Guide de l’utilisateur

AWS Accès vérifié

AWS Accès vérifié: Guide de l’utilisateur

Table of Contents

Qu'est-ce que c'est Accès vérifié par AWS ?

Vous pouvez ainsi fournir un accès sécurisé à vos applications sans avoir besoin d'un réseau privé virtuel (VPN). Accès vérifié par AWS Verified Access évalue chaque demande d'application et permet de garantir que les utilisateurs ne peuvent accéder à chaque application que lorsqu'elle répond aux exigences de sécurité spécifiées.

Avantages de l'accès vérifié

- Position de sécurité améliorée — Un modèle de sécurité traditionnel évalue l'accès une seule fois et accorde à l'utilisateur l'accès à toutes les applications. Verified Access évalue chaque demande d'accès aux applications en temps réel. Il est donc difficile pour les acteurs malveillants de passer d'une application à l'autre.
- Intégration aux services de sécurité — Verified Access s'intègre aux services de gestion des identités et des appareils, y compris les services tiers AWS et les services tiers. À l'aide des données de ces services, Verified Access vérifie la fiabilité des utilisateurs et des appareils par rapport à un ensemble d'exigences de sécurité et détermine si l'utilisateur doit avoir accès à une application.
- Expérience utilisateur améliorée : Verified Access évite aux utilisateurs d'utiliser un pour accéder VPN à vos applications. Cela permet de réduire le nombre de demandes d'assistance VPN liées à des problèmes connexes.
- Résolution des problèmes et audits simplifiés : Verified Access enregistre toutes les tentatives d'accès, offrant ainsi une visibilité centralisée sur l'accès aux applications, afin de vous aider à répondre rapidement aux incidents de sécurité et aux demandes d'audit.

Accès à l'accès vérifié

Vous pouvez utiliser l'une des interfaces suivantes pour utiliser Verified Access :

- AWS Management Console— Fournit une interface Web que vous pouvez utiliser pour créer et gérer des ressources d'accès vérifié. Connectez-vous à la VPC console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/vpc/.
- AWS Command Line Interface (AWS CLI) — Fournit des commandes pour un large éventail de AWS services, y compris Accès vérifié par AWS. AWS CLI Il est pris en charge sur Windows, macOS et Linux. Pour l'obtenir AWS CLI, voyez AWS Command Line Interface.

- AWS SDKs— Fournissez des informations spécifiques à la langueAPIs. Ils AWS SDKs prennent en charge de nombreux détails de connexion, tels que le calcul des signatures et la gestion des nouvelles tentatives et des erreurs de demande. Pour plus d'informations, consultez AWS SDKs.
- Requête API — Fournit des API actions de bas niveau que vous appelez à l'aide de HTTPS requêtes. L'utilisation de la requête API est le moyen le plus direct d'accéder à l'accès vérifié. Cependant, cela nécessite que votre application gère des détails de bas niveau tels que la génération du hachage pour signer la demande et la gestion des erreurs. Pour plus d'informations, consultez la section Actions d'accès vérifié dans la EC2APIréférence Amazon.

Ce guide explique comment utiliser les ressources AWS Management Console pour créer, accéder et gérer les ressources d'accès vérifié.

Tarification

Vous êtes facturé à l'heure pour chaque demande sur Verified Access, et vous êtes facturé pour la quantité de données traitées par Verified Access. Pour en savoir plus, consultez Pricing Accès vérifié par AWS (Tarification).

Comment fonctionne Verified Access

Accès vérifié par AWS évalue chaque demande d'application de vos utilisateurs et autorise l'accès en fonction de :

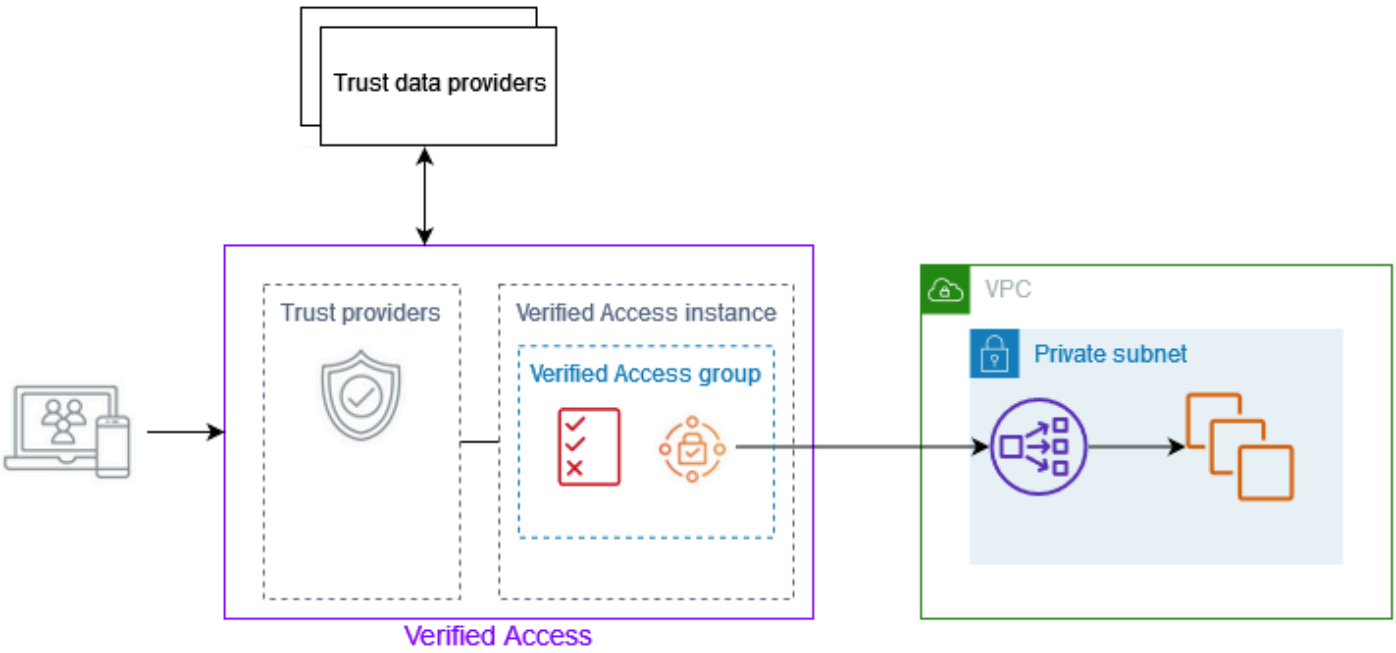
- Données de confiance envoyées par le fournisseur de confiance que vous avez choisi (provenant AWS ou d'un tiers).
- Politiques d'accès que vous créez dans Verified Access.

Lorsqu'un utilisateur essaie d'accéder à une application, Verified Access obtient ses données auprès du fournisseur de confiance et les évalue par rapport aux politiques que vous avez définies pour l'application. L'accès vérifié accorde l'accès à l'application demandée uniquement si l'utilisateur répond aux exigences de sécurité que vous avez spécifiées. Toutes les demandes d'application sont refusées par défaut, jusqu'à ce qu'une politique soit définie.

En outre, Verified Access enregistre chaque tentative d'accès afin de vous aider à répondre rapidement aux incidents de sécurité et aux demandes d'audit.

Principaux éléments de Verified Access

Le schéma suivant fournit un aperçu général de Verified Access. Les utilisateurs envoient des demandes pour accéder à une application. Verified Access évalue la demande par rapport à la politique d'accès du groupe et à toute politique de point de terminaison spécifique à l'application. Si l'accès est autorisé, la demande est envoyée à l'application via le point de terminaison.



- Instances à accès vérifié : une instance évalue les demandes d'application et n'accorde l'accès que lorsque vos exigences de sécurité sont satisfaites.
- Points de terminaison d'accès vérifiés : chaque point de terminaison représente une application. Vous pouvez créer un point de terminaison d'équilibrage de charge ou un point de terminaison d'interface réseau.
- Groupe d'accès vérifié : ensemble de points de terminaison d'accès vérifié. Nous vous recommandons de regrouper les points de terminaison des applications présentant des exigences de sécurité similaires afin de simplifier l'administration des politiques. Par exemple, vous pouvez regrouper les points de terminaison de toutes vos applications de vente.
- Politiques d'accès : ensemble de règles définies par l'utilisateur qui déterminent s'il convient d'autoriser ou de refuser l'accès à une application. Vous pouvez spécifier une combinaison de facteurs, notamment l'identité de l'utilisateur et l'état de sécurité de l'appareil. Vous créez une politique d'accès de groupe pour chaque groupe d'accès vérifié, qui est héritée par tous les points de terminaison du groupe. Vous pouvez éventuellement créer des politiques spécifiques à l'application et les associer à des points de terminaison spécifiques.
- Fournisseurs de confiance : service qui gère les identités des utilisateurs ou l'état de sécurité des appareils. Verified Access fonctionne à la fois avec des fournisseurs de confiance AWS et avec des fournisseurs de confiance tiers. Vous devez associer au moins un fournisseur de confiance à chaque instance d'accès vérifié. Vous pouvez associer un seul fournisseur de confiance en matière d'identité et plusieurs fournisseurs de confiance en matière d'appareils à chaque instance d'accès vérifié.

- Données de confiance : données relatives à la sécurité des utilisateurs ou des appareils que votre fournisseur de confiance envoie à Verified Access. Également appelé « revendications des utilisateurs » ou « contexte de confiance ». Par exemple, l'adresse e-mail d'un utilisateur ou la version du système d'exploitation d'un appareil. Verified Access évalue ces données par rapport à vos politiques d'accès lorsqu'il reçoit chaque demande d'accès à une application.

Tutoriel : Commencez avec Verified Access

Utilisez ce didacticiel pour commencer Accès vérifié par AWS. Vous allez apprendre à créer et à configurer des ressources d'accès vérifié.

Dans le cadre de ce didacticiel, vous allez ajouter une application à Verified Access. À la fin du didacticiel, des utilisateurs spécifiques pourront accéder à cette application via Internet, sans l'utiliserVPN.

> **Note**
>
> Ce didacticiel ne montre pas l'intégration avec le fournisseur de confiance basé sur votre appareil. Au lieu de cela, nous travaillons uniquement avec un fournisseur de confiance basé sur l'identité.

Tâches

Prérequis du didacticiel Verified Access

Les conditions requises pour suivre ce didacticiel sont les suivantes :

- La disponibilité de deux Comptes AWS. Un compte héberge votre application cible et les ressources d'accès vérifié sont créées dans l'autre compte.
- AWS IAM Identity Center activé dans Région AWS celui dans lequel vous travaillez. Vous pouvez ensuite utiliser IAM Identity Center en tant que fournisseur de confiance avec Verified Access. Pour plus d'informations, consultez la section Activer IAM Identity Center dans le guide de AWS IAM Identity Center l'utilisateur.
- Un domaine public hébergé et les autorisations requises pour mettre à jour les DNS enregistrements du domaine.
- Une application exécutée derrière un équilibreur de charge interne dans un Compte AWS. L'exemple de nom de domaine d'application que nous allons utiliser est`www.myapp.example.com`.
- Une IAM politique qui dispose de toutes les autorisations requises pour créer une Accès vérifié par AWS instance indiquée iciPolitique de création d'instances d'accès vérifié.

Étape 1 : créer une instance d'accès vérifié

Utilisez la procédure suivante pour créer une instance Verified Access.

Pour créer une instance d'accès vérifié

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet VPC de navigation Amazon, choisissez Verified Access instances, puis Create Verified Access instance.
3. (Facultatif) Dans Nom et description, entrez un nom et une description pour l'instance d'accès vérifié.
4. Pour Trust provider, conservez l'option par défaut.
5. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
6. Choisissez Créer une instance d'accès vérifié.

Étape 2 : Configuration d'un fournisseur de confiance d'accès vérifié

Vous pouvez vous configurer en AWS IAM Identity Center tant que fournisseur de confiance.

Pour créer un fournisseur de confiance IAM Identity Center

1. Dans le volet VPC de navigation Amazon, choisissez Verified Access trust providers, puis Create Verified Access trust provider.
2. (Facultatif) Dans le champ Nom et description, entrez le nom et la description du fournisseur de confiance Verified Access.
3. Entrez un identifiant personnalisé à utiliser ultérieurement lorsque vous utiliserez des règles de stratégie pour le nom de référence de la stratégie. Par exemple, vous pouvez entrer**`idc`**.
4. Sous Type de fournisseur de confiance, sélectionnez Fournisseur de confiance utilisateur.
5. Sous Type de fournisseur de confiance utilisateur, sélectionnez IAMIdentity Center.
6. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l’identification.
7. Choisissez Create Verified Access trust provider.

Étape 3 : associer votre fournisseur de confiance à l'instance Verified Access

Maintenant que vous avez configuré un fournisseur de confiance, vous pouvez l'associer à l'instance Verified Access que vous avez créée précédemment. Utilisez la procédure suivante pour associer le fournisseur de confiance à votre instance Verified Access.

Pour associer un fournisseur de confiance à votre instance

1. Dans le volet VPC de navigation Amazon, sélectionnez Verified Access instances.
2. Sélectionnez votre instance.
3. Choisissez Actions, puis attachez le fournisseur de confiance Verified Access.
4. Pour le fournisseur de confiance Verified Access, choisissez votre fournisseur de confiance.
5. Choisissez Attach Verified Access Trust Provider.

Étape 4 : Création d'un groupe d'accès vérifié

Au cours de cette étape, vous créez un groupe que vous utiliserez comme point de terminaison à l'étape 5.

Pour créer un groupe d'accès vérifié

1. Dans le volet VPC de navigation Amazon, choisissez Verified Access groups, puis Create Verified Access group.
2. (Facultatif) Pour le tag de nom et la description, entrez un nom et une description pour le groupe.
3. Pour l'instance Verified Access, choisissez votre instance Verified Access.
4. Pour la définition de la politique, laissez ce champ vide. Vous allez créer une politique plus loin dans ce didacticiel.
5. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l’identification.
6. Choisissez Créer un groupe d'accès vérifié.

Étape 5 : Partagez votre groupe d'accès vérifié via AWS Resource Access Manager

Au cours de cette étape, vous partagez le groupe que vous venez de créer avec le groupe Compte AWS dans lequel s'exécute votre application cible. Pour partager un groupe à accès vérifié, vous devez l'ajouter à un partage de ressources. Si vous ne disposez pas d'un partage de ressources, vous devez d'abord en créer un.

Si vous faites partie d'une organisation et que le partage au sein de votre organisation est activé, les clients de votre organisation ont automatiquement accès au groupe Verified Access partagé. AWS Organizations Dans le cas contraire, les consommateurs reçoivent une invitation à rejoindre le partage de ressources et ont accès au groupe d'accès vérifié partagé après avoir accepté l'invitation.

Suivez les étapes décrites dans la section Créer un partage de ressources du Guide de l’utilisateur AWS RAM . Pour Sélectionner le type de ressource, choisissez le groupe d'accès vérifié, puis cochez la case correspondant à votre groupe d'accès vérifié.

Pour plus d'informations, consultez Démarrer dans le Guide de l'utilisateur AWS RAM .

Étape 6 : Ajoutez votre application en créant un point de terminaison d'accès vérifié

Utilisez les procédures suivantes pour créer un point de terminaison d'accès vérifié. Cette étape suppose qu'une application s'exécute derrière un équilibreur de charge interne d'Elastic Load Balancing.

Pour créer un point de terminaison d'accès vérifié

1. Dans le volet de VPC navigation Amazon, choisissez Verified Access endpoints, puis Create Verified Access endpoint.
2. (Facultatif) Dans les champs Name tag et Description, entrez un nom et une description pour le point de terminaison.
3. Pour le groupe Verified Access, choisissez votre groupe Verified Access.
4. Pour les détails de l'application, procédez comme suit :
    a. Dans le champ Domaine de l'application, entrez DNS le nom de votre application.
    b. Sous Certificat de domaine ARN, sélectionnez le nom de ressource Amazon (ARN) de votre TLS certificat public.
5. Pour obtenir des informations détaillées sur le point de terminaison, procédez comme suit :
    a. Pour Type de pièce jointe, sélectionnez VPC.
    b. Pour les groupes de sécurité, sélectionnez un groupe de sécurité à associer au point de terminaison.
    c. Pour le préfixe de domaine Endpoint, entrez un identifiant personnalisé. Il sera ajouté au début du DNS nom généré par Verified Access. Pour cet exemple, nous pouvons utiliser**`my-ava-app`**.
    d. Pour le type de point de terminaison, choisissez l'équilibreur de charge.
    e. Pour Protocole, sélectionnez HTTPSou HTTP. Cela dépend de la configuration de votre équilibreur de charge.
    f. Pour Port, saisissez le numéro de port. Cela dépend de la configuration de votre équilibreur de charge.
    g. Pour Équilibreur de chargeARN, choisissez votre équilibreur de charge.
    h. Pour les sous-réseaux, sélectionnez les sous-réseaux associés à votre équilibreur de charge.

6. Pour la définition de la stratégie, n'entrez pas de stratégie pour le moment. Nous aborderons ce sujet plus loin dans le didacticiel.
7. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
8. Choisissez Créer un point de terminaison d'accès vérifié.

Étape 7 : Configuration des DNS paramètres du point de terminaison Verified Access

Pour cette étape, vous devez mapper le nom de domaine de votre application (par exemple, www.myapp.example.com) au nom de domaine de votre point de terminaison Verified Access. Pour terminer le DNS mappage, créez un enregistrement de nom canonique (CNAME) avec votre DNS fournisseur. Après avoir créé l'CNAMEenregistrement, toutes les demandes des utilisateurs adressées à votre application seront envoyées à Verified Access.

Pour obtenir le nom de domaine de votre terminal

1. Dans le volet de VPC navigation Amazon, choisissez Verified Access endpoints.
2. Sélectionnez le point de terminaison que vous avez créé précédemment.
3. Choisissez l'onglet Détails pour le point de terminaison.
4. Sous Domaine du point de terminaison, copiez le domaine du point de terminaison.

Pour ce didacticiel, le nom de domaine du point de terminaison sera`my-ava-app.edge-1a2b3c4d5e6f7g.vai-1a2b3c4d5e6f7g.prod.verified-access.us-west-2.amazonaws.com`.

Créez un CNAME enregistrement auprès de votre DNS fournisseur :

Nom de l'enregistrement	Type	Valeur
www.myapp.exemple.com	CNAME	my-ava-app.edge-1a 2b3c4d5e6f7g.vai-1 a2b3c4d5e6f7g.prod. verified-access.us-west-2.amazonaws. com

Étape 8 : tester la connectivité à l'application que vous avez ajoutée à Verified Access

Vous pouvez désormais tester la connectivité à votre application. Entrez le nom de domaine de votre application dans votre navigateur Web. Le comportement par défaut des politiques d'accès vérifié est de refuser toutes les demandes. Comme nous n'avons pas encore mis en place de politique permettant à quiconque d'y accéder, toutes les demandes devraient être refusées.

Étape 9 : Configuration d'une politique d'accès au niveau du groupe d'accès vérifié

Utilisez la procédure suivante pour modifier le groupe d'accès vérifié et configurer une politique d'accès qui autorise la connectivité à votre application. Les détails de la politique dépendront des utilisateurs et des groupes configurés dans IAM Identity Center. Pour plus d'informations sur la création d'une politique, consultezPolitiques d'accès vérifiées.

Pour modifier un groupe d'accès vérifié

1. Dans le volet VPC de navigation Amazon, sélectionnez Verified Access groups.
2. Sélectionnez le groupe .
3. Choisissez Actions, Modifier la politique de groupe d'accès vérifié.
4. Entrez la politique.
5. Choisissez Modifier la politique de groupe d'accès vérifié.

Étape 10 : retester la connectivité à l'application que vous avez ajoutée à Verified Access

Maintenant que votre politique de groupe est en place, vous pouvez accéder à votre application. Entrez le nom de domaine de votre application dans votre navigateur Web. La demande doit être autorisée et vous devez être redirigé vers l'application.

Nettoyez les ressources d'accès vérifié que vous avez créées

Une fois le test terminé, suivez les étapes ci-dessous pour supprimer les ressources créées.

Pour supprimer les ressources d'accès vérifié créées avec ce didacticiel

1. Dans le volet de VPC navigation Amazon, choisissez Verified Access endpoints. Sélectionnez le point de terminaison que vous souhaitez supprimer. Choisissez Actions, puis Supprimer le point de terminaison d'accès vérifié.
2. Dans le volet de navigation, sélectionnez Groupes d'accès vérifiés. Sélectionnez le groupe que vous souhaitez supprimer. Choisissez Actions, puis Supprimer le groupe d'accès vérifié. Remarque : vous devrez peut-être attendre quelques minutes jusqu'à ce que le processus de suppression du terminal soit terminé.
3. Dans le volet VPC de navigation Amazon, sélectionnez Verified Access instances. Sélectionnez l'instance que vous avez créée pour ce didacticiel. Choisissez Actions, détachez le fournisseur de confiance Verified Access. Sélectionnez le fournisseur de confiance dans la liste déroulante, puis choisissez Detach Verified Access Trust Provider.
4. Dans le volet VPC de navigation Amazon, sélectionnez Verified Access trust providers. Sélectionnez le fournisseur de confiance que vous avez créé pour ce didacticiel. Choisissez Actions, puis Supprimer le fournisseur de confiance Verified Access.
5. Dans le volet VPC de navigation Amazon, sélectionnez Verified Access instances. Sélectionnez l'instance que vous avez créée pour ce didacticiel. Choisissez Actions, puis Supprimer l'instance d'accès vérifié.

Instances d'accès vérifié

Une Accès vérifié par AWS instance est une AWS ressource qui vous aide à organiser vos fournisseurs de confiance et vos groupes d'accès vérifié. Une instance évalue les demandes d'application et n'accorde l'accès que lorsque vos exigences de sécurité sont satisfaites.

Rubriques

Création et gestion d'une instance d'accès vérifié

Vous utilisez une instance d'accès vérifié pour organiser vos fournisseurs de confiance et vos groupes d'accès vérifié. Utilisez les procédures suivantes pour créer une instance d'accès vérifié, puis attachez un fournisseur de confiance à Verified Access ou détachez un fournisseur de confiance de Verified Access.

Rubriques

Création d'une instance d'accès vérifié

Utilisez la procédure suivante pour créer une instance d'accès vérifié.

Pour créer une instance d'accès vérifié

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Instances d'accès vérifié, puis Créer une instance d'accès vérifié.
3. (Facultatif) Dans Nom et description, entrez un nom et une description pour l'instance d'accès vérifié.

4. (Facultatif) Choisissez Activer les normes fédérales de traitement de l'information (FIPS) si vous avez besoin de Verified Access pour être FIPS conforme.
5. (Facultatif) Pour le fournisseur de confiance, choisissez un fournisseur de confiance à associer à l'instance d'accès vérifié.
6. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
7. Choisissez Créer une instance d'accès vérifié.

Associer un fournisseur de confiance à une instance d'accès vérifié

Utilisez la procédure suivante pour associer un fournisseur de confiance à une instance Verified Access.

Pour associer un fournisseur de confiance à une instance d'accès vérifié

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance.
4. Choisissez Actions, puis attachez le fournisseur de confiance Verified Access.
5. Pour le fournisseur de confiance Verified Access, choisissez un fournisseur de confiance.
6. Choisissez Attach Verified Access Trust Provider.

Détacher un fournisseur de confiance d'une instance d'accès vérifié

Utilisez la procédure suivante pour détacher un fournisseur de confiance d'une instance Verified Access.

Pour détacher un fournisseur de confiance d'une instance d'accès vérifié

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance.
4. Choisissez Actions, détachez le fournisseur de confiance Verified Access.
5. Pour le fournisseur de confiance Verified Access, choisissez le fournisseur de confiance.
6. Choisissez le fournisseur de confiance Detach Verified Access.

Supprimer une instance d'accès vérifié

Lorsque vous avez terminé d'utiliser une instance Verified Access, vous pouvez la supprimer. Avant de pouvoir supprimer une instance, vous devez supprimer tous les fournisseurs de confiance ou groupes d'accès vérifié associés.

Pour supprimer une instance d'accès vérifié

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance Verified Access.
4. Choisissez Actions, puis Supprimer l'instance d'accès vérifié.
5. Lorsque vous êtes invité à confirmer, saisissez **`delete`**, puis choisissez Delete (Supprimer).

Intégrez Verified Access à AWS WAF

Outre les règles d'authentification et d'autorisation appliquées par Verified Access, vous souhaiterez peut-être également appliquer une protection périmétrique. Cela peut vous aider à protéger vos applications contre des menaces supplémentaires. Vous pouvez y parvenir AWS WAF en l'intégrant à votre déploiement de Verified Access. AWS WAF est un pare-feu d'applications Web qui vous permet de surveiller les HTTP (S) demandes qui sont transmises aux ressources protégées de votre application Web. Pour plus d'informations à ce sujet AWS WAF, consultez AWS WAFle guide du AWS WAF développeur.

Vous pouvez intégrer AWS WAF Verified Access en associant une liste de contrôle d'accès AWS WAF Web (ACL) à une instance Verified Access. Un site Web ACL est une AWS WAF ressource qui vous permet de contrôler avec précision toutes les requêtes HTTP (S) Web auxquelles votre ressource protégée répond. Pendant le traitement de la demande d' AWS WAF association ou de dissociation, le statut de tous les points de terminaison Verified Access attachés à l'instance est affiché sous la forme. `updating` Une fois la demande terminée, le statut revient à`active`. Vous pouvez consulter le statut dans le AWS Management Console ou en décrivant le point de terminaison à l'aide du AWS CLI.

> **Note**
>
> Vous pouvez également utiliser la AWS WAF console ou API effectuer cette intégration. Vous aurez besoin du nom de ressource Amazon (ARN) de votre instance

Verified Access. Vous pouvez le construire en ARN utilisant le format suivant :`arn:${Partition}:ec2:${Region}:${Account}:verified-access-instance/${VerifiedAccessInstanceId}`.

Rubriques

- IAMautorisations requises pour intégrer Verified Access à AWS WAF
- Associer un AWS WAF site Web ACL
- Vérifier l'état de l' AWS WAF intégration
- Dissocier un site Web AWS WAF ACL

IAMautorisations requises pour intégrer Verified Access à AWS WAF

L'intégration AWS WAF à Verified Access inclut des actions avec autorisation uniquement qui ne correspondent pas directement à une opération. API Ces actions sont indiquées dans la référence d'autorisation de AWS Identity and Access Management service avec`[permission only]`. Consultez la section Actions, ressources et clés de condition pour Amazon EC2 dans le Service Authorization Reference.

Pour utiliser un site WebACL, votre AWS Identity and Access Management principal doit disposer des autorisations suivantes.

- `ec2:AssociateVerifiedAccessInstanceWebAcl`
- `ec2:DisassociateVerifiedAccessInstanceWebAcl`
- `ec2:DescribeVerifiedAccessInstanceWebAclAssociations`
- `ec2:GetVerifiedAccessInstanceWebAcl`

Associer un AWS WAF site Web ACL

Les étapes suivantes montrent comment associer une liste de contrôle d'accès AWS WAF Web (ACL) à une instance d'accès vérifié à l'aide du AWS Management Console.

> **Tip**
>
> Vous devez disposer d'un AWS WAF site Web existant ACL pour effectuer la procédure ci-dessous. Pour plus d'informations sur le Web, ACLs consultez les listes de contrôle d'accès Web dans le guide du AWS WAF développeur.

Pour associer un AWS WAF site Web ACL à une instance d'accès vérifié

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance Verified Access.
4. Sélectionnez l'onglet Intégrations.
5. Choisissez Actions, puis Associer le Web ACL.
6. Pour le Web ACL, choisissez un site Web existantACL, puis sélectionnez Associer le Web ACL.

Vous pouvez également utiliser le AWS Management Console for AWS WAF pour accomplir cette tâche. Pour plus d'informations, consultez la section Associer ou dissocier un site Web ACL à une AWS ressource dans le Guide du AWS WAF développeur.

Vérifier l'état de l' AWS WAF intégration

Vous pouvez vérifier si une liste de contrôle d'accès AWS WAF Web (ACL) est associée à une instance d'accès vérifié ou non en utilisant le AWS Management Console.

Pour consulter l'état de l' AWS WAF intégration avec une instance Verified Access

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance Verified Access.
4. Sélectionnez l'onglet Intégrations.
5. Vérifiez les informations répertoriées sous État de WAF l'intégration. Le statut sera affiché comme Associé ou Non associé, ainsi que l'ACLidentifiant Web, s'il est dans l'état Associé.

Dissocier un site Web AWS WAF ACL

Les étapes suivantes montrent comment dissocier une liste de contrôle d'accès AWS WAF Web (ACL) d'une instance d'accès vérifié à l'aide du AWS Management Console.

Pour dissocier un AWS WAF site Web ACL d'une instance d'accès vérifié

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance Verified Access.
4. Sélectionnez l'onglet Intégrations.
5. Choisissez Actions, puis Dissocier le Web ACL.
6. Confirmez en choisissant Dissociate Web. ACL

Vous pouvez également utiliser le AWS Management Console for AWS WAF pour accomplir cette tâche. Pour plus d'informations, consultez la section Associer ou dissocier un site Web ACL à une AWS ressource dans le Guide du AWS WAF développeur.

FIPSconformité pour Verified Access

La norme fédérale de traitement de l'information (FIPS) est une norme gouvernementale américaine et canadienne qui spécifie les exigences de sécurité pour les modules cryptographiques qui protègent les informations sensibles. Accès vérifié par AWS offre la possibilité de configurer votre environnement pour qu'il adhère à la FIPS publication 140-2. FIPSla conformité à l'accès vérifié est disponible dans les AWS régions suivantes :

- USA Est (Ohio)
- USA Est (Virginie du Nord)
- USA Ouest (Californie du Nord)
- US West (Oregon)
- Canada (Centre)
- AWS GovCloud (US) Ouest
- AWS GovCloud (US) Est

Cette page explique comment configurer un environnement Verified Access, nouveau ou existant, pour qu'il soit FIPS conforme.

Rubriques

Configurer un environnement d'accès vérifié existant à des fins de FIPS conformité

Si vous disposez d'un environnement d'accès vérifié existant et que vous souhaitez le configurer pour qu'il soit FIPS conforme, certaines ressources devront être supprimées et recréées afin d'activer la FIPS conformité.

Pour reconfigurer un Accès vérifié par AWS environnement existant afin qu'il soit FIPS conforme, suivez les étapes ci-dessous.

1. Supprimez vos points de terminaison, groupes et instance Verified Access d'origine. Vos fournisseurs de confiance configurés peuvent être réutilisés.
2. Créez une instance d'accès vérifié, en veillant à activer les normes fédérales de traitement de l'information (FIPS) lors de la création. Lors de la création, associez également le fournisseur de confiance Verified Access que vous souhaitez utiliser en le sélectionnant dans la liste déroulante.
3. Créez un groupe d'accès vérifié. Lors de la création du groupe, vous l'associez à l'instance Verified Access qui vient d'être créée.
4. Créez-en un ou plusieursPoints de terminaison d'accès vérifiés. Lors de la création de vos points de terminaison, vous les associez au groupe créé à l'étape précédente.

Configurer un nouvel environnement d'accès vérifié à des fins de FIPS conformité

Pour configurer un nouvel Accès vérifié par AWS environnement FIPS conforme, suivez les étapes ci-dessous.

1. Configurez un fournisseur de confiance. Vous devrez créer un fournisseur de confiance en matière d'identité utilisateur et (éventuellement) un fournisseur de confiance basé sur l'appareil, en fonction de vos besoins.

2. Créez une instance d'accès vérifié, en veillant à activer les normes fédérales en matière de processus d'information (FIPS) pendant le processus. Lors de la création, attachez également le fournisseur de confiance Verified Access que vous avez créé à l'étape précédente, en le sélectionnant dans la liste déroulante.
3. Créez un groupe d'accès vérifié. Lors de la création du groupe, vous l'associez à l'instance Verified Access qui vient d'être créée.
4. Créez-en un ou plusieursPoints de terminaison d'accès vérifiés. Lors de la création de vos points de terminaison, vous les associez au groupe créé à l'étape précédente.

Faites confiance aux fournisseurs pour un accès vérifié

Un fournisseur de confiance est un service qui envoie des informations sur les utilisateurs et les appareils à Accès vérifié par AWS. Ces informations sont appelées contexte de confiance. Il peut inclure des attributs basés sur l'identité de l'utilisateur, tels qu'une adresse e-mail ou l'adhésion à l'organisation « commerciale », ou des informations sur l'appareil telles que les correctifs de sécurité installés ou la version du logiciel antivirus.

Verified Access prend en charge les catégories de fournisseurs de confiance suivantes :

- Identité utilisateur : service de fournisseur d'identité (IdP) qui stocke et gère les identités numériques des utilisateurs.
- Gestion des appareils : système de gestion des appareils pour les appareils tels que les ordinateurs portables, les tablettes et les smartphones.

Table des matières

Fournisseurs de confiance en matière d'identité utilisateur pour Verified Access

Vous pouvez choisir d'utiliser l'un AWS IAM Identity Center ou l'autre fournisseur de confiance en matière d'identité utilisateur compatible avec OpenID Connect.

Table des matières

Utiliser IAM Identity Center en tant que fournisseur de confiance

Vous pouvez l'utiliser AWS IAM Identity Center comme fournisseur de confiance en matière d'identité utilisateur avec AWS Verified Access.

Prérequis et considérations

- Votre instance IAM Identity Center doit être une AWS Organizations instance. Une instance IAM Identity Center de AWS compte autonome ne fonctionnera pas.
- Votre instance IAM Identity Center doit être activée dans la même AWS région que celle dans laquelle vous souhaitez créer le fournisseur de confiance Verified Access.

Voir Gérer les instances d'organisation et de compte d'IAMIdentity Center dans le guide de AWS IAM Identity Center l'utilisateur pour plus de détails sur les différents types d'instances.

Création d'un fournisseur de confiance IAM Identity Center

Une fois IAM Identity Center activé sur votre AWS compte, vous pouvez utiliser la procédure suivante pour configurer IAM Identity Center en tant que fournisseur de confiance pour l'accès vérifié.

Pour créer un fournisseur de confiance IAM Identity Center (AWS console)

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access trust providers, puis Create Verified Access trust provider.
3. (Facultatif) Dans les champs Name tag et Description, entrez un nom et une description pour le fournisseur de confiance.
4. Pour le nom de référence de la stratégie, entrez un identifiant à utiliser ultérieurement lors de l'utilisation des règles de stratégie.
5. Sous Type de fournisseur de confiance, sélectionnez Fournisseur de confiance utilisateur.
6. Sous Type de fournisseur de confiance utilisateur, sélectionnez IAMIdentity Center.
7. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
8. Choisissez Create Verified Access trust provider.

Pour créer un fournisseur de confiance IAM Identity Center (AWS CLI)

- create-verified-access-trust-fournisseur ()AWS CLI

Supprimer un fournisseur de confiance IAM Identity Center

Avant de pouvoir supprimer un fournisseur de confiance, vous devez supprimer toutes les configurations de point de terminaison et de groupe de l'instance à laquelle le fournisseur de confiance est attaché.

Pour supprimer un fournisseur de confiance IAM Identity Center (AWS console)

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access trust providers, puis sélectionnez le fournisseur de confiance que vous souhaitez supprimer sous Verified Access trust providers.
3. Choisissez Actions, puis Supprimer le fournisseur de confiance Verified Access.
4. Confirmez la suppression en entrant `delete` dans la zone de texte.
5. Sélectionnez Delete (Supprimer).

Pour supprimer un fournisseur de confiance IAM Identity Center (AWS CLI)

- delete-verified-access-trust-fournisseur ()AWS CLI

Utiliser un fournisseur de confiance OpenID Connect

Accès vérifié par AWS prend en charge les fournisseurs d'identité qui utilisent les méthodes standard OpenID Connect (OIDC). Vous pouvez utiliser des fournisseurs OIDC compatibles en tant que fournisseurs de confiance en matière d'identité utilisateur avec Verified Access. Cependant, en raison du large éventail de OIDC fournisseurs potentiels, AWS il n'est pas en mesure de tester chaque OIDC intégration avec Verified Access.

Verified Access obtient les données de confiance qu'il évalue auprès du OIDC fournisseur. `UserInfo Endpoint` Le `Scope` paramètre est utilisé pour déterminer quels ensembles de données de confiance seront récupérés. Une fois les données de confiance reçues, la politique d'accès vérifié est évaluée par rapport à celles-ci.

> **Note**
>
> Verified Access n'utilise pas les données de confiance `ID token` envoyées par le OIDC fournisseur lors de l'évaluation de la politique d'accès vérifié. Seules les données de confiance provenant de `UserInfo Endpoint` sont évaluées par rapport à la politique.

Table des matières

Conditions préalables à la création d'un fournisseur de OIDC confiance

Vous devrez recueillir les informations suivantes directement auprès du service de votre fournisseur de confiance :

- Emetteur
- Point final d'autorisation
- Point de terminaison de jeton
- UserInfo point final
- ID de client
- Secret client
- Portée

Créez un fournisseur de OIDC confiance

Utilisez la procédure suivante pour créer un OIDC en tant que fournisseur de confiance.

Pour créer un fournisseur de OIDC confiance (AWS console)

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access trust providers, puis Create Verified Access trust provider.
3. (Facultatif) Dans les champs Name tag et Description, entrez un nom et une description pour le fournisseur de confiance.
4. Pour le nom de référence de la stratégie, entrez un identifiant à utiliser ultérieurement lors de l'utilisation des règles de stratégie.
5. Sous Type de fournisseur de confiance, sélectionnez Fournisseur de confiance utilisateur.
6. Sous Type de fournisseur de confiance utilisateur, sélectionnez OIDC(OpenID Connect).

7. Dans Émetteur, entrez l'identifiant de l'OIDCémetteur.
8. Pour Point de terminaison d'autorisation, entrez la valeur complète URL du point de terminaison d'autorisation.
9. Pour le point de terminaison du jeton, entrez la valeur complète URL du point de terminaison du jeton.
10. Pour Point de terminaison utilisateur, entrez la valeur complète URL du point de terminaison utilisateur.
11. Entrez l'identifiant du client OAuth 2.0 pour l'ID client.
12. Entrez le secret client OAuth 2.0 pour le secret client.
13. Entrez une liste délimitée par des espaces de champs définis avec votre fournisseur d'identité. Au minimum, la portée « openid » est requise pour Scope.
14. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
15. Choisissez Create Verified Access trust provider.

> **Note**
>
> Vous devrez ajouter une redirection URI vers la liste d'autorisation de votre OIDC fournisseur. Vous souhaiterez utiliser le point `ApplicationDomain` de terminaison Verified Access à cette fin. Vous pouvez le trouver dans l' AWS Management Console onglet Détails de votre point de terminaison d'accès vérifié ou en utilisant le AWS CLI pour décrire le point de terminaison. Ajoutez ce qui suit à la liste des autorisations de votre OIDC fournisseur : https ://`ApplicationDomain`/oauth2/idpresponse

Pour créer un fournisseur de OIDC confiance (AWS CLI)

- create-verified-access-trust-fournisseur ()AWS CLI

Modifier un fournisseur de OIDC confiance

Après avoir créé un fournisseur de confiance, vous pouvez mettre à jour sa configuration.

Pour modifier un fournisseur de OIDC confiance (AWS console)

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.

2. Dans le volet de navigation, choisissez Fournisseurs de confiance Verified Access, puis sélectionnez le fournisseur de confiance que vous souhaitez modifier sous Fournisseurs de confiance Verified Access.
3. Choisissez Actions, puis Modifier le fournisseur de confiance Verified Access.
4. Modifiez les options que vous souhaitez modifier.
5. Choisissez Modifier le fournisseur de confiance Verified Access.

Pour modifier un fournisseur de OIDC confiance (AWS CLI)

- modify-verified-access-trust-fournisseur ()AWS CLI

Supprimer un fournisseur de OIDC confiance

Avant de supprimer un fournisseur de confiance utilisateur, vous devez d'abord supprimer toutes les configurations de point de terminaison et de groupe de l'instance à laquelle le fournisseur de confiance est attaché.

Pour supprimer un fournisseur de OIDC confiance (AWS console)

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access trust providers, puis sélectionnez le fournisseur de confiance que vous souhaitez supprimer sous Verified Access trust providers.
3. Choisissez Actions, puis Supprimer le fournisseur de confiance Verified Access.
4. Confirmez la suppression en entrant `delete` dans la zone de texte.
5. Sélectionnez Delete (Supprimer).

Pour supprimer un fournisseur de OIDC confiance (AWS CLI)

- delete-verified-access-trust-fournisseur ()AWS CLI

Fournisseurs de confiance basés sur les appareils pour un accès vérifié

Vous pouvez utiliser des fournisseurs de confiance en matière d'appareils dotés d' AWS un accès vérifié. Vous pouvez utiliser un ou plusieurs fournisseurs de confiance pour appareils avec votre instance Verified Access.

Table des matières

Fournisseurs de confiance en matière d'appareils compatibles

Les fournisseurs de confiance en matière d'appareils suivants peuvent être intégrés à Verified Access :

- CrowdStrike — Sécurisation des applications privées avec CrowdStrike accès vérifié
- Jamf — Intégration de l'accès vérifié à l'identité des appareils Jamf
- JumpCloud — Intégration JumpCloud et accès AWS vérifié

Création d'un fournisseur de confiance basé sur l'appareil

Suivez ces étapes pour créer et configurer un fournisseur de confiance pour les appareils à utiliser avec Verified Access.

Pour créer un fournisseur de confiance pour les appareils à accès vérifié (AWS console)

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access trust providers, puis Create Verified Access trust provider.
3. (Facultatif) Dans les champs Name tag et Description, entrez un nom et une description pour le fournisseur de confiance.

4. Entrez un identifiant à utiliser ultérieurement lorsque vous utiliserez des règles de stratégie pour le nom de référence de la stratégie.
5. Pour le type de fournisseur de confiance, sélectionnez Identité de l'appareil.
6. Pour le type d'identité de l'appareil CrowdStrike, choisissez Jamf ou JumpCloud.
7. Dans le champ ID du locataire, entrez l'identifiant de l'application du locataire.
8. (Facultatif) Pour la clé de signature publique URL, entrez la clé unique URL partagée par le fournisseur de confiance de votre appareil. (Ce paramètre n'est pas obligatoire pour Jamf CrowdStrike ou Jumpcloud.)
9. Choisissez Create Verified Access trust provider.

> **Note**
>
> Vous devrez ajouter une redirection URI vers la liste d'autorisation de votre OIDC fournisseur. Vous souhaiterez utiliser le point `DeviceValidationDomain` de terminaison Verified Access à cette fin. Vous pouvez le trouver dans l' AWS Management Console onglet Détails de votre point de terminaison d'accès vérifié ou en utilisant le AWS CLI pour décrire le point de terminaison. Ajoutez ce qui suit à la liste des autorisations de votre OIDC fournisseur : https ://`DeviceValidationDomain`/oauth2/idpresponse

Pour créer un fournisseur de confiance pour les appareils à accès vérifié (AWS CLI)

- create-verified-access-trust-fournisseur ()AWS CLI

Modifier un fournisseur de confiance basé sur un appareil

Après avoir créé un fournisseur de confiance, vous pouvez mettre à jour sa configuration.

Pour modifier un fournisseur de confiance pour les appareils à accès vérifié (AWS console)

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access trust providers.
3. Sélectionnez le fournisseur de confiance.
4. Choisissez Actions, puis sélectionnez Modifier le fournisseur de confiance Verified Access.
5. Modifiez la description selon vos besoins.

6. (Facultatif) Pour la clé de signature publique URL, modifiez la clé unique URL partagée par le fournisseur de confiance de votre appareil. (Ce paramètre n'est pas obligatoire si le fournisseur de confiance de votre appareil est Jamf CrowdStrike ou Jumpcloud.)
7. Choisissez Modifier le fournisseur de confiance Verified Access.

Pour modifier un fournisseur de confiance d'un appareil à accès vérifié (AWS CLI)

- modify-verified-access-trust-fournisseur ()AWS CLI

Supprimer un fournisseur de confiance basé sur un appareil

Lorsque vous en avez terminé avec un fournisseur de confiance, vous pouvez le supprimer.

Pour supprimer un fournisseur de confiance d'appareils à accès vérifié (AWS console)

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access trust providers.
3. Sélectionnez le fournisseur de confiance que vous souhaitez supprimer sous Fournisseurs de confiance à accès vérifié.
4. Choisissez Actions, puis sélectionnez Supprimer le fournisseur de confiance Verified Access.
5. Lorsque vous êtes invité à confirmer, saisissez **`delete`**, puis choisissez Delete (Supprimer).

Pour supprimer un fournisseur de confiance d'appareils à accès vérifié (AWS CLI)

- delete-verified-access-trust-fournisseur ()AWS CLI

Groupes d'accès vérifiés

Un Accès vérifié par AWS groupe est un ensemble de points de terminaison d'accès vérifié et une politique d'accès vérifié au niveau du groupe. Chaque point de terminaison d'un groupe partage la politique d'accès vérifié. Vous pouvez utiliser des groupes pour rassembler des points de terminaison présentant des exigences de sécurité communes. Cela peut contribuer à simplifier l'administration des politiques en utilisant une seule stratégie pour répondre aux besoins de sécurité de plusieurs applications.

Par exemple, vous pouvez regrouper toutes les applications de vente et définir une politique d'accès à l'échelle du groupe. Vous pouvez ensuite utiliser cette politique pour définir un ensemble commun d'exigences de sécurité minimales pour toutes les applications commerciales. Cette approche permet de simplifier l'administration des politiques.

Lorsque vous créez un groupe, vous devez l'associer à une instance d'accès vérifié. Au cours du processus de création d'un point de terminaison, vous associerez le point de terminaison à un groupe.

Tâches

- Création d'un groupe d'accès vérifié
- Modifier une politique de groupe d'accès vérifié
- Supprimer un groupe d'accès vérifié

Création d'un groupe d'accès vérifié

Utilisez la procédure suivante pour créer un groupe d'accès vérifié.

Pour créer un groupe d'accès vérifié

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Groupes d'accès vérifiés, puis Créer un groupe d'accès vérifié.
3. (Facultatif) Pour le tag de nom et la description, entrez un nom et une description pour le groupe.
4. Pour l'instance Verified Access, sélectionnez une instance Verified Access à associer au groupe.
5. (Facultatif) Pour la définition de la politique, entrez une politique d'accès vérifié à appliquer au groupe.

6. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
7. Choisissez Créer un groupe d'accès vérifié.

Modifier une politique de groupe d'accès vérifié

Utilisez la procédure suivante pour modifier une politique de groupe Verified Access.

Pour modifier une politique de groupe d'accès vérifié

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Groupes d'accès vérifiés, puis sélectionnez le groupe dont vous souhaitez modifier la politique.
3. Choisissez Actions, puis Modifier la politique de groupe d'accès vérifié.
4. (Facultatif) Activez ou désactivez la politique d'activation en fonction de votre objectif actuel.
5. (Facultatif) Pour Politique, entrez une politique d'accès vérifié à appliquer au groupe.
6. Choisissez Modifier la politique de groupe d'accès vérifié.

Supprimer un groupe d'accès vérifié

Lorsque vous avez terminé avec un groupe d'accès vérifié, vous pouvez le supprimer.

Pour supprimer un groupe d'accès vérifié

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Groupes d'accès vérifiés.
3. Sélectionnez le groupe .
4. Choisissez Actions, puis Supprimer le groupe d'accès vérifié.
5. Lorsque vous êtes invité à confirmer, saisissez **`delete`**, puis choisissez Delete (Supprimer).

Points de terminaison d'accès vérifiés

Un point de terminaison d'accès vérifié représente une application. Chaque point de terminaison est associé à un groupe d'accès vérifié et hérite de la stratégie d'accès du groupe. Vous pouvez éventuellement associer une politique de point de terminaison spécifique à l'application à chaque point de terminaison.

Table des matières

Types de points de terminaison d'accès vérifiés

Les types de point de terminaison d'accès vérifié possibles sont les suivants :

- Équilibreur de charge : les demandes d'application sont envoyées à un équilibreur de charge pour être distribuées à votre application.
- Interface réseau : les demandes d'application sont envoyées à une interface réseau à l'aide du protocole et du port spécifiés.

Comment fonctionne Verified Access avec les réseaux partagés VPCs et les sous-réseaux

Les comportements relatifs aux VPC sous-réseaux partagés sont les suivants :

- Les points de terminaison Verified Access sont pris en charge par le partage de VPC sous-réseau. Un participant peut créer un point de terminaison d'accès vérifié dans un sous-réseau partagé.

- Le participant qui a créé le point de terminaison sera le propriétaire du point de terminaison et la seule personne autorisée à modifier le point de terminaison. Le VPC propriétaire ne sera pas autorisé à modifier le point de terminaison.
- Les points de terminaison Verified Access ne peuvent pas être créés dans une zone AWS locale et le partage via les zones locales n'est donc pas possible.

Pour plus d'informations, consultez la section Partagez votre compte VPC avec d'autres comptes dans le guide de VPC l'utilisateur Amazon.

Création d'un point de terminaison d'équilibrage de charge pour Verified Access

Utilisez la procédure suivante pour créer un point de terminaison d'équilibrage de charge pour Verified Access. Pour plus d'informations sur les équilibreurs de charge, consultez le guide de l'utilisateur d'Elastic Load Balancing.

Prérequis

- Seul IPv4 le trafic est pris en charge.
- Seuls les HTTPS protocoles HTTP et sont pris en charge.
- L'équilibreur de charge doit être soit un Application Load Balancer, soit un Network Load Balancer, et il doit s'agir d'un équilibreur de charge interne.
- L'équilibreur de charge et les sous-réseaux doivent appartenir au même cloud privé virtuel ()VPC.
- HTTPSles équilibreurs de charge peuvent utiliser des certificats autosignés ou publicsTLS.
- Vous devez fournir un nom de domaine pour votre application. Il s'agit du DNS nom public que vos utilisateurs utiliseront pour accéder à votre application. Vous devrez également fournir un SSL certificat public avec un CN correspondant à ce nom de domaine. Vous pouvez créer ou importer le certificat à l'aide de AWS Certificate Manager.

Pour créer un point de terminaison d'équilibrage de charge

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access endpoints.
3. Choisissez Créer un point de terminaison d'accès vérifié.

4. (Facultatif) Dans les champs Name tag et Description, entrez un nom et une description pour le point de terminaison.
5. Pour le groupe d'accès vérifié, choisissez un groupe d'accès vérifié pour le point de terminaison.
6. Pour les détails de l'application, procédez comme suit :
    a. Dans le champ Domaine de l'application, entrez DNS le nom de votre application.
    b. Sous Certificat de domaine ARN, choisissez le TLS certificat public.
7. Pour obtenir des informations détaillées sur le point de terminaison, procédez comme suit :
    a. Pour Type de pièce jointe, sélectionnez VPC.
    b. Pour les groupes de sécurité, choisissez les groupes de sécurité pour le point de terminaison. Le trafic provenant du point de terminaison Verified Access qui entre dans votre équilibreur de charge sera associé à ce groupe de sécurité.
    c. Pour le préfixe de domaine du point de terminaison, entrez un identifiant personnalisé à ajouter au DNS nom généré par Verified Access pour le point de terminaison.
    d. Pour le type de point de terminaison, choisissez l'équilibreur de charge.
    e. Dans Protocole, sélectionnez HTTPSou HTTP.
    f. Sous Port, entrez le numéro de port.
    g. Pour Équilibreur de chargeARN, choisissez l'équilibreur de charge.
    h. Pour les sous-réseaux, choisissez les sous-réseaux pour votre équilibreur de charge.
8. (Facultatif) Pour la définition de la politique, entrez une politique d'accès vérifié pour le point de terminaison.
9. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l’identification.
10. Choisissez Créer un point de terminaison d'accès vérifié.

Création d'un point de terminaison d'interface réseau pour Verified Access

Utilisez la procédure suivante pour créer un point de terminaison d'interface réseau.

Prérequis

- Seul IPv4 le trafic est pris en charge.

- Seuls les HTTPS protocoles HTTP et sont pris en charge.
- L'interface réseau doit appartenir au même cloud privé virtuel (VPC) que les groupes de sécurité.
- Nous utilisons l'adresse IP privée sur l'interface réseau pour transférer le trafic.
- Vous devez fournir un nom de domaine pour votre application. Il s'agit du DNS nom public que vos utilisateurs utiliseront pour accéder à votre application. Vous devrez également fournir un SSL certificat public avec un CN correspondant à ce nom de domaine. Vous pouvez créer ou importer le certificat à l'aide de AWS Certificate Manager.

Pour créer un point de terminaison d'interface réseau

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access endpoints.
3. Choisissez Créer un point de terminaison d'accès vérifié.
4. (Facultatif) Dans les champs Name tag et Description, entrez un nom et une description pour le point de terminaison.
5. Pour le groupe d'accès vérifié, choisissez un groupe d'accès vérifié pour le point de terminaison.
6. Pour les détails de l'application, procédez comme suit :
   a. Dans le champ Domaine de l'application, entrez le DNS nom de votre application.
   b. Sous Certificat de domaine ARN, choisissez le TLS certificat public.
7. Pour obtenir des informations détaillées sur le point de terminaison, procédez comme suit :
   a. Pour Type de pièce jointe, sélectionnez VPC.
   b. Pour les groupes de sécurité, choisissez les groupes de sécurité pour le point de terminaison. Le trafic provenant du point de terminaison d'accès vérifié qui entre dans votre interface réseau sera associé à ce groupe de sécurité.
   c. Pour le préfixe de domaine du point de terminaison, entrez un identifiant personnalisé à ajouter au DNS nom généré par Verified Access pour le point de terminaison.
   d. Pour le type de point de terminaison, choisissez Interface réseau.
   e. Dans Protocole, sélectionnez HTTPSou HTTP.
   f. Sous Port, entrez le numéro de port.
   g. Pour Interface réseau, choisissez l'interface réseau.
8. (Facultatif) Pour la définition de la politique, entrez une politique d'accès vérifié pour le point de terminaison.

9. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
10. Choisissez Créer un point de terminaison d'accès vérifié.

Autoriser le trafic provenant de votre point de terminaison Verified Access

Vous pouvez configurer les groupes de sécurité pour vos applications afin qu'ils autorisent le trafic provenant de votre point de terminaison Verified Access. Pour ce faire, ajoutez une règle entrante qui indique le groupe de sécurité du point de terminaison comme source. Nous vous recommandons de supprimer toutes les règles entrantes supplémentaires afin que votre application ne reçoive du trafic que depuis votre point de terminaison Verified Access.

Nous vous recommandons de conserver vos règles sortantes existantes.

Pour mettre à jour les règles du groupe de sécurité pour votre application

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access endpoints.
3. Choisissez le point de terminaison d'accès vérifié, recherchez IDs le groupe de sécurité dans l'onglet Détails et copiez l'ID du groupe de sécurité pour votre point de terminaison.
4. Dans le panneau de navigation, choisissez Groupes de sécurité.
5. Cochez la case correspondant au groupe de sécurité associé à votre cible, puis choisissez Actions, Modifier les règles entrantes.
6. Pour ajouter une règle de groupe de sécurité autorisant le trafic provenant de votre point de terminaison Verified Access, procédez comme suit :
    a. Choisissez Ajouter une règle.
    b. Dans Type, choisissez Tout le trafic ou le trafic spécifique à autoriser.
    c. Pour Source, choisissez Personnalisé et collez l'ID du groupe de sécurité de votre terminal.
7. (Facultatif) Pour exiger que le trafic provienne uniquement de votre point de terminaison Verified Access, supprimez toutes les autres règles du groupe de sécurité entrant.
8. Sélectionnez Enregistrer les règles.

Modifier un point de terminaison d'accès vérifié

Après avoir créé un point de terminaison d'accès vérifié, vous pouvez modifier sa configuration.

Pour modifier un point de terminaison d'accès vérifié

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access endpoints.
3. Sélectionnez le point de terminaison.
4. Choisissez Actions, Modifier le point de terminaison d'accès vérifié.
5. Modifiez les détails du point de terminaison selon vos besoins.
6. Choisissez Modifier le point de terminaison d'accès vérifié.

Modifier une politique de point de terminaison d'accès vérifié

Après avoir créé un point de terminaison d'accès vérifié, vous pouvez modifier sa politique.

Pour modifier une politique de point de terminaison d'accès vérifié

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Verified Access endpoints.
3. Sélectionnez le point de terminaison dont vous souhaitez modifier la politique.
4. Choisissez Actions, puis Modifier la politique du point de terminaison d'accès vérifié.
5. (Facultatif) Activez ou désactivez la politique d'activation en fonction de votre objectif actuel.
6. (Facultatif) Pour Politique, entrez une politique d'accès vérifié à appliquer au point de terminaison.
7. Choisissez Modifier la politique du point de terminaison d'accès vérifié.

Supprimer un point de terminaison d'accès vérifié

Lorsque vous avez terminé d'utiliser un point de terminaison d'accès vérifié, vous pouvez le supprimer.

Pour supprimer un point de terminaison avec accès vérifié

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.

2. Dans le volet de navigation, choisissez Verified Access endpoints.
3. Sélectionnez le point de terminaison.
4. Choisissez Actions, puis Supprimer le point de terminaison d'accès vérifié.
5. Lorsque vous êtes invité à confirmer, entrez **`delete`**, puis choisissez Delete (Supprimer).

Données de confiance envoyées à Verified Access par des fournisseurs de confiance

Les données de confiance sont des données envoyées Accès vérifié par AWS par un fournisseur de confiance. Les données de confiance sont également appelées « réclamations des utilisateurs » ou « contexte de confiance ». Les données incluent généralement des informations concernant un utilisateur ou un appareil. Les exemples de données de confiance incluent le courrier électronique de l'utilisateur, l'appartenance à un groupe, la version du système d'exploitation de l'appareil, l'état de sécurité de l'appareil, etc. Les informations envoyées varient en fonction du fournisseur de confiance. Vous devez donc vous référer à la documentation de votre fournisseur de confiance pour obtenir une liste complète et actualisée des données de confiance.

Toutefois, en utilisant les fonctionnalités de journalisation des accès vérifiés, vous pouvez également voir quelles données de confiance sont envoyées par votre fournisseur de confiance. Cela peut être utile lorsque vous définissez des politiques qui autorisent ou refusent l'accès à vos applications. Pour plus d'informations sur l'inclusion d'un contexte de confiance dans vos journaux, consultezActiver ou désactiver le contexte de confiance d'accès vérifié.

Cette section contient des exemples de données de confiance et des exemples pour vous aider à commencer à rédiger des politiques. Les informations fournies ici sont uniquement destinées à des fins d'illustration et ne constituent pas une référence officielle.

Table des matières

Contexte par défaut pour les données de confiance Verified Access

Accès vérifié par AWS inclut par défaut certains éléments relatifs à la HTTP demande en cours dans toutes les évaluations de Cedar, quels que soient vos fournisseurs de confiance configurés. Lorsqu'une politique est évaluée, Verified Access inclut les données relatives à la HTTP demande en cours dans le contexte de Cedar sous le`context.http_request key`. Vous pouvez rédiger une

politique qui évalue par rapport aux données si vous le souhaitez. Le JSONschéma suivant indique quelles données sont incluses dans l'évaluation.

```
{
     "title": "HTTP Request data included by Verified Access",
     "type": "object",
     "properties": {
         "user_agent": {
             "type": "string",
             "description": "The value of the User-Agent request header"
         },
         "x_forwarded_for": {
             "type": "string",
             "description": "The value of the X-Forwarded-For request header"
         },
         "http_method": {
             "type": "string",
             "description": "The HTTP Method provided (e.g. GET or POST)"
         },
         "hostname": {
             "type": "string",
             "description": "The value of the Host request header"
         },
         "port": {
            "type": "integer",
            "description": "The value of the verified access endpoint port"
         },
         "client_ip": {
             "type": "string",
             "description": "User ip connecting to the verified access endpoint"
         }
     }
 }
```

Voici un exemple de politique qui évalue par rapport aux données de la HTTP demande.

```
forbid(principal, action, resource) when {
   context.http_request.http_method == "POST"
   && !(context.identity.roles.contains("Administrator"))
 };
```

AWS IAM Identity Center contexte pour les données de confiance Verified Access

Lorsqu'une politique est évaluée, si vous la définissez en AWS IAM Identity Center tant que fournisseur de confiance, Accès vérifié par AWS inclut les données de confiance dans le contexte Cedar sous la clé que vous spécifiez comme « nom de référence de la politique » dans la configuration du fournisseur de confiance. Vous pouvez rédiger une politique qui évalue par rapport aux données de confiance si vous le souhaitez.

> **Note**
>
> La clé de contexte de votre fournisseur de confiance provient du nom de référence de politique que vous configurez lorsque vous créez le fournisseur de confiance. Par exemple, si vous configurez le nom de référence de la politique comme « idp123 », la clé de contexte sera « context.idp123 ». Vérifiez que vous utilisez la bonne clé de contexte lorsque vous créez la politique.

Le JSONschéma suivant indique quelles données sont incluses dans l'évaluation.

```
{
   "title": "AWS IAM Identity Center context specification",
   "type": "object",
   "properties": {
     "user": {
       "type": "object",
       "properties": {
         "user_id": {
           "type": "string",
           "description": "a unique user id generated by AWS IdC"
         },
         "user_name": {
           "type": "string",
           "description": "username provided in the directory"
         },
         "email": {
           "type": "object",
           "properties": {
             "address": {
               "type": "email",
```

```
              "description": "email address associated with the user"
            },
            "verified": {
              "type": "boolean",
              "description": "whether the email address has been verified by AWS IdC"
            }
          }
        }
      }
    },
    "groups": {
      "type": "object",
      "description": "A list of groups the user is a member of",
      "patternProperties": {
        "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{12}$": {
          "type": "object",
          "description": "The Group ID of the group",
          "properties": {
            "group_name": {
              "type": "string",
              "description": "The customer-provided name of the group"
            }
          }
        }
      }
    }
  }
}
```

Voici un exemple de politique qui évalue par rapport aux données de confiance fournies par AWS IAM Identity Center.

```
permit(principal, action, resource) when {
   context.idc.user.email.verified == true
   // User is in the "sales" group with specific ID
   && context.idc.groups has "c242c5b0-6081-1845-6fa8-6e0d9513c107"
};
```

> **Note**
>
> Comme les noms de groupes peuvent être modifiés, IAM Identity Center fait référence aux groupes en utilisant leur identifiant de groupe. Cela permet d'éviter de violer une déclaration de politique lorsque vous modifiez le nom d'un groupe.

Contexte du fournisseur de confiance tiers pour les données de confiance Verified Access

Cette section décrit les données de confiance fournies Accès vérifié par AWS par les fournisseurs de confiance tiers.

> **Note**
>
> La clé de contexte de votre fournisseur de confiance provient du nom de référence de politique que vous configurez lorsque vous créez le fournisseur de confiance. Par exemple, si vous configurez le nom de référence de la politique comme « idp123 », la clé de contexte sera « context.idp123 ». Assurez-vous d'utiliser la bonne clé de contexte lorsque vous créez la politique.

Table des matières

Extension de navigateur

Si vous envisagez d'intégrer un contexte de confiance aux appareils dans vos politiques d'accès, vous aurez besoin de l'extension de navigateur AWS Verified Access ou de l'extension de navigateur d'un autre partenaire. Verified Access est actuellement compatible avec les navigateurs Google Chrome et Mozilla Firefox.

Nous soutenons actuellement trois fournisseurs de confiance en matière d'appareils : Jamf (qui prend en charge les appareils macOS), CrowdStrike (qui prend en charge les appareils Windows 11 et Windows 10) et JumpCloud (qui prend en charge à la fois Windows et macOS).

- Si vous utilisez les données de confiance Jamf dans vos politiques, vos utilisateurs doivent télécharger et installer l'extension de Accès vérifié par AWS navigateur depuis le Chrome Web Store ou le site du module complémentaire Firefox sur leurs appareils.
- Si vous utilisez des données de CrowdStrikeconfiance dans vos politiques, vos utilisateurs doivent d'abord installer le Accès vérifié par AWS Native Messaging Host (lien de téléchargement direct). Ce composant est nécessaire pour obtenir les données de confiance de l' CrowdStrike agent exécuté sur les appareils des utilisateurs. Ensuite, après avoir installé ce composant, les utilisateurs doivent installer l'extension de Accès vérifié par AWS navigateur depuis le Chrome Web Store ou le site du module complémentaire Firefox sur leurs appareils.
- Si vous l'utilisez JumpCloud, l'extension de JumpCloud navigateur du Chrome Web Store ou du site du module complémentaire Firefox doit être installée sur leurs appareils.

Jamf

Jamf est un fournisseur de confiance tiers. Lorsqu'une politique est évaluée, si vous définissez Jamf comme un fournisseur de confiance, Verified Access inclut les données de confiance dans le contexte Cedar sous la clé que vous spécifiez comme « nom de référence de la politique » dans la configuration du fournisseur de confiance. Vous pouvez rédiger une politique qui évalue par rapport aux données de confiance si vous le souhaitez. Le JSONschéma suivant indique quelles données sont incluses dans l'évaluation.

Pour plus d'informations sur l'utilisation de Jamf avec accès vérifié, consultez la section Intégration de l'accès AWS vérifié à Jamf Device Identity sur le site Web de Jamf.

```
{
    "title": "Jamf device data specification",
    "type": "object",
    "properties": {
        "iss": {
            "type": "string",
            "description": "\"Issuer\" - the Jamf customer ID"
        },
        "iat": {
            "type": "integer",
```

```
            "description": "\"Issued at Time\" - a unixtime (seconds since epoch) value
 of when the device information data was generated"
        },
        "exp": {
            "type": "integer",
            "description": "\"Expiration\" - a unixtime (seconds since epoch) value for
 when this device information is no longer valid"
        },
        "sub": {
            "type": "string",
            "description": "\"Subject\" - either the hardware UID or a value generated
 based on device location"
        },
        "groups": {
            "type": "array",
            "description": "Group IDs from UEM connector sync",
            "items": {
                "type": "string"
            }
        },
        "risk": {
            "type": "string",
            "enum": [
                "HIGH",
                "MEDIUM",
                "LOW",
                "SECURE",
                "NOT_APPLICABLE"
            ],
            "description": "a Jamf-reported level of risk associated with the device."
        },
        "osv": {
            "type": "string",
            "description": "The version of the OS that is currently running, in Apple
 version number format (https://support.apple.com/en-us/HT201260)"
        }
    }
}
```

Voici un exemple de politique qui évalue par rapport aux données de confiance fournies par Jamf.

```
permit(principal, action, resource) when {
   context.jamf.risk == "LOW"
```

```
};
```

Cedar fournit une `.contains()` fonction utile pour vous aider avec des énumérations telles que le score de risque de Jamf.

```
permit(principal, action, resource) when {
   ["LOW", "SECURE"].contains(context.jamf.risk)
};
```

CrowdStrike

CrowdStrike est un fournisseur de confiance tiers. Lorsqu'une politique est évaluée, si vous la définissez en CrowdStrike tant que fournisseur de confiance, Verified Access inclut les données de confiance dans le contexte Cedar sous la clé que vous spécifiez comme « nom de référence de la politique » dans la configuration du fournisseur de confiance. Vous pouvez rédiger une politique qui évalue par rapport aux données de confiance si vous le souhaitez. Le JSONschéma suivant indique quelles données sont incluses dans l'évaluation.

Pour plus d'informations sur l'utilisation CrowdStrike avec Verified Access, voir Sécurisation des applications privées avec CrowdStrike et Accès vérifié par AWS sur le GitHub site Web.

```
{
  "title": "CrowdStrike device data specification",
  "type": "object",
  "properties": {
    "assessment": {
      "type": "object",
      "description": "Data about CrowdStrike's assessment of the device",
      "properties": {
        "overall": {
          "type": "integer",
          "description": "A single metric, between 1-100, that accounts as a weighted
 average of the OS and and Sensor Config scores"
        },
        "os": {
          "type": "integer",
          "description": "A single metric, between 1-100, that accounts for the OS-
specific settings monitored on the host"
        },
        "sensor_config": {
          "type": "integer",
```

```
          "description": "A single metric, between 1-100, that accounts for the
different sensor policies monitored on the host"
        },
        "version": {
          "type": "string",
          "description": "The version of the scoring algorithm being used"
        }
      }
    },
    "cid": {
      "type": "string",
      "description": "Customer ID (CID) unique to the customer's environemnt"
    },
    "exp": {
      "type": "integer",
      "description": "unixtime, The expiration time of the token"
    },
    "iat": {
      "type": "integer",
      "description": "unixtime, The issued time of the token"
    },
    "jwk_url": {
      "type": "string",
      "description": "URL that details the JWT signing"
    },
    "platform": {
      "type": "string",
      "enum": ["Windows 10", "Windows 11", "macOS"],
      "description": "Operating system of the endpoint"
    },
    "serial_number": {
      "type": "string",
      "description": "The serial number of the device derived by unique system
information"
    },
    "sub": {
      "type": "string",
      "description": "Unique CrowdStrike Agent ID (AID) of machine"
    },
    "typ": {
      "type": "string",
      "enum": ["crowdstrike-zta+jwt"],
      "description": "Generic name for this JWT media. Client MUST reject any other
type"
```

```
    }
  }
}
```

Voici un exemple de politique qui évalue par rapport aux données de confiance fournies par CrowdStrike.

```
permit(principal, action, resource) when {
   context.crowdstrike.assessment.overall > 50
};
```

JumpCloud

JumpCloud est un fournisseur de confiance tiers. Lorsqu'une politique est évaluée, si vous la définissez en JumpCloud tant que fournisseur de confiance, Verified Access inclut les données de confiance dans le contexte Cedar sous la clé que vous spécifiez comme « nom de référence de la politique » dans la configuration du fournisseur de confiance. Vous pouvez rédiger une politique qui évalue par rapport aux données de confiance si vous le souhaitez. Le JSONschéma suivant indique quelles données sont incluses dans l'évaluation.

Pour plus d'informations sur l'utilisation JumpCloud avec AWS Verified Access, voir Intégration JumpCloud et accès AWS vérifié sur le JumpCloud site Web.

```
{
  "title": "JumpCloud device data specification",
  "type": "object",
  "properties": {
    "device": {
      "type": "object",
      "description": "Properties of the device",
      "properties": {
        "is_managed": {
          "type": "boolean",
          "description": "Boolean to indicate if the device is under management"
        }
      }
    },
    "exp": {
      "type": "integer",
      "description": "Expiration. Unixtime of the token's expiration."
    },
```

```
    "durt_id": {
      "type": "string",
      "description": "Device User Refresh Token ID. Unique ID that represents the
 device + user."
    },
    "iat": {
      "type": "integer",
      "description": "Issued At. Unixtime of the token's issuance."
    },
    "iss": {
      "type": "string",
      "description": "Issuer. This will be 'go.jumpcloud.com'"
    },
    "org_id": {
      "type": "string",
      "description": "The JumpCloud Organization ID"
    },
    "sub": {
      "type": "string",
      "description": "Subject. The managed JumpCloud user ID on the device."
    },
    "system": {
      "type": "string",
      "description": "The JumpCloud system ID"
    }
  }
}
```

Voici un exemple de politique qui évalue par rapport au contexte de confiance fourni par JumpCloud.

```
permit(principal, action, resource) when {
   context.jumpcloud.org_id = 'Unique_orgnaization_identifier'
};
```

L'utilisateur affirme avoir réussi et vérifié sa signature dans Verified Access

Une fois qu'une Accès vérifié par AWS instance a authentifié un utilisateur avec succès, elle envoie les demandes d'utilisateur reçues de l'IdP au point de terminaison Verified Access. Les demandes des utilisateurs sont signées afin que les applications puissent vérifier les signatures et également

vérifier que les demandes ont été envoyées par Verified Access. Au cours de ce processus, l'HTTPen-tête suivant est ajouté :

`x-amzn-ava-user-context`

Cet en-tête contient les revendications de l'utilisateur au format JSON web token (JWT). Le JWT format inclut un en-tête, une charge utile et une signature codés en base64URL. Verified Access utilise ES384 (algorithme de ECDSA signature utilisant l'algorithme de hachage SHA -384) pour générer la JWT signature.

Les applications peuvent utiliser ces allégations à des fins de personnalisation ou pour d'autres expériences spécifiques aux utilisateurs. Les développeurs d'applications doivent se renseigner sur le niveau d'unicité et de vérification de chaque réclamation fournie par le fournisseur d'identité avant utilisation. En général, la `sub` réclamation est le meilleur moyen d'identifier un utilisateur donné.

Table des matières

Exemple : Signé JWT pour les réclamations des OIDC utilisateurs

Les exemples suivants montrent à quoi ressembleront l'en-tête et la charge utile des réclamations des OIDC utilisateurs dans le JWT format.

Exemple d'en-tête :

```
{
"alg": "ES384",
"kid": "12345678-1234-1234-1234-123456789012",
"signer": "arn:aws:ec2:us-east-1:123456789012:verified-access-instance/vai-
abc123xzy321a2b3c",
"iss": "OIDC Issuer URL"
"exp": "expiration" (120 secs)
}
```

Exemple de charge utile :

```
{
"sub": "xyzsubject",
"email": "xxx@amazon.com",
"email_verified": true,
"groups": [
"Engineering",
"finance"
]
}
```

Exemple : Signé JWT pour les réclamations des utilisateurs d'IAMIdentity Center

Les exemples suivants montrent à quoi ressembleront l'en-tête et la charge utile des réclamations des utilisateurs d'IAMIdentity Center dans le JWT format.

> **Note**
>
> Pour IAM Identity Center, seules les informations relatives aux utilisateurs seront incluses dans les réclamations.

Exemple d'en-tête :

```
{
"alg": "ES384",
"kid": "12345678-1234-1234-1234-123456789012",
"signer": "arn:aws:ec2:us-east-1:123456789012:verified-access-instance/vai-
abc123xzy321a2b3c",
"iss": "arn:aws:ec2:us-east-1:123456789012:verified-access-trust-provider/vatp-
abc123xzy321a2b3c",
"exp": "expiration" (120 secs)
}
```

Exemple de charge utile :

```
{
"user": {
        "user_id": "f478d4c8-a001-7064-6ea6-12423523",
        "user_name": "test-123",
```

```
        "email": {
            "address": "test@amazon.com",
            "verified": false
        }
    }
}
```

Clés publiques

Étant donné que les instances Verified Access ne chiffrent pas les demandes des utilisateurs, nous vous recommandons de configurer les points de terminaison Verified Access à utiliser. HTTPS Si vous configurez votre point de terminaison Verified Access pour l'utiliserHTTP, veillez à limiter le trafic vers le point de terminaison à l'aide de groupes de sécurité.

Nous vous recommandons de vérifier la signature avant de procéder à toute autorisation sur la base des réclamations. Pour obtenir la clé publique, récupérez l'identifiant de la clé dans l'JWTen-tête et utilisez-le pour rechercher la clé publique depuis le point de terminaison. Le point final de chacun Région AWS est le suivant :

`https://public-keys.prod.verified-access.<region>.amazonaws.com/<key-id>`

Exemple : récupération et décodage JWT

L'exemple de code suivant montre comment obtenir l'ID de clé, la clé publique et la charge utile dans Python 3.9.

```
import jwt
import requests
import base64
import json

# Step 1: Get the key id from JWT headers (the kid field)
encoded_jwt = headers.dict['x-amzn-ava-user-context']
jwt_headers = encoded_jwt.split('.')[0]
decoded_jwt_headers = base64.b64decode(jwt_headers)
decoded_jwt_headers = decoded_jwt_headers.decode("utf-8")
decoded_json = json.loads(decoded_jwt_headers)
kid = decoded_json['kid']

# Step 2: Get the public key from Regional endpoint
```

```
url = 'https://public-keys.prod.verified-access.' + region + '.amazonaws.com/' + kid
req = requests.get(url)
pub_key = req.text

# Step 3: Get the payload
payload = jwt.decode(encoded_jwt, pub_key, algorithms=['ES384'])
```

Politiques d'accès vérifiées

Accès vérifié par AWS les politiques vous permettent de définir des règles d'accès à vos applications hébergées dans AWS. Ils sont rédigés en cèdre, un langage AWS politique. À l'aide de Cedar, vous pouvez créer des politiques qui sont évaluées par rapport aux données de confiance envoyées par les fournisseurs de confiance basés sur l'identité ou les appareils que vous configurez pour utiliser avec Verified Access.

Pour des informations plus détaillées sur le langage politique de Cedar, consultez le guide de référence de Cedar.

Cette section décrit comment les politiques d'accès vérifié sont structurées, ce qu'elles contiennent, comment les définir, et fournit quelques exemples.

Table des matières

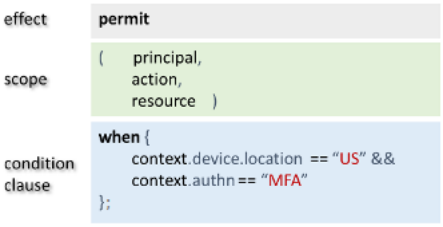
Travaillez avec les politiques d'accès vérifié

Lorsque vous créez un groupe d'accès vérifié ou un point de terminaison d'accès vérifié, vous avez la possibilité de définir la politique d'accès vérifié. Vous pouvez créer un groupe ou un point de terminaison sans définir la politique d'accès vérifié, mais toutes les demandes d'accès seront bloquées jusqu'à ce que vous définissiez une politique.

Pour ajouter ou modifier une politique sur un groupe d'accès vérifié ou un point de terminaison existant après sa création, consultez Modifier une politique de groupe d'accès vérifié ouModifier une politique de point de terminaison d'accès vérifié.

Structure de la déclaration de politique d'accès vérifié

Cette section décrit la déclaration Accès vérifié par AWS de politique et la manière dont elle est évaluée. Vous pouvez avoir plusieurs déclarations dans une seule politique d'accès vérifié. Le schéma suivant montre la structure d'une politique d'accès vérifié.



La politique contient les éléments suivants :

- Effet — Spécifie si la déclaration de politique est `permit` (`Allow`) ou `forbid` (`Deny`).
- Champ d'application — Spécifie les principes, les actions et les ressources auxquels l'effet s'applique. Vous pouvez laisser le champ d'application indéfini dans Cedar en n'identifiant pas de principes, d'actions ou de ressources spécifiques (comme indiqué dans l'exemple précédent). Dans ce cas, la politique s'applique à tous les principes, actions et ressources possibles.
- Clause de condition — Spécifie le contexte dans lequel l'effet s'applique.

> **Important**
>
> Pour l'accès vérifié, les politiques sont pleinement exprimées en faisant référence aux données de confiance dans la clause de condition. Le champ d'application de la politique doit toujours rester indéfini. Vous pouvez ensuite spécifier l'accès en utilisant l'identité et le contexte de confiance de l'appareil dans la clause de condition.

Exemple de politique simple

```
permit(principal,action,resource)
when{
 context.<policy-reference-name>.<attribute> &&
 context.<policy-reference-name>.<attribute2>
};
```

Dans l'exemple précédent, notez que vous pouvez utiliser plusieurs clauses de condition dans une déclaration de politique à l'aide de l'&&opérateur. Le langage politique de Cedar vous donne le pouvoir d'expression nécessaire pour créer des déclarations de politique personnalisées, détaillées et détaillées. Pour accéder à des exemples supplémentaires, consultez Exemples de politiques d'accès vérifié.

Évaluation de la politique d'accès vérifié

Un document de politique est un ensemble d'une ou plusieurs déclarations de politique (`permit`ou `forbid` déclarations). La politique s'applique si la clause conditionnelle (la `when` déclaration) est vraie. Pour qu'un document de politique autorise l'accès, au moins une politique d'autorisation du document doit s'appliquer et aucune politique d'interdiction ne peut s'appliquer. Si aucune politique d'autorisation ne s'applique et/ou si une ou plusieurs politiques d'interdiction s'appliquent, le document de politique refuse l'accès. Si vous avez défini des documents de politique pour le groupe Verified Access et le point de terminaison Verified Access, les deux documents doivent autoriser l'accès. Si vous n'avez pas défini de document de politique pour le point de terminaison Verified Access, seule la politique de groupe Verified Access doit y accéder.

> **Note**
>
> Accès vérifié par AWS valide la syntaxe lorsque vous créez la politique, mais ne valide pas les données que vous avez saisies dans la clause conditionnelle.

Opérateurs intégrés pour les politiques d'accès vérifié

Lorsque vous créez le contexte d'une Accès vérifié par AWS politique à l'aide de diverses conditions, comme indiqué dansStructure de la déclaration de politique d'accès vérifié, vous pouvez utiliser l'&&opérateur pour ajouter des conditions supplémentaires. Il existe également de nombreux autres opérateurs intégrés que vous pouvez utiliser pour ajouter un pouvoir d'expression supplémentaire à vos conditions de politique. Le tableau suivant contient tous les opérateurs intégrés à titre de référence.

Opérateur	Types et surcharges	Description
!	Booléen → Booléen	C'est logique, non.

Opérateur	Types et surcharges	Description
==	n'importe lequel → n'importe quel	Égalité. Fonctionne sur tous les types d'arguments, même si les types ne correspondent pas. Les valeurs de différent s types ne sont jamais égales entre elles.
!=	n'importe lequel → n'importe quel	Inégalité ; l'exact inverse de l'égalité (voir ci-dessus).
<	(long, long) → booléen	Nombre entier long inférieur à.
<=	(long, long) → booléen	Entier long less-than-or-equal -to.
>	(long, long) → booléen	Nombre entier long supérieur à.
>=	(long, long) → booléen	Entier long greater-than-or-eq ual -to.
dans	(entité, entité) → Booléen	Appartenance à la hiérarchi e (réflexive : A dans A est toujours vrai).
	(entité, ensemble (entité)) → booléen	Appartenance à la hiérarchie : A dans [B, C,...] est vrai si (A et B) || (A dans C) ||... erreur si l'ensemble contient une non-entité.
&&	(booléen, booléen) → booléen	Logique et (court-circuit).
||	(booléen, booléen) → booléen	Logique ou (court-circuit).
.existe ()	entité → Booléen	Existence de l'entité.

Opérateur	Types et surcharges	Description
a	(entité, attribut) → Booléen	Opérateur Infix. `e has f` teste si l'enregistrement ou l'entité `e` possède une liaison pour l'attribut`f`. Renvoie `false` s'il `e` n'existe pas ou s'`e`il existe mais n'a pas l'attribu `tf`. Les attributs peuvent être exprimés sous forme d'identif iants ou de chaînes littérales.
like	(chaîne, chaîne) → Booléen	Opérateur Infix. `t like p` vérifie si le texte `t` correspon d au modèle`p`, qui peut inclure des caractères `*` générique s correspondant à 0 ou plus de n'importe quel caractère . Pour faire correspondre un caractère étoile littéral dans`t`, vous pouvez utiliser la séquence spéciale de caractères échappés `\*` dans`p`.
.contient ()	(ensemble, n'importe lequel) → Booléen	Définissez l'appartenance (B est-il un élément de A).
.containsAll()	(set, set) → Booléen	Teste si l'ensemble A contient tous les éléments de l'ensembl e B.
.containsAny()	(set, set) → Booléen	Teste si l'ensemble A contient l'un des éléments de l'ensembl e B.

Commentaires sur la politique d'accès vérifiés

Vous pouvez inclure des déclarations de commentaires dans vos Accès vérifié par AWS politiques. Les commentaires sont définis comme une ligne commençant par une nouvelle ligne `//` et se terminant par une nouvelle ligne.

L'exemple suivant montre les déclarations de commentaires contenues dans la politique.

```
// this policy grants access to users in a given domain with trusted devices
permit(principal, action, resource)
when {
  // the user's email address is in the @example.com domain
  context.idc.user.email.address.contains("@example.com")
  // Jamf thinks the user's computer is low risk or secure.
  && ["LOW", "SECURE"].contains(context.jamf.risk)
};
```

Court-circuit logique de politique d'accès vérifié

Vous souhaiterez peut-être rédiger une Accès vérifié par AWS politique évaluant les données présentes ou non dans un contexte donné. Si vous référencez des données dans un contexte qui n'existe pas, Cedar produira une erreur et évaluera la politique de refus d'accès, quelle que soit votre intention. Par exemple, cela entraînerait un refus, car `fake_provider` cela `bogus_key` n'existe pas dans ce contexte.

```
permit(principal, action, resource) when {
  context.fake_provider.bogus_key > 42
};
```

Pour éviter cette situation, vous pouvez vérifier si une clé est présente en utilisant l'`has`opérateur. Si l'`has`opérateur renvoie la valeur false, l'évaluation ultérieure de l'instruction chaînée est interrompue et Cedar ne produit aucune erreur en tentant de faire référence à un élément qui n'existe pas.

```
permit(principal, action, resource) when {
  context.identity.user has "some_key" && context.identity.user.some_key > 42
};
```

Cela est particulièrement utile lorsque vous spécifiez une politique qui fait référence à deux fournisseurs de confiance différents.

```
permit(principal, action, resource) when {
  // user is in an allowed group
  context.aws_idc.groups has "c242c5b0-6081-1845-6fa8-6e0d9513c107"
  &&(
    (
      // if CrowdStrike data is present,
      // permit if CrowdStrike's overall assessment is over 50
      context has "crowdstrike" && context.crowdstrike.assessment.overall > 50
    )
    ||
    (
      // if Jamf data is present,
      // permit if Jamf's risk score is acceptable
      context has "jamf" && ["LOW", "NOT_APPLICABLE", "MEDIUM",
 "SECURE"].contains(context.jamf.risk)
    )
  )
};
```

Exemples de politiques d'accès vérifié

Exemple 1 : création de politiques pour IAM Identity Center

> **Note**
>
> Comme les noms de groupes peuvent être modifiés, IAM Identity Center fait référence aux groupes en utilisant leur identifiant de groupe. Cela permet d'éviter de violer une déclaration de politique lorsque vous modifiez le nom d'un groupe.

L'exemple de politique suivant autorise l'accès uniquement lorsqu'un utilisateur appartient au `finance` groupe (dont l'ID de groupe est dec242c5b0-6081-1845-6fa8-6e0d9513c107) et possède une adresse e-mail vérifiée.

```
permit(principal,action,resource)
when {
    context.<policy-reference-name>.groups has "c242c5b0-6081-1845-6fa8-6e0d9513c107"
    && context.<policy-reference-name>.user.email.verified == true
};
```

Exemple 1b : ajout de conditions supplémentaires à une déclaration de politique pour IAM Identity Center

L'exemple de politique suivant autorise l'accès uniquement lorsqu'un utilisateur appartient au `finance` groupe (dont l'identifiant de groupe est `dec242c5b0-6081-1845-6fa8-6e0d9513c107`), possède une adresse e-mail vérifiée et le score de risque de l'appareil Jamf est `LOW` égal à.

```
permit(principal,action,resource)
when {
    context.<policy-reference-name>.groups has "c242c5b0-6081-1845-6fa8-6e0d9513c107"
    && context.<policy-reference-name>.user.email.verified == true
    && context.jamf.risk == "LOW"
};
```

Exemple 2 : la même politique pour un OIDC fournisseur tiers

L'exemple de politique suivant autorise l'accès uniquement lorsque l'utilisateur appartient au groupe « finance », qu'il possède une adresse e-mail vérifiée et que le score de risque de l'appareil Jamf est LOW égal à.

```
permit(principal,action,resource)
when {
     context.<policy-reference-name>.groups.contains("finance")
     && context.<policy-reference-name>.email_verified == true
     && context.jamf.risk == "LOW"
};
```

Exemple 3 : utilisation CrowdStrike

L'exemple de politique suivant autorise l'accès lorsque le score d'évaluation global est supérieur à 50.

```
permit(principal,action,resource)
when {
    context.crwd.assessment.overall > 50
};
```

Exemple 4 : utilisation de caractères spéciaux

L'exemple suivant montre comment écrire une politique si une propriété de contexte utilise un `:` (point-virgule), qui est un caractère réservé dans le langage de stratégie.

```
permit(principal, action, resource)
when {
    context.<policy-reference-name>["namespace:groups"].contains("finance")
};
```

Exemple 5 : Autoriser une adresse IP spécifique

L'exemple suivant montre une politique qui n'autorise qu'une adresse IP spécifique.

```
permit(principal, action, resource)
when {
    context.http_request.client_ip == "192.0.2.1"
};
```

Exemple 5a : Bloquer une adresse IP spécifique

L'exemple suivant montre une politique qui bloquera une adresse IP spécifique.

```
forbid(principal,action,resource)
when {
ip(context.http_request.client_ip).isInRange(ip("192.0.2.1/32"))
};
```

Assistant de politique d'accès vérifié

L'assistant de politique d'accès vérifié est un outil de la console d'accès vérifié que vous pouvez utiliser pour tester et développer vos politiques. Il présente la politique du point de terminaison, la stratégie de groupe et le contexte de confiance sur un seul écran, où vous pouvez tester et modifier les politiques.

Les formats de contexte de confiance varient selon les fournisseurs de confiance, et il arrive que l'administrateur de Verified Access ne connaisse pas le format exact utilisé par un certain fournisseur de confiance. C'est pourquoi il peut être très utile de consulter le contexte de confiance et les politiques de groupe et de point de terminaison au même endroit à des fins de test et de développement.

Les sections suivantes décrivent les principes de base de l'utilisation de l'éditeur de politiques.

Tâches

- Étape 1 : Spécifiez vos ressources

Étape 1 : Spécifiez vos ressources

Sur la première page de l'assistant de politique, vous spécifiez le point de terminaison Verified Access avec lequel vous souhaitez travailler. Vous indiquerez également un utilisateur (identifié par adresse e-mail) et, éventuellement, le nom de l'utilisateur et/ou un identifiant d'appareil. Par défaut, la décision d'autorisation la plus récente est extraite des journaux d'accès vérifié pour l'utilisateur spécifié. Vous pouvez éventuellement choisir spécifiquement la décision d'autorisation ou de refus la plus récente.

Enfin, le contexte de confiance, la décision d'autorisation, la politique du point de terminaison et la politique de groupe sont tous affichés sur l'écran suivant.

Pour ouvrir l'assistant de politique et spécifier vos ressources

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Instances d'accès vérifié, puis cliquez sur l'ID d'instance d'accès vérifié pour l'instance avec laquelle vous souhaitez travailler.
3. Choisissez Launch Policy Assistant.
4. Dans le champ Adresse e-mail de l'utilisateur, entrez l'adresse e-mail de l'utilisateur.
5. Pour le point de terminaison d'accès vérifié, sélectionnez le point de terminaison pour lequel vous souhaitez modifier et tester les politiques.
6. (Facultatif) Dans Nom, entrez le nom de l'utilisateur.
7. (Facultatif) Sous Identifiant de l'appareil, indiquez l'identifiant unique de l'appareil.
8. (Facultatif) Pour le résultat de l'autorisation, choisissez le type de résultat d'autorisation récent que vous souhaitez utiliser. Par défaut, le dernier résultat d'autorisation sera utilisé.
9. Choisissez Suivant.

Étape 2 : tester et modifier les politiques

Sur cette page, les informations suivantes vous seront présentées pour travailler :

- Le contexte de confiance envoyé par votre fournisseur de confiance à l'utilisateur et (éventuellement) à l'appareil que vous avez spécifié à l'étape précédente.

- La politique Cedar pour le point de terminaison Verified Access spécifiée à l'étape précédente.
- La politique Cedar pour le groupe d'accès vérifié auquel appartient le point de terminaison.

Les politiques Cedar pour le point de terminaison et le groupe Verified Access peuvent être modifiées sur cette page, mais le contexte de confiance est statique. Vous pouvez désormais utiliser cette page pour consulter le contexte de confiance ainsi que les politiques de Cedar.

Testez les politiques par rapport au contexte de confiance en cliquant sur le bouton Tester les politiques, et le résultat de l'autorisation sera affiché à l'écran. Vous pouvez apporter des modifications aux politiques et retester vos modifications, en répétant le processus si nécessaire.

Une fois que vous êtes satisfait des modifications apportées aux politiques, choisissez Next pour passer à l'écran suivant de l'assistant de stratégie.

Étape 3 : Vérifiez et appliquez les modifications

Sur la dernière page de l'assistant aux politiques, vous verrez les modifications que vous avez apportées aux politiques surlignées pour en faciliter la consultation. Vous pouvez maintenant les consulter une dernière fois et choisir Appliquer les modifications pour valider les modifications.

Vous avez également la possibilité de revenir à la page précédente en choisissant Précédent, ou de vous désinscrire complètement de l'assistant des politiques en choisissant Annuler.

Sécurité en matière d'accès vérifié

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures 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 cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Verified Access, voir AWS Services concernés par programme de conformitéAWS .
- 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 l'utilisation de Verified Access. Les rubriques suivantes expliquent comment configurer l'accès vérifié pour répondre à 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 ressources d'accès vérifié.

Table des matières

Protection des données dans Verified Access

Le modèle de responsabilité AWS partagée Le modèle s'applique à la protection des données dans AWS Verified Access. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure

mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des AWS services que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la section Confidentialité des données FAQ. Pour plus d'informations sur la protection des données en Europe, consultez le modèle de responsabilitéAWS partagée et le billet de GDPR blog sur le blog sur la AWS sécurité.

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) pour chaque compte.
- UtilisezSSL/TLSpour communiquer avec les AWS ressources. Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Configuration API et journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent AWS services.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de FIPS 140 à 3 modules cryptographiques validés pour accéder AWS via une interface de ligne de commande ou unAPI, utilisez un point de terminaison. FIPS Pour plus d'informations sur les FIPS points de terminaison disponibles, voir Federal Information Processing Standard (FIPS) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Verified Access ou autre AWS services à l'aide de la consoleAPI, AWS CLI, ou AWS SDKs. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez un URL à un serveur externe, nous vous recommandons vivement de ne pas inclure d'informations d'identification dans le URL afin de valider votre demande auprès de ce serveur.

Chiffrement en transit

Verified Access chiffre toutes les données en transit entre les utilisateurs finaux et les points de terminaison Verified Access via Internet à l'aide de Transport Layer Security (TLS) 1.2 ou version ultérieure.

Confidentialité du trafic inter-réseaux

Vous pouvez configurer l'accès vérifié pour restreindre l'accès à des ressources spécifiques de votreVPC. Pour l'authentification basée sur les utilisateurs, vous pouvez également restreindre l'accès à certaines parties de votre réseau, en fonction du groupe d'utilisateurs qui accède aux points de terminaison. Pour de plus amples informations, veuillez consulter Politiques d'accès vérifiées.

Chiffrement des données au repos pour AWS un accès vérifié

AWS Verified Access chiffre les données au repos par défaut, à l'aide de KMS clés AWS détenues. Lorsque le chiffrement des données au repos est effectué par défaut, cela permet de réduire la charge opérationnelle et la complexité liées à la protection des données sensibles. Dans le même temps, il vous permet de créer des applications sécurisées qui répondent aux exigences réglementaires et de conformité strictes en matière de chiffrement. Les sections suivantes expliquent en détail comment Verified Access utilise KMS les clés pour le chiffrement des données au repos.

Table des matières

Accès et KMS clés vérifiés

AWS clés possédées

Verified Access utilise des KMS clés pour chiffrer automatiquement les informations personnelles identifiables (PII). Cela se produit par défaut, et vous ne pouvez pas vous-même consulter, gérer,

utiliser ou auditer l'utilisation des clés AWS détenues. Toutefois, vous n'avez pas besoin de prendre de mesure ou de modifier les programmes pour protéger les clés qui chiffrent vos données. Pour plus d'informations, consultez Clés détenues par AWS dans le Guide du développeur AWS Key Management Service .

Bien que vous ne puissiez pas désactiver cette couche de chiffrement ou sélectionner un autre type de chiffrement, vous pouvez ajouter une deuxième couche de chiffrement aux clés de chiffrement AWS détenues existantes en choisissant une clé gérée par le client lorsque vous créez vos ressources d'accès vérifié.

Clés gérées par le client

Verified Access prend en charge l'utilisation de clés symétriques gérées par le client que vous créez et gérez, afin d'ajouter une deuxième couche de chiffrement au chiffrement par défaut existant. Étant donné que vous avez le contrôle total de cette couche de chiffrement, vous pouvez effectuer les tâches suivantes :

- Établissement et gestion des stratégies de clé
- Établir et maintenir IAM des politiques et des subventions
- Activation et désactivation des stratégies de clé
- Rotation des matériaux de chiffrement de clé
- Ajout de balises
- Création d'alias de clé
- Planification des clés pour la suppression

Pour plus d'informations, consultez Clés gérées par le client dans le Guide du développeur AWS Key Management Service (langue française non garantie).

> **Note**
>
> Verified Access active automatiquement le chiffrement au repos à l'aide de clés AWS détenues afin de protéger gratuitement les données personnelles identifiables. Toutefois, AWS KMS des frais s'appliquent lorsque vous utilisez une clé gérée par le client. Pour plus d'informations sur les tarifs, consultez les AWS Key Management Service tarifs.

Informations personnelles identifiables

Le tableau suivant résume les informations personnelles identifiables (PII) utilisées par Verified Access et la manière dont elles sont cryptées.

Type de données	AWS chiffrement par clé détenue	Chiffrement par clé gérée par le client (facultatif)
`Trust provider (user-type)` Les fournisseurs de confiance de type utilisateur contiennent des OIDC options telles que AuthorizationEndpoint, UserInfoEndpoint, ClientId, ClientSecret,,, etc., qui sont prises en comptePII.	Activées	Activées
`Trust provider (device-type)` Les fournisseurs de confiance de type appareil contiennent un TenantId, qui est pris en compte. PII	Activées	Activées
`Group policy` Fourni lors de la création ou de la modification du groupe d'accès vérifié. Contient des règles pour autoriser les demandes d'accès. Peut contenir PII un nom d'utilisateur et une adresse e-mail, etc.	Activées	Activées
`Endpoint policy`	Activées	Activées

Type de données	AWS chiffrement par clé détenue	Chiffrement par clé gérée par le client (facultatif)
Fourni lors de la création ou de la modification du point de terminaison Verified Access. Contient des règles pour autoriser les demandes d'accès. Peut contenir PII un nom d'utilisateur et une adresse e-mail, etc.		

Comment AWS Verified Access utilise les subventions dans AWS KMS

L'accès vérifié nécessite une autorisation pour utiliser votre clé gérée par le client.

Lorsque vous créez des ressources Verified Access chiffrées à l'aide d'une clé gérée par le client, Verified Access crée une subvention en votre nom en envoyant une CreateGrantdemande à AWS KMS. Les subventions AWS KMS sont utilisées pour donner à Verified Access l'accès à une clé gérée par le client dans votre compte.

L'accès vérifié nécessite l'autorisation d'utiliser votre clé gérée par le client pour les opérations internes suivantes :

- Envoyez des demandes de déchiffrement AWS KMS à pour déchiffrer les clés de données chiffrées afin qu'elles puissent être utilisées pour déchiffrer vos données.
- Envoyez RetireGrantdes demandes AWS KMS de suppression d'une subvention.

Vous pouvez révoquer l'accès à l'octroi ou supprimer l'accès du service à la clé gérée par le client à tout moment. Dans ce cas, Verified Access ne pourra accéder à aucune des données chiffrées par la clé gérée par le client, ce qui affectera les opérations qui dépendent de ces données.

Utilisation de clés gérées par le client avec accès vérifié

Vous pouvez créer une clé symétrique gérée par le client en utilisant le AWS Management Console, ou le AWS KMS APIs. Suivez les étapes de la rubrique Création d'une clé symétrique gérée par le client dans le Guide du développeur AWS Key Management Service .

Politiques clés

Les politiques de clés contrôlent l'accès à votre clé gérée par le client. Chaque clé gérée par le client doit avoir exactement une stratégie de clé, qui contient des instructions qui déterminent les personnes pouvant utiliser la clé et comment elles peuvent l'utiliser. Lorsque vous créez votre clé gérée par le client, vous pouvez spécifier une stratégie de clé. Pour plus d'informations, consultez Gestion de l'accès aux clés gérées par le client dans le Guide du développeur AWS Key Management Service .

Pour utiliser votre clé gérée par le client avec vos ressources d'accès vérifié, les API opérations suivantes doivent être autorisées dans la politique des clés :

- `kms:CreateGrant` : ajoute une attribution à une clé gérée par le client. Accorde un accès de contrôle à une KMS clé spécifiée, ce qui permet d'accéder aux opérations d'autorisation requises par Verified Access. Pour plus d'informations sur l'utilisation des subventions, consultez le guide du AWS Key Management Service développeur.

  Cela permet à Verified Access d'effectuer les opérations suivantes :

  - Appelez `GenerateDataKeyWithoutPlainText` pour générer une clé de données chiffrée et la stocker, car la clé de données n'est pas immédiatement utilisée pour chiffrer.
  - Appelez `Decrypt` pour utiliser la clé de données chiffrée stockée afin d'accéder aux données chiffrées.
  - Configurez un directeur partant à la retraite pour permettre au service de`RetireGrant`.
- `kms:DescribeKey`— Fournit les informations clés gérées par le client pour permettre à Verified Access de valider la clé.
- `kms:GenerateDataKey`— Permet à Verified Access d'utiliser une clé pour chiffrer les données.
- `kms:Decrypt`— Autoriser Verified Access pour déchiffrer les clés de données cryptées.

Voici un exemple de politique clé que vous pouvez utiliser pour l'accès vérifié.

```
"Statement" : [
    {
      "Sid" : "Allow access to principals authorized to use Verified Access",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "*"
      },
      "Action" : [
```

```
        "kms:DescribeKey",
        "kms:CreateGrant",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "kms:ViaService" : "verified-access.region.amazonaws.com",
          "kms:CallerAccount" : "111122223333"
        }
    },
    {
      "Sid": "Allow access for key administrators",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
       },
      "Action" : [
        "kms:*"
       ],
      "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
    },
    {
      "Sid" : "Allow read-only access to key metadata to the account",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "arn:aws:iam::111122223333:root"
      },
      "Action" : [
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "kms:RevokeGrant"
      ],
      "Resource" : "*"
    }
  ]
```

Pour plus d'informations sur la spécification d'autorisations dans une politique, consultez le Guide du développeur AWS Key Management Service .

Pour plus d'informations sur le dépannage des clés d'accès, consultez le Guide du développeur AWS Key Management Service .

Spécification d'une clé gérée par le client pour les ressources d'accès vérifié

Vous pouvez spécifier une clé gérée par le client afin de fournir un chiffrement de deuxième couche pour les ressources suivantes :

- Groupe d'accès vérifié
- Point de terminaison d'accès vérifié
- Fournisseur de confiance Verified Access

Lorsque vous créez l'une de ces ressources à l'aide de AWS Management Console, vous pouvez spécifier une clé gérée par le client dans la section Chiffrement supplémentaire -- facultatif. Au cours du processus, cochez la case Personnaliser les paramètres de chiffrement (avancés), puis entrez l'ID de AWS KMS clé que vous souhaitez utiliser. Cela peut également être fait lors de la modification d'une ressource existante ou en utilisant le AWS CLI.

> **Note**
>
> Si la clé gérée par le client utilisée pour ajouter un chiffrement supplémentaire à l'une des ressources ci-dessus est perdue, les valeurs de configuration des ressources ne seront plus accessibles. Les ressources peuvent toutefois être modifiées en utilisant le AWS Management Console ou AWS CLI pour appliquer une nouvelle clé gérée par le client et réinitialiser les valeurs de configuration.

AWS Contexte de chiffrement de Verified Access

Un contexte de chiffrement est un ensemble facultatif de paires clé-valeur contenant des informations contextuelles supplémentaires sur les données. AWS KMS utilise le contexte de chiffrement comme données authentifiées supplémentaires pour prendre en charge le chiffrement authentifié. Lorsque vous incluez un contexte de chiffrement dans une demande de chiffrement de données, AWS KMS lie le contexte de chiffrement aux données chiffrées. Pour déchiffrer les données, vous devez inclure le même contexte de chiffrement dans la demande.

AWS Contexte de chiffrement de Verified Access

Verified Access utilise le même contexte de chiffrement dans toutes les opérations AWS KMS cryptographiques, où la clé `aws:verified-access:arn` et la valeur sont la ressource Amazon Resource Name (ARN). Vous trouverez ci-dessous les contextes de chiffrement pour les ressources d'accès vérifié.

Fournisseur de confiance Verified Access

```
"encryptionContext": {
    "aws:verified-access:arn":
    "arn:aws:ec2:region:111122223333:VerifiedAccessTrustProviderId"
}
```

Groupe d'accès vérifié

```
"encryptionContext": {
    "aws:verified-access:arn":
    "arn:aws:ec2:region:111122223333:VerifiedAccessGroupId"
}
```

Point de terminaison d'accès vérifié

```
"encryptionContext": {
    "aws:verified-access:arn":
    "arn:aws:ec2:region:111122223333:VerifiedAccessEndpointId"
}
```

Pour plus d'informations sur l'utilisation du contexte de chiffrement pour les subventions ou dans les politiques, consultez la section Contexte de chiffrement dans le guide du AWS Key Management Service développeur.

Surveillance de vos clés de chiffrement pour AWS un accès vérifié

Lorsque vous utilisez une KMS clé gérée par le client avec vos ressources AWS Verified Access, vous pouvez l'utiliser AWS CloudTrailpour suivre les demandes auxquelles Verified Access envoie AWS KMS.

Les exemples suivants sont AWS CloudTrail des événements pour`CreateGrant`,`RetireGrant`,`Decrypt`, et `DescribeKeyGenerateDataKey`, qui surveillent les KMS opérations appelées par Verified Access pour accéder aux données chiffrées par la KMS clé gérée par votre client :

CreateGrant

Lorsque vous utilisez une clé gérée par le client pour chiffrer vos ressources, Verified Access envoie une `CreateGrant` demande en votre nom pour accéder à la clé de votre AWS compte. L'autorisation créée par Verified Access est spécifique à la ressource associée à la clé gérée par le client.

L'exemple d'événement suivant enregistre l'opération `CreateGrant` :


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T16:27:12Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T16:41:42Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "operations": [
            "Decrypt",
            "RetireGrant",
```

```
            "GenerateDataKey"
        ],
        "keyId": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae",
        "constraints": {
            "encryptionContextSubset": {
                "aws:verified-access:arn": "arn:aws:ec2:ca-
central-1:111122223333:verified-access-trust-provider/vatp-0e54f581e2e5c97a2"
            }
        },
        "granteePrincipal": "verified-access.ca-central-1.amazonaws.com",
        "retiringPrincipal": "verified-access.ca-central-1.amazonaws.com"
    },
    "responseElements": {
        "grantId":
 "e5a050fff9893ba1c43f83fddf61e5f9988f579beaadd6d4ad6d1df07df6048f",
        "keyId": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae"
    },
    "requestID": "0faa837e-5c69-4189-9736-3957278e6444",
    "eventID": "1b6dd8b8-cbee-4a83-9b9d-d95fa5f6fd08",
    "readOnly": false,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


RetireGrant

L'accès vérifié utilise l'`RetireGrant`opération pour supprimer une subvention lorsque vous supprimez une ressource.

L'exemple d'événement suivant enregistre l'opération `RetireGrant` :


```
{
```

```
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T16:42:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T16:47:53Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RetireGrant",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": null,
    "responseElements": {
        "keyId": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae"
    },
    "additionalEventData": {
        "grantId":
 "b35e66f9bacb266cec214fcaa353c9cf750785e28773e61ba6f434d8c5c7632f"
    },
    "requestID": "7d4a31c2-d426-434b-8f86-336532a70462",
    "eventID": "17edc343-f25b-43d4-bbff-150d8fff4cf8",
    "readOnly": false,
    "resources": [
        {
            "accountId": "AWS Internal",
```

```
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt

Verified Access appelle l'`Decrypt`opération pour utiliser la clé de données cryptée stockée afin d'accéder aux données cryptées.

L'exemple d'événement suivant enregistre l'opération `Decrypt` :

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T17:19:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T17:47:05Z",
    "eventSource": "kms.amazonaws.com",
```

```
    "eventName": "Decrypt",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e",
        "encryptionContext": {
            "aws:verified-access:arn": "arn:aws:ec2:ca-
central-1:111122223333:verified-access-trust-provider/vatp-00f20a4e455e9340f",
            "aws-crypto-public-key": "AkK+vi1W/
acBKv7OR8p2DeUrA8EgpTffSrjBqNucODuBYhyZ3hlMuYYJz9x7CwQWZw=="
        }
    },
    "responseElements": null,
    "requestID": "2e920fd3-f2f6-41b2-a5e7-2c2cb6f853a9",
    "eventID": "3329e0a3-bcfb-44cf-9813-8106d6eee31d",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


DescribeKey

Verified Access utilise cette `DescribeKey` opération pour vérifier si la clé gérée par le client associée à votre ressource existe dans le compte et dans la région.

L'exemple d'événement suivant enregistre l'opération `DescribeKey` :


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
```

```
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T17:19:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T17:46:48Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
    },
    "responseElements": null,
    "requestID": "5b127082-6691-48fa-bfb0-4d40e1503636",
    "eventID": "ffcfc2bb-f94b-4c00-b6fb-feac77daff2a",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
```

```
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateDataKey

L'exemple d'événement suivant enregistre l'opération `GenerateDataKey` :

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T17:19:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T17:46:49Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:verified-access:arn": "arn:aws:ec2:ca-
central-1:111122223333:verified-access-trust-provider/vatp-00f20a4e455e9340f",
            "aws-crypto-public-key": "A/ATGxaYatPUlOtM+l/mfDndkzHUmX5Hav+29IlIm
+JRBKFuXf24ulztmOIsqFQliw=="
```

```
        },
        "numberOfBytes": 32,
        "keyId": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
    },
    "responseElements": null,
    "requestID": "06535808-7cce-4ae1-ab40-e3afbf158a43",
    "eventID": "1ce79601-5a5e-412c-90b3-978925036526",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Gestion des identités et des accès pour Verified Access

AWS Identity and Access Management (IAM) est un outil AWS service qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. IAMles administrateurs contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources d'accès vérifié. IAMest un AWS service outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- AWS politiques gérées pour l'accès vérifié

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Verified Access.

Utilisateur du service : si vous utilisez le service Verified Access pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités d'accès vérifié pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne parvenez pas à accéder à une fonctionnalité dans Verified Access, consultezRésolution des problèmes liés à l'identité et à l'accès vérifiés.

Administrateur du service — Si vous êtes responsable des ressources d'accès vérifié au sein de votre entreprise, vous avez probablement un accès complet à l'accès vérifié. C'est à vous de déterminer les fonctionnalités et les ressources d'accès vérifié auxquelles les utilisateurs du service doivent accéder. Vous devez ensuite envoyer des demandes à votre IAM administrateur pour modifier les autorisations des utilisateurs de votre service. Consultez les informations de cette page pour comprendre les concepts de base deIAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM l'accès vérifié, consultezComment fonctionne Verified Access avec IAM.

IAMadministrateur : si vous êtes IAM administrateur, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Verified Access. Pour consulter des exemples de politiques basées sur l'identité d'accès vérifié que vous pouvez utiliserIAM, consultez. Exemples de politiques basées sur l'identité pour l'accès vérifié

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant que Utilisateur racine d'un compte AWS, en tant qu'IAMutilisateur ou en assumant un IAM rôle.

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAMIdentity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez en tant

qu'identité fédérée, votre administrateur a préalablement configuré la fédération d'identité à l'aide de IAM rôles. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des AWS API demandes dans le guide de IAM l'utilisateur.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le guide de AWS IAM Identity Center l'utilisateur et Utilisation de l'authentification multifactorielle (MFA) AWS dans le guide de l'IAMutilisateur.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes AWS services les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui nécessitent que vous vous connectiez en tant qu'utilisateur root, consultez la section Tâches nécessitant des informations d'identification utilisateur root dans le guide de IAM l'utilisateur.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide AWS services d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies AWS services par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour plus d'informations sur IAM Identity Center, consultez Qu'est-ce qu'IAMIdentity Center ? dans le guide de AWS IAM Identity Center l'utilisateur.

Utilisateurs et groupes IAM

Un IAMutilisateur est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des IAM utilisateurs dotés d'informations d'identification à long terme, telles que des mots de passe et des clés d'accès. Toutefois, si vous avez des cas d'utilisation spécifiques qui nécessitent des informations d'identification à long terme auprès des IAM utilisateurs, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, voir Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme dans le Guide de IAM l'utilisateur.

Un IAMgroupe est une identité qui définit un ensemble d'IAMutilisateurs. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer IAM des ressources.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, voir Quand créer un IAM utilisateur (au lieu d'un rôle) dans le Guide de IAM l'utilisateur.

IAMrôles

Un IAMrôle est une identité au sein de Compte AWS vous dotée d'autorisations spécifiques. Il est similaire à un IAM utilisateur, mais n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un IAM rôle dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une AWS API opération AWS CLI or ou en utilisant une option personnaliséeURL. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section Utilisation IAM des rôles dans le Guide de IAM l'utilisateur.

IAMles rôles dotés d'informations d'identification temporaires sont utiles dans les situations suivantes :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour plus d'informations sur les rôles pour la fédération, voir Création d'un rôle pour un fournisseur d'identité tiers dans le guide de IAM l'utilisateur. Si vous utilisez IAM Identity Center, vous configurez un ensemble d'autorisations. Pour contrôler les accès auxquels vos identités peuvent accéder après leur authentification, IAM Identity Center met en corrélation l'ensemble d'autorisations avec un rôle dans. IAM Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations IAM utilisateur temporaires : un IAM utilisateur ou un rôle peut assumer un IAM rôle afin d'obtenir temporairement différentes autorisations pour une tâche spécifique.
- Accès entre comptes : vous pouvez utiliser un IAM rôle pour autoriser une personne (un mandant fiable) d'un autre compte à accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains AWS services cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.
- Accès multiservices — Certains AWS services utilisent des fonctionnalités dans d'autres AWS services. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès transmises (FAS) — Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre

service. FASutilise les autorisations du principal appelant an AWS service, combinées à la demande AWS service pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes AWS services ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.

- Rôle de service — Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, consultez la section Création d'un rôle auquel déléguer des autorisations AWS service dans le Guide de IAM l'utilisateur.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. AWS service Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui AWS CLI soumettent des AWS API demandes. Cela est préférable au stockage des clés d'accès dans l'EC2instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l'EC2instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section Utilisation d'un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le Guide de IAM l'utilisateur.

Pour savoir s'il faut utiliser IAM des rôles ou des IAM utilisateurs, voir Quand créer un IAM rôle (au lieu d'un utilisateur) dans le guide de IAM l'utilisateur.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de JSON documents. Pour plus d'informations sur la structure et le contenu

des documents de JSON politique, voir Présentation des JSON politiques dans le guide de IAM l'utilisateur.

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

IAMles politiques définissent les autorisations pour une action, quelle que soit la méthode que vous utilisez pour effectuer l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur doté de cette politique peut obtenir des informations sur le rôle auprès du AWS Management Console AWS CLI, ou du AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section Création de IAM politiques dans le Guide de l'IAMutilisateur.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour savoir comment choisir entre une politique gérée ou une politique intégrée, voir Choisir entre des politiques gérées et des politiques intégrées dans le Guide de l'IAMutilisateur.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de

service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. AWS services

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser de politiques AWS gérées depuis une IAM stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

Amazon S3 et Amazon VPC sont des exemples de services compatiblesACLs. AWS WAF Pour en savoir plusACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limites d'autorisations — Une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une IAM entité (IAMutilisateur ou rôle). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez la section Limites d'autorisations pour les IAM entités dans le Guide de IAM l'utilisateur.
- Politiques de contrôle des services (SCPs) : SCPs JSON politiques qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les

fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Les SCP limites d'autorisations pour les entités présentes dans les comptes des membres, y compris chacune d'entre elles Utilisateur racine d'un compte AWS. Pour plus d'informations sur les Organizations et consultez SCPs les politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.

- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez la section Politiques de session dans le guide de IAM l'utilisateur.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de IAM l'utilisateur.

Comment fonctionne Verified Access avec IAM

Avant de commencer IAM à gérer l'accès à Verified Access, découvrez quelles IAM fonctionnalités peuvent être utilisées avec Verified Access.

IAMfonctionnalité	Support d'accès vérifié
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d'une politique	Oui

IAMfonctionnalité	Support d'accès vérifié
ACLs	Non
ABAC(balises dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble du fonctionnement de Verified Access et AWS des autres services avec la plupart des IAM fonctionnalités, consultez la section AWS Services compatibles IAM dans le Guide de IAM l'utilisateur.

Politiques basées sur l'identité pour l'accès vérifié

Prend en charge les politiques basées sur l'identité : oui

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section Création de IAM politiques dans le Guide de l'IAMutilisateur.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier les actions et les ressources autorisées ou refusées ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour en savoir plus sur tous les éléments que vous pouvez utiliser dans une JSON politique, consultez la référence aux éléments de IAM JSON politique dans le Guide de IAM l'utilisateur.

Exemples de politiques basées sur l'identité pour l'accès vérifié

Pour consulter des exemples de politiques basées sur l'identité d'accès vérifié, consultez. Exemples de politiques basées sur l'identité pour l'accès vérifié

Politiques basées sur les ressources au sein de Verified Access

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. AWS services

Pour activer l'accès entre comptes, vous pouvez spécifier un compte entier ou IAM des entités d'un autre compte comme principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un IAM administrateur du compte de confiance doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez la section Accès aux ressources entre comptes IAM dans le Guide de IAM l'utilisateur.

Actions politiques pour l'accès vérifié

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'`Action`élément d'une JSON politique décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès dans une politique. Les actions de stratégie portent généralement le même nom que l' AWS APIopération associée. Il existe certaines exceptions, telles que les actions avec autorisation uniquement qui n'ont pas d'opération correspondante. API Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions d'accès vérifié, consultez la section Actions définies par Amazon EC2 dans le Service Authorization Reference.

Les actions de politique dans Verified Access utilisent le préfixe suivant avant l'action :

```
ec2
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
    "ec2:action1",
    "ec2:action2"
]
```

Pour consulter des exemples de politiques basées sur l'identité d'accès vérifié, consultez. Exemples de politiques basées sur l'identité pour l'accès vérifié

Ressources relatives aux politiques relatives à l'accès vérifié

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Resource` JSON de stratégie indique le ou les objets auxquels s'applique l'action. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de spécifier une ressource en utilisant son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources Verified Access et leurs caractéristiquesARNs, consultez la section Ressources définies par Amazon EC2 dans le Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier pour chaque ressource, consultez Actions définies par Amazon EC2. ARN

Pour consulter des exemples de politiques basées sur l'identité d'accès vérifié, consultez. Exemples de politiques basées sur l'identité pour l'accès vérifié

Clés de conditions de politique pour l'accès vérifié

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez autoriser un IAM utilisateur à accéder à une ressource uniquement si celle-ci est étiquetée avec son nom IAM d'utilisateur. Pour plus d'informations, consultez IAMla section Éléments de politique : variables et balises dans le Guide de IAM l'utilisateur.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés contextuelles de condition AWS globales dans le guide de IAM l'utilisateur.

Pour consulter la liste des clés de condition d'accès vérifiées, consultez la section Clés de condition pour Amazon EC2 dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par Amazon EC2.

Pour consulter des exemples de politiques basées sur l'identité d'accès vérifié, consultez. Exemples de politiques basées sur l'identité pour l'accès vérifié

ACLsdans Verified Access

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

ABACavec accès vérifié

Supports ABAC (balises dans les politiques) : Partiel

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises à IAM des entités (utilisateurs ou rôles) et à de nombreuses AWS ressources. Le balisage des entités et des ressources est la première étape deABAC. Vous concevez ensuite des ABAC politiques pour autoriser les opérations lorsque le tag du principal correspond à celui de la ressource à laquelle il essaie d'accéder.

ABACest utile dans les environnements qui se développent rapidement et aide dans les situations où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informationsABAC, voir Qu'est-ce que c'est ABAC ? dans le guide de IAM l'utilisateur. Pour consulter un didacticiel présentant les étapes de configurationABAC, voir Utiliser le contrôle d'accès basé sur les attributs (ABAC) dans le guide de l'IAMutilisateur.

Utilisation d'informations d'identification temporaires avec accès vérifié

Prend en charge les informations d'identification temporaires : oui

Certains AWS services ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui AWS services fonctionnent avec des informations d'identification temporaires, consultez AWS services la section relative à l'utilisation IAM dans le Guide de IAM l'utilisateur.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez la section Passage à un rôle (console) dans le guide de IAM l'utilisateur.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide du AWS CLI ou AWS API. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez la section Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour l'accès vérifié

Prend en charge les sessions d'accès transféré (FAS) : Oui

Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FASutilise les autorisations du principal appelant an AWS service, combinées à la demande AWS service pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes AWS services ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.

Rôles de service pour Verified Access

Supporte les rôles de service : Non

Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus

d'informations, consultez la section Création d'un rôle auquel déléguer des autorisations AWS service dans le Guide de IAM l'utilisateur.

Rôles liés à un service pour l'accès vérifié

Prend en charge les rôles liés aux services : Oui

Un rôle lié à un service est un type de rôle de service lié à un. AWS service Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.

Pour plus de détails sur la création ou la gestion des rôles liés au service Verified Access, consultez. Utiliser des rôles liés à un service pour l'accès vérifié

Exemples de politiques basées sur l'identité pour l'accès vérifié

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources d'accès vérifié. Ils ne peuvent pas non plus effectuer de tâches en utilisant le AWS Management Console, AWS Command Line Interface (AWS CLI) ou AWS API. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de JSON stratégie, consultez la section Création de IAM politiques dans le guide de l'IAMutilisateur.

Pour plus de détails sur les actions et les types de ressources définis par Verified Access, y compris le ARNs format de chaque type de ressource, consultez Actions, ressources et clés de condition pour Amazon EC2 dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Politique de création d'instances d'accès vérifié
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources d'accès vérifié dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez les politiques AWS gérées ou les politiques AWS gérées pour les fonctions professionnelles dans le Guide de IAM l'utilisateur.
- Appliquer les autorisations du moindre privilège : lorsque vous définissez des autorisations à IAM l'aide de politiques, accordez uniquement les autorisations nécessaires à l'exécution d'une tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation IAM pour appliquer des autorisations, consultez la section Politiques et autorisations IAM dans le guide de IAM l'utilisateur.
- Utilisez des conditions dans IAM les politiques pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques pour limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez rédiger une condition de politique pour spécifier que toutes les demandes doivent être envoyées en utilisantSSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique AWS service, tel que AWS CloudFormation. Pour plus d'informations, voir Éléments IAM JSON de politique : Condition dans le guide de IAM l'utilisateur.
- Utilisez IAM Access Analyzer pour valider vos IAM politiques afin de garantir des autorisations sécurisées et fonctionnelles. IAM Access Analyzer valide les politiques nouvelles et existantes afin qu'elles soient conformes au langage des IAM politiques (JSON) et IAM aux meilleures pratiques. IAMAccess Analyzer fournit plus de 100 vérifications des politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez la section Validation des politiques d'IAMAccess Analyzer dans le guide de IAM l'utilisateur.
- Exiger une authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des IAM utilisateurs ou un utilisateur root Compte AWS, activez-le MFA pour une sécurité supplémentaire.

Pour exiger le MFA moment où les API opérations sont appelées, ajoutez MFA des conditions à vos politiques. Pour plus d'informations, consultez la section Configuration de l'APIaccès MFA protégé dans le Guide de l'IAMutilisateur.

Pour plus d'informations sur les meilleures pratiques en matière de sécuritéIAM, consultez la section Bonnes pratiques en matière de sécurité IAM dans le Guide de IAM l'utilisateur.

Politique de création d'instances d'accès vérifié

Pour créer une instance d'accès vérifié, IAM les principaux doivent ajouter cette déclaration supplémentaire à leur IAM politique.

```
{
    "Effect": "Allow",
    "Action": "verified-access:AllowVerifiedAccess",
    "Resource": "*"
}
```

> **Note**
>
> `verified-access:AllowVerifiedAccess`est un environnement virtuel à action uniquement. API Il ne prend pas en charge l'autorisation basée sur les ressources, les balises ou les clés de condition. Utilisez une autorisation basée sur une ressource, une balise ou une clé de condition pour l'`ec2:CreateVerifiedAccessInstance`APIaction.

Exemple de politique pour créer une instance d'accès vérifié. Dans cet exemple, `123456789012` il s'agit du numéro de AWS compte et `us-east-1` de la AWS région.

```
{
      "Version": "2012-10-17",
      "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVerifiedAccessInstance",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:verified-access-instance/*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": "verified-access:AllowVerifiedAccess",
            "Resource": "*"
        }
    ]
}
```

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux IAM utilisateurs de consulter les politiques intégrées et gérées associées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide du AWS CLI ou. AWS API

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Résolution des problèmes liés à l'identité et à l'accès vérifiés

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation de Verified Access etIAM.

Problèmes

- Je ne suis pas autorisé à effectuer une action dans Verified Access
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources d'accès vérifié

Je ne suis pas autorisé à effectuer une action dans Verified Access

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit lorsque l'`mateojacksonIAM`utilisateur essaie d'utiliser la console pour afficher les détails d'une *`my-example-widget`* ressource fictive mais ne dispose pas des `ec2:`*`GetWidget`* autorisations fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `ec2:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Verified Access.

Certains vous AWS services permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un IAM utilisateur nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Verified Access. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources d'accès vérifié

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Verified Access prend en charge ces fonctionnalités, consultezComment fonctionne Verified Access avec IAM.
- Pour savoir comment donner accès à vos ressources sur un site Comptes AWS qui vous appartient, consultez la section Fournir l'accès à un IAM utilisateur dans un autre site Compte AWS que vous possédez dans le Guide de IAM l'utilisateur.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le Guide de IAM l'utilisateur.

- Pour savoir comment fournir un accès via la fédération d'identité, consultez la section Fournir un accès aux utilisateurs authentifiés de manière externe (fédération d'identité) dans le guide de l'IAMutilisateur.
- Pour connaître la différence entre l'utilisation de rôles et l'utilisation de politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.

Utiliser des rôles liés à un service pour l'accès vérifié

Accès vérifié par AWS utilise AWS Identity and Access Management (IAM) des rôles liés à un service. Un rôle lié à un service est un type unique de IAM rôle directement lié à Verified Access. Les rôles liés au service sont prédéfinis par Verified Access et incluent toutes les autorisations dont le service a besoin pour appeler d'autres personnes en votre AWS services nom.

Un rôle lié à un service facilite la configuration de l'accès vérifié, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. L'accès vérifié définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul l'accès vérifié peut assumer ses rôles. Les autorisations définies incluent la politique de confiance et la politique d'autorisations, et cette politique d'autorisations ne peut être attachée à aucune autre IAM entité.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez la section AWS Services qui fonctionnent avec IAM et recherchez les services dont la valeur est Oui dans la colonne Rôles liés à un service. Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées au service pour l'accès vérifié

L'accès vérifié utilise le rôle lié au service nommé AWSServiceRoleForVPCVerifiedAccesspour fournir les ressources de votre compte nécessaires à l'utilisation du service.

Le rôle AWSServiceRoleForVPCVerifiedAccesslié à un service fait confiance aux services suivants pour assumer le rôle :

- `verified-access.amazonaws.com`

La politique d'autorisation des rôles, nommée AWSVPCVerifiedAccessServiceRolePolicy, permet à Verified Access d'effectuer les actions suivantes sur les ressources spécifiées :

- Action `ec2:CreateNetworkInterface` sur tous les sous-réseaux et groupes de sécurité, ainsi que sur toutes les interfaces réseau comportant le tag `VerifiedAccessManaged=true`
- Action `ec2:CreateTags` sur toutes les interfaces réseau au moment de la création
- Action `ec2:DeleteNetworkInterface` sur toutes les interfaces réseau avec le tag `VerifiedAccessManaged=true`
- Action `ec2:ModifyNetworkInterfaceAttribute` sur tous les groupes de sécurité et toutes les interfaces réseau avec le tag `VerifiedAccessManaged=true`

Vous pouvez également consulter les autorisations associées à cette politique dans le AWS Management Console AWSVPCVerifiedAccessServiceRolePolicy, ou vous pouvez consulter la AWSVPCVerifiedAccessServiceRolePolicypolitique dans le Guide de référence des politiques AWS gérées.

Vous devez configurer les autorisations pour autoriser une IAM entité (telle qu'un utilisateur, un groupe ou un rôle) à créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez la section Autorisations relatives aux rôles liés à un service dans le Guide de l'IAMutilisateur.

Création d'un rôle lié à un service pour Verified Access

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous appelez CreateVerifiedAccessEndpointle AWS Management Console, le ou le AWS CLI AWS API, Verified Access crée le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous appelez à CreateVerifiedAccessEndpointnouveau, Verified Access crée à nouveau le rôle lié au service pour vous.

Modifier un rôle lié à un service pour Verified Access

L'accès vérifié ne vous permet pas de modifier le rôle AWSServiceRoleForVPCVerifiedAccesslié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Vous pouvez toutefois modifier la description du rôle à l'aide deIAM. Pour plus d'informations, consultez la section Modification d'un rôle lié à un service dans le Guide de l'IAMutilisateur.

Supprimer un rôle lié à un service pour Verified Access

Il n'est pas nécessaire de supprimer le AWSServiceRoleForVPCVerifiedAccessrôle manuellement. Lorsque vous appelez DeleteVerifiedAccessEndpointle AWS Management Console, le ou le AWS CLI AWS API, Verified Access nettoie les ressources et supprime le rôle lié au service pour vous.

Pour supprimer manuellement le rôle lié à un service à l'aide de IAM

Utilisez la IAM console AWS CLI, le ou le AWS API pour supprimer le rôle AWSServiceRoleForVPCVerifiedAccesslié au service. Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le Guide de l'IAMutilisateur.

Régions prises en charge pour les rôles liés au service Verified Access

Verified Access prend en charge l'utilisation de rôles liés au service partout Régions AWS où le service est disponible. Pour de plus amples informations, veuillez consulter AWS Régions et points de terminaison.

AWS politiques gérées pour l'accès vérifié

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle AWS service est lancée ou que de nouvelles API opérations sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques AWS gérées dans le Guide de IAM l'utilisateur.

AWS politique gérée : AWSVPCVerifiedAccessServiceRolePolicy

Cette politique est associée à un rôle lié à un service qui permet à Verified Access d'effectuer des actions en votre nom. Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service. Pour consulter les autorisations associées à cette politique, vous pouvez consulter AWSVPCVerifiedAccessServiceRolePolicyle AWS Management Console, ou vous pouvez consulter la AWSVPCVerifiedAccessServiceRolePolicypolitique dans le Guide de référence des politiques AWS gérées.

Accès vérifié : mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées pour Verified Access depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au RSS fil sur la page d'historique des documents d'accès vérifiés.

Modification	Description	Date
AWSVPCVerifiedAccessServiceRolePolicy- Politique mise à jour	Verified Access a mis à jour sa politique gérée pour inclure des descriptions de toutes les actions dans le champ « sid ».	17 novembre 2023
AWSVPCVerifiedAccessServiceRolePolicy- Politique mise à jour	Verified Access a mis à jour sa politique gérée pour ajouter une ressource de groupe de sécurité à `ec2:CreateNetworkInterface` l'autorisation.	31 mai 2023
AWSVPCVerifiedAccessServiceRolePolicy : nouvelle politique	Verified Access a ajouté une nouvelle politique lui permettant de fournir les ressources nécessaires à l'utilisation du service sur votre compte.	29 novembre 2022
Verified Access a commencé à suivre les modifications	Verified Access a commencé à suivre les modifications	29 novembre 2022

Modification	Description	Date
	apportées AWS à ses politiques gérées.	

Validation de conformité pour Verified Access

Accès vérifié par AWS peut être configuré pour garantir la conformité aux normes fédérales de traitement de l'information (FIPS). Pour plus d'informations et de détails sur la configuration de FIPS la conformité pour Verified Access, rendez-vous surFIPSconformité pour Verified Access.

Pour savoir si un programme AWS services de conformité AWS service s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez AWS services 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 AWS services 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 HIPAA sécurité et la conformité sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent AWS créer HIPAA des applications éligibles.

> **Note**
>
> Tous ne AWS services sont pas HIPAA éligibles. Pour plus d'informations, consultez la référence des services HIPAA éligibles.

- 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 AWS services et reprennent 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 AWS service 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 AWS service 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 PCIDSS, par exemple en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous AWS service 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 en matière d'accès vérifié

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS 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 à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Outre l'infrastructure AWS mondiale, Verified Access propose les fonctionnalités suivantes pour répondre à vos besoins en matière de haute disponibilité.

Plusieurs sous-réseaux pour une haute disponibilité

Lorsque vous créez un point de terminaison d'accès vérifié de type équilibreur de charge, vous pouvez associer plusieurs sous-réseaux au point de terminaison. Chaque sous-réseau que vous associez au point de terminaison doit appartenir à une zone de disponibilité différente. En associant plusieurs sous-réseaux, vous pouvez garantir une haute disponibilité en utilisant plusieurs zones de disponibilité.

Surveillance Accès vérifié par AWS

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de Accès vérifié par AWS. AWS fournit les outils de surveillance suivants pour surveiller l'accès vérifié, signaler un problème et prendre des mesures automatiques le cas échéant :

- Journaux d'accès — Capturez des informations détaillées sur les demandes d'accès aux applications. Pour de plus amples informations, veuillez consulter the section called “Journaux d'accès vérifiés”.
- AWS CloudTrail— Capture les API appels et les événements connexes effectués par vous ou en votre nom Compte AWS et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour de plus amples informations, veuillez consulter the section called “CloudTrail journaux”.

Journaux d'accès vérifiés

Après avoir Accès vérifié par AWS évalué chaque demande d'accès, il enregistre toutes les tentatives d'accès. Cela vous fournit une visibilité centralisée sur l'accès aux applications et vous aide à répondre rapidement aux incidents de sécurité et aux demandes d'audit. Verified Access prend en charge le format de journalisation Open Cybersecurity Schema Framework (OCSF).

Lorsque vous activez la journalisation, vous devez configurer une destination pour les journaux à envoyer. Le IAM principal utilisé pour configurer la destination de journalisation doit disposer de certaines autorisations pour que la journalisation fonctionne correctement. Les IAM autorisations requises pour chaque destination de journalisation sont indiquées dans la Autorisations de journalisation des accès vérifiées section. Verified Access prend en charge les destinations suivantes pour la publication des journaux d'accès :

- Groupes de CloudWatch journaux Amazon Logs
- Compartiments Amazon S3
- Flux de livraison Amazon Data Firehose

Table des matières

- Autorisations de journalisation des accès vérifiées
- Activer ou désactiver les journaux d'accès vérifiés
- Activer ou désactiver le contexte de confiance d'accès vérifié
- OCSFexemples de journaux de version 0.1 pour Verified Access
- OCSFexemples de journaux de la version 1.0.0-rc.2 pour Verified Access

Versions d'enregistrement de Verified Access

Par défaut, le système de journalisation des accès vérifiés utilise Open Cybersecurity Schema Framework (OCSF) version 0.1. Des exemples de journaux utilisant la version 0.1 peuvent être consultés dans la OCSFexemples de journaux de version 0.1 pour Verified Access section.

La dernière version de journalisation est compatible avec la OCSF version 1.0.0-rc.2. Des détails spécifiques sur le schéma peuvent être trouvés ici OCSFSchéma. Des exemples de journaux utilisant la version 1.0.0-rc.2 peuvent être consultés dans cette section. OCSFexemples de journaux de la version 1.0.0-rc.2 pour Verified Access

Si vous souhaitez mettre à niveau la version de journalisation utilisée, procédez comme suit.

Pour mettre à niveau la version de journalisation à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance Verified Access appropriée.
4. Dans l'onglet Configuration de la journalisation de l'instance Verified Access, choisissez Modifier la configuration de journalisation de l'instance Verified Access.
5. Sélectionnez ocsf-1.0.0-rc.2 dans la liste déroulante des versions du journal des mises à jour.
6. Choisissez Modifier la configuration de journalisation de l'instance Verified Access.

Pour mettre à niveau la version de journalisation à l'aide du AWS CLI

Utilisez la commande modify-verified-access-instance-logging-configuration.

Autorisations de journalisation des accès vérifiées

Le IAM principal utilisé pour configurer la destination de journalisation doit disposer de certaines autorisations pour que la journalisation fonctionne correctement. Les sections suivantes indiquent les autorisations requises pour chaque destination de journalisation.

Pour la livraison à CloudWatch Logs :

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration`sur l'instance Verified Access
- `logs:CreateLogDelivery`,`logs:DeleteLogDelivery`, `logs:GetLogDeliverylogs:ListLogDeliveries`, et `logs:UpdateLogDelivery` sur toutes les ressources
- `logs:DescribeLogGroupslogs:DescribeResourcePolicies`, et `logs:PutResourcePolicy` sur le groupe de journaux de destination

Pour la livraison vers Amazon S3 :

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration`sur l'instance Verified Access
- `logs:CreateLogDelivery`,`logs:DeleteLogDelivery`, `logs:GetLogDeliverylogs:ListLogDeliveries`, et `logs:UpdateLogDelivery` sur toutes les ressources
- `s3:GetBucketPolicy`et `s3:PutBucketPolicy` sur le compartiment de destination

Pour la livraison à Firehose :

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration`sur l'instance Verified Access
- `firehose:TagDeliveryStream`sur toutes les ressources
- `iam:CreateServiceLinkedRole`sur toutes les ressources
- `logs:CreateLogDelivery`,`logs:DeleteLogDelivery`, `logs:GetLogDeliverylogs:ListLogDeliveries`, et `logs:UpdateLogDelivery` sur toutes les ressources

Activer ou désactiver les journaux d'accès vérifiés

Vous pouvez utiliser les procédures décrites dans cette section pour activer ou désactiver la journalisation. Lorsque vous activez la journalisation, vous devez configurer une destination pour les journaux à envoyer. Le IAM principal utilisé pour configurer la destination de journalisation doit disposer de certaines autorisations pour que la journalisation fonctionne correctement. Les IAM autorisations requises pour chaque destination de journalisation sont indiquées dans la Autorisations de journalisation des accès vérifiées section.

Table des matières

Activer les journaux d'accès

Pour activer les journaux d'accès vérifiés à

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance Verified Access.
4. Dans l'onglet Configuration de la journalisation de l'instance Verified Access, choisissez Modifier la configuration de journalisation de l'instance Verified Access.
5. (Facultatif) Pour inclure les données de confiance envoyées par les fournisseurs de confiance dans les journaux, procédez comme suit :

   a. Sélectionnez ocsf-1.0.0-rc.2 dans la liste déroulante des versions du journal des mises à jour.

   b. Choisissez Inclure le contexte de confiance.
6. Effectuez l'une des actions suivantes :
   - Activez Deliver to Amazon CloudWatch Logs. Choisissez le groupe de journaux de destination.
   - Activez Deliver to Amazon S3. Entrez le nom, le propriétaire et le préfixe du compartiment de destination.
   - Activez Deliver to Firehose. Choisissez le flux de livraison de destination.
7. Choisissez Modifier la configuration de journalisation de l'instance Verified Access.

Pour activer les journaux d'accès vérifiés à l'aide du AWS CLI

Utilisez la commande modify-verified-access-instance-logging-configuration.

Désactiver les journaux d'accès

Vous pouvez désactiver les journaux d'accès pour votre instance Verified Access à tout moment. Une fois que vous avez désactivé les journaux d'accès, les données de vos journaux restent dans votre destination de journal jusqu'à ce que vous les supprimiez.

Pour désactiver les journaux d'accès vérifiés à

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance Verified Access.
4. Dans l'onglet Configuration de la journalisation de l'instance Verified Access, choisissez Modifier la configuration de journalisation de l'instance Verified Access.
5. Désactivez la livraison du journal.
6. Choisissez Modifier la configuration de journalisation de l'instance Verified Access.

Pour désactiver les journaux d'accès vérifiés à l'aide du AWS CLI

Utilisez la commande modify-verified-access-instance-logging-configuration.

Activer ou désactiver le contexte de confiance d'accès vérifié

Le contexte de confiance envoyé par votre fournisseur de confiance peut éventuellement être activé pour être inclus dans vos journaux d'accès vérifié. Cela peut être utile lorsque vous définissez des politiques qui autorisent ou refusent l'accès à vos applications. Une fois que vous l'avez activé, le contexte de confiance se trouve dans le journal situé sous le `data` champ. Si le contexte de confiance est désactivé, le `data` champ est défini sur`null`. Pour configurer Verified Access afin d'inclure le contexte de confiance dans les journaux, procédez comme suit.

> **Note**
>
> L'inclusion d'un contexte de confiance dans vos journaux d'accès vérifié nécessite une mise à niveau vers la dernière version de journalisation`ocsf-1.0.0-rc.2`. La procédure suivante

suppose que la journalisation est déjà activée. Si ce n'est pas le cas, consultez Activer les journaux d'accès la procédure complète.

Table des matières

Activer le contexte de confiance

Pour inclure un contexte de confiance dans les journaux d'accès vérifié à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance Verified Access appropriée.
4. Dans l'onglet Configuration de la journalisation de l'instance Verified Access, choisissez Modifier la configuration de journalisation de l'instance Verified Access.
5. Sélectionnez ocsf-1.0.0-rc.2 dans la liste déroulante des versions du journal des mises à jour.
6. Activez l'option Inclure le contexte de confiance.
7. Choisissez Modifier la configuration de journalisation de l'instance Verified Access.

Pour inclure un contexte de confiance dans les journaux d'accès vérifié à l'aide du AWS CLI

Utilisez la commande modify-verified-access-instance-logging-configuration.

Désactiver le contexte de confiance

Si vous ne souhaitez plus inclure le contexte de confiance dans les journaux, vous pouvez le supprimer en suivant la procédure suivante.

Pour supprimer le contexte de confiance des journaux d'accès vérifié à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Verified Access instances.
3. Sélectionnez l'instance Verified Access appropriée.

4. Dans l'onglet Configuration de la journalisation de l'instance Verified Access, choisissez Modifier la configuration de journalisation de l'instance Verified Access.
5. Désactivez l'option Inclure le contexte de confiance.
6. Choisissez Modifier la configuration de journalisation de l'instance Verified Access.

Pour supprimer le contexte de confiance des journaux d'accès vérifié à l'aide du AWS CLI

Utilisez la commande modify-verified-access-instance-logging-configuration.

OCSFexemples de journaux de version 0.1 pour Verified Access

Voici des exemples de journaux utilisant la OCSF version de journalisation par défaut 0.1.

Exemples

- Accès accordé avec OIDC
- Accès accordé avec OIDC et JAMF
- Accès accordé avec OIDC et CrowdStrike
- Accès refusé en raison d'un cookie manquant
- Accès refusé par la politique
- Entrée de journal inconnue

Accès accordé avec OIDC

Dans cet exemple d'entrée de journal, Verified Access autorise l'accès à un point de terminaison auprès d'un fournisseur de confiance OIDC utilisateur.


```
{
    "activity": "Access Granted",
    "activity_id": "1",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": {
        "ip": "10.2.7.68",
        "type": "Unknown",
        "type_id": 0
    },
```

```
    "duration": "0.004",
    "end_time": "1668580194344",
    "time": "1668580194344",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "https",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "python-requests/2.28.1",
        "version": "HTTP/1.1"
    },
    "http_response": {
        "code": 200
    },
    "identity": {
        "authorizations": [
            {
                "decision": "Allow",
                "policy": {
                    "name": "inline"
                }
            }
        ],
        "idp": {
            "name": "user",
            "uid": "vatp-09bc4cbce2EXAMPLE"
        },
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "00u6wj48lbxTAEXAMPLE"
        }
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-63748362-6408d24241120b942EXAMPLE",
        "logged_time": 1668580281337,
        "version": "0.1",
        "product": {
```

```
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T06:29:54.344948Z",
    "proxy": {
        "ip": "192.168.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-002fa341aeEXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "172.24.57.68",
        "port": "48234"
    },
    "start_time": "1668580194340",
    "status_code": "100",
    "status_details": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "20800101",
    "type_name": "AccessLogs: Access Granted",
    "unmapped": null
}
```

Accès accordé avec OIDC et JAMF

Dans cet exemple d'entrée de journal, Verified Access autorise l'accès à un point de terminaison auprès à la fois de fournisseurs de confiance OIDC et de fournisseurs de confiance en matière d'JAMFappareils.

```
{
    "activity": "Access Granted",
    "activity_id": "1",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": {
        "ip": "10.2.7.68",
        "type": "Unknown",
```

```
        "type_id": 0,
        "uid": "41b07859-4222-4f41-f3b9-97dc1EXAMPLE"
    },
    "duration": "0.347",
    "end_time": "1668804944086",
    "time": "1668804944086",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "h2",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36",
        "version": "HTTP/2.0"
    },
    "http_response": {
        "code": 304
    },
    "identity": {
        "authorizations": [
            {
                "decision": "Allow",
                "policy": {
                    "name": "inline"
                }
            }
        ],
        "idp": {
            "name": "oidc",
            "uid": "vatp-9778003bc2EXAMPLE"
        },
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "4f040d0f96becEXAMPLE"
        }
    },
    "message": "",
    "metadata": {
```

```
        "uid": "Root=1-321318ce-6100d340adf4fb29dEXAMPLE",
        "logged_time": 1668805278555,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-18T20:55:44.086480Z",
    "proxy": {
        "ip": "10.5.192.96",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-3598f66575EXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "192.168.20.246",
        "port": 61769
    },
    "start_time": "1668804943739",
    "status_code": "100",
    "status_details": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "20800101",
    "type_name": "AccessLogs: Access Granted",
    "unmapped": null
}
```

Accès accordé avec OIDC et CrowdStrike

Dans cet exemple d'entrée de journal, Verified Access autorise l'accès à un point de terminaison auprès à la fois de fournisseurs de confiance OIDC et de fournisseurs de confiance en matière d' CrowdStrike appareils.

```
{
    "activity": "Access Granted",
    "activity_id": "1",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
```

```
    "class_uid": "208001",
    "device": {
        "ip": "10.2.173.3",
        "os": {
            "name": "Windows 11",
            "type": "Windows",
            "type_id": 100
        },
        "type": "Unknown",
        "type_id": 0,
        "uid": "122978434f65093aee5dfbdc0EXAMPLE",
        "hw_info": {
            "serial_number": "751432a1-d504-fd5e-010d-5ed11EXAMPLE"
        }
    },
    "duration": "0.028",
    "end_time": "1668816620842",
    "time": "1668816620842",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "test.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "h2",
            "text": "https://test.app.example.com:443/"
        },
        "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36",
        "version": "HTTP/2.0"
    },
    "http_response": {
        "code": 304
    },
    "identity": {
        "authorizations": [
            {
                "decision": "Allow",
                "policy": {
                    "name": "inline"
                }
            }
        ],
        "idp": {
```

```
            "name": "oidc",
            "uid": "vatp-506d9753f6EXAMPLE"
        },
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "23bb45b16a389EXAMPLE"
        }
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-c16c5a65-b641e4056cc6cb0eeEXAMPLE",
        "logged_time": 1668816977134,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-19T00:10:20.842295Z",
    "proxy": {
        "ip": "192.168.144.62",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-2f80f37e64EXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "10.14.173.3",
        "port": 55706
    },
    "start_time": "1668816620814",
    "status_code": "100",
    "status_details": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "20800101",
    "type_name": "AccessLogs: Access Granted",
    "unmapped": null
}
```

Accès refusé en raison d'un cookie manquant

Dans cet exemple d'entrée de journal, Verified Access refuse l'accès en raison de l'absence d'un cookie d'authentification.


```
{
    "activity": "Access Denied",
    "activity_id": "2",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": null,
    "duration": "0.0",
    "end_time": "1668593568259",
    "time": "1668593568259",
    "http_request": {
        "http_method": "POST",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/dns-query",
            "port": 443,
            "scheme": "h2",
            "text": "https://hello.app.example.com:443/dns-query"
        },
        "user_agent": "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML",
        "version": "HTTP/2.0"
    },
    "http_response": {
        "code": 302
    },
    "identity": null,
    "message": "",
    "metadata": {
        "uid": "Root=1-5cf1c832-a565309ce20cc7dafEXAMPLE",
        "logged_time": 1668593776720,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T10:12:48.259762Z",
```

```
    "proxy": {
        "ip": "192.168.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-108ed7a672EXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "10.7.178.16",
        "port": "46246"
    },
    "start_time": "1668593568258",
    "status_code": "200",
    "status_details": "Authentication Denied",
    "status_id": "2",
    "status": "Failure",
    "type_uid": "20800102",
    "type_name": "AccessLogs: Access Denied",
    "unmapped": null
}
```

Accès refusé par la politique

Dans cet exemple d'entrée de journal, Verified Access refuse une demande authentifiée car celle-ci n'est pas autorisée par les politiques d'accès.

```
{
    "activity": "Access Denied",
    "activity_id": "2",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": {
        "ip": "10.4.133.137",
        "type": "Unknown",
        "type_id": 0
    },
    "duration": "0.023",
    "end_time": "1668573630978",
    "time": "1668573630978",
    "http_request": {
```

```
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "h2",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36",
        "version": "HTTP/2.0"
    },
    "http_response": {
        "code": 401
    },
    "identity": {
        "authorizations": [],
        "idp": {
            "name": "user",
            "uid": "vatp-e048b3e0f8EXAMPLE"
        },
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "0e1281ad3580aEXAMPLE"
        }
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-531a036a-09e95794c7b96aefbEXAMPLE",
        "logged_time": 1668573773753,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T04:40:30.978732Z",
    "proxy": {
        "ip": "3.223.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-021d5eaed2EXAMPLE"
```

```
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "10.4.133.137",
        "port": "31746"
    },
    "start_time": "1668573630955",
    "status_code": "300",
    "status_details": "Authorization Denied",
    "status_id": "2",
    "status": "Failure",
    "type_uid": "20800102",
    "type_name": "AccessLogs: Access Denied",
    "unmapped": null
}
```

Entrée de journal inconnue

Dans cet exemple d'entrée de journal, Verified Access ne peut pas générer une entrée de journal complète. Il émet donc une entrée de journal inconnue. Cela garantit que chaque demande apparaît dans le journal d'accès.

```
{
    "activity": "Unknown",
    "activity_id": "0",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": null,
    "duration": "0.004",
    "end_time": "1668580207898",
    "time": "1668580207898",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "https",
            "text": "https://hello.app.example.com:443/"
        },
```

```
        "user_agent": "python-requests/2.28.1",
        "version": "HTTP/1.1"
    },
    "http_response": {
        "code": 200
    },
    "identity": null,
    "message": "",
    "metadata": {
        "uid": "Root=1-435eb955-6b5a1d529343f5adaEXAMPLE",
        "logged_time": 1668580579147,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T06:30:07.898344Z",
    "proxy": {
        "ip": "10.1.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-6c32b53b3cEXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "172.28.57.68",
        "port": "47220"
    },
    "start_time": "1668580207893",
    "status_code": "000",
    "status_details": "Unknown",
    "status_id": "0",
    "status": "Unknown",
    "type_uid": "20800100",
    "type_name": "AccessLogs: Unknown",
    "unmapped": null
}
```


OCSFexemples de journaux de la version 1.0.0-rc.2 pour Verified Access

Voici des exemples de journaux utilisant la OCSF version de journalisation 1.0.0-rc.2.

Table des matières

Accès accordé avec contexte de confiance inclus


```
{
    "activity_name": "Access Grant",
    "activity_id": "1",
    "actor": {
        "authorizations": [{
            "decision": "Allow",
            "policy": {
                "name": "inline"
            }
        }],
        "idp": {
            "name": "user",
            "uid": "vatp-09bc4cbce2EXAMPLE"
        },
        "invoked_by": "",
        "process": {},
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "00u6wj48lbxTAEXAMPLE"
        },
        "session": {}
    },
    "category_name": "Audit Activity",
    "category_uid": "3",
    "class_name": "Access Activity",
    "class_uid": "3006",
    "device": {
        "ip": "10.2.7.68",
        "type": "Unknown",
        "type_id": 0
    },
    "duration": "0.004",
    "end_time": "1668580194344",
    "time": "1668580194344",
```

```
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "https",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "python-requests/2.28.1",
        "version": "HTTP/1.1"
    },
    "http_response": {
        "code": 200
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-63748362-6408d24241120b942EXAMPLE",
        "logged_time": 1668580281337,
        "version": "1.0.0-rc.2",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T06:29:54.344948Z",
    "proxy": {
        "ip": "192.168.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-002fa341aeEXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "172.24.57.68",
        "port": "48234"
    },
    "start_time": "1668580194340",
    "status_code": "100",
    "status_detail": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "300601",
```

```
    "type_name": "Access Activity: Access Grant",
    "data": {
        "context": {
            "oidc": {
                "family_name": "Last",
                "zoneinfo": "America/Los_Angeles",
                "exp": 1670631145,
                "middle_name": "Middle",
                "given_name": "First",
                "email_verified": true,
                "name": "Test User Display",
                "updated_at": 1666305953,
                "preferred_username": "johndoe-user@test.com",
                "profile": "http://www.example.com",
                "locale": "US",
                "nickname": "Tester",
                "email": "johndoe-user@test.com"
            },
            "http_request": {
                "x_forwarded_for": "1.1.1.1,2.2.2.2",
                "http_method": "GET",
                "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36",
                "port": "80",
                "hostname": "hostname.net"
            }
        }
    }
}
```

Accès accordé sans contexte de confiance

```
{
    "activity_name": "Access Grant",
    "activity_id": "1",
    "actor": {
        "authorizations": [{
            "decision": "Allow",
            "policy": {
                "name": "inline"
            }
        }],
        "idp": {
```

```
            "name": "user",
            "uid": "vatp-09bc4cbce2EXAMPLE"
        },
        "invoked_by": "",
        "process": {},
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "00u6wj48lbxTAEXAMPLE"
        },
        "session": {}
    },
    "category_name": "Audit Activity",
    "category_uid": "3",
    "class_name": "Access Activity",
    "class_uid": "3006",
    "device": {
        "ip": "10.2.7.68",
        "type": "Unknown",
        "type_id": 0
    },
    "duration": "0.004",
    "end_time": "1668580194344",
    "time": "1668580194344",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "https",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "python-requests/2.28.1",
        "version": "HTTP/1.1"
    },
    "http_response": {
        "code": 200
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-63748362-6408d24241120b942EXAMPLE",
        "logged_time": 1668580281337,
```

```
        "version": "1.0.0-rc.2",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T06:29:54.344948Z",
    "proxy": {
        "ip": "192.168.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-002fa341aeEXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "172.24.57.68",
        "port": "48234"
    },
    "start_time": "1668580194340",
    "status_code": "100",
    "status_detail": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "300601",
    "type_name": "Access Activity: Access Grant",
    "data": null
}
```


Enregistrez les API appels Verified Access en utilisant AWS CloudTrail

AWS L'accès vérifié est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service accès vérifié. CloudTrail capture tous les API appels pour un accès vérifié sous forme d'événements. Les appels capturés incluent les appels provenant de la console Verified Access et les appels codés vers les API opérations Verified Access. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrailévénements vers un compartiment Amazon S3, y compris des événements pour Verified Access. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par

CloudTrail, vous pouvez déterminer la demande qui a été faite à Verified Access, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations d'accès vérifiées dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans Verified Access, cette activité est enregistrée dans un CloudTrail événement avec d'autres AWS service événements dans l'historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements à l'aide de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre site Compte AWS, y compris les événements pour Verified Access, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez en configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- CloudTrail services et intégrations pris en charge
- Configuration des SNS notifications Amazon pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les actions d'accès vérifié sont enregistrées CloudTrail et documentées dans le Amazon EC2 API Reference. Par exemple, les appels au`CreateVerifiedAccessInstance`, `DeleteVerifiedAccessInstance` et les `ModifyVerifiedAccessInstance` actions génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre AWS service.

Pour plus d'informations, voir CloudTrail userIdentity élément.

Comprendre les entrées du fichier journal d'accès vérifié

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande individuelle d'une source quelconque. Il inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des API appels publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal pour l'`CreateVerifiedAccessInstance`action.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIKK4OOINJWEXAMPLE:jdoe",
        "arn": "arn:aws:iam::123456789012:user/jdoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "jdoe"
    },
    "eventTime": "2022-11-18T20:44:04Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateVerifiedAccessInstance",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "CreateVerifiedAccessInstanceRequest": {
            "Description": "",
            "ClientToken": "85893b1e-49f6-4d24-97de-280c664edf1b"
```

```
        }
    },
    "responseElements": {
        "CreateVerifiedAccessInstanceResponse": {
            "verifiedAccessInstance": {
                "creationTime": "2022-11-18T20:44:04",
                "description": "",
                "verifiedAccessInstanceId": "vai-0d79d91875542c549",
                "verifiedAccessTrustProviderSet": ""
            },
            "requestId": "2eae195d-6bfd-46d7-b46e-a68cb791de09"
        }
    },
    "requestID": "2eae195d-6bfd-46d7-b46e-a68cb791de09",
    "eventID": "297d6529-1144-40f6-abf8-3a76f18d88f0",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Quotas pour Accès vérifié par AWS

Vous Compte AWS disposez de quotas par défaut, anciennement appelés limites, pour chacun d'entre eux AWS service. Sauf indication contraire, chaque quota est spécifique à la région.

Compte AWS quotas de niveau -niveau

Vous Compte AWS disposez des quotas suivants relatifs à l'accès vérifié.

Nom	Par défaut	Ajustable	Description
Instances d'accès vérifiées	5	Oui	Le nombre maximum d'instances à accès vérifié que les clients peuvent créer dans la région actuelle.
Groupes d'accès vérifiés	10	Oui	Le nombre maximum de groupes d'accès vérifiés que les clients peuvent créer dans la région actuelle.
Fournisseurs d'accès sécurisés vérifiés	15	Oui	Le nombre maximum de fournisseurs d'accès sécurisés vérifiés que les clients peuvent créer dans la région actuelle.
Points de terminaison d'accès vérifiés	50	Oui	Le nombre maximum de points de terminaison d'accès vérifiés que les clients peuvent créer dans la région actuelle.

HTTPen-têtes

Les limites de taille pour les HTTP en-têtes sont les suivantes.

Nom	Par défaut	Ajustable
Ligne de demande	16 K	Non

Nom	Par défaut	Ajustable
En-tête seul	16 K	Non
En-tête de réponse entier	32 K	Non
En-tête de demande entier	64 K	Non

OIDCtaille de la réclamation

Voici la limite de OIDC taille des demandes.

Nom	Par défaut	Ajustable
OIDCtaille de la réclamation	11 KM	Non

Historique des documents pour le guide de l'utilisateur de Verified Access

Le tableau suivant décrit les versions de documentation relatives à Verified Access.

Modification	Description	Date
AWS politique gérée mise à jour	Mise à jour apportée à IAM la politique AWS gérée pour l'accès vérifié.	17 novembre 2023
Chiffrement des données au repos	AWS Verified Access chiffre les données au repos par défaut, à l'aide de KMS clés AWS détenues.	28 septembre 2023
Support en matière de FIPS conformité	Configurez l'accès vérifié pour garantir FIPS la conformité.	26 septembre 2023
Journalisation améliorée	Ajout d'une fonctionnalité de journalisation qui ajoute des contextes de confiance aux journaux.	19 juin 2023
AWS politique gérée mise à jour	Mise à jour apportée à IAM la politique AWS gérée pour l'accès vérifié.	31 mai 2023
Version GA	Publication générale du guide de l'utilisateur de Verified Access. Inclut AWS WAF l'intégration.	27 avril 2023
Version préliminaire	Version préliminaire du guide de l'utilisateur de Verified Access	29 novembre 2022

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.