier le mot de passe la première fois, un administrateur de domaine doit mettre à jour le mot de passe utilisateur à l'aide des outils de gestion Active Directory.

Gérer des comptes à partir d'une instance Linux

Pour gérer des comptes dans Simple AD à partir d'une instance Linux, vous devez mettre à jour des fichiers de configuration spécifiques sur votre instance Linux comme suit :

1. Définissez krb5_use_kdcinfo sur False dans le fichier /etc/sssd/sssd.conf. Par exemple :

   ```
   [domain/example.com]
       krb5_use_kdcinfo = False
   ```

2. Pour que la configuration soit appliquée, vous devez redémarrer le service sssd :

   ```
   $ sudo systemctl restart sssd.service
   ```

   Vous pouvez également utiliser :

   ```
   $ sudo service sssd start
   ```

3. Si vous allez gérer les utilisateurs à partir d'une instance Linux CentOS, vous devez également modifier le fichier /etc/smb.conf pour inclure :

   ```
   [global]
     workgroup = EXAMPLE.COM
     realm = EXAMPLE.COM
     netbios name = EXAMPLE
     security = ads
   ```

Restriction de l'accès de connexion à un compte

Comme tous les comptes sont définis dans Active Directory, par défaut, tous les utilisateurs de l'annuaire peuvent se connecter à l'instance. Vous pouvez autoriser uniquement certains utilisateurs à se connecter à l'instance à l'aide de la commande ad_access_filterdans sssd.conf. Par exemple :

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Indique que les utilisateurs ne peuvent accéder qu'à l'instance s'ils sont membres d'un groupe spécifique.

cn

Nom canonique du groupe disposant d'un accès. Dans cet exemple, le nom du groupe est *admins*.

ou

Il s'agit de l'unité d'organisation dans laquelle se trouve le groupe ci-dessus. Dans cet exemple, l'unité d'organisation est *Testou*.

dc

Il s'agit du composant de domaine de votre domaine. Dans cet exemple, *example*.

dc

Il s'agit d'un composant de domaine supplémentaire. Dans cet exemple, *com*.

Vous devez ajouter manuellement ad_access_filter à votre /etc/sssd/sssd.conf.

Ouvrez le fichier /etc/sssd/sssd.conf dans un éditeur de texte.

```
sudo vi /etc/sssd/sssd.conf
```

Une fois l'opération effectuée, votre commande sssd.conf pourrait ressembler à ce qui suit :

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam
```

```
[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

Pour que la configuration soit appliquée, vous devez redémarrer le service sssd :

```
sudo systemctl restart sssd.service
```

Vous pouvez également utiliser :

```
sudo service sssd restart
```

Cartographie des identifiants

Le mappage des identifiants peut être effectué par deux méthodes afin de maintenir une expérience unifiée entre les identités UNIX/Linux User Identifier (UID) et Group Identifier (GID) et Windows et Active Directory Security Identifier (SID).

1. Centralisé
2. Distribué

> **Note**
>
> Le mappage centralisé de l'identité utilisateur Active Directory nécessite une interface de système d'exploitation portable ou POSIX.

Cartographie centralisée de l'identité des utilisateurs

Active Directoryou un autre service LDAP (Lightweight Directory Access Protocol) fournit un UID et un GID aux utilisateurs de Linux. DansActive Directory, ces identifiants sont stockés dans les attributs des utilisateurs :

- UID - Le nom d'utilisateur Linux (chaîne)
- Numéro UID : numéro d'identification utilisateur Linux (entier)
- Numéro GID : numéro d'identification du groupe Linux (entier)

Pour configurer une instance Linux afin d'utiliser l'UID et le GID à partir deActive Directory, définissez-les `ldap_id_mapping = False` dans le fichier sssd.conf. Avant de définir cette valeur, vérifiez que vous avez ajouté un UID, un numéro UID et un numéro GID aux utilisateurs et aux groupes dans. Active Directory

Cartographie distribuée de l'identité des utilisateurs

S'il Active Directory ne possède pas l'extension POSIX ou si vous choisissez de ne pas gérer de manière centralisée le mappage des identités, Linux peut calculer les valeurs UID et GID. Linux utilise l'identifiant de sécurité (SID) unique de l'utilisateur pour garantir la cohérence.

Pour configurer le mappage d'ID utilisateur distribué, définissez-le `ldap_id_mapping = True` dans le fichier sssd.conf.

Connect à l'instance Linux

Lorsqu'un utilisateur se connecte à l'instance à l'aide d'un client SSH, il est invité à indiquer son nom d'utilisateur. L'utilisateur peut entrer le nom d'utilisateur au format `username@example.com` ou au format `EXAMPLE\username`. La réponse ressemblera à la suivante, selon la distribution Linux que vous utilisez :

Amazon Linux, Red Hat Enterprise Linux et CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)

As "root" (sudo or sudo -i) use the:
```

```
  - zypper command for package management
  - yast command for configuration management

Management and Config: https://www.suse.com/suse-in-the-cloud-basics
Documentation: https://www.suse.com/documentation/sles-15/
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud

Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

  System information as of Sat Apr 18 22:03:35 UTC 2020

  System load:  0.01              Processes:           102
  Usage of /:   18.6% of 7.69GB   Users logged in:     2
  Memory usage: 16%               IP address for eth0: 10.24.34.1
  Swap usage:   0%
```

Délégation des privilèges de jonction d'annuaire pour Simple AD

Pour joindre un ordinateur à votre annuaire, vous devez disposer d'un compte doté des privilèges de jonction des ordinateurs à l'annuaire.

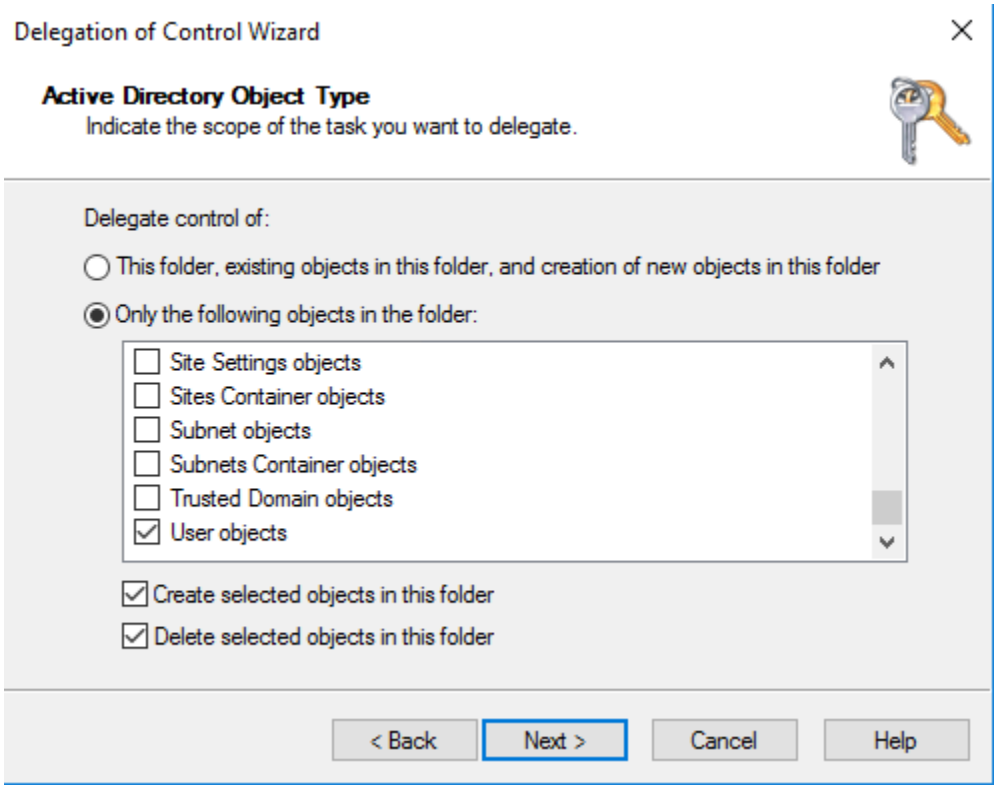
Avec Simple AD, les membres du groupe Administrateurs de domaine ont les privilèges nécessaires pour joindre les ordinateurs à l'annuaire.

Cependant, en tant que bonne pratique, vous devez utiliser un compte disposant uniquement des privilèges minimum nécessaires. La procédure suivante montre comment créer un nouveau groupe appelé `Joiners` et déléguer les privilèges à ce groupe qui sont nécessaires pour joindre des ordinateurs à l'annuaire.

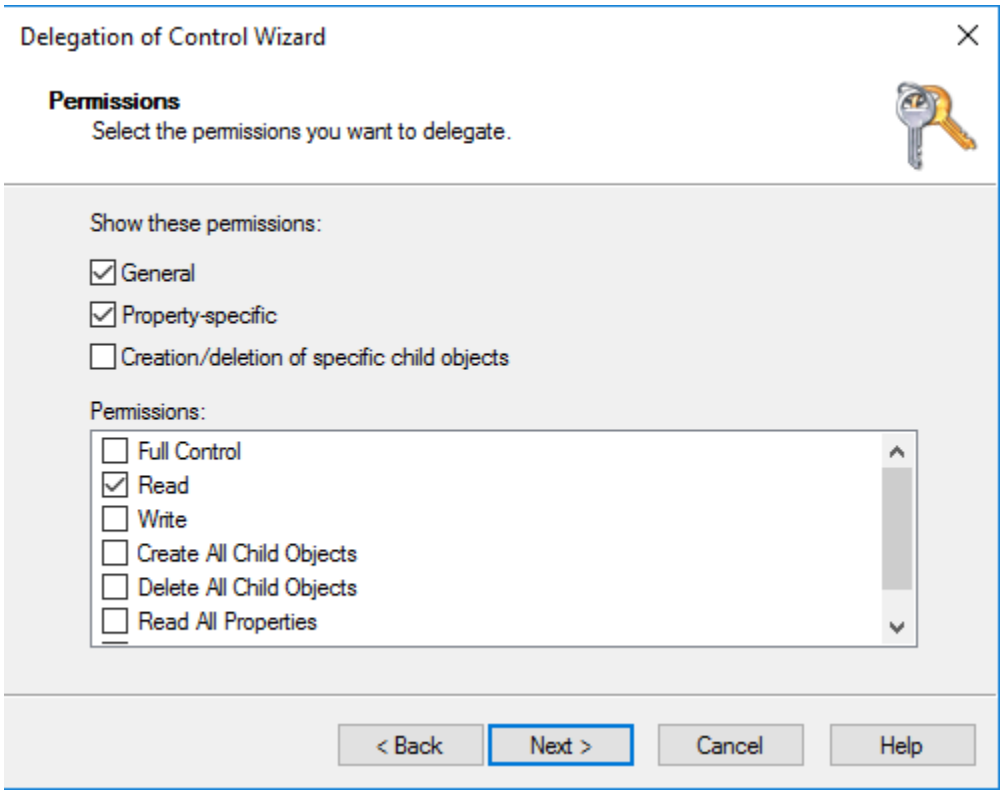
Vous devez effectuer cette procédure sur un ordinateur qui est joint à votre annuaire et qui dispose du composant logiciel enfichable Utilisateurs et ordinateurs Active Directory. Vous devez également être connecté en tant qu'administrateur de domaine.

Pour déléguer des privilèges de jonction pour Simple AD

1. Ouvrez Utilisateurs et ordinateurs Active Directory, puis sélectionnez votre domaine dans l'arborescence de navigation.
2. Dans l'arborescence de navigation de gauche, ouvrez le menu contextuel (clic droit) Utilisateurs, choisissez Nouveau, puis Groupe.
3. Dans la zone Nouvel objet - groupe, saisissez ce qui suit et choisissez OK.
   - Pour Nom du groupe, tapez **`Joiners`**.
   - Pour Étendue du groupe, choisissez Global.
   - Pour Type de groupe, choisissez Sécurité.
4. Dans l'arborescence de navigation, sélectionnez la racine de votre domaine. A partir du menu Action, choisissez Déléguer le contrôle.
5. Sur la page Delegation of Control Wizard, choisissez Next, puis choisissez Add.
6. Dans la zone Select Users, Computers, or Groups, saisissez `Joiners`, puis choisissez OK. Si vous trouvez plusieurs objets, sélectionnez le groupe `Joiners` créé précédemment. Choisissez Suivant.
7. Sur la page Tâches à déléguer, sélectionnez Créer une tâche personnalisée à déléguer, puis choisissez Suivant.
8. Sélectionnez Only the following objects in the folder, puis Computer objects.
9. Sélectionnez Créer les objets sélectionnés dans ce dossier et Supprimer les objets sélectionnés dans ce dossier. Ensuite, sélectionnez Suivant.



10. Sélectionnez Lecture et Ecriture, puis choisissez Suivant.



11. Vérifiez les informations de la page Fin de l'Assistant Délégation de contrôle, puis choisissez Terminer.
12. Créez un utilisateur avec un mot de passe fort et ajoutez-le au groupe `Joiners`. L'utilisateur disposera alors de privilèges suffisants pour se connecter AWS Directory Service à l'annuaire.

Créer un jeu d'options DHCP

AWS vous recommande de créer un ensemble d'options DHCP pour votre AWS Directory Service répertoire et d'attribuer le jeu d'options DHCP au VPC dans lequel se trouve votre répertoire. Cela permet à toutes les instances de ce VPC de pointer vers le domaine spécifié, et aux serveurs DNS de résoudre leurs noms de domaine.

Pour en savoir plus sur les jeux d'options DHCP, veuillez consulter la section DHCP options sets (français non garanti) dans le Guide de l'utilisateur Amazon VPC.

Pour créer un jeu d'options DHCP défini pour votre annuaire

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez DHCP Options Sets, puis sélectionnez Create DHCP options set.
3. Dans la page Créer un jeu d'options DHCP, saisissez les valeurs suivantes pour votre annuaire :

   Nom

   Une balise facultative pour le jeu d'options.

   Nom de domaine

   Nom complet de votre annuaire, par exemple `corp.example.com`.

   Serveurs de noms de domaine

   Les adresses IP des serveurs DNS du répertoire AWS que vous avez fourni.

   > **Note**
   >
   > Vous pouvez trouver ces adresses en accédant au volet de navigation de la console AWS Directory Service, en sélectionnant Directories (Annuaires), puis en choisissant l'ID d'annuaire correct.

Serveurs NTP

Laissez ce champ vide.

Serveur de nom NetBIOS

Laissez ce champ vide.

Type de nœud NetBIOS

Laissez ce champ vide.

4. Choisissez Créer un jeu d'options DHCP. Le nouveau jeu d'options DHCP apparaît dans votre liste d'options DHCP.
5. Notez l'ID du nouveau jeu d'options DHCP (dopt-*xxxxxxxx*). Vous l'utilisez pour associer le nouveau jeu d'options à votre VPC.

Pour modifier le jeu d'options DHCP associé à un VPC

Vous ne pouvez pas modifier un jeu d'options DHCP après l'avoir créé. Si vous voulez que votre VPC utilise un jeu différent d'options DHCP, vous devez créer un nouveau jeu et l'associer à votre VPC. Vous pouvez également configurer votre VPC pour ne pas utiliser d'options DHCP du tout.

1. Ouvrez la console VPC d'Amazon sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sélectionnez Your VPCs (Vos VPC).
3. Sélectionnez le VPC, puis choisissez Actions, Modifier les paramètres du VPC.
4. Pour le jeu d'options DHCP, sélectionnez-en un ou choisissez No DHCP options set (Aucun jeu d'option DHCP), puis sélectionnez Save (Enregistrer).

Pour modifier le jeu d'options DHCP associé à un VPC à l'aide de la ligne de commande, consultez ce qui suit :

- AWS CLI: associate-dhcp-options
- AWS Tools for Windows PowerShell: Register-EC2DhcpOption

Maintenance de votre annuaire Simple AD

Cette section décrit comment assurer la gestion des tâches administratives courantes pour votre environnement Simple AD.

Rubriques

Supprimer votre Simple AD

Lorsqu'un Simple AD est supprimé, toutes les données de l'annuaire et tous les instantanés sont supprimés et ne peuvent pas être récupérés. Une fois que l'annuaire est supprimé, toutes les instances qui sont jointes à l'annuaire restent intactes. Toutefois, vous ne pouvez pas utiliser les informations d'identification de votre annuaire pour vous connecter à ces instances. Vous devez vous y connecter avec un compte utilisateur qui est local à l'instance.

Pour supprimer un annuaire

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires). Assurez-vous que vous vous trouvez Région AWS là où vous Active Directory êtes déployé. Pour plus d'informations, consultez la section Choix d'une région.
2. Assurez-vous qu'aucune AWS application n'est activée pour le répertoire que vous souhaitez supprimer. AWS Les applications activées vous empêcheront de supprimer votre AWS Managed Microsoft AD ou Simple AD.

    a. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.

    b. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications). Dans la section AWS Applications et services, vous pouvez voir quelles AWS applications sont activées pour votre annuaire.

    - Désactivez AWS Management Console l'accès. Pour plus d'informations, consultez Désactiver l'accès à AWS Management Console.
    - Pour désactiver Amazon WorkSpaces, vous devez désenregistrer le service depuis le répertoire de la WorkSpaces console. Pour plus d'informations, consultez la section Désenregistrement d'un annuaire dans le guide d'administration Amazon WorkSpaces .

- Pour désactiver Amazon WorkDocs, vous devez supprimer le WorkDocs site Amazon dans la WorkDocs console Amazon. Pour plus d'informations, consultez Supprimer un site dans le guide d' WorkDocs administration Amazon.
- Pour désactiver Amazon WorkMail, vous devez supprimer l' WorkMail organisation Amazon dans la WorkMail console Amazon. Pour plus d'informations, consultez Supprimer une organisation dans le manuel Amazon WorkMail Administrator Guide.
- Pour désactiver Amazon FSx for Windows File Server, vous devez supprimer le système de fichiers Amazon FSx du domaine. Pour plus d'informations, consultez la section Travailler avec un Active Directory serveur de fichiers FSx for Windows dans le guide de l'utilisateur d'Amazon FSx for Windows File Server.
- Pour désactiver Amazon Relational Database Service, vous devez supprimer l'instance Amazon RDS du domaine. Pour plus d'informations, veuillez consulter la section Managing a DB instance in a domain (français non garanti) dans le Guide de l'utilisateur Amazon RDS.
- Pour désactiver le AWS Client VPN service, vous devez supprimer le service d'annuaire du point de terminaison VPN du Client. Pour plus d'informations, consultez la section Active DirectoryAuthentification dans le guide de AWS Client VPN l'administrateur.
- Pour désactiver Amazon Connect, vous devez supprimer l'instance Amazon Connect. Pour plus d'informations, veuillez consulter Deleting an Amazon Connect instance (français non garanti) dans le Guide d'administration Amazon Connect.
- Pour désactiver Amazon QuickSight, vous devez vous désinscrire d'Amazon QuickSight. Pour plus d'informations, consultez la section Fermeture de votre Amazon QuickSight compte dans le guide de QuickSight l'utilisateur Amazon.

> **Note**
>
> Si vous l'utilisez AWS IAM Identity Center et que vous l'avez déjà connecté au répertoire AWS Managed Microsoft AD que vous prévoyez de supprimer, vous devez d'abord modifier la source d'identité avant de pouvoir la supprimer. Pour plus d'informations, veuillez consulter la section Change your identity source (français non garanti) dans le Guide de l'utilisateur IAM Identity Center.

3. Dans le volet de navigation, choisissez Directories (Annuaires).

4. Sélectionnez uniquement l'annuaire à supprimer, puis cliquez sur Supprimer. La suppression de l'annuaire prend plusieurs minutes. Lorsque l'annuaire a été supprimé, il est retiré de votre liste d'annuaires.

Création d'un instantané ou d'une restauration de votre annuaire

AWS Directory Service permet de prendre des instantanés manuels des données de votre annuaire Simple AD. Ces instantanés peuvent être utilisés pour effectuer une point-in-time restauration de votre répertoire. Il est impossible de prendre des instantanés des annuaires AD Connector.

Rubriques

- Création d'un instantané de votre annuaire.
- Restauration de l'annuaire à partir d'un instantané.
- Suppression d'un instantané

Création d'un instantané de votre annuaire.

Un instantané vous permet de restaurer votre répertoire tel qu'il était au moment où il a été pris. Pour créer un instantané manuel de votre annuaire, exécutez les étapes suivantes.

> **Note**
>
> Vous êtes limité à 5 instantanés manuels par annuaire. Si vous avez déjà atteint cette limite, vous devez supprimer un de vos instantanés manuels existants avant de pouvoir en créer un autre.

Pour créer un snapshot manuel

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Maintenance.
4. Dans la section Instantanés, choisissez Actions, puis sélectionnez Créer un instantané.
5. Dans la boîte de dialogue Créer un instantané d'annuaire, entrez une description de l'instantané, si vous le souhaitez. Lorsque vous êtes prêt, choisissez Créer.

Selon la taille de votre répertoire, la création de l'instantané peut prendre plusieurs minutes. Lorsque l'instantané est prêt, la valeur Statut devient `Completed`.

Restauration de l'annuaire à partir d'un instantané.

Restaurer un annuaire à partir d'un instantané revient à le déplacer dans le temps. Les instantanés d'annuaire sont propres à l'annuaire à partir duquel ils ont été créés. Un instantané ne peut être restauré que dans l'annuaire à partir duquel il a été créé. En outre, la durée maximale de prise en charge pour un instantané manuel est de 180 jours. Pour plus d'informations, veuillez consulter la section Useful shelf life of a system-state backup of Active Directory (français non garanti) sur le site web Microsoft.

> **Warning**
>
> Nous vous recommandons de contacter le Centre AWS Support avant toute restauration à partir d'un instantané ; nous pourrons peut-être vous aider à éviter d'avoir à effectuer une restauration à partir d'un instantané. Toute restauration à partir d'un instantané peut entraîner une perte de données, car les instantanés correspondent à un moment donné. Il est important que vous sachiez que tous les contrôleurs de domaine et serveurs DNS associés à l'annuaire seront hors ligne jusqu'à ce que l'opération de restauration soit terminée.

Pour restaurer un annuaire à partir d'un instantané, procédez comme suit :

Pour restaurer un annuaire à partir d'un instantané

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Maintenance.
4. Dans la section Instantanés, sélectionnez un instantané dans la liste, choisissez Actions, puis sélectionnez Restaurer l'instantané.
5. Passez en revue les informations contenues dans la boîte de dialogue Restaurer un instantané d'annuaire, puis sélectionnez Restaurer.

La restauration d'un répertoire peut prendre plusieurs minutes. Une fois la restauration réussie, la valeur Statut du répertoire devient `Active`. Toutes les modifications apportées à l'annuaire après la date de l'instantané sont remplacées.

Suppression d'un instantané

Pour supprimer un instantané

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Maintenance.
4. Dans la section Instantanés, choisissez Actions, puis Supprimer l'instantané.
5. Vérifiez que vous souhaitez supprimer l'instantané, puis sélectionnez Supprimer.

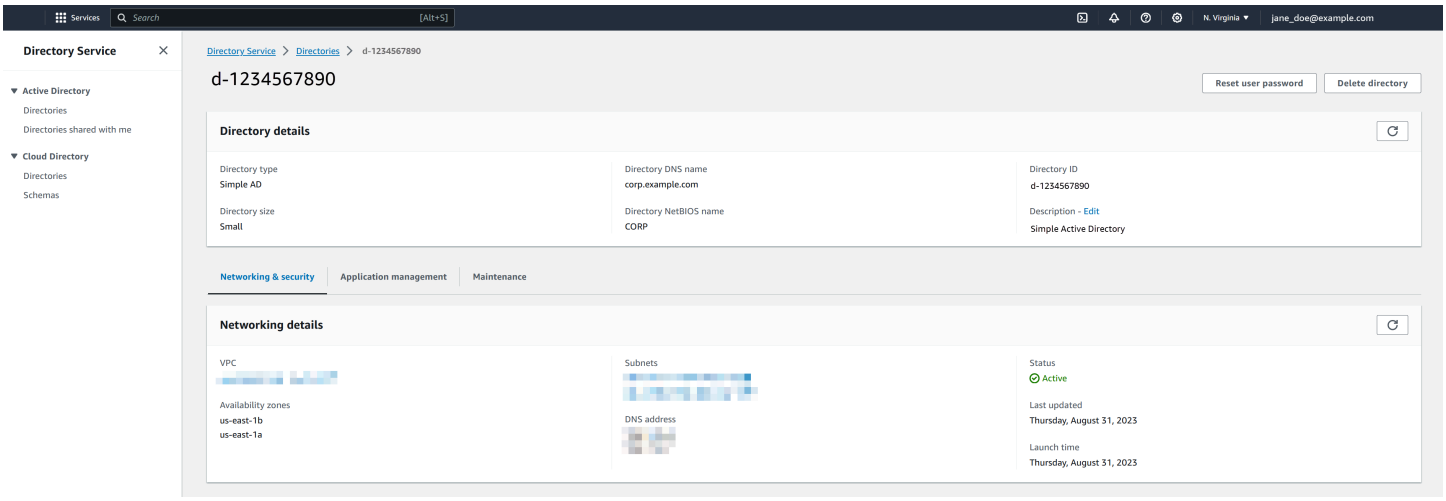
Affichage des informations d'annuaire

Vous pouvez afficher des informations détaillées sur un annuaire.

Pour afficher les informations détaillées de l'annuaire

1. Dans le volet de navigation de la AWS Directory Service console, sous Active Directory, sélectionnez Répertoires.
2. Cliquez sur le lien de l'ID correspondant à votre annuaire. Les informations relatives à l'annuaire sont affichées sur la page Détails de l'annuaire.

Pour de plus amples informations sur le champ Status (Statut), veuillez consulter Comprendre le statut de votre annuaire.



Permettre l'accès aux AWS applications et aux services

Les utilisateurs peuvent autoriser Simple AD à autoriser AWS des applications et des services, tels qu'Amazon WorkSpaces, à accéder à votreActive Directory. Les AWS applications et services suivants peuvent être activés ou désactivés pour fonctionner avec Simple AD.

AWS application/service	En savoir plus...
Amazon Chime	Pour plus d'informations, veuillez consulter le Guide d'administration Amazon Chime.
Amazon WorkDocs	Pour plus d'informations, consultez le guide d' WorkDocs administration Amazon
Amazon WorkMail	Pour plus d'informations, consultez le guide de WorkMail l'administrateur Amazon.
Amazon WorkSpaces	Vous pouvez créer un Simple AD, AWS Managed Microsoft AD ou AD Connector directement à partir de WorkSpaces. Il vous suffit de lancer la configuration avancée lors de la création de votre Workspace. Pour plus d'informations, consultez le guide d' WorkSpaces administration Amazon.
AWS Management Console	Pour de plus amples informations, veuillez consulter Activation de l'accès à AWS Management Console avec les informations d'identification AD.

Une fois activé, vous gérez l'accès à vos annuaires dans la console de l'application ou du service auquel vous souhaitez donner accès à votre répertoire. Pour trouver les liens vers AWS les applications et les services décrits ci-dessus dans la AWS Directory Service console, effectuez les opérations suivantes.

Pour afficher les applications et les services d'un annuaire

1. Dans le panneau de navigation de la consoleAWS Directory Service, choisissez Annuaires.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications).
4. Consultez la liste dans la section Applications et servicesAWS .

Pour plus d'informations sur la manière d'autoriser ou d'annuler l'autorisation d' AWS applications et de services utilisant AWS Directory Service, consultezAutorisation pour AWS les applications et les services utilisant AWS Directory Service.

Rubriques

- Création d'une URL d'accès
- Authentification unique

Création d'une URL d'accès

Une URL d'accès est utilisée avec les applications et services AWS, tels qu'Amazon WorkDocs, pour accéder à une page de connexion associée à votre annuaire. L'URL doit être globalement unique. Vous pouvez créer une URL d'accès pour votre annuaire en effectuant les étapes suivantes.

> **Warning**
>
> Une fois l'URL d'accès aux applications créée pour cet annuaire, elle ne peut pas être modifiée. Une fois votre URL d'accès créée, personne d'autre que vous ne pourra l'utiliser. Si vous supprimez votre annuaire, l'URL d'accès sera également supprimée et pourra alors être utilisée par un autre compte.

Pour créer une URL d'accès

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.

3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications).
4. Dans la section Application access URL (URL d'accès à l'application), si aucune URL d'accès n'a été attribuée à l'annuaire, le bouton Créer s'affiche. Entrez un alias d'annuaire, puis choisissez Créer. Si l'erreur Entity Already Exists (entité déjà existante) est renvoyée, cela veut dire que l'alias de l'annuaire spécifié a déjà été alloué. Choisissez un autre alias et répétez cette procédure.

   Votre URL d'accès est affichée au format *<alias>*.awsapps.com.

Authentification unique

AWS Directory Servicepermet à vos utilisateurs d'accéder à Amazon WorkDocs depuis un ordinateur connecté à l'annuaire sans avoir à saisir leurs informations d'identification séparément.

Avant d'activer l'authentification unique, vous devez prendre des mesures supplémentaires pour permettre aux navigateurs Web de vos utilisateurs de prendre en charge l'authentification unique. Les utilisateurs peuvent avoir besoin de modifier les paramètres de leur navigateur Web pour activer l'authentification unique.

> **Note**
>
> L'authentification unique fonctionne uniquement lorsqu'elle est utilisée sur un ordinateur qui est associé à l'annuaire AWS Directory Service. Elle ne peut pas être utilisée sur les ordinateurs qui ne sont pas joints à l'annuaire.

Si votre annuaire est un annuaire AD Connector et que le compte de service AD Connector ne dispose pas de l'autorisation d'ajouter ou de supprimer son attribut de nom principal de service, vous disposez de deux options pour les étapes 5 et 6 ci-dessous :

1. Vous pouvez continuer et vous serez invité à saisir le nom d'utilisateur et le mot de passe d'un utilisateur d'annuaire qui dispose de cette autorisation pour ajouter ou supprimer l'attribut de nom principal de service sur le compte de service AD Connector. Ces informations d'identification servent uniquement à activer l'authentification unique et ne sont pas stockées par le service. Les autorisations du compte de service AD Connector ne sont pas modifiées.
2. Vous pouvez déléguer des autorisations pour permettre au compte de service AD Connector d'ajouter ou de supprimer l'attribut du nom principal du service sur lui-même. Vous pouvez

exécuter les PowerShell commandes ci-dessous à partir d'un ordinateur joint au domaine à l'aide d'un compte autorisé à modifier les autorisations sur le compte de service AD Connector. La commande ci-dessous donnera au compte de service AD Connector la possibilité d'ajouter et de supprimer un attribut de nom principal de service uniquement pour lui-même.

```
$AccountName = 'ConnectorAccountName'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$RootDse = Get-ADRootDSE
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'servicePrincipalName' } -
Properties 'schemaIDGUID').schemaIDGUID
# Getting AD Connector service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AclPath = $AccountProperties.DistinguishedName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for AD Connector service account.
$ObjectAcl = Get-ACL -Path "AD:\$AclPath"
# Setting ACL allowing the AD Connector service account the ability to add and remove a
 Service Principal Name (SPN) to itself
$AddAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
 'Allow', $ServicePrincipalNameGUID, 'None'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$AclPath"
```

Pour activer ou désactiver l'authentification unique avec Amazon WorkDocs

1. Dans le volet de navigation de la console AWS Directory Service, sélectionnez Directories (Annuaires).
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications).
4. Dans la section URL d'accès à l'application, choisissez Activer pour activer l'authentification unique pour Amazon WorkDocs.

Si vous ne voyez pas le bouton Activer, vous devez d'abord créer une URL d'accès pour pouvoir afficher cette option. Pour plus d'informations sur la création d'une URL d'accès, veuillez consulter Création d'une URL d'accès.

5. Dans la boîte de dialogue Activer l'authentification unique pour cet annuaire, choisissez Activer. L'authentification unique est activée pour l'annuaire.
6. Si vous souhaitez désactiver ultérieurement l'authentification unique avec Amazon WorkDocs, choisissez Disable, puis dans la boîte de dialogue Désactiver l'authentification unique pour ce répertoire, choisissez à nouveau Disable.

Rubriques

- Authentification unique pour IE et Chrome
- Authentification unique pour Firefox

Authentification unique pour IE et Chrome

Pour permettre aux navigateurs Microsoft Internet Explorer (IE) et Google Chrome de prendre en charge l'authentification unique, les tâches suivantes doivent être effectuées sur l'ordinateur client :

- Ajoutez votre URL d'accès (par exemple, https://*<alias>*.awsapps.com) à la liste des sites approuvés pour l'authentification unique.
- Activez le script actif (JavaScript).
- Autorisez l'ouverture de session automatique.
- Activez l'authentification intégrée.

Vous ou vos utilisateurs pouvez effectuer ces tâches manuellement, ou vous pouvez modifier ces paramètres à l'aide des paramètres de politique de groupe.

Rubriques

- Mise à jour manuelle pour authentification unique sous Windows
- Mise à jour manuelle pour authentification unique sous OS X
- Paramètres de stratégie de groupe pour authentification unique

Mise à jour manuelle pour authentification unique sous Windows

Pour activer manuellement l'authentification unique sur un ordinateur Windows, effectuez les étapes suivantes sur l'ordinateur client. Certains de ces paramètres sont peut-être déjà définis correctement.

Pour activer manuellement l'authentification unique pour Internet Explorer et Chrome sous Windows

1. Pour ouvrir la boîte de dialogue Propriétés Internet, sélectionnez le menu Démarrer, tapez `Internet 0ptions` dans la zone de recherche, puis sélectionnez Options Internet.
2. Ajoutez votre URL d'accès à la liste des sites approuvés pour l'authentification unique en effectuant les étapes suivantes :
    a. Dans la boîte de dialogue Propriétés Internet, sélectionnez l'onglet Sécurité.
    b. Sélectionnez Intranet local, puis Sites.
    c. Dans la boîte de dialogue Intranet local, sélectionnez Avancé.
    d. Ajoutez votre URL d'accès à la liste des sites Web et choisissez Fermer.
    e. Dans la boîte de dialogue Intranet local, sélectionnez OK.
3. Pour activer les scripts actifs, effectuez les opérations suivantes :
    a. Dans l'onglet Sécurité de la boîte de dialogue Propriétés Internet, sélectionnez Personnaliser le niveau.
    b. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, faites défiler la page jusqu'à Scripts et sélectionnez Activer sous Scripts actifs.
    c. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, cliquez sur OK.
4. Pour activer la connexion automatique, effectuez les opérations suivantes :
    a. Dans l'onglet Sécurité de la boîte de dialogue Propriétés Internet, sélectionnez Personnaliser le niveau.
    b. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, faites défiler l'écran jusqu'à Authentification utilisateur et sélectionnez Connexion automatique uniquement dans la zone Intranet sous Connexion.
    c. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, cliquez sur OK.
    d. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, cliquez sur OK.
5. Pour activer l'authentification intégrée, effectuez les opérations suivantes :

a. Dans la boîte de dialogue Propriétés Internet, sélectionnez l'onglet Avancé.

b. Faites défiler la page jusqu'à Sécurité et sélectionnez Activer l'authentification Windows intégrée.

c. Dans la boîte de dialogue Propriétés Internet, choisissez OK.

6. Fermez puis rouvrez votre navigateur pour que ces modifications prennent effet.

Mise à jour manuelle pour authentification unique sous OS X

Pour activer manuellement l'authentification unique pour Chrome sous OS X, effectuez les étapes suivantes sur l'ordinateur client. Vous devez disposer des droits d'administrateur sur votre ordinateur pour effectuer ces opérations.

Pour activer manuellement l'authentification unique pour Chrome sous OS X

1. Ajoutez votre URL d'accès à la AuthServerAllowlistpolitique en exécutant la commande suivante :

```
defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
```

2. Ouvrez les Préférences système, accédez au panneau Profils et supprimez le profil `Chrome Kerberos Configuration`.
3. Redémarrez Chrome et ouvrez chrome://policy dans Chrome pour vérifier que les nouveaux paramètres sont en place.

Paramètres de stratégie de groupe pour authentification unique

L'administrateur de domaine peut implémenter des paramètres de stratégie de groupe pour apporter les modifications d'authentification unique sur les ordinateurs clients joints au domaine.

> **Note**
>
> Si vous gérez les navigateurs Web Chrome sur les ordinateurs de votre domaine à l'aide des politiques Chrome, vous devez y ajouter votre URL d'AuthServerAllowlistaccès. Pour plus d'informations sur la définition des politiques de Chrome, veuillez consulter la section Policy Settings in Chrome (français non garanti).

Pour activer l'authentification unique pour Internet Explorer et Chrome à l'aide des paramètres de stratégie de groupe

1. Créez un nouvel objet de stratégie de groupe en procédant comme suit :

   a. Ouvrez l'outil de gestion des stratégies de groupe, accédez à votre domaine et sélectionnez Objets de stratégie de groupe.

   b. Dans le menu principal, choisissez Action, puis Nouveau.

   c. Dans la boîte de dialogue New GPO, entrez un nom descriptif pour l'objet de stratégie de groupe, tel que `IAM Identity Center Policy` et laissez Source Starter GPO défini sur (none). Cliquez sur OK.

2. Ajoutez l'URL d'accès à la liste des sites approuvés pour l'authentification unique en effectuant les étapes suivantes :

   a. Dans l'outil de gestion des politiques de groupe, accédez à votre domaine, sélectionnez Objets de stratégie de groupe, ouvrez le menu contextuel (clic droit) de votre politique IAM Identity Center, puis choisissez Modifier.

   b. Dans l'arborescence des politiques, accédez à Configuration utilisateur > Préférences > Paramètres Windows.

   c. Dans la liste Paramètres Windows, ouvrez le menu contextuel (clic droit) pour Registre et choisissez Nouvel élément de Registre.

   d. Dans la boîte de dialogue Propriétés du nouveau registre, entrez les paramètres suivants et cliquez sur OK :

      Action

      ```
      Update
      ```

      Hive

      ```
      HKEY_CURRENT_USER
      ```

      Chemin

      ```
      Software\Microsoft\Windows\CurrentVersion\Internet Settings
      \ZoneMap\Domains\awsapps.com\<alias>
      ```

      La valeur de *<alias>* est dérivée de votre URL d'accès. Si votre URL d'accès est `https://examplecorp.awsapps.com`, l'alias est `examplecorp` et la clé de registre

sera `Software\Microsoft\Windows\CurrentVersion\Internet Settings \ZoneMap\Domains\awsapps.com\examplecorp`.

Nom de la valeur

`https`

Type de la valeur

`REG_DWORD`

Données de valeur

`1`

3. Pour activer les scripts actifs, effectuez les opérations suivantes :

   a. Dans l'outil de gestion des politiques de groupe, accédez à votre domaine, sélectionnez Objets de stratégie de groupe, ouvrez le menu contextuel (clic droit) de votre politique IAM Identity Center, puis choisissez Modifier.

   b. Dans l'arborescence des politiques, accédez à Configuration informatique > Politiques > Modèles d'administration > Composants Windows > Internet Explorer > Panneau de configuration Internet > Page de sécurité > Zone intranet.

   c. Dans la liste Zone Intranet, ouvrez le menu contextuel (clic droit) pour Autoriser les scripts actifs et choisissez Modifier.

   d. Dans la boîte de dialogue Autoriser les scripts actifs, entrez les paramètres suivants et cliquez sur OK :

      - Sélectionnez le bouton radio Activé.
      - Sous Options, définissez Autoriser les scripts actifs sur Activer.

4. Pour activer la connexion automatique, effectuez les opérations suivantes :

   a. Dans l'outil de gestion des politiques de groupe, accédez à votre domaine, sélectionnez Objets de stratégie de groupe, ouvrez le menu contextuel (clic droit) de votre politique SSO (authentification unique), puis choisissez Modifier.

   b. Dans l'arborescence des politiques, accédez à Configuration informatique > Politiques > Modèles d'administration > Composants Windows > Internet Explorer > Panneau de configuration Internet > Page de sécurité > Zone intranet.

   c. Dans la liste Zone Intranet, ouvrez le menu contextuel (clic droit) pour Options de connexion et choisissez Modifier.

d. Dans la boîte de dialogue Options de connexion, entrez les paramètres suivants et cliquez sur OK :

- Sélectionnez le bouton radio Activé.
- Sous Options, définissez les options de connexion sur Connexion automatique uniquement dans la zone Intranet.

5. Pour activer l'authentification intégrée, effectuez les opérations suivantes :

a. Dans l'outil de gestion des politiques de groupe, accédez à votre domaine, sélectionnez Objets de stratégie de groupe, ouvrez le menu contextuel (clic droit) de votre politique IAM Identity Center, puis choisissez Modifier.

b. Dans l'arborescence des politiques, accédez à Configuration utilisateur > Préférences > Paramètres Windows.

c. Dans la liste Paramètres Windows, ouvrez le menu contextuel (clic droit) pour Registre et choisissez Nouvel élément de Registre.

d. Dans la boîte de dialogue Propriétés du nouveau registre, entrez les paramètres suivants et cliquez sur OK :

Action

```
Update
```

Hive

```
HKEY_CURRENT_USER
```

Chemin

```
Software\Microsoft\Windows\CurrentVersion\Internet Settings
```

Nom de la valeur

```
EnableNegotiate
```

Type de la valeur

```
REG_DWORD
```

Données de valeur

```
1
```

6. Fermez la fenêtre de l'éditeur de gestion des politiques de groupe si elle est toujours ouverte.

7. Attribuez la nouvelle politique à votre domaine en procédant comme suit :

    a. Dans l'arborescence Gestion des politiques de groupe, ouvrez le menu contextuel (clic droit) de votre domaine et choisissez Lier un GPO existant.

    b. Dans la liste Objets de politique de groupe, sélectionnez votre politique IAM Identity Center et cliquez sur OK.

Ces modifications prendront effet après la prochaine mise à jour de la politique de groupe sur le client, ou la prochaine fois que l'utilisateur se connectera.

Authentification unique pour Firefox

Pour autoriser le navigateur Mozilla Firefox à prendre en charge l'authentification unique, ajoutez votre URL d'accès (par exemple, https://*<alias>*.awsapps.com) à la liste des sites approuvés pour l'authentification unique. Cela peut être fait manuellement ou automatiquement à l'aide d'un script.

Rubriques

- Mise à jour manuelle pour authentification unique
- Mise à jour automatique pour authentification unique

Mise à jour manuelle pour authentification unique

Pour ajouter manuellement votre URL d'accès à la liste des sites approuvés dans Firefox, effectuez les étapes suivantes sur l'ordinateur client.

Pour ajouter manuellement votre URL d'accès à la liste des sites approuvés dans Firefox

1. Ouvrez Firefox et ouvrez la page `about:config`.
2. Ouvrez la préférence `network.negotiate-auth.trusted-uris` et ajoutez votre URL d'accès à la liste des sites. Utilisez une virgule (,) pour séparer plusieurs entrées.

Mise à jour automatique pour authentification unique

En tant qu'administrateur de domaine, vous pouvez utiliser un script pour ajouter votre URL d'accès aux préférences utilisateur de Firefox `network.negotiate-auth.trusted-uris` sur tous les ordinateurs de votre réseau. Pour de plus amples informations, veuillez consulter https://support.mozilla.org/en-US/questions/939037.

Activation de l'accès à AWS Management Console avec les informations d'identification AD

AWS Directory Service vous permet d'accorder aux membres de votre annuaire l'accès à AWS Management Console. Par défaut, les utilisateurs et les groupes de votre annuaire n'ont pas accès à toutes les ressources AWS. Vous attribuez des rôles IAM aux membres de votre annuaire pour leur donner accès aux différents services et ressources AWS. Le rôle IAM définit les services, les ressources et le niveau d'accès des membres de votre annuaire.

Avant que vous puissiez accorder l'accès à la console aux membres de votre annuaire, celui-ci doit disposer d'une URL d'accès. Pour plus d'informations sur la manière d'afficher les détails de l'annuaire et d'obtenir votre URL d'accès, veuillez consulter Affichage des informations d'annuaire. Pour plus d'informations sur la création d'une URL d'accès, consultez Création d'une URL d'accès.

Pour plus d'informations sur la façon de créer et d'attribuer des rôles IAM aux membres de votre annuaire, consultez Accorder aux utilisateurs et aux groupes l'accès aux ressources AWS.

Rubriques

- Activer l'accès à AWS Management Console
- Désactivez l'accès à AWS Management Console.
- Définir la durée de la session de connexion

Article du blog sur la sécurité AWS connexe

- How to Access the AWS Management Console Using AWS Managed Microsoft AD and Your On-Premises Credentials

Activer l'accès à AWS Management Console

Par défaut, l'accès à la console n'est activé pour aucun annuaire. Pour activer l'accès à la console pour les utilisateurs et les groupes de votre annuaire, effectuez les opérations suivantes :

Pour activer l'accès à la console

1. Dans le panneau de navigation de la console AWS Directory Service, choisissez Annuaires.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.

3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications).
4. Dans la section AWS Management Console, choisissez Activer. L'accès à la console est désormais activé pour votre annuaire.

   Avant que les utilisateurs puissent se connecter à la console avec votre URL d'accès, vous devez d'abord ajouter vos utilisateurs au rôle. Pour des informations générales sur l'attribution d'utilisateurs à des rôles IAM, consultez Attribution d'utilisateurs et de groupes à un rôle existant. Une fois les rôles IAM attribués, les utilisateurs peuvent accéder à la console à l'aide de votre URL d'accès. Par exemple, si l'URL d'accès à votre annuaire est example-corp.awsapps.com, l'URL permettant d'accéder à la console est https://example-corp.awsapps.com/console/.

Désactivez l'accès à AWS Management Console.

Pour désactiver l'accès à la console pour les utilisateurs et les groupes de votre annuaire, effectuez les opérations suivantes :

Pour désactiver l'accès à la console

1. Dans le panneau de navigation de la console AWS Directory Service, choisissez Annuaires.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications).
4. Dans la section AWS Management Console, choisissez Désactiver. L'accès à la console est désormais désactivé pour votre annuaire.
5. Si des rôles IAM ont été attribués à des utilisateurs ou à des groupes dans l'annuaire, le bouton Désactiver n'est peut-être pas disponible. Dans ce cas, vous devez supprimer toutes les affectations de rôles IAM correspondant à l'annuaire avant de continuer, y compris les affectations d'utilisateurs ou de groupes de votre annuaire qui ont été supprimées et qui apparaissent sous le libellé Utilisateur supprimé ou Groupe supprimé.

   Une fois que toutes les affectations de rôles IAM ont été supprimées, répétez les étapes ci-dessus.

Définir la durée de la session de connexion

Par défaut, les utilisateurs disposent d'une heure pour utiliser leur session après s'être correctement connectés à la console avant d'être déconnectés. Ensuite, les utilisateurs doivent se reconnecter pour démarrer la prochaine session d'une heure avant d'être à nouveau déconnectés. Vous pouvez utiliser la procédure suivante pour modifier la durée jusqu'à 12 heures par session.

Définir la durée de la session de connexion

1. Dans le panneau de navigation de la console AWS Directory Service, choisissez Annuaires.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications).
4. Sous la section Applications et services AWS, choisissez AWS Management Console.
5. Dans la boîte de dialogue Gérer l'accès à la ressource AWS, choisissez Continuer.
6. Sur la page Affecter des utilisateurs et des groupes à des rôles IAM, sous Définir la durée de la session de connexion, modifiez la valeur numérotée, puis choisissez Enregistrer.

Tutoriel : Création d'un Simple AD Active Directory

Le didacticiel suivant explique toutes les étapes nécessaires à la configuration d'un répertoire Active Directory Simple AD. Il est destiné à vous permettre de démarrer Active Directory rapidement et facilement avec Simple AD, mais il n'est pas destiné à être utilisé dans un environnement de production à grande échelle.

Prérequis du didacticiel

Ce didacticiel suppose ce qui suit :

- Vous avez un actif Compte AWS.
- Votre compte n'a pas atteint la limite de VPC Amazon pour la région dans laquelle vous souhaitez utiliser Simple AD. Pour plus d'informations sur le VPC, consultez Qu'est-ce qu'Amazon VPC ? et les sous-réseaux de votre VPC dans le guide de l'utilisateur Amazon VPC.
- Vous n'avez pas de VPC existant dans la région avec un CIDR de. `10.0.0.0/16`

Pour plus d'informations, consultez Prérequis pour Simple AD.

Étape 1 : créer et configurer votre Amazon VPC pour Simple AD Active Directory

Créez et configurez un Amazon VPC à utiliser avec Simple AD. Avant de commencer cette procédure, assurez-vous que vous avez terminé Prérequis du didacticiel.

Créez un VPC pour votre Simple AD Active Directory

Créez un VPC avec deux sous-réseaux publics. AWS Directory Service nécessite deux sous-réseaux dans votre VPC, et chaque sous-réseau doit se trouver dans une zone de disponibilité différente.

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le tableau de bord VPC, choisissez Créer un VPC.
3. Sous Paramètres VPC, choisissez VPC et plus encore.
4. Complétez les champs comme suit :
   - Conservez l'option Généré automatiquement sélectionnée sous Génération automatique d'identifications de noms. Redéfinissez le projet sur `ADS VPC`.
   - Le bloc CIDR IPv4 doit être `10.0.0.0/16`.
   - Conservez l'option Pas de bloc d'adresse CIDR IPv6 sélectionnée.
   - La location doit rester par défaut.
   - Sélectionnez 2 pour le champ Nombre de zones de disponibilité.
   - Sélectionnez 2 pour le champ Nombre de sous-réseaux publics. Le nombre de sous-réseaux privés peut être redéfini sur 0.
   - Choisissez Personnaliser les blocs CIDR du sous-réseau pour configurer la plage d'adresses IP du sous-réseau public. Les blocs CIDR du sous-réseau public doivent être `10.0.0.0/20` et. `10.0.16.0/20`
5. Sélectionnez Create VPC (Créer un VPC). La création du VPC prend quelques minutes.

Étape 2 : Création de votre répertoire Active Directory Simple AD

Pour créer un nouveau répertoire Simple AD Active Directory, effectuez les étapes suivantes. Avant de commencer cette procédure, assurez-vous d'avoir rempli les conditions requises identifiées dans Prérequis du didacticiel l'étape 1 : créer et configurer votre Amazon VPC pour Simple AD. Active Directory

Pour créer un répertoire Active Directory Simple AD

1. Dans le panneau de navigation de la console AWS Directory Service, choisissez Annuaires, puis Configurer un annuaire.
2. Sur la page Sélectionner un type d'annuaire, choisissez Simple AD, puis Suivant.
3. Sur la page Enter directory information (Saisir les détails de l'annuaire), renseignez les informations suivantes :

   Taille de l'annuaire

   Faites votre choix parmi les options de taille Petit ou Large. Pour en savoir plus sur les tailles, veuillez consulter Simple AD.

   Nom de l'organisation

   Nom d'organisation unique pour votre répertoire qui sera utilisé pour enregistrer les appareils clients.

   Ce champ n'est disponible que si vous créez votre répertoire dans le cadre du lancement WorkSpaces.

   Nom de DNS de l'annuaire

   Nom complet de l'annuaire, par exemple `corp.example.com`.

   Nom NetBIOS de l'annuaire

   Nom court de l'annuaire, par exemple `CORP`.

   Mot de passe administrateur

   Mot de passe de l'administrateur de l'annuaire. Le processus de création du répertoire crée un compte administrateur avec le nom d'utilisateur `Administrator` et ce mot de passe.

   Le mot de passe de l'administrateur de l'annuaire est sensible à la casse et doit comporter entre 8 et 64 caractères (inclus). Il doit également contenir au moins un caractère de trois des quatre catégories suivantes :

   - Lettres minuscules (a-z)
   - Lettres majuscules (A-Z)
   - Chiffres (0-9)
   - Caractères non alphanumériques (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirmer le mot de passe

Saisissez à nouveau le mot de passe de l'administrateur.

Description de l'annuaire

Description facultative de l'annuaire.

4. Sur la page Choose VPC and subnets (Choisir un VPC et des sous-réseaux), indiquez les informations suivantes, puis choisissez Next (Suivant).

   VPC

   VPC de l'annuaire.

   Sous-réseaux

   Choisissez les sous-réseaux pour les contrôleurs de domaine. Les deux sous-réseaux doivent être dans des zones de disponibilité différentes.

5. Sur la page Review & create (Vérifier et créer), vérifiez les informations concernant l'annuaire et effectuez les modifications nécessaires. Lorsque les informations sont correctes, choisissez Create directory (Créer l'annuaire). La création de l'annuaire prend plusieurs minutes. Une fois l'annuaire créé, le champ Statut prend la valeur Actif.

Bonnes pratiques pour Simple AD

Voici quelques suggestions et directives à prendre en compte pour éviter les problèmes et tirer le meilleur parti de Simple AD.

Configuration : prérequis

Pensez à utiliser ces consignes avant de créer votre annuaire.

Vérifiez que vous avez le type d'annuaire approprié

AWS Directory Service propose plusieurs méthodes d'utilisation Microsoft Active Directory avec d'autres AWS services. Vous pouvez choisir le service d'annuaire doté des fonctionnalités dont vous avez besoin à un prix adapté à votre budget :

- AWS Directory Service pour Microsoft Active Directory est un service géré riche en fonctionnalités Microsoft Active Directory hébergé sur le AWS cloud. AWS Managed Microsoft AD est votre

meilleur choix si vous avez plus de 5 000 utilisateurs et que vous avez besoin d'établir une relation de confiance entre un annuaire AWS hébergé et vos annuaires locaux.

- AD Connector connecte simplement votre site existant Active Directory à AWS. AD Connector est votre meilleur allié si vous souhaitez utiliser votre annuaire sur site existant avec les services AWS .
- Simple AD est un annuaire à petite échelle et à faible coût doté d'une Active Directory compatibilité de base. Il prend en charge jusqu'à 5 000 utilisateurs, des applications compatibles avec Samba 4 et une compatibilité LDAP pour les applications LDAP.

Pour une comparaison plus détaillée des AWS Directory Service options, voirQue choisir ?.

Assurez-vous que vos VPC et instances sont correctement configurés

Pour vous connecter à vos annuaires, les gérer et les utiliser, vous devez configurer correctement les VPC auxquels les annuaires sont associés. Consultez AWS Conditions préalables à la gestion de Microsoft AD, Conditions préalables requises pour AD Connector ou Prérequis pour Simple AD pour obtenir plus d'informations sur les exigences de sécurité et de mise en réseau des VPC.

Si vous ajoutez une instance à votre domaine, assurez-vous de disposer d'une connectivité et d'un accès à distance à votre instance, comme décrit dans Joindre une instance Amazon EC2 à votre compte AWS Microsoft AD géré Active Directory.

Tenez compte des limites

Découvrez les différentes limites applicables à votre type d'annuaire spécifique. Le stockage disponible et la taille globale de vos objets sont les seules limites quant au nombre d'objets que vous pouvez stocker dans votre annuaire. Consultez AWS Quotas Managed Microsoft AD, Quotas AD Connector ou Quotas Simple AD pour plus d'informations sur l'annuaire que vous avez choisi.

Comprenez la configuration et l'utilisation AWS des groupes de sécurité de votre annuaire

AWS crée un groupe de sécurité et l'attache aux interfaces réseau élastiques du contrôleur de domaine de votre annuaire. AWS configure le groupe de sécurité pour bloquer le trafic inutile vers le répertoire et autorise le trafic nécessaire.

Modification du groupe de sécurité de l'annuaire

Si vous souhaitez modifier la sécurité des groupes de sécurité des annuaires, vous pouvez le faire. Effectuez ces modifications uniquement si vous avez entièrement compris le fonctionnement du filtrage des groupes de sécurité. Pour plus d'informations, veuillez consulter la section Amazon EC2 security groups for Linux instances (français non garanti) dans le Guide de l'utilisateur Amazon EC2. Des modifications inappropriées peuvent entraîner une perte de communication avec les ordinateurs et les instances concernés. AWS recommande de ne pas essayer d'ouvrir des ports supplémentaires vers votre répertoire car cela réduit la sécurité de votre répertoire. Veuillez lire attentivement le modèle de responsabilité partagée AWS.

> **Warning**
>
> Vous êtes techniquement en mesure d'associer le groupe de sécurité de l'annuaire à d'autres instances EC2 que vous créez. Il AWS déconseille toutefois cette pratique. AWS peut avoir des raisons de modifier le groupe de sécurité sans préavis pour répondre aux besoins fonctionnels ou de sécurité du répertoire géré. Ces modifications affectent toutes les instances auxquelles vous associez le groupe de sécurité d'annuaire et peuvent interrompre le fonctionnement des instances associées. De plus, l'association du groupe de sécurité de l'annuaire avec vos instances EC2 peut créer un risque de sécurité potentiel pour vos instances EC2.

Utilisez AWS Managed Microsoft AD si des approbations sont requises

Simple AD ne prend pas en charge des relations d'approbation. Si vous devez établir une relation de confiance entre votre AWS Directory Service annuaire et un autre annuaire, vous devez utiliser AWS Directory Service pour Microsoft Active Directory.

Configuration : création de votre annuaire

Voici quelques suggestions à prendre en compte lorsque vous créez votre annuaire.

Rétention de vos ID et mot de passe d'administrateur

Lorsque vous configurez votre annuaire, vous fournissez un mot de passe pour le compte d'administrateur. Cet ID de compte est un administrateur pour Simple AD. Retenez le mot de passe créé pour ce compte, sinon vous ne serez pas en mesure d'ajouter des objets à votre annuaire.

Comprendre les restrictions relatives aux noms d'utilisateur pour AWS les applications

AWS Directory Service prend en charge la plupart des formats de caractères pouvant être utilisés dans la construction des noms d'utilisateur. Cependant, certaines restrictions de caractères sont appliquées aux noms d'utilisateur qui seront utilisés pour se connecter à AWS des applications, telles qu'Amazon WorkSpaces WorkDocs WorkMail, Amazon ou Amazon QuickSight. Ces restrictions empêchent l'utilisation des caractères suivants :

- Espaces
- Caractères multioctets
- !"#$%&'()*+,/:;<=>?@[\]^`{|}~

> **Note**
>
> Le symbole @ est autorisé s'il précède un suffixe UPN.

Programmation de vos applications

Avant de programmer vos applications, prenez en compte les éléments suivants :

Utilisez le service de localisation des contrôleurs de domaine de Windows

Lorsque vous développez des applications, utilisez le service de localisation Windows DC ou le service DNS dynamique (DDNS) de votre Managed AWS Microsoft AD pour localiser les contrôleurs de domaine (DC). Ne codez pas en dur les applications avec l'adresse d'un contrôleur de domaine. Le service de localisation des contrôleurs de domaine permet de garantir que l'annuaire est distribué et vous permet de tirer parti de la mise à l'échelle horizontale en ajoutant des contrôleurs de domaine à votre déploiement. Si vous liez votre application à un contrôleur de domaine corrigé et que celui-ci subit une application de correctifs ou une récupération, votre application perdra l'accès au contrôleur de domaine au lieu d'utiliser l'un des contrôleurs de domaine restants. En outre, le codage en dur du contrôleur de domaine peut entraîner la création d'un point chaud sur un seul contrôleur de domaine. Dans des cas extrêmes, la création de ce point chaud peut entraîner une absence de réponse de votre contrôleur de domaine. Dans de tels cas, l'automatisation de l' AWS annuaire peut également signaler le répertoire comme étant altéré et peut déclencher des processus de restauration qui remplacent le contrôleur de domaine qui ne répond pas.

Testez la charge avant de lancer la production

Assurez-vous de procéder à des tests avec des objets et des requêtes représentatifs de votre charge de travail de production afin de confirmer que l'annuaire s'adapte à la charge de travail de votre application. Si vous avez besoin de capacité supplémentaire, vous devez utiliser AWS Directory Service Microsoft Active Directory, qui vous permet d'ajouter des contrôleurs de domaine pour des performances élevées. Pour plus d'informations, consultez Déploiement de contrôleurs de domaine supplémentaires.

Utilisez des requêtes LDAP efficaces

De vastes requêtes LDAP effectuées dans un contrôleur de domaine sur des milliers d'objets peuvent consommer des cycles de processeur considérables sur un seul contrôleur de domaine, ce qui se traduit par la création de points chauds. Ces points chauds peuvent affecter les applications qui partagent le même contrôleur de domaine lors de la requête.

Quotas Simple AD

En général, vous ne devez pas ajouter plus de 500 utilisateurs à un petit annuaire Simple AD et pas plus de 5 000 à un grand annuaire Simple AD. Pour bénéficier d'options de mise à l'échelle plus flexibles et d'autres fonctionnalités Active Directory, envisagez d'utiliser plutôt AWS Service d'annuaire pour Microsoft Active Directory (Standard Edition ou Enterprise Edition).

Voici les quotas par défaut pour Simple AD. Sauf indication contraire, chaque quota est spécifique à une région.

Quotas Simple AD

Ressource	Quota par défaut
Annuaires Simple AD	10
Instantanés manuels *	5 par Simple AD

* Le quota d'instantanés manuels ne peut pas être modifié.

> **Note**
>
> Vous ne pouvez pas attacher une adresse IP publique à votre interface réseau Elastic (ENI) AWS.

Politique de compatibilité des applications pour Simple AD

Simple AD est une implémentation de Samba qui fournit la plupart des fonctionnalités de base d'Active Directory. En raison du grand nombre d'applications commerciales et personnalisées prêtes à l'emploi qui utilisent Active Directory, AWS n'est pas en mesure de vérifier formellement ou de manière systématique la compatibilité des applications tierces avec Simple AD. AWS travaille aux côtés de ses clients pour tenter de surmonter les éventuels défis d'installation d'applications qu'ils sont susceptibles de rencontrer. Cependant, nous ne pouvons pas garantir la compatibilité présente ou future de chaque application avec Simple AD.

Les applications tierces suivantes sont compatibles avec Simple AD :

- Microsoft Internet Information Services (IIS) sur les plateformes suivantes :
  - Windows Server 2003 R2
  - Windows Server 2008 R1
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
- Microsoft SQL Server:
  - SQL Server 2005 R2 (éditions Express, Web et Standard)
  - SQL Server 2008 R2 (éditions Express, Web et Standard)
  - SQL Server 2012 (éditions Express, Web et Standard)
  - SQL Server 2014 (éditions Express, Web et Standard)
- Microsoft SharePoint:
  - SharePoint 2010 Foundation
  - SharePoint 2010 Enterprise
  - SharePoint 2013 Enterprise

Les clients peuvent choisir d'utiliser AWS Service d'annuaire pour Microsoft Active Directory (AWS Microsoft AD géré) pour bénéficier d'un niveau de compatibilité supérieur basé sur Active Directory proprement dit.

Résolution des problèmes de Simple AD

Les sections suivantes peuvent vous aider à résoudre certains problèmes courants que vous pourriez rencontrer lors de la création ou de l'utilisation de votre annuaire.

Rubriques

Récupération d'un mot de passe

Si un utilisateur oublie un mot de passe ou rencontre des difficultés pour se connecter à votre annuaire Simple AD ou AWS Managed Microsoft AD, vous pouvez réinitialiser son mot de passe à l'aide du AWS Management Console, Windows PowerShell ou du AWS CLI.

Pour plus d'informations, consultez Réinitialiser un mot de passe utilisateur.

Je reçois une erreur « KDC ne peut pas traiter l'option demandée » lors de l'ajout d'un utilisateur à Simple AD

Cela peut se produire lorsque le client Samba CLI n'envoie pas correctement les commandes « net » à tous les contrôleurs de domaine. Si ce message d'erreur s'affiche lors de l'utilisation de la commande « net ads » pour ajouter un utilisateur à votre annuaire Simple AD, utilisez l'argument -S

et spécifiez l'adresse IP de l'un de vos contrôleurs de domaine. Si l'erreur persiste, essayez l'autre contrôleur de domaine. Vous pouvez également utiliser les outils d'administration d'Active Directory pour ajouter des utilisateurs à votre annuaire. Pour plus d'informations, consultez Installation des outils d'administration Active Directory pour Simple AD.

Je ne parviens pas à mettre à jour le nom DNS ou l'adresse IP d'une instance jointe à mon domaine (mise à jour dynamique DNS)

Les mises à jour dynamiques DNS ne sont pas prises en charge dans les domaines Simple AD. En revanche, vous pouvez effectuer les modifications directement en connectant votre annuaire à l'aide du Gestionnaire DNS sur une instance qui est jointe à votre domaine.

Je ne peux pas me connecter à SQL Server à l'aide d'un compte SQL Server

Une erreur peut être générée si vous tentez d'utiliser SQL Server Management Studio (SSMS) avec un compte SQL Server pour vous connecter à SQL Server exécuté sur une instance EC2 Windows 2012 R2. Le problème se produit lorsque SSMS s'exécute en tant qu'utilisateur de domaine et peut se traduire par l'erreur « Échec de la connexion pour l'utilisateur », même si les informations d'identification valides sont fournies. Il s'agit d'un problème connu et AWS nous nous efforçons activement de le résoudre.

Pour contourner ce problème, vous pouvez vous connecter à SQL Server avec l'authentification Windows au lieu de l'authentification SQL. Vous pouvez également lancer SSMS en tant qu'utilisateur local et non utilisateur de domaine Simple AD.

Mon annuaire est bloqué à l'état « demandé »

Si vous avez un annuaire qui se trouve à l'état « Demandé » depuis plus de cinq minutes, essayez de supprimer l'annuaire et de le recréer. Si le problème persiste, contactez le Centre AWS Support.

L'erreur « AZ constrained » s'affiche lorsque je crée un annuaire

Certains AWS comptes créés avant 2012 peuvent avoir accès à des zones de disponibilité dans les régions de l'est des États-Unis (Virginie du Nord), de l'ouest des États-Unis (Californie du Nord) ou de l'Asie-Pacifique (Tokyo) qui ne prennent pas en charge AWS Directory Service les annuaires. Si vous voyez une erreur comme celle-ci lors de la création d'un annuaire, choisissez un sous-réseau dans une autre zone de disponibilité et essayez de recréer l'annuaire.

Certains de mes utilisateurs ne peuvent pas s'authentifier avec mon annuaire

Vos comptes d'utilisateur doivent avoir une pré-authentification Kerberos activée. Il s'agit du paramètre par défaut pour les nouveaux comptes d'utilisateur, et il ne doit pas être modifié. Pour plus d'informations sur ce paramètre, consultez la section Préauthentification sur Microsoft TechNet.

Ressources supplémentaires

Les ressources suivantes peuvent vous aider à résoudre les problèmes pendant que vous travaillez avec AWS.

- AWS Centre de connaissances : trouvez des FAQ et des liens vers d'autres ressources pour vous aider à résoudre les problèmes.
- AWS Centre de support : bénéficiez d'une assistance technique.
- AWS Premium Support Center : bénéficiez d'un support technique haut de gamme.

Rubriques

Motifs de statut d'annuaire Simple AD

Lorsqu'un annuaire est dégradé ou ne fonctionne pas, le message de statut de l'annuaire contient des informations supplémentaires. Le message de statut s'affiche dans la console AWS Directory Service ou est retourné dans le membre `DirectoryDescription.StageReason` par l'API `DescribeDirectories`. Pour plus d'informations sur le statut de l'annuaire, consultez Comprendre le statut de votre annuaire.

Voici les messages de statut d'un annuaire Simple AD :

Rubriques

- The critical AWS Directory Service reserved user is disabled
- The main domain controller does not have all FSMO roles
- Domain controller replication failures

L'interface réseau Elastic (ENI) du service d'annuaire n'est pas connectée

Description

L'interface réseau Elastic (ENI) critique créée en votre nom lors de la création de l'annuaire afin d'établir une connectivité réseau avec votre VPC n'est pas attachée à l'instance d'annuaire. Les applications AWS soutenues par cet annuaire ne fonctionneront pas. Votre annuaire ne peut pas se connecter à votre réseau sur site.

Résolution des problèmes

Si l'ENI est détachée, mais existe toujours, contactez AWS Support. Si l'ENI est supprimée, il n'y a aucun moyen de résoudre le problème et votre annuaire est définitivement inutilisable. Vous devez supprimer votre annuaire et en créer un nouveau.

Problèmes détectés par l'instance

Description

Une erreur interne a été détectée par l'instance. Cela signifie généralement que le service de surveillance tente activement de récupérer les instances endommagées.

Résolution des problèmes

Dans la plupart des cas, il s'agit d'un problème temporaire et le répertoire finit par revenir à l'état actif. Si le problème persiste, accédez à AWS Support pour obtenir de l'aide.

The critical AWS Directory Service reserved user is missing from the directory

Description

Lorsqu'un annuaire Simple AD est créé, AWS Directory Service crée un compte de service dans l'annuaire avec le nom `AWSAdmin`*`D-xxxxxxxxxx`*. Cette erreur est générée lorsque ce compte de service est introuvable. Sans ce compte, AWS Directory Service ne peut pas exécuter de fonctions administratives sur l'annuaire, ce qui rend l'annuaire inutilisable.

Résolution des problèmes

Pour résoudre ce problème, restaurez l'annuaire pour revenir à un instantané précédent ayant été créé avant la suppression du compte de service. Des instantanés automatiques de votre annuaire Simple AD sont pris une fois par jour. Si l'instantané a été pris plus de cinq jours après la suppression de ce compte, vous ne pourrez pas restaurer l'annuaire à l'état d'existence du compte. Si vous n'êtes pas en mesure de restaurer l'annuaire à partir d'un instantané où le compte existait, votre annuaire peut devenir définitivement hors d'usage. Si tel est le cas, vous devez supprimer votre annuaire et en créer un nouveau.

The critical AWS Directory Service reserved user needs to belong to the Domain Admins AD group

Description

Lorsqu'un annuaire Simple AD est créé, AWS Directory Service crée un compte de service dans l'annuaire avec le nom `AWSAdmin`*`D-xxxxxxxxx`*. Cette erreur est générée lorsque ce compte de service n'est pas un membre du groupe `Domain Admins`. L'adhésion à ce groupe est nécessaire pour accorder à AWS Directory Service les privilèges nécessaires pour effectuer des opérations de maintenance et de récupération, telles que le transfert des rôles FSMO, la jonction de nouveaux contrôleurs d'annuaire et la restauration à partir d'instantanés.

Résolution des problèmes

Utilisez l'outil Utilisateurs et ordinateurs Active Directory pour ajouter à nouveau le compte de service au groupe `Domain Admins`.

The critical AWS Directory Service reserved user is disabled

Description

Lorsqu'un annuaire Simple AD est créé, AWS Directory Service crée un compte de service dans l'annuaire avec le nom `AWSAdmin`*`D-xxxxxxxxx`*. Cette erreur est générée lorsque ce compte de service est désactivé. Ce compte doit être activé afin que AWS Directory Service puisse effectuer des opérations de maintenance et de récupération dans l'annuaire.

Résolution des problèmes

Utilisez l'outil Utilisateurs et ordinateurs Active Directory pour réactiver le compte de service.

The main domain controller does not have all FSMO roles

Description

Tous les rôles FSMO ne sont pas détenus par le contrôleur d'annuaire Simple AD. AWS Directory Service ne peut pas garantir le comportement et la fonctionnalité si les rôles FSMO ne font pas partie du contrôleur d'annuaire Simple AD approprié.

Résolution des problèmes

Utilisez les outils Active Directory pour redéplacer les rôles FSMO vers le contrôleur de l'annuaire actif original. Pour de plus amples informations sur le déplacement des rôles FSMO, consultez https://docs.microsoft.com/troubleshoot/windows-server/identity/transfer-or-seize-fsmo-roles-in-ad-ds. Si cela ne résout pas le problème, veuillez contacter le AWS Support pour obtenir de l'aide.

Domain controller replication failures

Description

Les contrôleurs d'annuaire Simple AD n'effectuent pas de réplication entre eux. Cela peut être causé par un ou plusieurs des problèmes suivants :

- Les groupes de sécurité des contrôleurs d'annuaire n'ont pas les ports corrects ouverts.
- Les listes ACL réseau sont trop restrictives.
- La table de routage du VPC n'achemine pas correctement le trafic réseau entre les contrôleurs d'annuaire.
- Une autre instance a été promue à un contrôleur de domaine dans l'annuaire.

Résolution des problèmes

Pour plus d'informations sur vos besoins en matière de réseau VPC, consultez AWS Managed Microsoft AD AWS Conditions préalables à la gestion de Microsoft AD, AD Connector Conditions préalables requises pour AD Connector ou Simple AD Prérequis pour Simple AD. Si votre annuaire comporte un contrôleur de domaine inconnu, vous devez le rétrograder. Si la configuration réseau de votre VPC est correcte, mais que l'erreur persiste, veuillez contacter le AWS Support pour obtenir de l'aide.

Sécurité dans AWS Directory Service

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 cette notion par les termes sécurité du cloud et 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 conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Directory Service, consultez la section AWS Services concernés par programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation AWS Directory Service. Les rubriques suivantes expliquent comment procéder à la configuration AWS Directory Service pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos AWS Directory Service ressources.

Rubriques de sécurité

Les rubriques de sécurité suivantes sont disponibles dans cette section :

- Gestion des identités et des accès pour AWS Directory Service
- Connexion et surveillance AWS Directory Service
- Validation de conformité pour AWS Directory Service
- Résilience dans AWS Directory Service
- Sécurité de l'infrastructure dans AWS Directory Service

Rubriques de sécurité supplémentaires

Les rubriques de sécurité supplémentaires suivantes sont disponibles dans ce guide :

Comptes, trusts et accès aux AWS ressources

- Autorisations pour le compte administrateur
- Comptes de service administrés de groupe
- Création d'une relation d'approbation
- Délégation Kerberos contrainte
- Accorder aux utilisateurs et aux groupes l'accès aux ressources AWS
- Autorisation pour AWS les applications et les services utilisant AWS Directory Service

Sécurisation de votre annuaire

- Sécuriser votre annuaire AWS Managed Microsoft AD
- Sécurisation de votre annuaire AD Connector

Journalisation et surveillance

- Surveiller votre AWS Managed Microsoft AD
- Surveillance de votre annuaire AD Connector

Résilience

- Application de correctifs et maintenance pour AWS Managed Microsoft AD

Gestion des identités et des accès pour AWS Directory Service

L'accès à AWS Directory Service nécessite des informations d'identification qui AWS peuvent être utilisées pour authentifier vos demandes. Ces informations d'identification doivent être autorisées à accéder à AWS des ressources, telles qu'un AWS Directory Service annuaire. Les sections suivantes fournissent des informations détaillées sur la manière dont vous pouvez utiliser AWS Identity and Access Management (IAM) et vous aider AWS Directory Service à sécuriser vos ressources en contrôlant les personnes autorisées à y accéder :

- Authentification

- Contrôle d'accès

Authentification

Découvrez comment accéder à l' AWS aide des identités IAM.

Contrôle d'accès

Vous pouvez disposer d'informations d'identification valides pour authentifier vos demandes, mais vous ne pouvez pas créer de AWS Directory Service ressources ou y accéder sans autorisation. Par exemple, vous devez être autorisé à créer un AWS Directory Service répertoire ou à créer un instantané de répertoire.

Les sections suivantes décrivent comment gérer les autorisations pour AWS Directory Service. Nous vous recommandons de lire d'abord la présentation.

- Vue d'ensemble de la gestion des autorisations d'accès à vos AWS Directory Service ressources
- Utilisation de politiques basées sur l'identité (politiques IAM) pour AWS Directory Service
- AWS Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions

Vue d'ensemble de la gestion des autorisations d'accès à vos AWS Directory Service ressources

Chaque AWS ressource appartient à un AWS compte, et les autorisations de création ou d'accès aux ressources sont régies par des politiques d'autorisation. Un administrateur de compte peut associer des politiques d'autorisations aux identités IAM (c'est-à-dire aux utilisateurs, aux groupes et aux rôles), et certains services (tels que AWS Lambda) prennent également en charge l'attachement de politiques d'autorisations aux ressources.

> **Note**
>
> Un administrateur de compte (ou utilisateur administrateur) est un utilisateur doté des privilèges d'administrateur. Pour plus d'informations, consultez Bonnes pratiques IAM dans le Guide de l'utilisateur IAM.

Rubriques

AWS Directory Service ressources et opérations

Dans AWS Directory Service, la ressource principale est un répertoire. AWS Directory Service prend également en charge les ressources de capture d'annuaire. Cependant, vous pouvez créer des instantanés uniquement dans le cadre d'un annuaire existant. Par conséquent, un instantané est appelé sous-ressource.

Ces ressources ont des noms ARN (Amazon Resource Name) uniques qui leur sont associés, comme cela est illustré dans la table suivante.

Type de ressource	Format ARN
Annuaire	`arn:aws:ds:` *`region`*`:`*`account-id`* `:directory/` *`external-directory-id`*
Instantané	`arn:aws:ds:` *`region`*`:`*`account-id`* `:snapshot/` *`external-snapshot-id`*

AWS Directory Service fournit un ensemble d'opérations permettant de travailler avec les ressources appropriées. Pour obtenir la liste des opérations disponibles, veuillez consulter Directory Service Actions (français non garanti).

Présentation de la propriété des ressources

Le propriétaire d'une ressource est le AWS compte qui a créé une ressource. En d'autres termes, le propriétaire de la ressource est le AWS compte de l'entité principale (le compte root, un utilisateur IAM ou un rôle IAM) qui authentifie la demande qui crée la ressource. Les exemples suivants illustrent comment cela fonctionne :

- Si vous utilisez les informations d'identification du compte root de votre AWS compte pour créer une AWS Directory Service ressource, telle qu'un répertoire, votre AWS compte est le propriétaire de cette ressource.
- Si vous créez un utilisateur IAM dans votre AWS compte et que vous accordez des autorisations pour créer AWS Directory Service des ressources à cet utilisateur, celui-ci peut également créer des AWS Directory Service ressources. Cependant, votre AWS compte, auquel appartient l'utilisateur, est propriétaire des ressources.
- Si vous créez un rôle IAM dans votre AWS compte avec les autorisations nécessaires pour créer AWS Directory Service des ressources, toute personne pouvant assumer ce rôle peut créer des AWS Directory Service ressources. Votre AWS compte, auquel appartient le rôle, possède les AWS Directory Service ressources.

Gestion de l'accès aux ressources

Une politique d'autorisation décrit qui a accès à quoi. La section suivante explique les options disponibles pour créer des politiques d'autorisations.

> **Note**
>
> Cette section décrit l'utilisation d'IAM dans le contexte de AWS Directory Service. Elle ne fournit pas d'informations détaillées sur le service IAM. Pour une documentation complète sur IAM, veuillez consulter la section What is IAM? (français non garanti) dans le Guide de l'utilisateur IAM. Pour plus d'informations sur la syntaxe et les descriptions des politiques IAM, veuillez consulter IAM JSON policy reference (français non garanti) dans le Guide de l'utilisateur IAM.

Les politiques associées à une identité IAM sont appelées politiques basées sur l'identité (politiques IAM) et les politiques associées à une ressource sont appelées politiques basées sur les ressources. AWS Directory Service prend uniquement en charge les politiques basées sur l'identité (politiques IAM).

Rubriques

- Politiques basées sur une identité (politiques IAM)
- Politiques basées sur les ressources

Politiques basées sur une identité (politiques IAM)

Vous pouvez attacher des politiques à des identités IAM. Par exemple, vous pouvez effectuer les opérations suivantes :

- Associer une politique d'autorisation à un utilisateur ou à un groupe de votre compte : un administrateur de compte peut utiliser une politique d'autorisation associée à un utilisateur particulier pour autoriser cet utilisateur à créer une AWS Directory Service ressource, telle qu'un nouveau répertoire.
- Attacher une politique d'autorisations à un rôle (accorder des autorisations entre comptes) : vous pouvez attacher une politique d'autorisation basée sur une identité à un rôle IAM afin d'accorder des autorisations entre comptes.

  Pour plus d'informations sur l'utilisation d'IAM pour déléguer des autorisations, veuillez consulter la section Access management (français non garanti) dans le Guide de l'utilisateur IAM.

La politique d'autorisation suivante accorde des autorisations à un utilisateur lui permettant d'exécuter toutes les actions commençant par `Describe`. Ces actions affichent des informations sur une AWS Directory Service ressource, telle qu'un répertoire ou un instantané. Notez que le caractère générique (*) dans l'`Resource`élément indique que les actions sont autorisées pour toutes les AWS Directory Service ressources détenues par le compte.

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

Pour plus d'informations sur l'utilisation de politiques basées sur l'identité avec AWS Directory Service, consultez. Utilisation de politiques basées sur l'identité (politiques IAM) pour AWS Directory Service Pour plus d'informations sur les utilisateurs, les groupes, les rôles et les autorisations, consultez Identités (utilisateurs, groupes et rôles) dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

D'autres services, tels qu'Amazon S3, prennent également en charge les politiques d'autorisation basées sur une ressource. Par exemple, vous pouvez associer une politique à un compartiment S3 pour gérer les autorisations d'accès à ce compartiment. AWS Directory Service ne prend pas en charge les politiques basées sur les ressources.

Spécification des éléments d'une politique : actions, effets, ressources et principaux

Pour chaque AWS Directory Service ressource, le service définit un ensemble d'opérations d'API. Pour plus d'informations, consultez AWS Directory Service ressources et opérations. Pour obtenir la liste des opérations d'API disponibles, veuillez consulter Directory Service Actions (français non garanti).

Pour accorder des autorisations pour ces opérations d'API AWS Directory Service , définissez un ensemble d'actions que vous pouvez spécifier dans une politique. Notez que l'exécution d'une opération d'API peut exiger des autorisations pour plusieurs actions.

Voici les éléments de base d'une politique :

- Ressource : dans une politique, vous utilisez un Amazon Resource Name (ARN) pour identifier la ressource à laquelle la politique s'applique. Pour les AWS Directory Service ressources, vous utilisez toujours le caractère générique (*) dans les politiques IAM. Pour plus d'informations, consultez AWS Directory Service ressources et opérations.
- Action : vous utilisez des mots clés d'action pour identifier les opérations de ressource que vous voulez accorder ou refuser. Par exemple, l'autorisation `ds:DescribeDirectories` permet à l'utilisateur d'effectuer l'opération AWS Directory Service `DescribeDirectories`.
- Effet – Vous spécifiez l'effet produit lorsque l'utilisateur demande l'action spécifique. Il peut s'agir d'un accord ou d'un refus. Si vous n'accordez pas explicitement l'accès pour (autoriser) une ressource, l'accès est implicitement refusé. Vous pouvez aussi explicitement refuser l'accès à une ressource, ce que vous pouvez faire afin de vous assurer qu'un utilisateur n'y a pas accès, même si une politique différente accorde l'accès.
- Principal – dans les politiques basées sur une identité (politiques IAM), l'utilisateur auquel la politique est attachée est le principal implicite. Pour les politiques basées sur les ressources, vous spécifiez l'utilisateur, le compte, le service ou toute autre entité pour lequel vous souhaitez recevoir des autorisations (s'applique uniquement aux politiques basées sur les ressources). AWS Directory Service ne prend pas en charge les politiques basées sur les ressources.

Pour plus d'informations sur la syntaxe des politiques IAM et pour obtenir des descriptions, veuillez consulter IAM JSON policy reference (français non garanti) dans le manuel Guide de l'utilisateur IAM.

Pour un tableau présentant toutes les actions d' AWS Directory Service API et les ressources auxquelles elles s'appliquent, consultezAWS Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions.

Spécification de conditions dans une politique

Lorsque vous accordez des autorisations, vous pouvez utiliser le langage de la politique d'accès pour spécifier les conditions définissant quand une politique doit prendre effet. Par exemple, il est possible d'appliquer une politique après seulement une date spécifique. Pour plus d'informations sur la spécification de conditions dans un langage de politique, consultez Condition dans le Guide de l'utilisateur IAM.

Pour exprimer des conditions, vous utilisez des clés de condition prédéfinies. Il n'existe pas de clés de condition spécifiques à AWS Directory Service. Cependant, il existe des clés de AWS condition que vous pouvez utiliser selon les besoins. Pour obtenir la liste complète des AWS clés, consultez la section Clés de condition globales disponibles dans le guide de l'utilisateur IAM.

Utilisation de politiques basées sur l'identité (politiques IAM) pour AWS Directory Service

Cette rubrique fournit des exemples de politiques basées sur une identité dans lesquelles un administrateur de compte peut attacher des politiques d'autorisation aux identités IAM (c'est-à-dire aux utilisateurs, groupes et rôles).

> **Important**
>
> Nous vous recommandons de consulter d'abord les rubriques d'introduction qui expliquent les concepts de base et les options disponibles pour gérer l'accès à vos AWS Directory Service ressources. Pour plus d'informations, consultez Vue d'ensemble de la gestion des autorisations d'accès à vos AWS Directory Service ressources.

Les sections de cette rubrique couvrent les sujets suivants :

- Autorisations requises pour utiliser la AWS Directory Service console

- AWS politiques gérées (prédéfinies) pour AWS Directory Service
- Exemples de politiques gérées par le client
- Utilisation des balises avec des politiques IAM

Un exemple de politique d'autorisation est exposé ci-dessous.

```
{
   "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDsEc2IamGetRole",
            "Effect": "Allow",
            "Action": [
                "ds:CreateDirectory",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeVpcs",
                "ec2:CreateSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeSubnets",
                "iam:GetRole"
            ],
            "Resource": "*"
        },
        {
            "Sid": "WarningAllowsCreatingRolesWithDirSvcPrefix",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::111122223333:role/DirSvc*"
        },
        {
            "Sid": "AllowPassRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "cloudwatch.amazonaws.com"
                }
            }
        }
    ]
}
```

La politique comprend les éléments suivants :

- La première instruction autorise la création d'un AWS Directory Service répertoire. AWS Directory Service ne prend pas en charge les autorisations pour cette action particulière au niveau des ressources. Par conséquent, la politique spécifie un caractère générique (*) comme étant la valeur `Resource`.
- La deuxième instruction accorde des autorisations à certaines actions IAM. L'accès aux actions IAM est nécessaire pour AWS Directory Service pouvoir lire et créer des rôles IAM en votre nom. Le caractère générique (*) à la fin de la valeur `Resource` signifie que l'instruction accepte les autorisations pour les actions IAM sur n'importe quel rôle IAM. Pour limiter cette autorisation à un rôle spécifique, remplacez le caractère générique (*) dans la ressource ARN par un nom de rôle spécifique. Pour plus d'informations, veuillez consulter IAM Actions (français non garanti).
- La troisième déclaration accorde des autorisations à un ensemble spécifique de ressources Amazon EC2 nécessaires à la création, à la configuration et AWS Directory Service à la destruction de ses répertoires. Le caractère générique (*) à la fin de la valeur `Resource` signifie que l'instruction accepte les autorisations pour les actions EC2 sur n'importe quelle ressource ou sous-ressource EC2. Pour limiter cette autorisation à un rôle spécifique, remplacez le caractère générique (*) dans la ressource ARN par une ressource ou sous-ressource. Pour plus d'informations, veuillez consulter la page Amazon EC2 Actions (français non garanti).

La politique ne spécifie pas l'élément `Principal`, car dans une politique basée sur une identité, vous ne spécifiez pas le principal qui obtient l'autorisation. Quand vous attachez une politique à un utilisateur, l'utilisateur est le principal implicite. Lorsque vous attachez une politique d'autorisation à un rôle IAM, le principal identifié dans la politique d'approbation de ce rôle obtient les autorisations.

Pour un tableau présentant toutes les actions d' AWS Directory Service API et les ressources auxquelles elles s'appliquent, consultezAWS Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions.

Autorisations requises pour utiliser la AWS Directory Service console

Pour qu'un utilisateur puisse utiliser la AWS Directory Service console, il doit disposer des autorisations répertoriées dans la politique précédente ou des autorisations accordées par le rôle d'accès complet du service d'annuaire ou le rôle de lecture seule du service d'annuaire, décrits dansAWS politiques gérées (prédéfinies) pour AWS Directory Service.

Si vous créez une politique IAM plus restrictive que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les utilisateurs dotés de cette politique IAM.

AWS politiques gérées (prédéfinies) pour AWS Directory Service

AWS répond à de nombreux cas d'utilisation courants en fournissant des politiques IAM autonomes créées et administrées par. AWS Les politiques gérées octroient les autorisations requises dans les cas d'utilisation courants et vous évitent d'avoir à réfléchir aux autorisations qui sont requises. Pour plus d'informations, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

Les politiques AWS gérées suivantes, que vous pouvez associer aux utilisateurs de votre compte, sont spécifiques à AWS Directory Service :

- AWSDirectoryServiceReadOnlyAccess— Accorde à un utilisateur ou à un groupe un accès en lecture seule à toutes les AWS Directory Service ressources, aux sous-réseaux EC2, aux interfaces réseau EC2 et aux rubriques et abonnements Amazon Simple Notification Service (Amazon SNS) pour le compte root. AWS Pour plus d'informations, consultez Utilisation des stratégies gérées AWS avec AWS Directory Service.
- AWSDirectoryServiceFullAccess : accorde à un utilisateur ou à un groupe les éléments suivants :
  - Accès complet à AWS Directory Service
  - Accès aux principaux services Amazon EC2 requis pour utiliser AWS Directory Service
  - Possibilité de répertorier les rubriques Amazon SNS
  - Possibilité de créer, gérer et supprimer des rubriques Amazon SNS dont le nom commence par « » DirectoryMonitoring

  Pour plus d'informations, consultez Utilisation des stratégies gérées AWS avec AWS Directory Service.

En outre, d'autres politiques AWS gérées peuvent être utilisées avec d'autres rôles IAM. Ces politiques sont attribuées aux rôles associés aux utilisateurs de votre AWS Directory Service annuaire. Ces politiques sont nécessaires pour que ces utilisateurs aient accès à d'autres AWS

ressources, telles qu'Amazon EC2. Pour plus d'informations, consultez Accorder aux utilisateurs et aux groupes l'accès aux ressources AWS.

Vous pouvez également créer des politiques IAM personnalisées qui autorisent les utilisateurs à accéder aux ressources et aux actions d'API requises. Vous pouvez attacher ces politiques personnalisées aux utilisateurs ou groupes IAM qui nécessitent ces autorisations.

Exemples de politiques gérées par le client

Dans cette section, vous trouverez des exemples de politiques utilisateur qui accordent des autorisations pour diverses AWS Directory Service actions.

> **Note**
>
> Tous les exemples utilisent la région USA Ouest (Oregon) (`us-west-2`) et contiennent des ID de compte fictifs.

Exemples

- Exemple 1 : Autoriser un utilisateur à effectuer n'importe quelle action de description sur n'importe quelle AWS Directory Service ressource
- Exemple 2 : Permettre à un utilisateur de créer un annuaire

Exemple 1 : Autoriser un utilisateur à effectuer n'importe quelle action de description sur n'importe quelle AWS Directory Service ressource

La politique d'autorisation suivante accorde des autorisations à un utilisateur lui permettant d'exécuter toutes les actions commençant par `Describe`. Ces actions affichent des informations sur une AWS Directory Service ressource, telle qu'un répertoire ou un instantané. Notez que le caractère générique (*) dans l'`Resource`élément indique que les actions sont autorisées pour toutes les AWS Directory Service ressources détenues par le compte.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ds:Describe*",
         "Resource":"*"
```

```
      }
   ]
}
```

Exemple 2 : Permettre à un utilisateur de créer un annuaire

La politique d'autorisations suivante accorde des autorisations pour permettre à un utilisateur de créer un annuaire et toutes les autres ressources connexes, telles que les instantanés et les approbations. Pour ce faire, les autorisations pour certains services Amazon EC2 sont également requises.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                "ds:Create*",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
                  ],
         "Resource":"*"
         ]
      }
   ]
}
```

Utilisation des balises avec des politiques IAM

Vous pouvez appliquer des autorisations au niveau des ressources basées sur des balises dans les politiques IAM que vous utilisez pour la plupart des actions d'API. AWS Directory Service Vous bénéficiez ainsi d'un meilleur contrôle sur les ressources qu'un utilisateur peut créer, modifier ou utiliser. Vous pouvez utiliser l'élément `Condition` (également appelé bloc `Condition`) avec les

clés et valeurs de contexte de condition suivantes dans une politique IAM pour contrôler l'accès des utilisateurs (autorisations) en fonction des balises d'une ressource :

- Utilisez `aws:ResourceTag/`**`tag-key`**: **`tag-value`** pour accorder ou refuser aux utilisateurs des actions sur des ressources ayant des balises spécifiques.
- Utilisez `aws:ResourceTag/`**`tag-key`**: **`tag-value`** pour exiger qu'une balise spécifique soit utilisée (ou ne soit pas utilisée) lorsque vous effectuez une demande d'API pour créer ou modifier une ressource qui autorise les balises.
- Utilisez `aws:TagKeys`: [**`tag-key`**, ...] pour exiger qu'un ensemble de clés de balise spécifique soit utilisé (ou ne soit pas utilisé) lorsque vous effectuez une demande d'API pour créer ou modifier une ressource qui autorise les balises.

> **Note**
>
> Les clés et les valeurs de contexte de condition dans une politique IAM s'appliquent uniquement aux actions AWS Directory Service dans lesquelles un identifiant pour une ressource pouvant être balisée est un paramètre obligatoire.

La section Contrôle de l'accès à l'aide de balises dans le Guide d'utilisateur IAM contient des informations supplémentaires sur l'utilisation des balises. La section Référence de politique JSON IAM de ce guide fournit la syntaxe détaillée, des descriptions, ainsi que des exemples des éléments, des variables et de la logique d'évaluation des politiques JSON dans IAM.

L'exemple de politique de balise suivant autorise tous les appels `ds` tant qu'ils contiennent la paire de clés de balise « `fooKey` »:« `fooValue` ».

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "ds:*"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
```

```
                "aws:ResourceTag/fooKey":"fooValue"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:*"
         ],
         "Resource":"*"
      }
   ]
}
```

L'exemple de politique de ressource suivant autorise tous les appels `ds` tant que la ressource contient l'ID d'annuaire « `d-1234567890` ».

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "ds:*"
         ],
         "Resource":"arn:aws:ds:us-east-1:123456789012:directory/d-1234567890"
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:*"
         ],
         "Resource":"*"
      }
   ]
}
```

Pour plus d'informations sur les ARN, consultez Amazon Resource Names (ARN) et AWS Service Namespaces.

La liste suivante des opérations d' AWS Directory Service API prend en charge les autorisations au niveau des ressources basées sur des balises :

- AcceptSharedDirectory
- AddIpRoutes
- AddTagsToResource
- CancelSchemaExtension
- CreateAlias
- CreateComputer
- CreateConditionalForwarder
- CreateSnapshot
- CreateLogSubscription
- CreateTrust
- DeleteConditionalForwarder
- DeleteDirectory
- DeleteLogSubscription
- DeleteSnapshot
- DeleteTrust
- DeregisterEventTopic
- DescribeConditionalForwarders
- DescribeDomainControllers
- DescribeEventTopics
- DescribeSharedDirectories
- DescribeSnapshots
- DescribeTrusts
- DisableRadius
- DisableSso
- EnableRadius
- EnableSso
- GetSnapshotLimits
- ListIpRoutes
- ListSchemaExtensions
- ListTagsForResource

- RegisterEventTopic
- RejectSharedDirectory
- RemoveIpRoutes
- RemoveTagsFromResource
- ResetUserPassword
- RestoreFromSnapshot
- ShareDirectory
- StartSchemaExtension
- UnshareDirectory
- UpdateConditionalForwarder
- UpdateNumberOfDomainControllers
- UpdateRadius
- UpdateTrust
- VerifyTrust

AWS Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions

Lorsque vous configurez des politiques d'autorisation d'écriture et de Contrôle d'accès que vous pouvez attacher à une entité IAM (politiques basées sur une identité), vous pouvez utiliser le tableau AWS Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions comme référence. Chaque entrée d'API du inclut les éléments suivants :

- Nom de l'opération AWS Directory Service d'API
- Actions correspondantes pour lesquelles vous pouvez accorder des autorisations pour effectuer l'action
- La AWS ressource pour laquelle vous pouvez accorder les autorisations

Vous spécifiez les actions dans le champ `Action` de la politique, ainsi que la valeur des ressources dans le champ `Resource` de la politique. Pour indiquer une action, utilisez le préfixe `ds:` suivi du nom de l'opération d'API (par exemple, `ds:CreateDirectory`). Certaines AWS applications peuvent nécessiter l'utilisation d'opérations d' AWS Directory Service API non publiques telles

queds:AuthorizeApplication,ds:CheckAlias,ds:CreateIdentityPoolDirectory,ds:GetAuth et ds:UnauthorizeApplication dans leurs politiques.

Certaines AWS Directory Service API ne peuvent être appelées que via le AWS Management Console. Ce ne sont pas des API publiques, dans le sens où elles ne peuvent pas être appelées par programmation, et elles ne sont fournies par aucun SDK. Ils acceptent les informations d'identification des utilisateurs. Ces opérations d'API incluent ds:DisableRoleAccessds:EnableRoleAccess, etds:UpdateDirectory.

Vous pouvez utiliser des clés de condition AWS globales dans vos AWS Directory Service politiques pour exprimer des conditions. Pour obtenir la liste complète des AWS clés, consultez la section Clés de condition globale disponibles dans le guide de l'utilisateur IAM.

Rubriques connexes

- Contrôle d'accès

Autorisation pour AWS les applications et les services utilisant AWS Directory Service

Autoriser une AWS application sur un Active Directory

AWS Directory Service accorde des autorisations spécifiques aux applications sélectionnées afin qu'elles s'intègrent parfaitement à votre Active Directory lorsque vous autorisez une AWS application. AWS les applications ne reçoivent que l'accès nécessaire à leur cas d'utilisation. L'ensemble des autorisations internes accordées aux applications et aux administrateurs d'applications après autorisation est fourni ci-dessous :

> **Note**
>
> L'ds:AuthorizationApplicationautorisation est requise pour autoriser une nouvelle AWS application Active Directory. Les autorisations relatives à cette action ne doivent être accordées qu'aux administrateurs qui configurent les intégrations avec Directory Service.

- Accès en lecture aux données des utilisateurs, des groupes, des unités organisationnelles, des ordinateurs ou des autorités de certification Active Directory dans toutes les unités organisationnelles (UO) des annuaires AWS Managed Microsoft AD, Simple AD, AD Connector,

ainsi que dans les domaines approuvés pour AWS Managed Microsoft AD si une relation de confiance l'autorise.

- Accès en écriture aux utilisateurs, aux groupes, aux membres de groupes, aux ordinateurs ou aux données d'autorité de certification dans votre unité organisationnelle de AWS Managed Microsoft AD. Accès en écriture à toutes les UO de Simple AD.
- Authentification et gestion de session des utilisateurs d'Active Directory pour tous les types d'annuaires.

Certaines applications Microsoft AD AWS gérées, telles qu'Amazon RDS et Amazon FSx, s'intègrent via une connexion réseau directe à votre Active Directory. Dans ce cas, les interactions d'annuaire utilisent des protocoles Active Directory natifs tels que LDAP et Kerberos. Les autorisations de ces AWS applications sont contrôlées par un compte utilisateur d'annuaire créé dans l'unité organisationnelle AWS réservée (UO) lors de l'autorisation de l'application, qui inclut la gestion du DNS et l'accès complet à une unité d'organisation personnalisée créée pour l'application. Pour utiliser ce compte, l'application doit être autorisée à agir `ds:GetAuthorizedApplicationDetails` via les informations d'identification de l'appelant ou un rôle IAM.

Pour plus d'informations sur les autorisations d' AWS Directory Service API, consultezAWS Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions.

Pour plus d'informations sur l'activation AWS des applications et des services pour AWS Managed Microsoft AD, consultezPermettre l'accès aux AWS applications et aux services. Pour plus d'informations sur l'activation AWS des applications et des services pour AD Connector, consultezPermettre l'accès aux AWS applications et aux services. Pour plus d'informations sur l'activation AWS des applications et des services pour Simple AD, consultezPermettre l'accès aux AWS applications et aux services.

Annulation de l'autorisation d'une AWS application sur un Active Directory

Pour supprimer les autorisations permettant à une AWS application d'accéder à Active Directory, l'`ds:UnauthorizedApplication`autorisation est requise. Suivez les étapes indiquées par l'application pour la désactiver.

Connexion et surveillance AWS Directory Service

La bonne pratique consiste à surveiller votre organisation pour vous assurer que les modifications sont journalisées. Cela vous permet de vous assurer que tout changement inattendu peut être étudié et que les modifications indésirables peuvent être annulées. AWS Directory Service prend

actuellement en charge les deux AWS services suivants afin que vous puissiez surveiller votre organisation et les activités qui s'y déroulent.

- Amazon CloudWatch - Vous pouvez utiliser CloudWatch Events avec le type d'annuaire AWS Managed Microsoft AD. Pour plus d'informations, consultez Activer le transfert de journaux. En outre, vous pouvez utiliser CloudWatch les métriques pour surveiller les performances du contrôleur de domaine. Pour plus d'informations, consultez Déterminez quand ajouter des contrôleurs de domaine avec des CloudWatch métriques.
- AWS CloudTrail - Vous pouvez l'utiliser CloudTrail avec tous les types de AWS Directory Service répertoires. Pour plus d'informations, consultez la section Journalisation des appels d' AWS Directory Service API avec CloudTrail.

Validation de conformité pour AWS Directory Service

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.

Résilience dans AWS Directory Service

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité 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.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Outre l'infrastructure AWS mondiale, AWS Directory Service offre la possibilité de prendre des instantanés manuels des données à tout moment pour répondre à vos besoins en matière de résilience et de sauvegarde des données. Pour plus d'informations, consultez Création d'un instantané ou d'une restauration de votre annuaire.

Sécurité de l'infrastructure dans AWS Directory Service

En tant que service géré, AWS Directory Service il est protégé par les procédures de sécurité du réseau AWS mondial décrites dans le livre blanc Amazon Web Services : présentation des processus de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder AWS Directory Service via le réseau. Les clients doivent prendre en charge le protocole TLS (Transport Layer Security). Nous recommandons TLS 1.2 ou version ultérieure. Les clients doivent aussi prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

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 en savoir plus sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, veuillez consulter Federal information processing standard (FIPS) 140-2 (français non garanti).

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.

Prévention du cas de figure de l'adjoint désorienté entre services

Le problème de député confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à le faire. En AWS, l'usurpation d'identité interservices peut entraîner la confusion des adjoints. L'usurpation d'identité entre services peut se produire lorsqu'un service (le service appelant) appelle un autre service (le

service appelé). Le service appelant peut être manipulé et ses autorisations utilisées pour agir sur les ressources d'un autre client auxquelles on ne serait pas autorisé d'accéder autrement. Pour éviter cela, AWS fournit des outils qui vous aident à protéger vos données pour tous les services avec des principaux de service qui ont eu accès aux ressources de votre compte.

Nous recommandons d'utiliser les clés contextuelles de condition `aws:SourceAccount`globale `aws:SourceArn`et les clés contextuelles dans les politiques de ressources afin de limiter les autorisations que AWS Directory Service for Microsoft Active Directory accorde à un autre service à la ressource. Si la valeur `aws:SourceArn` ne contient pas l'ID du compte, tel qu'un ARN de compartiment Amazon S3, vous devez utiliser les deux clés de contexte de condition globale pour limiter les autorisations. Si vous utilisez les deux clés de contexte de condition globale et que la valeur `aws:SourceArn` contient l'ID de compte, la valeur `aws:SourceAccount` et le compte dans la valeur `aws:SourceArn` doivent utiliser le même ID de compte lorsqu'ils sont utilisés dans la même instruction de politique. Utilisez `aws:SourceArn` si vous souhaitez qu'une seule ressource soit associée à l'accès entre services. Utilisez `aws:SourceAccount` si vous souhaitez autoriser l'association d'une ressource de ce compte à l'utilisation interservices.

Dans l'exemple suivant, la valeur de `aws:SourceArn` doit être un groupe de CloudWatch journaux.

Le moyen le plus efficace de se protéger contre le problème de député confus consiste à utiliser la clé de contexte de condition globale `aws:SourceArn` avec l'ARN complet de la ressource. Si vous ne connaissez pas l'ARN complet de la ressource ou si vous spécifiez plusieurs ressources, utilisez la clé de contexte de condition globale `aws:SourceArn` avec des caractères génériques (*) pour les parties inconnues de l'ARN. Par exemple, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

L'exemple suivant montre comment utiliser les clés contextuelles `aws:SourceArn` et les clés de contexte de condition `aws:SourceAccount` globale dans AWS Managed Microsoft AD pour éviter le problème de confusion des adjoints.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
```

```
            ],
    "Resource": [
      "arn:aws:logs:YOUR_REGION:YOUR_ACCOUNT_NUMBER:log-group:/aws/
directoryservice/YOUR_LOG_GROUP:*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
 "arn:aws:ds:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Dans l'exemple suivant, la valeur de `aws:SourceArn` doit être une rubrique SNS de votre compte. Par exemple, vous pouvez utiliser quelque chose comme `arn:aws:sns:ap-southeast-1:123456789012:DirectoryMonitoring_d-966739499f` « ap-southeast-1 » correspondant à votre région, « 123456789012 » à votre identifiant client et « _d-966739499f » au nom de rubrique Amazon SNS que vous avez créé. DirectoryMonitoring

Le moyen le plus efficace de se protéger contre le problème de député confus consiste à utiliser la clé de contexte de condition globale `aws:SourceArn` avec l'ARN complet de la ressource. Si vous ne connaissez pas l'ARN complet de la ressource ou si vous spécifiez plusieurs ressources, utilisez la clé de contexte de condition globale `aws:SourceArn` avec des caractères génériques (*) pour les parties inconnues de l'ARN. Par exemple, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

L'exemple suivant montre comment utiliser les clés contextuelles `aws:SourceArn` et les clés de contexte de condition `aws:SourceAccount` globale dans AWS Managed Microsoft AD pour éviter le problème de confusion des adjoints.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": ["SNS:GetTopicAttributes",
```

```
      "SNS:SetTopicAttributes",
         "SNS:AddPermission",
      "SNS:RemovePermission",
      "SNS:DeleteTopic",
      "SNS:Subscribe",
      "SNS:ListSubscriptionsByTopic",
      "SNS:Publish"],
    "Resource": [
      "arn:aws:sns:YOUR_REGION:YOUR_ACCOUNT_NUMBER:YOUR_SNS_TOPIC_NAME"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
 "arn:aws:sns:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_EXTERNAL_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

L'exemple suivant montre une politique d'approbations IAM pour un rôle auquel l'accès à la console a été délégué. La valeur de `aws:SourceArn` doit être une ressource d'annuaire de votre compte. Pour plus d'informations, consultez la section Types de ressources définis par AWS Directory Service. Par exemple, vous pouvez utiliser `arn:aws:ds:us-east-1:123456789012:directory/d-1234567890`, où `123456789012` correspond à votre identifiant client et `d-1234567890` à votre identifiant d'annuaire.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": [
                "sts:AssumeRole"
            ],
    "Condition": {
      "ArnLike": {
```

```
        "aws:SourceArn":
 "arn:aws:ds:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Accédez aux AWS Directory Service API à l'aide d'un point de terminaison d'interface - AWS PrivateLink

Vous pouvez l'utiliser AWS PrivateLink pour créer une connexion privée entre votre VPC et AWS Directory Service les API. Vous pouvez accéder aux AWS Directory Service API comme si elles se trouvaient dans votre VPC, sans utiliser de passerelle Internet, de périphérique NAT, de connexion VPN ou AWS Direct Connect de connexion. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour accéder AWS Directory Service aux API.

Vous établissez cette connexion privée en créant un point de terminaison d'interface optimisé par AWS PrivateLink. Nous créons une interface réseau de point de terminaison dans chaque sous-réseau que vous activez pour le point de terminaison d'interface. Il s'agit d'interfaces réseau gérées par le demandeur qui servent de point d'entrée pour le trafic destiné à AWS Directory Service.

Pour plus d'informations, consultez la section Accès Services AWS par AWS PrivateLink le biais du AWS PrivateLink guide.

Considérations relatives à AWS Directory Service

Avant de configurer un point de terminaison d'interface pour les points de terminaison d' AWS Directory Service API, consultez les considérations du AWS PrivateLink guide.

AWS Directory Service prend en charge les appels à toutes ses actions d'API via le point de terminaison de l'interface.

Disponibilité

AWS Directory Service prend en charge les points de terminaison VPC dans les domaines suivants : Régions AWS

- USA Est (Virginie du Nord)
- AWS GovCloud (US-Ouest)
- AWS GovCloud (USA Est)

Créez un point de terminaison d'interface pour AWS Directory Service

Vous pouvez créer un point de terminaison d'interface pour les AWS Directory Service API à l'aide de la console Amazon VPC ou du AWS Command Line Interface ()AWS CLI. Pour plus d'informations, consultez Création d'un point de terminaison d'interface dans le Guide AWS PrivateLink .

Créez un point de terminaison d'interface pour AWS Directory Service les API en utilisant le nom de service suivant :

```
com.amazonaws.region.ds
```

Création d'une politique de point de terminaison pour votre point de terminaison d'interface

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 aux AWS Directory Service API via le point de terminaison de l'interface. Pour contrôler l'accès autorisé aux AWS Directory Service API depuis votre VPC, associez une politique de point de terminaison personnalisée au point de terminaison de l'interface.

Une politique de point de terminaison spécifie les informations suivantes :

- Les principaux qui peuvent effectuer des actions (Comptes AWS, utilisateurs IAM et rôles IAM).
- Les actions qui peuvent être effectuées.
- La ressource sur laquelle les actions peuvent être effectuées.

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 .

Exemple : politique de point de terminaison VPC pour les actions d'API AWS Directory Service

Voici un exemple de politique de point de terminaison personnalisée. Lorsque vous attachez cette politique au point de terminaison de votre interface, elle accorde l'accès aux AWS Directory

Service actions répertoriées à tous les principaux sur toutes les ressources. Remplacez *action-1*, *action-2* et *action-3* par les autorisations requises pour les AWS Directory Service API que vous souhaitez inclure dans votre politique. Pour obtenir une liste complète, veuillez consulter AWS Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "ds:action-1",
            "ds:action-2",
            "ds:action-3"
         ],
         "Resource":"*"
      }
   ]
}
```

Contrat de niveau de service pour AWS Directory Service

AWS Directory Service est un service hautement disponible, qui repose sur une infrastructure gérée par AWS. Il est soutenu par un accord de niveau de service qui définit la stratégie de disponibilité de notre service.

Pour plus d'informations, consultez le contrat de niveau de service pour AWS Directory Service.

Disponibilité de la région pour AWS Directory Service

Le tableau suivant propose une liste décrivant les points de terminaison spécifiques à la région pris en charge par type d'annuaire.

Nom de la région	Région	Point de terminaison	Protocole	AWS Microsoft AD géré	AD Connector	Simple AD
USA Est (Ohio)	us-east-2	ds.us-east-2.amazonaws.com	HTTPS	Oui	Oui	Non
US East (Virginie du Nord)	us-east-1	ds.us-east-1.amazonaws.com	HTTPS	Oui	Oui	Oui
USA Ouest (Californie du Nord)	us-west-1	ds.us-west-1.amazonaws.com	HTTPS	Oui	Oui	Non
USA Ouest (Oregon)	us-west-2	ds.us-west-2.amazonaws.com	HTTPS	Oui	Oui	Oui
Afrique (Le Cap)	af-south-1	ds.af-south-1.amazonaws.com	HTTPS	Oui	Oui	Non
Asie-Pacifique	ap-east-1	ds.ap-east-1.amazonaws.com	HTTPS	Oui	Oui	Non

Nom de la région	Région	Point de terminaison	Protocole	AWS Microsoft AD géré	AD Connector	Simple AD
(Hong Kong)						
Asie-Pacifique (Mumbai	ap-south-1	ds.ap-south-1.amazonaws.com	HTTPS	 O	 O	 Non
Asie-Pacifique (Hyderab d)	ap-south-2	ds.ap-south-2.amazonaws.com	HTTPS	 O	 O	 Non
Asie-Pacifique (Osaka)	ap-northeast-3	ds.ap-northeast-3.amazonaws.com	HTTPS	 O	 O	 Non
Asie-Pacifique (Séoul)	ap-northeast-2	ds.ap-northeast-2.amazonaws.com	HTTPS	 O	 O	 Non
Asie-Pacifique (Singapo r)	ap-southeast-1	ds.ap-southeast-1.amazonaws.com	HTTPS	 O	 O	 Oui

Nom de la région	Région	Point de terminaison	Protocole	AWS Microsoft AD géré	AD Connector	Simple AD
Asie-Pacifique (Sydney)	ap-southeast-2	ds.ap-southeast-2.amazonaws.com	HTTPS	Oui	Oui	Oui
Asie-Pacifique (Jakarta)	ap-southeast-3	ds.ap-southeast-3.amazonaws.com	HTTPS	Oui	Oui	Non
Asie-Pacifique (Melbourne)	ap-southeast-4	ds.ap-southeast-4.amazonaws.com	HTTPS	Oui	Oui	Non
Asie-Pacifique (Tokyo)	ap-northeast-1	ds.ap-northeast-1.amazonaws.com	HTTPS	Oui	Oui	Oui
Canada (Centre)	ca-central-1	ds.ca-central-1.amazonaws.com	HTTPS	Oui	Oui	Non
Canada Ouest (Calgary)	ca-west-1	ds.ca-west-1.amazonaws.com	HTTPS	Oui	Oui	Non
Chine (Beijing)	cn-north-1	ds.cn-north-1.amazonaws.com.cn	HTTPS	Oui	Oui	Non

Nom de la région	Région	Point de terminaison	Protocole	AWS Microsoft AD géré	AD Connector	Simple AD
Chine (Ningxia)	cn-northwest-1	ds.cn-northwest-1.amazonaws.com.cn	HTTPS	Oui	Oui	Non
Europe (Francfort)	eu-central-1	ds.eu-central-1.amazonaws.com	HTTPS	Oui	Oui	Non
Europe (Zurich)	eu-central-2	ds.eu-central-2.amazonaws.com	HTTPS	Oui	Oui	Non
Europe (Irlande)	eu-west-1	ds.eu-west-1.amazonaws.com	HTTPS	Oui	Oui	Oui
Europe (Londres)	eu-west-2	ds.eu-west-2.amazonaws.com	HTTPS	Oui	Oui	Non
Europe (Paris)	eu-west-3	ds.eu-west-3.amazonaws.com	HTTPS	Oui	Oui	Non
Europe (Stockholm)	eu-north-1	ds.eu-north-1.amazonaws.com	HTTPS	Oui	Oui	Non
Europe (Milan)	eu-south-1	ds.eu-south-1.amazonaws.com	HTTPS	Oui	Oui	Non
Europe (Espagne)	eu-south-2	ds.eu-south-2.amazonaws.com	HTTPS	Oui	Oui	Non

Nom de la région	Région	Point de terminaison	Protocole	AWS Microsoft AD géré	AD Connector	Simple AD
Israël (Tel Aviv)	il-central-1	ds.il-central-1.amazonaws.com	HTTPS	Oui	Oui	Non
Moyen-Orient (Bahreïn)	me-south-1	ds.me-south-1.amazonaws.com	HTTPS	Oui	Oui	Non
Moyen-Orient (EAU)	me-central-1	ds.me-central-1.amazonaws.com	HTTPS	Oui	Oui	Non
Amérique du Sud (São Paulo)	sa-east-1	ds.sa-east-1.amazonaws.com	HTTPS	Oui	Oui	Non
AWS GovCloud (US-Ouest)	us-gov-west-1	ds. us-gov-west-1. amazonaws.com	HTTPS	Oui	Oui	Non
AWS GovCloud (USA Est)	us-gov-east-1	ds. us-gov-east-1. amazonaws.com	HTTPS	Oui	Oui	Non

Pour plus d'informations sur l'utilisation AWS Directory Service dans la région AWS GovCloud (USA Ouest) et dans la région AWS GovCloud (USA Est), voir Points de terminaison de service.

Pour plus d'informations sur l'utilisation AWS Directory Service dans les régions de Pékin et du Ningxia, consultez Endpoints and ARN for Amazon Web Services in China.

Compatibilité des navigateurs

AWS les applications et services tels qu'Amazon WorkSpaces WorkMail, Amazon Connect, Amazon Chime, Amazon WorkDocs, etc. nécessitent des AWS IAM Identity Center informations de connexion valides provenant d'un navigateur compatible avant de pouvoir y accéder. Le tableau suivant décrit uniquement les navigateurs et les versions de navigateur compatibles pour les connexions.

Navigateur	Version	Compatibilité
Microsoft Edge	3 dernières versions	Compatible
Mozilla Firefox	3 dernières versions	Compatible
Google Chrome	3 dernières versions	Compatible
Apple Safari	3 dernières versions	Compatible

Maintenant que vous avez vérifié que vous utilisez une version prise en charge de votre navigateur, nous vous recommandons également de consulter la section ci-dessous pour vérifier que votre navigateur a été configuré pour utiliser le protocole TLS (Transport Layer Security) requis par AWS.

Qu'est-ce que TLS ?

TLS est un protocole utilisé par des navigateurs Web et d'autres applications pour échanger des données en toute sécurité sur un réseau. TLS permet de s'assurer qu'une connexion à un point de terminaison distant correspond au point de terminaison prévu via le chiffrement et la vérification d'identité du point de terminaison. À ce jour, les versions de TLS disponibles sont TLS 1.0, 1.1, 1.2 et 1.3.

Quelles sont les versions de TLS prises en charge par l'IAM Identity Center ?

AWS les applications et les services prennent en charge les protocoles TLS 1.1, 1.2 et 1.3 pour les connexions sécurisées. À compter du 30 octobre 2019, TLS 1.0 n'est plus pris en charge. Il est donc important que tous les navigateurs soient configurés pour prendre en charge TLS 1.1 ou version

ultérieure. En d'autres termes, vous ne serez pas en mesure de vous connecter à des applications et services AWS si vous y accédez alors que TLS 1.0 est activé. Pour obtenir de l'aide relative à cette modification, contactez votre administrateur.

Comment puis-je activer les versions de TLS prises en charge dans mon navigateur

Cela dépend de votre navigateur. Généralement, vous devez accéder aux paramètres avancés dans les paramètres de votre navigateur. Par exemple, dans Internet Explorer, vous trouverez diverses options TLS sous Propriétés Internet, l'onglet Paramètres avancés, puis la section Sécurité. Consultez le site web d'assistance du fournisseur de votre navigateur pour obtenir des instructions spécifiques.

Historique du document

Le tableau suivant décrit les modifications significatives apportées depuis la publication du Guide de l'administrateur AWS Directory Service .

Modification	Description	Date
Paramètres d'authentification basés sur des certificats	Ajout de contenu concernant deux nouveaux paramètres de sécurité pour AWS Managed Microsoft AD.	11 avril 2023
AWS PrivateLink	Ajout de contenu concernant AWS PrivateLink.	31 mars 2023
Points de terminaison d'un VPC Simple AD	Ajout de contenu indiquant quels points de terminaison d'un VPC ne doivent pas être configurés.	25 août 2021
Points de terminaison d'un VPC AD Connector	Ajout de contenu indiquant quels points de terminaison d'un VPC ne doivent pas être configurés.	25 août 2021
Prendre en charge des cartes intelligentes	Ajout de contenu sur la prise en charge des cartes à puce et d'Amazon WorkSpaces Application Manager dans la AWS GovCloud région (ouest des États-Unis)	1er décembre 2020
Réinitialisation du mot de passe	Ajout de contenu expliquant comment réinitialiser les mots de passe des utilisateurs à AWS Management Console	2 janvier 2019

	l'aide Windows PowerShell AWS CLI des	
Partage d'annuaire	Ajout de contenu expliquant comment utiliser le partage d'annuaires avec AWS Managed Microsoft AD.	25 septembre 2018
Contenu migré vers le nouveau Guide du développeur Amazon Cloud Directory	Le contenu d'Amazon Cloud Directory a été déplacé de ce guide vers le nouveau Guide du développeur Amazon Cloud Directory .	21 juin 2018
Révision de la table des matières du Guide de l'administrateur terminée	Contenu réorganisé pour répondre plus directement aux besoins du client. Du nouveau contenu a également été ajouté lorsqu'il était nécessaire.	5 avril 2018
AWS groupes délégués	Ajout de la liste des groupes AWS délégués pouvant être affectés aux utilisateurs locaux.	8 mars 2018
Stratégies de mot de passe affinées	Ajout de nouveau contenu sur les politiques de mot de passe.	5 juillet 2017
Contrôleurs de domaine supplémentaires	Ajout de contenu expliquant comment ajouter d'autres contrôleurs de domaine à votre annuaire dans AWS Managed Microsoft AD.	30 juin 2017

Didacticiels	Ajout de nouveaux didacticiels pour tester un environnement de laboratoire Microsoft AD AWS géré.	21 juin 2017
MFA avec AWS Microsoft AD géré	Ajout de contenu sur l'utilisation du MFA avec Managed AWS Microsoft AD.	13 février 2017
Amazon Cloud Directory	Ajout de contenu concernant un nouveau type d'annuaire.	26 janvier 2017
Extensions de schéma	Ajout de contenu sur les extensions de schéma avec AWS Directory Service pour Microsoft Active Directory.	14 novembre 2016
Réorganisation majeure du guide de AWS Directory Service l'administrateur	Contenu réorganisé pour répondre plus directement aux besoins du client.	14 novembre 2016
Notifications SNS	Ajout de contenu sur les notifications SNS.	25 février 2016
Autorisation et authentification	Ajout de contenu expliquant comment utiliser IAM avec AWS Directory Service.	25 février 2016
AWS Microsoft AD géré	Ajout de contenu sur AWS Managed Microsoft AD et de guides combinés en un seul guide.	17 novembre 2015
Permettre aux instances Linux d'être jointes à un annuaire Simple AD	Ajout de contenu expliquant comment joindre une instance Linux à un annuaire Simple AD.	23 juillet 2015

Séparation de manuel	Divisez le Guide de l'administrateur AWS Directory Service en guides distincts.	14 juillet 2015
Prise en charge de l'authentification unique	Ajout de contenu sur la prise en charge de l'authentification unique.	31 mars 2015
Nouveau guide	Il s'agit de la première version du Guide de l'utilisateur AWS Directory Service .	21 octobre 2014

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.