Manual do usuário

AWS Acesso verificado

AWS Acesso verificado: Manual do usuário

Table of Contents

O que é o Acesso Verificado pela AWS?

Com o Acesso Verificado pela AWS, você pode fornecer acesso seguro aos seus aplicativos sem exigir o uso de uma rede privada virtual (VPN). O acesso verificado avalia cada solicitação de aplicativo e ajuda a garantir que os usuários possam acessar cada aplicativo somente quando atenderem aos requisitos de segurança especificados.

Benefícios do acesso verificado

- Postura de segurança aprimorada: um modelo de segurança tradicional avalia o acesso uma vez e concede ao usuário acesso a todos os aplicativos. O acesso verificado avalia cada solicitação de acesso ao aplicativo em tempo real. Isso dificulta a migração de agentes mal-intencionados de um aplicativo para outro.
- Integração com serviços de segurança: o acesso verificado se integra aos serviços de gerenciamento de identidade e dispositivos, incluindo serviços da AWS e de terceiros. Usando dados desses serviços, o acesso verificado analisa a confiabilidade dos usuários e dispositivos em relação a um conjunto de requisitos de segurança e determina se o usuário deve ter acesso a um aplicativo.
- Experiência de usuário aprimorada: o acesso verificado elimina a necessidade de os usuários usarem uma VPN para acessar seus aplicativos. Isso ajuda a reduzir o número de casos de suporte decorrentes de problemas relacionados à VPN.
- Solução de problemas e auditorias simplificadas: o acesso verificado registra todas as tentativas de acesso, fornecendo visibilidade centralizada do acesso aos aplicativos, para ajudá-lo a responder rapidamente a incidentes de segurança e solicitações de auditoria.

Acessando o Acesso Verificado pela AWS

Você pode trabalhar com o acesso verificado usando qualquer uma das seguintes interfaces:

- AWS Management Console: fornece uma interface de usuário baseada na Web que pode ser usada para criar e gerenciar recursos do acesso verificado. Faça login no AWS Management Console e abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
- AWS Command Line Interface (AWS CLI): fornece comandos para um amplo conjunto de Serviços da AWS, inclusive o Acesso Verificado pelaa AWS. A AWS CLI é compatível com Windows, macOS e Linux. Para obter a AWS CLI, consulte AWS Command Line Interface.

- SDKs da AWS — fornecem APIs específicas da linguagem. Os AWS SDKs cuidam de muitos dos detalhes da conexão, como calcular assinaturas, com tentativas e erros de solicitação para controlar. Para obter mais informações, consulte AWS SDKs.
- API de consulta: fornece ações de API de baixo nível que são chamadas usando solicitações HTTPS. Usar a API de consulta é a maneira mais direta de acessar o acesso verificado. No entanto, ela exige que a aplicação trate detalhes de baixo nível, como gerar o hash para assinar a solicitação e tratar erros. Para obter mais informações, consulte Ações do acesso verificado na Referência de API do Amazon EC2.

Este guia descreve como usar AWS Management Console para criar, acessar e gerenciar recursos do acesso verificado.

Preços

Você será cobrado por hora por cada aplicativo no acesso verificado e pela quantidade de dados processada pelo acesso verificado. Para obter mais informações, consulte Definição de preço do Acesso Verificado pela AWS.

Como funciona o Acesso Verificado

AWS O Acesso Verificado avalia cada solicitação de aplicativo de seus usuários e permite o acesso com base em:

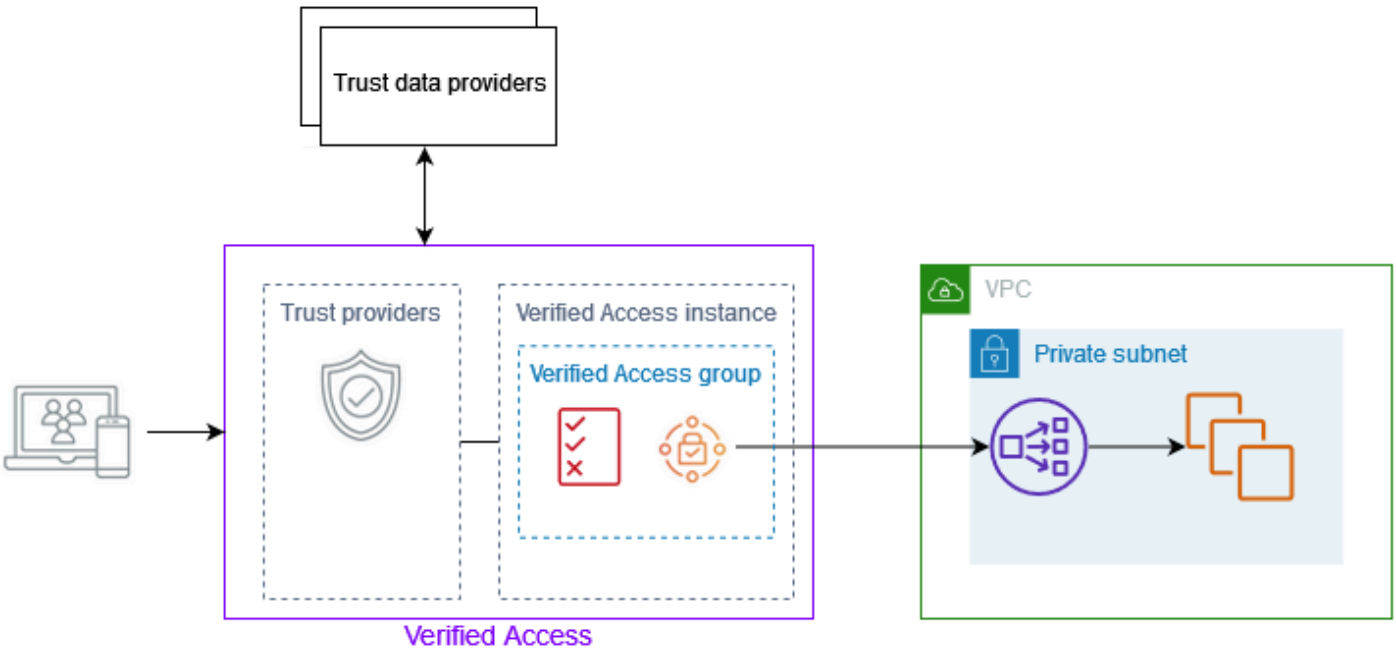
- Dados confiáveis enviados pelo provedor de confiança escolhido (de AWS ou de terceiros).
- Políticas de acesso que você cria no Acesso Verificado.

Quando um usuário tenta acessar um aplicativo, o Acesso Verificado obtém seus dados do provedor confiável e os avalia em relação às políticas que você definiu para o aplicativo. O Acesso Verificado concede acesso ao aplicativo solicitado somente se o usuário atender aos requisitos de segurança especificados. Todas as solicitações de aplicativos são negadas por padrão, até que uma política seja definida.

Além disso, o Acesso Verificado registra todas as tentativas de acesso, para ajudar você a responder rapidamente a incidentes de segurança e solicitações de auditoria.

Principais componentes do Acesso Verificado

O seguinte diagrama fornece uma visão geral de alto nível sobre como o Acesso Verificado funciona. Os usuários enviam solicitações para acessar um aplicativo. O Acesso Verificado avalia a solicitação em relação à política de acesso do grupo e a qualquer política de endpoint específica do aplicativo. Se o acesso for permitido, a solicitação será enviada para o aplicativo por meio do endpoint.



- Instâncias de Acesso Verificado: uma instância avalia as solicitações de aplicativos e concede acesso somente quando seus requisitos de segurança são atendidos.
- Endpoints de acesso verificado: cada endpoint representa um aplicativo. Você pode criar um endpoint de balanceador de carga ou um endpoint de interface de rede.
- Grupo de acesso verificado: uma coleção de endpoints de acesso verificado Recomendamos que você agrupe os endpoints para aplicativos com requisitos de segurança semelhantes para simplificar a administração de políticas. Por exemplo, você pode agrupar os endpoints de todos os seus aplicativos de vendas.
- Políticas de acesso — Um conjunto de regras definidas pelo usuário que determinam se o acesso a um aplicativo deve ser permitido ou negado. Você pode especificar uma combinação de fatores, incluindo identidade do usuário e estado de segurança do dispositivo. Você cria uma política de acesso de grupo para cada grupo de Acesso Verificado, que é herdada por todos os endpoints do grupo. Opcionalmente, você pode criar políticas específicas do aplicativo e anexá-las a endpoints específicos.
- Provedores confiáveis — um serviço que gerencia as identidades dos usuários ou o estado de segurança do dispositivo. O Acesso Verificado funciona com provedores AWS fiduciários e terceirizados. Você deve anexar pelo menos um provedor de confiança a cada instância de Acesso Verificado. Você pode anexar um único provedor de confiança de identidade e vários provedores de confiança de dispositivos a cada instância de Acesso Verificado.

- Dados confiáveis: os dados relacionados à segurança de usuários ou dispositivos que seu provedor confiável envia para o Acesso Verificado. Também conhecido como reivindicações do usuário ou contexto de confiança. Por exemplo, o endereço de e-mail de um usuário ou a versão do sistema operacional de um dispositivo. O Acesso Verificado avalia esses dados em relação às suas políticas de acesso ao receber cada solicitação para acessar um aplicativo.

Tutorial: conceitos básicos do Acesso Verificado

Use este tutorial para começar a usar o AWS Acesso Verificado. Você aprenderá a criar e configurar recursos de Acesso Verificado.

Antes de adicionar esse aplicativo ao Acesso Verificado, o aplicativo só era acessível pela sua rede privada. No final deste tutorial, usuários específicos podem acessar o mesmo aplicativo pela internet, sem usar VPN.

> **Note**
>
> Este exemplo não demonstra a integração com seu provedor de confiança baseado em dispositivos. Neste exemplo, estamos trabalhando apenas com um provedor de confiança baseado em identidade.

Tarefas

Pré-requisitos

Este tutorial requer os seguintes pré-requisitos:

- Para demonstrar esse exemplo de uso do Acesso Verificado, usaremos dois Contas da AWS. Uma conta hospedará seu aplicativo de destino e os recursos de Acesso Verificado serão criados na outra conta.
- Habilite o AWS IAM Identity Center em Região da AWS que você está trabalhando. Em seguida, você pode usar o IAM Identity Center como um provedor confiável com Acesso Verificado. Para obter mais informações, consulte What is IAM Identity Center (O que é o Centro de Identidade do IAM?) no Guia do usuário do AWS IAM Identity Center.
- Um domínio público hospedado e as permissões necessárias para atualizar os registros DNS do domínio.
- Um aplicativo executado por trás de um balanceador de carga interno em um Conta da AWS. O exemplo de nome de domínio do aplicativo que usaremos é `www.myapp.example.com`.
- Certifique-se de que sua política do IAM tenha todas as permissões necessárias para criar uma instância de AWS Acesso Verificado, indicada aqui Política para criar instâncias de Acesso Verificado.

Etapa 1: Criar uma instância do Acesso Verificado

Use o procedimento a seguir para criar uma instância do Acesso Verificado.

Para criar uma instância do acesso verificado

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação do Amazon VPC, escolha Instâncias de Acesso Verificado e, em seguida, Criar instância de Acesso Verificado.
3. (Opcional) Em Nome e Descrição, insira um nome e uma descrição para a instância do Acesso Verificado.
4. Para Trust provider, mantenha a opção padrão.
5. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
6. Escolha Criar instância de Acesso Verificado.

Etapa 2: Configurar um provedor de confiança

Você pode se configurar AWS IAM Identity Center como seu provedor de confiança.

Para criar um provedor de confiança do IAM Identity Center

1. No painel de navegação do Amazon VPC, escolha Provedores de confiança de Acesso Verificado e, em seguida, Criar provedor de confiança de Acesso Verificado.
2. (Opcional) Em Tag de nome e Descrição, insira um nome e uma descrição para o provedor confiável de Acesso Verificado.
3. Insira um identificador personalizado para usar posteriormente ao trabalhar com regras de política para o nome de referência da política. Por exemplo, insira: **`idc`**
4. Em Tipo de provedor confiável, selecione Provedor de confiança do usuário.
5. Em Tipo de provedor de confiança do usuário, selecione IAM Identity Center.
6. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
7. Escolha Criar provedor confiável de Acesso Verificado.

Etapa 3: Anexar seu provedor de confiança à instância

Use o procedimento a seguir para associar o provedor de confiança à sua instância do Acesso Verificado.

Para anexar um provedor de confiança à sua instância

1. No painel de navegação do Amazon VPC, escolha Instâncias de Acesso Verificado.
2. Selecione sua instância.
3. Escolha Ações, Anexar provedor confiável de Acesso Verificado.
4. Para provedor confiável de Acesso Verificado, escolha seu provedor de confiança.
5. Escolha Anexar provedor confiável de Acesso Verificado.

Etapa 4: Criar grupo do Acesso Verificado

Vamos criar um grupo que você pode usar para o endpoint que você criará na próxima etapa.

Para criar um grupo do Acesso Verificado

1. No painel de navegação do Amazon VPC, escolha Grupos de Acesso Verificado e, em seguida, Criar grupo de Acesso Verificado.
2. (Opcional) Em Tag de nome e Descrição, insira um nome e uma descrição para o grupo.

3. Para instância de Acesso Verificado, escolha sua instância de Acesso Verificado.
4. Para definição de política, mantenha isso em branco. Você vai criar uma política mais adiante neste tutorial.
5. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
6. Escolha Criar grupo de Acesso Verificado.

Etapa 5: compartilhe seu grupo de Acesso Verificado por meio de AWS Resource Access Manager

Nesta etapa, você compartilhará o grupo que acabou de criar com o Conta da AWS no qual seu aplicativo de destino está sendo executado. Para compartilhar um grupo de Acesso Verificado, é necessário adicioná-lo a um compartilhamento de recursos. Caso você não tenha um compartilhamento de recursos, primeiro será necessário criar um.

Se você fizer parte de uma organização no AWS Organizations e o compartilhamento estiver habilitado na organização, os consumidores da organização receberão acesso automaticamente ao Acesso Verificado compartilhado. Caso contrário, os consumidores receberão um convite para participar do compartilhamento de recursos e acesso ao Acesso Verificado compartilhado depois de aceitar o convite.

Siga as etapas em Criar um compartilhamento de recursos no Manual do usuário do AWS RAM. Em Selecionar tipo de recurso, escolha Grupo do Acesso Verificado e marque a caixa de seleção do seu grupo do Acesso Verificado.

Para obter mais informações, consulte Conceitos básicos no Guia do usuário do AWS RAM.

Etapa 6: adicione seu aplicativo criando um endpoint

Use o procedimento a seguir para criar um endpoint. Essa etapa pressupõe que você tenha um aplicativo em execução por trás de um balanceador de carga interno do Elastic Load Balancing.

Para criar um endpoint do Acesso Verificado

1. No painel de navegação do Amazon VPC, escolha Endpoints de acesso verificado e, em seguida, Criar endpoint de acesso verificado.
2. (Opcional) Em Tag de nome e Descrição, insira um nome e uma descrição para o endpoint.
3. Para Grupo de Acesso Verificado, escolha seu grupo de Acesso Verificado.

4. Para obter detalhes do aplicativo faça o seguinte:

    a. Em Domínio do aplicativo, insira um nome DNS para seu aplicativo.

    b. Em ARN do certificado de domínio, selecione o nome do recurso da Amazon (ARN) do seu certificado TLS público.

5. Em Detalhes do endpoint, faça o seguinte:

    a. Em Attachment type (Tipo de anexo), escolha VPC.

    b. Em Grupos de segurança, selecione o grupo de segurança a ser associado ao endpoint.

    c. Em Prefixo de domínio do Endpoint, insira um identificador personalizado. Isso será anexado ao nome DNS que o Acesso Verificado gera. Para este exemplo, usaremos **`my-ava-app`**.

    d. Em Tipo de endpoint escolha balanceador de carga.

    e. Em Protocolo, selecione HTTPS ou HTTP. Isso depende da configuração do seu balanceador de carga.

    f. Em Port (Porta), digite o número da porta. Isso depende da configuração do seu balanceador de carga.

    g. Em Load balancers ARN, selecione seu balanceador de carga.

    h. Em Sub-redes, selecione as sub-redes associadas ao seu balanceador de carga.

6. Para definição de política, não insira uma política no momento. Abordaremos isso posteriormente no tutorial.

7. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.

8. Escolha Criar endpoint de Acesso Verificado.

Etapa 7: definir as configurações de DNS

Nesta etapa, você mapeia o nome de domínio do seu aplicativo (por exemplo, www.myapp.example.com) para o nome de domínio do seu endpoint de Acesso Verificado. Para concluir o mapeamento do DNS, crie um Registro de Nome Canônico (CNAME) com seu provedor de DNS. Depois de criar o registro CNAME, todas as solicitações dos usuários ao seu aplicativo serão enviadas para o Acesso Verificado.

Para obter o nome de domínio do endpoint.

1. No painel de navegação do Amazon VPC, escolha Endpoints de acesso verificado.

2. Selecione o endpoint que você criou anteriormente.
3. Escolha a guia Detalhes para o endpoint.
4. Copie o domínio do endpoint em Domínio do endpoint.

Neste tutorial, o nome de domínio do endpoint será `my-ava-app.edge-1a2b3c4d5e6f7g.vai-1a2b3c4d5e6f7g.prod.verified-access.us-west-2.amazonaws.com`.

Crie um registro CNAME com seu provedor de DNS:

Nome de registro	Tipo	Valor
www.myapp.example.com	CNAME	my-ava-app.edge-1a 2b3c4d5e6f7g.vai-1 a2b3c4d5e6f7g.prod. verified-access.us-west-2.amazonaws. com

Etapa 8: Conectar um aplicativo ao operador

Agora você pode testar a conectividade com seu aplicativo. Insira o nome de domínio do seu aplicativo em seu navegador da web. O comportamento padrão das políticas de Acesso Verificado é negar todas as solicitações. Como ainda não implementamos uma política que permita o acesso de qualquer pessoa, todas as solicitações devem ser negadas.

Etapa 9: Configurar a política de acesso em nível de grupo

Use o procedimento a seguir para modificar o grupo de Acesso Verificado e configurar uma política de acesso que permita a conectividade com seu aplicativo. Os detalhes da política dependerão dos usuários e grupos configurados no IAM Identity Center. Para obter informações sobre a criação de uma política, consulte Políticas de acesso verificado.

Para modificar um grupo do Acesso Verificado

1. No painel de navegação do Amazon VPC, escolha Grupos de Acesso Verificado.
2. Selecione seu grupo do .

3. Escolha Ações, Modificar política de grupo de Acesso Verificado.
4. Insira a política.
5. Escolha Modificar política de grupo de Acesso Verificado.

Etapa 10: testar novamente a conectividade

Agora que sua política de grupo está em vigor, você pode acessar seu aplicativo. Insira o nome de domínio do seu aplicativo em seu navegador da web. A solicitação deve ser permitida e você deve ser redirecionado para o aplicativo.

Limpeza

Depois de concluir o teste, siga a etapa abaixo para excluir os recursos que foram criados.

Para excluir os recursos de Acesso Verificado criados com este tutorial

1. No painel de navegação do Amazon VPC, escolha Endpoints de acesso verificado. Selecione o endpoint que deseja remover. Escolha Ações, Excluir endpoint de acesso verificado.
2. No painel de navegação, escolha grupos de Acesso Verificado. Selecione o grupo que deseja remover. Escolha Ações, Excluir grupo de Acesso Verificado. Observação: talvez seja necessário aguardar alguns minutos até que o processo de exclusão do endpoint seja concluído.
3. No painel de navegação do Amazon VPC, escolha Instâncias de Acesso Verificado. Selecione a instância que você criou para este tutorial. Escolha Ações, Desanexe o provedor confiável de Acesso Verificado. Selecione o provedor de confiança na lista suspensa e escolha Desanexar provedor confiável de Acesso Verificado.
4. No painel de navegação do Amazon VPC, escolha Provedores de confiança de Acesso Verificado. Selecione o provedor de confiança que você criou para este tutorial. Escolha Ações, Excluir provedor confiável de Acesso Verificado.
5. No painel de navegação do Amazon VPC, escolha Instâncias de Acesso Verificado. Selecione a instância que você criou para este tutorial. Escolha Ações, Excluir instância de Acesso Verificado.

Instâncias de acesso verificado

Uma instância de Acesso Verificado pela AWS é um recurso da AWS que ajuda você a organizar seus provedores de confiança e grupos de acesso verificado.

Tópicos

Criar uma instância do acesso verificado

Use o procedimento a seguir para criar uma instância do acesso verificado.

Para criar uma instância do acesso verificado

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Instâncias de acesso verificado e, em seguida, Criar instância de acesso verificado.
3. (Opcional) Em Nome e Descrição, insira um nome e uma descrição para a instância do acesso verificado.
4. (Opcional) Escolha ativar para os Padrões Federais de Processo de Informações (FIPS) se você precisar que o acesso verificado seja compatível com FIPS.
5. (Opcional) Em Provedor confiável, escolha um provedor confiável para anexar à instância de acesso verificado.
6. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
7. Escolha Criar instância de acesso verificado.

Vincular um provedor de confiança a uma instância

Use o procedimento a seguir para associar um provedor de confiança a uma instância do acesso verificado.

Para anexar um provedor de confiança a uma instância do acesso verificado

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do acesso verificado.
3. Selecione a instância.
4. Escolha Ações, Anexar provedor confiável de acesso verificado.
5. Para provedor confiável de acesso verificado, escolha um provedor confiável.
6. Escolha Anexar provedor confiável de acesso verificado.

Desanexar um provedor de confiança de uma instância

Use o procedimento a seguir para desvincular um provedor de confiança de uma instância do acesso verificado.

Para desvincular um provedor de confiança de uma instância do acesso verificado

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do acesso verificado.
3. Selecione a instância.
4. Escolha Ações, Desanexe o provedor confiável de acesso verificado.
5. Para provedor confiável de acesso verificado, escolha o provedor confiável.
6. Escolha Desanexar provedor confiável de acesso verificado.

Excluir uma instância do acesso verificado

Quando não precisar mais de uma instância do acesso verificado, você poderá excluí-la. Antes de excluir uma instância, você deve remover todos os provedores de confiança ou grupos de acesso verificado associados.

Como excluir uma instância do acesso verificado

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do acesso verificado.
3. Selecione a instância de acesso verificado.
4. Escolha Ações, Excluir instância de acesso verificado.
5. Quando a confirmação for solicitada, insira **`delete`** e escolha Excluir.

Integração com o AWS WAF

Além das regras de autenticação e autorização impostas pelo acesso verificado, talvez você também queira aplicar a proteção de perímetro. Isso pode ajudar você a proteger seus aplicativos contra ameaças adicionais. Você pode fazer isso AWS WAF integrando-se à sua implantação do acesso verificado. AWS WAF é um firewall para aplicativos web que permite monitorar as solicitações HTTP (S) que são encaminhadas aos recursos protegidos do aplicativo web que permite monitorar as solicitações HTTP (S) que são encaminhadas aos recursos protegidos do aplicativo web. Para obter mais informações sobre as AWS WAF, consulte AWS WAF no Guia do desenvolvedor do AWS WAF.

É possível integrar o AWS WAF ao acesso verificado associando uma AWS WAF lista de controle de acesso (ACL) a uma instância do acesso verificado. A ACL da web é um AWS WAF recurso que oferece controle detalhado sobre todas as solicitações web HTTP (S) às quais o recurso protegido responde. Enquanto a solicitação de AWS WAF associação ou desassociação está sendo processada, o status de qualquer endpoint de acesso verificado anexado à instância é mostrado como `updating`. Depois que a solicitação for concluída, o status retornará a `active`. Você pode visualizar o status no AWS Management Console ou descrevendo o endpoint com o AWS CLI.

> **Note**
>
> Você também pode usar o AWS WAF console ou a API para realizar essa integração. Você precisará do nome do recurso da Amazon (ARN) da instância do acesso verificado. Esse nome ARN pode ser criado usando o seguinte formato: `arn:${Partition}:ec2:${Region}:${Account}:verified-access-instance/${VerifiedAccessInstanceId}`.

Tópicos

Permissões do IAM necessárias para integrar AWS WAF

Integração de AWS WAF com o acesso verificado inclui ações somente de permissão que não correspondem diretamente a uma operação de API. Essas ações são indicadas na AWS Identity and Access Management Referência de autorização de serviço com `[permission only]`. Consulte Ações, recursos e chaves de condição do Amazon EC2 na Referência de autorização do serviço.

Para trabalhar com uma ACL da web, seu AWS Identity and Access Management diretor deve ter as permissões a seguir.

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

Associar uma AWS WAF ACL da web

As etapas a seguir demonstram como associar uma AWS WAF lista de controle de acesso (ACL) a uma instância do acesso verificado usando o AWS Management Console.

> **Tip**
>
> Você precisará ter uma AWS WAF Web ACL existente para concluir o procedimento abaixo. Para obter mais informações sobre ACLs da web, consulte Listas de controle de acesso web no AWS WAFGuia do desenvolvedor.

Para associar uma ACL AWS WAF da web a uma instância de acesso verificado

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do acesso verificado.

3. Selecione a instância de acesso verificado.
4. Selecione a guia Integrações.
5. Selecione Ações e Associar Web ACL.
6. Para Web ACL, escolha uma Web ACL existente e, em seguida, escolha Associar Web ACL.

Você também pode usar o AWS Management Console for AWS WAF para realizar essa tarefa. Para obter mais informações, consulte Associar ou desassociar uma ACL da web a um recurso da AWS no Guia do desenvolvedor. AWS WAF

Verifique o status da AWS WAF integração

É possível verificar se uma lista de controle de acesso (ACL) à AWS WAF Web (ACL) do Web (ACL) está associada a uma instância do acesso verificado usando o AWS Management Console.

Como visualizar o status da AWS WAF integração com uma instância do acesso verificado

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do acesso verificado.
3. Selecione a instância de acesso verificado.
4. Selecione a guia Integrações.
5. Verifique os detalhes listados em Status de integração do WAF. O status será mostrado como Associado ou Não associado, junto com o identificador da Web ACL, se estiver no estado Associado.

Desassociar uma ACL AWS WAF da web

As etapas a seguir demonstram como desassociar uma lista AWS WAF de controle de acesso (ACL) de uma instância do acesso verificado usando o AWS Management Console.

Para desassociar uma ACL AWS WAF da web de uma instância do acesso verificado

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do acesso verificado.
3. Selecione a instância de acesso verificado.
4. Selecione a guia Integrações.

5. Escolha Ações e, em seguida, Desassociar Web ACL.
6. Confirme escolhendo Disassociate Web ACL.

Você também pode usar o AWS Management Console for AWS WAF para realizar essa tarefa. Para obter mais informações, consulte Associar ou desassociar uma ACL da web a um recurso da AWS no Guia do desenvolvedor. AWS WAF

Conformidade com FIPS para acesso verificado

A Federal Information Processing Standard (FIPS - Padrão de processamento de informações federal) é um padrão de segurança do governo dos Estados Unidos que especifica os requisitos de segurança para módulos de criptografia que protegem informações confidenciais. Acesso Verificado pela AWS fornece a opção de configurar seu ambiente para aderir à publicação FIPS 140-2. A conformidade com FIPS para acesso verificado está disponível nas AWS regiões a seguir:

- Leste dos EUA (Ohio)
- Leste dos EUA (N. da Virgínia)
- Oeste dos EUA (N. da Califórnia)
- Oeste dos EUA (Oregon)
- Canadá (Central)

Esta página mostra como configurar um ambiente novo ou existente de acesso verificado para ser compatível com FIPS.

Tópicos

Configurar um ambiente de acesso verificado existente para conformidade com FIPS

Se você tiver um ambiente de acesso verificado existente e quiser configurá-lo para ser compatível com FIPS, alguns dos recursos precisarão ser excluídos e recriados para ativar a conformidade com o FIPS.

Para reconfigurar um Acesso Verificado pela AWS ambiente existente para ser compatível com FIPS, siga as etapas abaixo.

1. Exclua seus endpoints, grupos e instância originais do acesso verificado. Seus provedores de confiança configurados podem ser reutilizados.
2. Crie uma instância de acesso verificado, certificando-se de ativar o Federal Information Process Standards (FIPS) durante a criação. Além disso, durante a criação, anexe o provedor confiável de acesso verificado que você deseja usar, selecionando-o na lista suspensa.
3. Crie um grupo de acesso verificado. Durante a criação do grupo, você o associa à instância de acesso verificado recém-criada.
4. Crie um ou mais Endpoints de acesso verificado. Durante a criação dos seus endpoints, você os associa ao grupo criado na etapa anterior.

Configure um novo ambiente de acesso verificado para conformidade com FIPS

Para configurar um novo Acesso Verificado pela AWS ambiente compatível com FIPS, siga as etapas abaixo.

1. Configure um provedor de confiança. Você precisará criar um provedor de confiança de identidade de usuário e (opcionalmente) um provedor de confiança baseado em dispositivo, dependendo de suas necessidades.
2. Crie uma instância de acesso verificado, certificando-se de ativar o Federal Information Process Standards (FIPS) durante o processo. Além disso, durante a criação, anexe o provedor confiável de acesso verificado que você criou na etapa anterior, selecionando-o na lista suspensa.
3. Crie um grupo de acesso verificado. Durante a criação do grupo, você o associa à instância de acesso verificado recém-criada.
4. Crie um ou mais Endpoints de acesso verificado. Durante a criação dos seus endpoints, você os associa ao grupo criado na etapa anterior.

Provedores confiáveis para Acesso Verificado

Um provedor de confiança é um serviço que envia informações sobre usuários e dispositivos ao Acesso Verificado pela AWS. Essas informações são chamadas de contexto de confiança. Elas podem incluir atributos baseados na identidade do usuário, como endereço de e-mail ou associação à organização de “vendas”, ou informações sobre os dispositivos, como patches de segurança ou versão do software antivírus.

O Acesso Verificado oferece suporte às seguintes categorias de provedores de confiança:

- Identidade do usuário: um serviço de provedor de identidade (IdP) que armazena e gerencia identidades digitais para usuários.
- Gerenciamento de dispositivos — Um sistema de gerenciamento de dispositivos para dispositivos como laptops, tablets e smartphones.

Conteúdos

Provedores de confiança de identidade de usuário

Você pode optar por usar um AWS IAM Identity Center ou um provedor confiável de identidade de usuário compatível com o OpenID Connect.

Conteúdos

Usar o IAM Identity Center como provedor confiável

Você pode usar AWS IAM Identity Center como seu provedor confiável de identidade de usuário com o AWS Acesso Verificado.

Pré-requisitos e considerações

- Sua instância do Centro de Identidade do IAM deve ser uma instância AWS Organizations. Uma instância do Centro de Identidade do IAM de uma conta da AWS autônoma não funcionará.
- A instância do Centro de Identidade do IAM deve estar habilitada na mesma região da AWS em que você deseja criar o provedor confiável do Acesso Verificado.

Consulte Gerenciar instâncias da organização e da conta do Centro de Identidade do IAM no Guia do usuário do AWS IAM Identity Center para obter detalhes sobre os diferentes tipos de instância.

Criar um provedor confiável do IAM Identity Center

Depois que o IAM Identity Center for ativado em sua AWS conta, você poderá usar o procedimento a seguir para configurar o IAM Identity Center como seu provedor confiável para Acesso Verificado.

Para criar um provedor confiável de identidade do IAM (AWS console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Provedores de confiança de Acesso Verificado e, em seguida, Criar provedor de confiança de Acesso Verificado.
3. (Opcional) Em Tag de nome e Descrição, insira um nome e uma descrição para o provedor confiável.
4. Em Nome de referência da política, insira um identificador para usar posteriormente ao trabalhar com regras de política.
5. Em Tipo de provedor confiável, selecione Provedor de confiança do usuário.
6. Em Tipo de provedor de confiança do usuário, selecione IAM Identity Center.
7. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
8. Escolha Criar provedor confiável de Acesso Verificado.

Para criar um provedor de confiança (AWS CLI) do IAM Identity Center

- criar provedor de confiança de Acesso Verificado (AWS CLI)

Excluir um provedor de confiança do IAM Identity Center

Antes de excluir um provedor confiável, você deve remover todas as configurações de endpoints e grupos da instância à qual o provedor de confiança está conectado.

Para excluir um centro de identidade do IAM (AWS console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Provedores de confiança de Acesso Verificado e, em seguida, selecione o provedor de confiança que você deseja excluir em Provedores de confiança de Acesso Verificado.
3. Escolha Ações e, em seguida, Excluir provedor confiável de Acesso Verificado.
4. Confirme a exclusão inserindo `delete` na caixa de texto.
5. Escolha Delete (Excluir).

Para excluir um provedor de confiança (AWS CLI) do IAM Identity Center

- excluir provedor de confiança de Acesso Verificado (AWS CLI)

Usando um provedor de confiança do OpenID Connect

AWS O Acesso Verificado oferece suporte a provedores de identidade que usam métodos padrão do OpenID Connect (OIDC). Você pode usar provedores compatíveis com OIDC como provedores de confiança de identidade de usuário com Acesso Verificado. No entanto, devido à grande variedade de possíveis fornecedores do OIDC, não AWS é possível testar cada integração do OIDC com o Acesso Verificado.

O Acesso Verificado obtém os dados de confiança que avalia do provedor do OIDC `UserInfo Endpoint`. O `Scope` parâmetro é usado para determinar quais conjuntos de dados confiáveis serão recuperados. Depois que os dados de confiança são recebidos, a política de Acesso Verificado é avaliada em relação a eles.

> **Note**
>
> O Acesso Verificado não usa dados confiáveis `ID token` enviados pelo provedor do OIDC ao avaliar a política do Acesso Verificado. Somente os dados confiáveis do `UserInfo Endpoint` são avaliados de acordo com a política.

Conteúdos

Pré-requisitos para criar um provedor de confiança do OIDC

Você precisará coletar as seguintes informações diretamente do serviço do seu provedor de confiança:

- Emissor
- Endpoint de Autorização
- Endpoint de token
- Endpoint UserInfo
- ID do cliente
- Segredo do cliente
- Escopo

Crie um provedor de confiança do OIDC

Use o procedimento a seguir para criar um OIDC como provedor de confiança.

Para criar um provedor de identidade OIDC do (AWS console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Provedores de confiança de Acesso Verificado e, em seguida, Criar provedor de confiança de Acesso Verificado.
3. (Opcional) Em Tag de nome e Descrição, insira um nome e uma descrição para o provedor confiável.
4. Em Nome de referência da política, insira um identificador para usar posteriormente ao trabalhar com regras de política.
5. Em Tipo de provedor confiável, selecione Provedor de confiança do usuário.
6. Em Tipo de provedor de confiança do usuário, selecione OIDC (OpenID Connect).

7. Em Emissor, insira o identificador do emissor do OIDC.
8. Em Endpoint de autorização, insira o URL completo do endpoint de autorização.
9. Em Endpoint do token, insira o URL completo do endpoint do token.
10. Em Endpoint do usuário, insira o URL completo do endpoint do usuário.
11. Insira o identificador de cliente OAuth 2.0 para ID do cliente.
12. Insira o segredo do cliente OAuth 2.0 em Segredo do cliente.
13. Insira uma lista delimitada por espaços dos escopos definidos com seu provedor de identidade. No mínimo, o escopo “openid” é necessário para o Scope.
14. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
15. Escolha Criar provedor confiável de Acesso Verificado.

> **Note**
>
> Você precisará adicionar um URI de redirecionamento à lista de permissões do seu provedor OIDC. Você desejará usar o endpoint `ApplicationDomain` de Acesso Verificado para essa finalidade. Isso pode ser encontrado na AWS Management Console guia Detalhes do seu endpoint de Acesso Verificado ou usando o AWS CLI para descrever o endpoint. Adicione o seguinte à lista de permissões do seu provedor OIDC: https:///oauth2/idpresponse `ApplicationDomain`

Para criar um provedor de identidade confiável OIDC (AWS CLI)

- criar provedor de confiança de Acesso Verificado (AWS CLI)

Modificar um provedor de confiança do OIDC

Depois de criar um provedor confiável, você poderá atualizar a configuração.

Para modificar um provedor de confiança do OIDC (console) AWS

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Provedores de confiança de Acesso Verificado e, em seguida, selecione o provedor de confiança que você deseja modificar em Provedores de confiança de Acesso Verificado.

3. Escolha Ações e, em seguida, Modificar provedor confiável de Acesso Verificado.
4. Altere as configurações que deseja modificar.
5. Escolha Modificar provedor confiável de Acesso Verificado.

Para modificar um provedor de confiança (AWS CLI) do OIDC

- modifique o provedor de confiança de Acesso Verificado (AWS CLI)

Para excluir um provedor OIDC

Antes de excluir um provedor confiável de usuários, primeiro você precisa remover todas as configurações de endpoints e grupos da instância à qual o provedor de confiança está vinculado.

Para excluir um provedor de identidade confiável OIDC do AWS (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Provedores de confiança de Acesso Verificado e, em seguida, selecione o provedor de confiança que você deseja excluir em Provedores de confiança de Acesso Verificado.
3. Escolha Ações e, em seguida, Excluir provedor confiável de Acesso Verificado.
4. Confirme a exclusão inserindo `delete` na caixa de texto.
5. Escolha Delete (Excluir).

Para excluir um provedor de identidade confiável OIDC (AWS CLI)

- excluir provedor de confiança de Acesso Verificado (AWS CLI)

Provedores de confiança baseados em dispositivos

Você pode usar provedores confiáveis de gerenciamento de dispositivos com o Acesso Verificado pela AWS. Você pode usar um ou vários provedores confiáveis de dispositivos com a instância do Acesso Verificado.

Conteúdos

- Crie um provedor de confiança baseado em dispositivos
- Modificar um provedor de confiança baseado em dispositivo
- Excluir um provedor de confiança baseado em dispositivo

Fornecedores confiáveis de dispositivos compatíveis

Os seguintes provedores confiáveis de dispositivos podem ser integrados ao Acesso Verificado:

- CrowdStrike — Protegendo aplicativos privados com CrowdStrike e Acesso Verificado
- Jamf — Integrando o Acesso Verificado com o Jamf Device Identity
- JumpCloud — Integrar o JumpCloud e o Acesso Verificado pelo AWS

Crie um provedor de confiança baseado em dispositivos

Siga estas etapas para criar e configurar um provedor confiável de dispositivos para usar com o Acesso Verificado.

Para criar um provedor confiável de dispositivos de Acesso Verificado (AWS console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Provedores de confiança de Acesso Verificado e, em seguida, Criar provedor de confiança de Acesso Verificado.
3. (Opcional) Em Tag de nome e Descrição, insira um nome e uma descrição para o provedor confiável.
4. Insira um identificador para usar posteriormente ao trabalhar com regras de política para o nome de referência da política.
5. Em Tipo de provedor confiável, selecione Identidade do dispositivo.
6. Para o Tipo de identidade do dispositivo, escolha Jamf, CrowdStrike ou JumpCloud.
7. Em ID do inquilino, insira o identificador do aplicativo do inquilino.
8. (Opcional) Em URL da chave de assinatura pública, insira a URL exclusiva da chave compartilhada pelo provedor confiável do seu dispositivo. (Esse parâmetro não é necessário para Jamf, CrowdStrike ou Jumpcloud).
9. Escolha Criar provedor confiável de Acesso Verificado.

> **Note**
>
> Você precisará adicionar um URI de redirecionamento à lista de permissões do seu provedor OIDC. Você desejará usar o endpoint `DeviceValidationDomain` de Acesso Verificado para essa finalidade. Isso pode ser encontrado na AWS Management Console guia Detalhes do seu endpoint de Acesso Verificado ou usando o AWS CLI para descrever o endpoint. Adicione o seguinte à lista de permissões do seu provedor OIDC: https:///oauth2/idpresponse `DeviceValidationDomain`

Para criar um provedor confiável de dispositivos de Acesso Verificado (AWS CLI)

- criar provedor de confiança de Acesso Verificado (AWS CLI)

Modificar um provedor de confiança baseado em dispositivo

Depois de criar um provedor confiável, você poderá atualizar a configuração.

Para modificar um provedor confiável de dispositivos de Acesso Verificado (AWS console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Fornecedores confiáveis de Acesso Verificado.
3. Selecione o provedor de confiança.
4. Escolha Ações e, em seguida, selecione Modificar provedor confiável de Acesso Verificado.
5. Modifique a descrição conforme necessário.
6. (Opcional) Em URL da chave de assinatura pública, modifique a URL exclusiva da chave compartilhada pelo provedor confiável do seu dispositivo. (Esse parâmetro não será necessário se o seu provedor confiável do dispositivo for o Jamf, o CrowdStrike ou o Jumpcloud).
7. Escolha Modificar provedor confiável de Acesso Verificado.

Para modificar um provedor confiável de dispositivos de Acesso Verificado (AWS CLI)

- modifique o provedor de confiança de Acesso Verificado (AWS CLI)

Excluir um provedor de confiança baseado em dispositivo

Quando terminar de usar um provedor confiável, você poderá excluí-lo.

Para excluir um provedor confiável de dispositivos de Acesso Verificado (AWS console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Fornecedores confiáveis de Acesso Verificado.
3. Selecione o provedor de confiança que você deseja excluir em Provedores de confiança de Acesso Verificado.
4. Escolha Ações e, em seguida, selecione Excluir provedor confiável de Acesso Verificado.
5. Quando a confirmação for solicitada, insira **`delete`** e escolha Excluir.

Para excluir um provedor confiável de dispositivos de Acesso Verificado (AWS CLI)

- excluir provedor de confiança de Acesso Verificado (AWS CLI)

Grupos de Acesso Verificado

Um grupo de acesso verificado pela é uma coleção de endpoints de acesso verificado e uma política de acesso verificado em nível de grupo. Cada endpoint dentro de um grupo compartilha a política de acesso verificado. Você pode usar grupos para reunir endpoints que tenham requisitos de segurança comuns. Isso pode ajudar a simplificar a administração de políticas usando uma política para as necessidades de segurança de vários aplicativos.

Por exemplo, você pode agrupar todos os aplicativos de vendas e definir uma política de acesso para todo o grupo. Em seguida, você pode usar essa política para definir um conjunto comum de requisitos mínimos de segurança para todos os aplicativos de vendas. Essa abordagem ajuda a simplificar a administração de políticas.

Quando você cria um grupo, é necessário associar o grupo a uma instância do Acesso Verificado. Durante o processo de criação de um endpoint, você associará o endpoint a um grupo.

Tarefas

- Criar um grupo do Acesso Verificado
- Modificar uma política de grupo do Acesso Verificado
- Excluir um grupo do Acesso Verificado

Criar um grupo do Acesso Verificado

Siga o procedimento abaixo para criar um novo grupo de Acesso Verificado.

Para criar um grupo do Acesso Verificado

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Grupos de Acesso Verificado e, em seguida, Criar grupo de Acesso Verificado.
3. (Opcional) Em Tag de nome e Descrição, insira um nome e uma descrição para o grupo.
4. Para Instância de Acesso Verificado, selecione uma instância de Acesso Verificado para associar ao grupo.
5. (Opcional) Para definição de política, insira uma política de acesso do Acesso Verificado a ser aplicada ao grupo.

6. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
7. Escolha Criar grupo de Acesso Verificado.

Modificar uma política de grupo do Acesso Verificado

Use o procedimento a seguir para modificar uma política de grupo do Acesso Verificado.

Para modificar uma política de grupo do Acesso Verificado

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha grupos do Acesso Verificado e, em seguida, selecione o grupo cuja política você deseja modificar.
3. Escolha Ações e, em seguida, Modificar política de grupo de Acesso Verificado.
4. (Opcional) Ative ou desative a opção Ativar política, dependendo da sua meta atual.
5. (Opcional) Em Política, insira uma política de acesso verificado a ser aplicada ao grupo.
6. Escolha Modificar política de grupo de Acesso Verificado.

Excluir um grupo do Acesso Verificado

Quando não precisar mais de um grupo de Acesso Verificado, você poderá excluir.

Para excluir um grupo do Acesso Verificado

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha grupos de Acesso Verificado.
3. Selecione o grupo do.
4. Escolha Ações, Excluir grupo de Acesso Verificado.
5. Quando a confirmação for solicitada, insira **`delete`** e escolha Excluir.

Endpoints de acesso verificado

Um endpoint de acesso verificado representa um aplicativo. Cada endpoint está associado a um grupo de acesso verificado e herda a política de acesso do grupo. Opcionalmente, você pode anexar uma política de endpoint específica do aplicativo a cada endpoint.

Índice

Tipos de endpoint de acesso verificados

Os possíveis tipos de endpoints são os seguintes:

- Balanceador de carga: as solicitações do aplicativo são enviadas a um balanceador de carga para distribuí-las ao seu aplicativo.
- Interface de rede: as solicitações do aplicativo são enviadas para uma interface de rede usando o protocolo e a porta especificados.

VPCs e sub-redes compartilhadas

A seguir estão os comportamentos em relação às sub-redes VPC compartilhadas:

- Os endpoints de acesso verificado são compatíveis com o compartilhamento de sub-rede VPC. Um participante pode criar um endpoint de acesso verificado em uma sub-rede compartilhada.
- O participante que criou o endpoint será o proprietário do endpoint e a única pessoa autorizada a modificá-lo. O proprietário da VPC não poderá modificar o endpoint.

- Os endpoints de acesso verificado não podem ser criados em uma Zona AWS Local e, portanto, o compartilhamento por meio de Zonas Locais não é possível.

Para obter mais informações, consulte Compartilhar sua VPC com outras contas no Guia do usuário da Amazon VPC.

Crie um endpoint de balanceador de carga para acesso verificado

Use o seguinte procedimento para criar um endpoint do balanceador de carga. Para mais informações sobre balanceador de carga consulte o Manual do usuário do balanceador de carga elástico.

Requisitos

- Somente o tráfego IPv4 é compatível.
- Somente os protocolos HTTP e HTTPS são compatíveis.
- O balanceador de carga precisa ser um Application Load Balancer ou um Network Load Balancer, e precisa ser um balanceador de carga interno.
- O balanceador de carga e as sub-redes precisam pertencer à mesma nuvem privada virtual (VPC).
- Os balanceadores de carga HTTPS podem usar certificados TLS autoassinados ou públicos.
- Você deve fornecer um nome de domínio para seu aplicativo. Este é o nome DNS público que os usuários usarão para acessar o aplicativo. Você também precisará fornecer um certificado SSL público com um CN que corresponda a esse nome de domínio. Crie ou importe o certificado usando o AWS Certificate Manager.

Para criar um endpoint do balanceador de carga

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints de acesso verificado.
3. Escolha Criar endpoint de acesso verificado.
4. (Opcional) Em Tag de nome e Descrição, insira um nome e uma descrição para o endpoint.
5. Para o grupo de acesso verificado, escolha um grupo de acesso verificado para o endpoint.
6. Para obter detalhes do aplicativo faça o seguinte:

    a. Em Domínio do aplicativo, insira um nome DNS para seu aplicativo.

b. Em Certificado de domínio ARN, escolha o certificado TLS público.

7. Em Detalhes do endpoint, faça o seguinte:

   a. Em Tipo de anexo, escolha VPC.

   b. Em Grupos de segurança selecione o grupos de segurança para o endpoint. O tráfego do endpoint de acesso verificado que entra no seu balanceador de carga será associado a esse grupo de segurança.

   c. Em Prefixo de domínio do Endpoint, insira um identificador personalizado para acrescentar ao nome DNS que o acesso verificado gera para o endpoint.

   d. Em Tipo de endpoint escolha balanceador de carga.

   e. Em Protocolo, escolha HTTP ou HTTPS.

   f. Em Porta, digite o número da porta.

   g. Em balanceador de carga ARN, selecione seu balanceador de carga.

   h. Em Sub-redes, escolha as sub-redes do seu balanceador de carga.

8. (Opcional) Para definição de política, insira uma política de acesso verificado para o endpoint.
9. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
10. Escolha Criar endpoint de acesso verificado.

Criar um endpoint da interface de rede para acesso verificado

Use o seguinte procedimento para criar um endpoint de interface de rede.

Requisitos

- Somente o tráfego IPv4 é compatível.
- Somente os protocolos HTTP e HTTPS são compatíveis.
- A interface de rede precisa pertencer à mesma nuvem privada virtual (VPC) que os grupos de segurança.
- Usamos o IP privado na interface de rede para encaminhar o tráfego.
- Você deve fornecer um nome de domínio para seu aplicativo. Este é o nome DNS público que os usuários usarão para acessar o aplicativo. Você também precisará fornecer um certificado SSL público com um CN que corresponda a esse nome de domínio. Crie ou importe o certificado usando o AWS Certificate Manager.

Para criar um endpoint de interface de rede

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints de acesso verificado.
3. Escolha Criar endpoint de acesso verificado.
4. (Opcional) Em Tag de nome e Descrição, insira um nome e uma descrição para o endpoint.
5. Para o grupo de acesso verificado, escolha um grupo de acesso verificado para o endpoint.
6. Para obter detalhes do aplicativo faça o seguinte:
   a. Em Domínio do aplicativo, insira o nome DNS do seu aplicativo.
   b. Em Certificado de domínio ARN, escolha o certificado TLS público.
7. Em Detalhes do endpoint, faça o seguinte:
   a. Em Tipo de anexo, escolha VPC.
   b. Em Grupos de segurança selecione o grupos de segurança para o endpoint. O tráfego do endpoint de acesso verificado que entra na interface de rede será associado a esse grupo de segurança.
   c. Em Prefixo de domínio do Endpoint, insira um identificador personalizado para acrescentar ao nome DNS que o acesso verificado gera para o endpoint.
   d. Em Tipo de endpoint, selecione Interface de rede.
   e. Em Protocolo, escolha HTTP ou HTTPS.
   f. Em Porta, digite o número da porta.
   g. Em Interface de rede, escolha a interface de rede.
8. (Opcional) Para definição de política, insira uma política de acesso verificado para o endpoint.
9. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
10. Escolha Criar endpoint de acesso verificado.

Permita o tráfego originado do seu endpoint de acesso verificado

Você pode configurar os grupos de segurança de seus aplicativos para que eles permitam o tráfego originado do seu endpoint de acesso verificado. Você faz isso adicionando uma regra de entrada que especifica o grupo de segurança do endpoint como a origem. Recomendamos que você remova todas as regras de entrada adicionais, para que seu aplicativo receba tráfego somente do seu endpoint de acesso verificado.

Recomendamos que você mantenha as regras de saída existentes.

Para atualizar as regras do grupo de segurança do seu aplicativo

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints de acesso verificado.
3. Escolha o endpoint de acesso verificado, encontre IDs do grupo de segurança na guia Detalhes e copie o ID do grupo de segurança do seu endpoint.
4. No painel de navegação, selecione Grupos de segurança.
5. Marque a caixa de seleção do grupo de segurança associado ao seu alvo e escolha Ações, Editar regras de entrada.
6. Para adicionar uma regra de grupo de segurança que permita o tráfego originado do seu endpoint de acesso verificado, faça o seguinte:
   a. Escolha Adicionar regra.
   b. Em Tipo, escolha Todo o tráfego, ou um tipo específico de tráfego que você deseja permitir.
   c. Para Origem, escolha Personalizada e digite o ID do grupo de segurança de seu endpoint.
7. (Opcional) Para exigir que o tráfego seja originado somente do seu endpoint de acesso verificado, exclua todas as outras regras do grupo de segurança de entrada.
8. Escolha Salvar regras.

Modificar um endpoint do acesso verificado

Depois de criar um endpoint do acesso verificado, você poderá atualizar a configuração.

Para modificar um endpoint do acesso verificado

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints de acesso verificado.
3. Selecione o endpoint.
4. Escolha Ações, Modificar ponto final de acesso verificado.
5. Modifique os detalhes do endpoint conforme necessário.
6. Escolha Modificar ponto final de acesso verificado.

Modificar uma política de endpoint do acesso verificado

Após criar um endpoint do acesso verificado, é possível modificar a política.

Para modificar uma política de endpoint do acesso verificado

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints de acesso verificado.
3. Selecione o endpoint cuja política você queira modificar.
4. Escolha Ações, Modificar política de endpoint de acesso verificado.
5. (Opcional) Ative ou desative a opção Ativar política, dependendo da sua meta atual.
6. (Opcional) Em Política, insira uma política de acesso verificado a ser aplicada ao endpoint.
7. Escolha Modificar política de endpoint de acesso verificado.

Excluir um endpoint do acesso verificado

Quando não precisar mais de um endpoint do acesso verificado, você poderá excluí-lo.

Para excluir um endpoint do acesso verificado

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints de acesso verificado.
3. Selecione o endpoint.
4. Escolha Ações, Excluir endpoint de acesso verificado.
5. Quando a confirmação for solicitada, insira **`delete`** e escolha Excluir.

Confie nos dados de provedores confiáveis

Dados confiáveis são dados enviados ao AWS Acesso Verificado por um provedor confiável. Às vezes, também é chamado de “reivindicações do usuário” ou “contexto de confiança”. Os dados geralmente incluem informações sobre um usuário ou um dispositivo. Exemplos de dados de confiança incluem e-mail do usuário, associação a grupos, versão do sistema operacional do dispositivo, estado de segurança do dispositivo e muito mais. As informações enviadas variam de acordo com o provedor confiável, portanto, consulte a documentação do provedor confiável para obter uma lista completa e atualizada dos dados confiáveis.

No entanto, usando os recursos de registro de Acesso Verificado, você também pode ver quais dados de confiança estão sendo enviados pelo seu provedor de confiança. Isso pode ser muito útil ao definir políticas que permitam ou neguem acesso aos aplicativos. Para obter informações sobre como incluir contexto de confiança em seus registros, consulte Incluindo contexto de confiança.

Esta seção contém exemplos de dados de confiança e exemplos para começar a escrever políticas. As informações fornecidas aqui são apenas para fins ilustrativos e não como referência oficial.

Conteúdos

Contexto padrão do Acesso Verificado

AWS O Acesso Verificado inclui alguns elementos sobre a solicitação HTTP atual por padrão em todas as avaliações do Cedar, independentemente dos provedores de confiança configurados. Quando uma política é avaliada, o Acesso Verificado inclui dados sobre a solicitação HTTP atual no contexto do Cedar sob o `context.http_request key`. Você pode escrever uma política que avalie os dados, se quiser. O esquema JSON a seguir mostra quais dados estão incluídos na avaliação.

```
{
     "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"
        }
    }
}
```

Veja a seguir um exemplo de política que avalia os dados da solicitação de HTTP.

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

Centro de Identidade do AWS IAM

Quando uma política é avaliada, se você definir AWS IAM Identity Center como um provedor de confiança, o AWS Acesso Verificado inclui os dados de confiança no contexto do Cedar sob a chave que você especifica como “Nome de referência da política” na configuração do provedor de confiança. Você pode escrever uma política que avalie os dados de confiança, se quiser.

> **Note**
>
> A chave de contexto do seu provedor de confiança vem do nome de referência da política que você configura ao criar o provedor de confiança. Por exemplo, se você configurar o nome de referência da política como “idp123", a chave de contexto será “context.idp123". Confira se está usando a chave de contexto correta ao criar a política.

O esquema JSON a seguir mostra quais dados estão incluídos na avaliação.

```
{
   "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"
             }
           }
         }
       }
     }
   }
 }
```

Veja a seguir um exemplo de política que avalia os dados de confiança fornecidos pelo 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**
>
> Como os nomes dos grupos podem ser alterados, o IAM Identity Center se refere aos grupos usando seu ID de grupo. Isso ajuda a evitar a violação de uma declaração de política ao alterar o nome de um grupo.

Provedores de confiança de terceiros

Esta seção descreve os dados de confiança fornecidos ao AWS Acesso Verificado por provedores de confiança terceirizados.

> **Note**
>
> A chave de contexto do seu provedor de confiança vem do nome de referência da política que você configura ao criar o provedor de confiança. Por exemplo, se você configurar o nome de referência da política como “idp123", a chave de contexto será “context.idp123". Confira se está usando a chave de contexto correta ao criar a política.

Conteúdos

Extensão do navegador

Se você planeja incorporar o contexto de confiança do dispositivo em suas políticas de acesso, será necessária a extensão de navegador do Acesso Verificado pela AWS ou a extensão de navegador de outro parceiro. Atualmente, o Acesso Verificado é compatível com os navegadores Google Chrome e Mozilla Firefox.

Atualmente, oferecemos suporte a dois provedores confiáveis de dispositivos: Jamf (compatível com dispositivos macOS), CrowdStrike (compatível com dispositivos Windows 10 e Windows 11) e JumpCloud (compatível com Windows e MacOS).

- Se você estiver usando dados de confiança do Jamf em suas políticas, seus usuários devem baixar e instalar a extensão de navegador do AWS Acesso Verificado da loja virtual do Chrome ou do site de complementos do Firefox em seus dispositivos.
- Se você estiver usando dados de confiança do CrowdStrike em suas políticas, primeiro seus usuários precisam instalar o Host de Native Messaging do Acesso Verificado pela AWS (link direto para download). Esse componente é necessário para obter os dados de confiança do agente CrowdStrike em execução nos dispositivos dos usuários. Depois de instalar esse componente, os usuários devem instalar a extensão de navegador AWS Acesso Verificado da loja virtual do Chrome ou do site de complementos do Firefox em seus dispositivos.

- Se você estiver usando o JumpCloud, seus usuários deverão ter a extensão do navegador JumpCloud da loja virtual do Chrome ou do site de complementos do Firefox instalada em seus dispositivos.

Jamf

Jamf é um provedor de confiança de terceiros. Quando uma política é avaliada, se você definir o Jamf como um provedor confiável, o Acesso Verificado incluirá os dados de confiança no contexto do Cedar sob a chave especificada como “Nome de referência da política” na configuração do provedor de confiança. Você pode escrever uma política que avalie os dados de confiança, se quiser. O esquema JSON a seguir mostra quais dados estão incluídos na avaliação.

Para obter mais informações sobre como usar o Jamf com o Acesso Verificado pela AWS, consulte Integração do Acesso Verificado pela AWS com o Jamf Device Identity no site do 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)"
        }
    }
}
```

Veja a seguir um exemplo de política que avalia os dados de confiança fornecidos pelo Jamf.

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

O Cedar fornece uma `.contains()` função útil para ajudar com enumerações, como a pontuação de risco de Jamf.

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

CrowdStrike

O CrowdStrike é um provedor de confiança de terceiros. Quando uma política é avaliada, se você definir o CrowdStrike como um provedor de confiança, o Acesso Verificado inclui os dados de confiança no contexto do Cedar sob a chave que você especifica como “Nome de referência da

política” na configuração do provedor de confiança. Você pode escrever uma política que avalie os dados de confiança, se quiser. O esquema JSON a seguir mostra quais dados estão incluídos na avaliação.

Para obter mais informações sobre o uso do CrowdStrike com Acesso Verificado consulte Protegendo aplicativos privados AWS com o AWS CrowdStrike e o Acesso Verificado no site do GitHub.

```
{
  "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"
    }
  }
}
```

Veja a seguir um exemplo de política que avalia os dados de confiança fornecidos pelo CrowdStrike.

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

JumpCloud

Jamf é um provedor de confiança terceirizado. Quando uma política é avaliada, se você definir o JumpCloud como um provedor de confiança, o Acesso Verificado incluirá os dados de confiança

no contexto do Cedar sob a chave que você especificar como “Nome de referência da política” na configuração do provedor de confiança. Você pode escrever uma política que avalie os dados de confiança, se quiser. O esquema JSON a seguir mostra quais dados estão incluídos na avaliação.

Para obter mais informações sobre como usar o JumpCloud com o Acesso Verificado pela AWS, consulte Integração do JumpCloud com o Acesso Verificado pela AWS no site do JumpCloud.

```
{
  "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"
    }
  }
}
```

Veja a seguir um exemplo de política que avalia o contexto de confiança fornecido pelo JumpCloud.

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

Passagem de reivindicações do usuário e verificação de assinatura

Depois que uma instância de AWS Acesso Verificado autentica um usuário com sucesso, ela envia as declarações de usuário recebidas do IdP para o endpoint de Acesso Verificado. As declarações do usuário são assinadas para que os aplicativos possam verificar as assinaturas e se as solicitações foram enviadas pelo Acesso Verificado. Durante esse processo, o seguinte cabeçalho HTTP é adicionado:

`x-amzn-ava-user-context`

Esse cabeçalho contém as declarações do usuário no formato de token da Web de JSON (JWT). O formato JWT inclui um cabeçalho, carga e assinatura que são codificados em URL base64. O Acesso Verificado usa o ES384 (algoritmo de assinatura ECDSA usando o algoritmo de hash SHA-384) para gerar a assinatura JWT.

Os aplicativos podem usar essas declarações para personalização ou outras experiências específicas do usuário. Os desenvolvedores de aplicativos devem se informar sobre o nível de exclusividade e verificação de cada declaração fornecida pelo provedor de identidade antes do uso. A reivindicação `sub` é a melhor maneira de identificar determinado usuário.

Conteúdos

- Chaves públicas
- Exemplo: recuperar e decodificar o JWT

Exemplo: JWT assinado para declarações de usuários do OIDC

Os exemplos a seguir demonstram a aparência do cabeçalho e da carga útil das declarações de usuários do OIDC no formato JWT.

Exemplo de cabeçalho:

```
{
"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)
}
```

Exemplo de carga:

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

Exemplo: JWT assinado para declarações de usuários do IAM Identity Center

Os exemplos a seguir demonstram a aparência do cabeçalho e da carga útil das declarações de usuário do IAM Identity Center no formato JWT.

> **Note**
>
> Para o IAM Identity Center, somente as informações do usuário serão incluídas nas declarações.

Exemplo de cabeçalho:

```
{
"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)
}
```

Exemplo de carga:

```
{
"user": {
        "user_id": "f478d4c8-a001-7064-6ea6-12423523",
        "user_name": "test-123",
        "email": {
            "address": "test@amazon.com",
            "verified": false
        }
    }
}
```

Chaves públicas

Como as instâncias de acesso verificado não criptografam declarações de usuários, recomendamos que você configure endpoints de acesso verificado para usar HTTPS. Se você configurar seu endpoint de Acesso Verificado para usar HTTP, certifique-se de restringir o tráfego para o endpoint usando grupos de segurança.

É recomendável verificar a assinatura antes de fazer qualquer autorização com base nas solicitações. Para obter a chave pública, obtenha o ID de chave no cabeçalho JWT e use-o para

procurar a chave pública do seguinte endpoint regional. O endpoint para cada região da Região da AWS é o seguinte:

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

Exemplo: recuperar e decodificar o JWT

O exemplo de código a seguir mostra como obter o ID de chave, a chave pública e a carga útil em 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'])
```

Políticas de acesso verificado

AWSAs políticas de acesso verificado permitem que você defina regras para acessar seus aplicativos hospedados emAWS. Eles são escritos em Cedar, uma linguagem de políticas da AWS. Usando o Cedar, você pode criar políticas que são avaliadas em relação ao contexto de confiança enviado pelos provedores de confiança baseados em identidade ou dispositivos que você configura para usar com o Acesso Verificado.

Para obter informações mais detalhadas sobre a linguagem política do Cedar, consulte o Guia de referência do Cedar.

Esta seção descreve como as políticas de acesso verificado são estruturadas, o que elas contêm, como defini-las e fornece alguns exemplos.

Índice

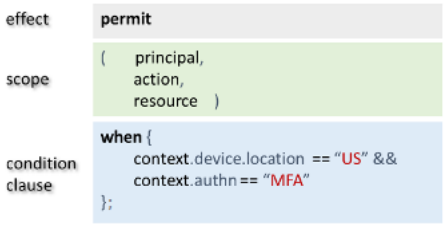
Trabalhe com políticas de acesso verificado

Ao criar um grupo de acesso verificado ou criar um endpoint de acesso verificado, você tem a opção de definir a política de acesso verificado. Você pode criar um grupo ou endpoint sem definir a política de acesso verificado, mas todas as solicitações de acesso serão bloqueadas até que você defina uma política.

Para adicionar ou alterar uma política em um grupo ou endpoint de acesso verificado existente após sua criação, consulte Modificar uma política de grupo do Acesso Verificado ouModificar uma política de endpoint do acesso verificado.

Estrutura da declaração de política

Esta seção descreve a declaração da política de Acesso Verificado pela AWS e como ela é avaliada. Você pode ter várias declarações em uma única política de acesso verificado. O diagrama a seguir mostra uma estrutura de uma política de acesso verificado.



A política contém os elementos a seguir:

- Efeito — Especifica se a declaração de política é `permit` (`Allow`) ou `forbid` (`Deny`).
- Escopo — especifica os princípios, as ações e os recursos aos quais o efeito se aplica. Você pode deixar o escopo no Cedar indefinido ao não identificar princípios, ações ou recursos específicos (conforme mostrado no exemplo anterior). Nesse caso, a política se aplica a todos os principais, ações e recursos possíveis.
- Cláusula de condição — especifica o contexto no qual o efeito se aplica.

> **Important**
>
> Para o Acesso Verificado, as políticas são totalmente expressas referindo-se ao contexto de confiança na cláusula condicional. O escopo da política deve sempre ser mantido indefinido. Em seguida, você pode especificar o acesso usando o contexto de confiança da identidade e do dispositivo na cláusula condicional.

Exemplo simples de política

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

No exemplo anterior, observe que você pode usar mais de uma cláusula de condição em uma declaração de política usando o && operador. A linguagem de políticas do Cedar oferece um poder expressivo para criar declarações de políticas personalizadas, refinadas e abrangentes. Para obter exemplos adicionais, consulte Exemplo de políticas.

Avaliação de políticas

Um documento de política é um conjunto de uma ou mais declarações de política (declarações `permit` ou `forbid`). A política se aplicará se a cláusula condicional (a declaração `when`) for verdadeira. Para que um documento de política permita o acesso, pelo menos uma política de permissão no documento deve ser aplicada e nenhuma política de proibição pode ser aplicada. Se nenhuma política de permissão se aplicar e/ou uma ou mais políticas de proibição se aplicarem, o documento de política negará o acesso. Se você definiu documentos de política para o grupo de acesso verificado e o endpoint de acesso verificado, ambos os documentos devem permitir o acesso. Se você não definiu um documento de política para o endpoint de acesso verificado, somente a política de grupo de acesso verificado precisará permitir o acesso.

> **Note**
>
> O Acesso Verificado pela AWS valida a sintaxe quando você cria a política, mas não valida os dados inseridos na cláusula condicional.

Operadores integrados

Ao criar o contexto de uma política de Acesso Verificado pela AWS usando várias condições, conforme discutido em Estrutura da declaração de política, você pode usar o && operador para adicionar outras condições. Há também muitos outros operadores integrados que você pode usar para adicionar mais poder expressivo às condições da sua política. A tabela a seguir contém todos os operadores integrados para referência.

Operador	Tipos e sobrecargas	Descrição
!	Booleano → Booleano	Lógico que não.
==	qualquer → qualquer	Igualdade. Funciona com argumentos de qualquer tipo,

Operador	Tipos e sobrecargas	Descrição
		mesmo que os tipos não correspondam. Valores de tipos diferentes nunca são iguais entre si.
!=	qualquer → qualquer	Desigualdade; o inverso exato da igualdade (veja acima).
<	(longo, longo) → Booleano	Número inteiro longo menor que.
<=	(longo, longo) → Booleano	Número inteiro longo menor ou igual a.
>	(longo, longo) → Booleano	Número inteiro longo maior que.
>=	(longo, longo) → Booleano	Número inteiro longo maior que ou igual a.
em	(entidade, entidade) → Booleano	Associação hierárquica (reflexiva: A em A é sempre verdadeiro).
	(entidade, conjunto (entidade)) → Booleano	Associação à hierarquia: A em [B, C,...] é verdadeiro se (A e B) || (A em C) ||... erro se o conjunto não contiver uma entidade.
&&	(Booleano, Booleano) → Booleano	Lógico e (curto-circuito).
||	(Booleano, Booleano) → Booleano	Lógico ou (curto-circuito).
.exists()	entidade→ Booleano	Existência de entidades.

Operador	Tipos e sobrecargas	Descrição
tem	(entidade, atributo) → Booleano	Operador infixo. `e has f` testa se o registro ou a entidade `e` tem uma associação para o atributo `f`. Retorna `false` se `e` não existe ou se `e` existe, mas não tem o atributo `f`. Os atributos podem ser expressos como identificadores ou literais de sequência de caracteres.
como	(string, string) → Booleano	Operador infixo. `t like p` verifica se o texto `t` corresponde ao padrão `p`, que pode incluir caracteres curinga `*` que correspondam a 0 ou mais de qualquer caractere. Para combinar literalmente um caractere estrela `t`, você pode usar a sequência especial de caracteres escapados `\*` em `p`.
.contém()	(conjunto, todos) → Booleano	Defina a associação (B é um elemento de A).
.contém tudo()	(conjunto, conjunto) → Booleano	Testa se o conjunto A contém todos os elementos do conjunto B.
.Contém qualquer()	(conjunto, conjunto) → Booleano	Testa se o conjunto A contém algum dos elementos do conjunto B.

Comentários da política

Você pode incluir declarações de comentários em suas políticas de Acesso Verificado pela AWS. Os comentários são definidos como uma linha que começa `//` e termina com uma nova linha.

O exemplo a seguir mostra a instrução correspondente na política.

```
// 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)
};
```

Curto-circuito da lógica política

Talvez você queira escrever uma política de Acesso Verificado pela AWS que avalie dados que podem ou não estar presentes em um determinado contexto. Se você referenciar dados em um contexto que não existe, o Cedar produzirá um erro e avaliará a política para negar o acesso, independentemente da sua intenção. Por exemplo, isso resultaria em uma negação, pois `fake_provider` e `bogus_key` não existem nesse contexto.

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

Para evitar essa situação, você pode verificar se uma chave está presente usando o `has` operador. Se o operador `has` retornar falso, a avaliação adicional da declaração encadeada será interrompida e o Cedar não produzirá um erro ao tentar referenciar um item que não existe.

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

Isso é mais útil ao especificar uma política que faz referência a dois provedores de confiança diferentes.

```
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)
    )
  )
};
```

Exemplo de políticas

Exemplo 1: criação de políticas para o IAM Identity Center

> **Note**
>
> Como os nomes dos grupos podem ser alterados, o IAM Identity Center se refere aos grupos usando seu ID de grupo. Isso ajuda a evitar a violação de uma declaração de política ao alterar o nome de um grupo.

O exemplo de política a seguir permite acesso somente quando um usuário pertence ao `finance` grupo (que tem ID de grupo de`c242c5b0-6081-1845-6fa8-6e0d9513c107`) e tem um endereço de e-mail verificado.

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

Exemplo 1b: adição de mais condições a uma declaração de política para o IAM Identity Center

O exemplo de política a seguir permite acesso somente quando um usuário pertence ao `finance` grupo (que tem um ID de grupo de `c242c5b0-6081-1845-6fa8-6e0d9513c107`), tem um endereço de e-mail verificado e a pontuação de risco do dispositivo Jamf é `LOW`.

```
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"
};
```

Exemplo 2: A mesma política para um provedor de OIDC terceirizado

O exemplo de política a seguir permite acesso somente quando o usuário é do grupo “financeiro”, tem um endereço de e-mail verificado e a pontuação de risco do dispositivo Jamf é BAIXA.

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

Exemplo 3: Usando o CrowdStrike

O exemplo de política a seguir permite acesso quando a pontuação geral da avaliação é maior que 50.

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

Exemplo 4: adicionar tags com caracteres especiais

O exemplo a seguir mostra como escrever uma política se uma propriedade de contexto estiver usando um `:` (ponto e vírgula), que é um caractere reservado na linguagem da política.

```
permit(principal, action, resource)
```

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

Exemplo 5: Permitir um endereço IP específico

O exemplo a seguir mostra uma política que permite somente um endereço IP específico.

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

Exemplo 5a: Bloquear um endereço IP específico

O exemplo a seguir mostra uma política que bloqueará um endereço IP específico.

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

Assistente de políticas do Acesso Verificado

O assistente de políticas do Acesso Verificado é uma ferramenta no console do Acesso Verificado que você pode usar para testar e desenvolver as políticas. Ele apresenta a política de endpoint, a política de grupo e o contexto de confiança em uma tela, na qual você pode testar e editar as políticas.

Os formatos do contexto de confiança variam entre os diferentes provedores de confiança e, às vezes, o administrador do Acesso Verificado pode não saber o formato exato que um determinado provedor de confiança usa. É por isso que pode ser muito útil ver o contexto de confiança e as políticas de grupo e de endpoint em um só lugar para fins de teste e desenvolvimento.

As seções a seguir descrevem os princípios do uso do editor de políticas.

Tarefas

- Etapa 1: especificar os recursos
- Etapa 2: testar e editar as políticas

- Etapa 3: revisar e aplicar as alterações

Etapa 1: especificar os recursos

Na primeira página do assistente de políticas, especifique o endpoint do Acesso Verificado que você deseja usar. Especifique também um usuário (identificado pelo endereço de e-mail) e, opcionalmente, o nome do usuário e/ou um identificador do dispositivo. Por padrão, a decisão de autorização mais recente é extraída dos logs do Acesso Verificado do usuário especificado. Opcionalmente, você pode escolher especificamente a decisão mais recente de permissão ou negação.

Por fim, o contexto de confiança, a decisão de autorização, a política de endpoint e a política de grupo serão todos exibidos na próxima tela.

Para abrir o assistente de políticas e especificar seus recursos

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Instâncias do Acesso Verificado e clique no ID da instância do Acesso Verificado para a instância com a qual você deseja trabalhar.
3. Escolha Iniciar assistente de políticas.
4. Em Endereço de e-mail do usuário, insira o endereço de e-mail do usuário.
5. Em Endpoint do Acesso Verificado, selecione o endpoint para o qual você deseja editar e testar as políticas.
6. (Opcional) Em Nome, forneça o nome do usuário.
7. (Opcional) Em Identificador do dispositivo, forneça o identificador exclusivo do dispositivo.
8. (Opcional) Em Resultado da autorização, escolha o tipo de resultado da autorização recente que você deseja usar. Por padrão, o resultado da autorização mais recente será usado.
9. Escolha Next (Próximo).

Etapa 2: testar e editar as políticas

Nesta página, você receberá as seguintes informações com as quais trabalhar:

- O contexto de confiança enviado pelo seu provedor de confiança para o usuário e (opcionalmente) para o dispositivo que você especificou na etapa anterior.
- A política do Cedar para o endpoint do Acesso Verificado especificada na etapa anterior.

- A política do Cedar para o grupo do Acesso Verificado ao qual o endpoint pertence.

As políticas do Cedar para o endpoint e o grupo do Acesso Verificado podem ser editadas nesta página, mas o contexto de confiança é estático. Agora você pode usar esta página para visualizar o contexto de confiança junto com as políticas do Cedar.

Teste as políticas em relação ao contexto de confiança escolhendo o botão Testar políticas e o resultado da autorização será exibido na tela. Você pode fazer edições nas políticas e testar novamente suas alterações, repetindo o processo conforme necessário.

Quando as alterações feitas nas políticas estiverem satisfatórias, escolha Avançar para continuar na próxima tela do assistente de políticas.

Etapa 3: revisar e aplicar as alterações

Na página final do assistente de políticas, as alterações feitas nas políticas serão destacadas para facilitar a revisão. Agora você pode revisar as políticas pela última vez e escolher Aplicar alterações para confirmá-las.

Você também tem a opção de voltar à página anterior escolhendo Anterior ou cancelar completamente o assistente de políticas escolhendo Cancelar.

Segurança no Acesso Verificado pela AWS

A segurança para com a nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se beneficiará de datacenters e arquiteturas de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isso como a segurança da nuvem e segurança na nuvem:

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa produtos da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao Acesso Verificado pela AWS, consulte Serviços da AWS no escopo por programa de conformidade.
- Segurança na nuvem: sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Acesso Verificado. Os tópicos a seguir mostram como configurar o Acesso Verificado para atender aos seus objetivos de segurança e conformidade. Saiba também como usar outros produtos da AWS que ajudam a monitorar e proteger os recursos do Acesso Verificado.

Índice

Proteção de dados no AWS Acesso Verificado

O AWSmodelo de responsabilidade compartilhada se aplica à proteção de dados no AWSAcesso Verificado. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle sobre

seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para mais informações sobre a proteção de dados na Europa, consulte o artigo AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja asConta da AWS credenciais da e configure as contas de usuário individuais com o AWS IAM Identity Center ou o AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA [multi-factor authentication]) com cada conta.
- Use SSL/TLS para se comunicar com os recursos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure o registro em log das atividades da API e do usuário com o .AWS CloudTrail
- Use AWS as soluções de criptografia da , juntamente com todos os controles de segurança padrão dos Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar a AWS por meio de uma interface de linha de comandos ou uma API, use um endpoint do FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de email dos seus clientes, em marcações ou campos de formato livre, como um campo Name (Nome). Isso também é válido para quando você trabalha com o Acesso Verificado ou outros produtos Serviços da AWS, usando o console, a API, a AWS CLI ou os SDKs AWS. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia em trânsito

O Acesso Verificado criptografa todos os dados em trânsito dos usuários finais para os endpoints de acesso verificado pela Internet usando Transport Layer Security (TLS) 1.2 ou posterior.

Privacidade do tráfego entre redes

Você pode configurar o Acesso Verificado para restringir o acesso a recursos específicos em sua VPC. Para autenticação baseada no usuário, você também pode restringir o acesso a partes da rede, com base no grupo de usuários que acessa os endpoints. Para ter mais informações, consulte Políticas de acesso verificado.

Criptografia de dados em repouso para AWS Acesso Verificado

Por padrão, o Acesso Verificado pela AWS criptografa dados em repouso, usando chaves KMS de propriedade da AWS. Quando a criptografia de dados em repouso ocorre por padrão, ela ajuda a reduzir a sobrecarga operacional e a complexidade envolvidas na proteção de dados confidenciais. Ao mesmo tempo, ele permite que você crie aplicativos seguros que atendam aos rigorosos requisitos regulatórios e de conformidade de criptografia. As seções a seguir fornecem os detalhes de como o Acesso Verificado usa chaves KMS para criptografia de dados em repouso.

Conteúdo

Acesso Verificado e chaves KMS

AWS chaves de propriedade

O Acesso Verificado usa chaves KMS para criptografar automaticamente as informações de identificação pessoal (PII). Isso acontece por padrão, e você não pode visualizar, gerenciar, usar

ou auditar o uso das chaves de propriedade da AWS. No entanto, você não precisa fazer nenhum trabalho nem alterar nenhum programa para proteger as chaves que criptografam seus dados. Para obter mais informações, consulte AWS Chaves de dados no AWS Key Management ServiceGuia do desenvolvedor.

Embora você não possa desabilitar essa camada de criptografia ou selecionar um tipo de criptografia alternativo, você pode adicionar uma segunda camada de criptografia sobre as chaves de criptografia de AWS propriedade existentes escolhendo uma chave gerenciada pelo cliente ao criar seus recursos de Acesso Verificado.

Chaves gerenciadas pelo cliente

O Acesso Verificado suporta o uso de chaves simétricas gerenciadas pelo cliente que você cria e gerencia para adicionar uma segunda camada de criptografia sobre a criptografia padrão existente. Como você tem controle total dessa camada de criptografia, você pode realizar tarefas como:

- Estabelecer e manter as políticas de chave
- Estabelecer e manter subsídios e políticas do IAM
- Habilitar e desabilitar políticas de chaves
- Alternar os materiais de criptografia de chaves
- Adicionar etiquetas
- Criar aliases de chaves
- Chaves de agendamento para exclusão

Para obter mais informações, consulte Chaves mestras do cliente (CMKs) no AWS Key Management Service Guia do desenvolvedor.

> **Note**
>
> O Acesso Verificado ativa automaticamente a criptografia em repouso usando chaves AWS próprias para proteger dados de identificação pessoal sem nenhum custo.
> No entanto, AWS KMS as cobranças serão aplicadas quando você usar uma chave gerenciada pelo cliente. Para obter mais informações sobre a definição de preço, consulte Definição de preço do AWS Key Management Service.

Informações de identificação pessoal

A tabela a seguir resume as informações de identificação pessoal (PII) que o Acesso Verificado usa e como elas são criptografadas.

Tipo de dados	Criptografia de chave própria da AWS	Criptografia de chave gerenciada pelo cliente (opcional)
`Trust provider (user-type)` Os provedores de confiança do tipo usuário contêm opções de OIDC AuthorizationEndpoint, como,, UserInfoEndpoint ClientId, e assim por diante ClientSecret, que são consideradas PII.	Habilitado	Habilitado
`Trust provider (device-type)` Os provedores de confiança do tipo de dispositivo contêm um TenantId, que é considerado PII.	Habilitado	Habilitado
`Group policy` Fornecido durante a criação ou modificação do grupo de Acesso Verificado. Contém regras para autorizar solicitações de acesso. Pode conter PII, como nome de usuário e endereço de e-mail, etc.	Habilitado	Habilitado
`Endpoint policy`	Habilitado	Habilitado

Tipo de dados	Criptografia de chave própria da AWS	Criptografia de chave gerenciada pelo cliente (opcional)
Fornecido durante a criação ou modificação do endpoint de Acesso Verificado. Contém regras para autorizar solicitaç ões de acesso. Pode conter PII, como nome de usuário e endereço de e-mail, etc.		

Como o AWS Acesso Verificado usa concessões em AWS KMS

O Acesso Verificado exige uma concessão para usar sua chave gerenciada pelo cliente.

Quando você cria recursos de Acesso Verificado criptografados com uma chave gerenciada pelo cliente, o Acesso Verificado cria uma concessão em seu nome enviando uma CreateGrantsolicitação paraAWS KMS. As concessões AWS KMS são usadas para dar Acesso Verificado a uma chave gerenciada pelo cliente em sua conta.

O Acesso Verificado exige a concessão para usar sua chave gerenciada pelo cliente para as seguintes operações internas:

- Enviar solicitações Decrypt para AWS KMS para descriptografar as chaves de dados criptografadas para que elas possam ser usadas para descriptografar seus dados.
- Envie RetireGrantsolicitações AWS KMS para excluir uma concessão.

É possível revogar o acesso à concessão, ou remover o acesso do serviço à chave gerenciada pelo cliente a qualquer momento. Se você fizer isso, o Acesso Verificado não poderá acessar nenhum dos dados criptografados pela chave gerenciada pelo cliente, o que afetará as operações que dependam desses dados.

Usando chaves gerenciadas pelo cliente com Acesso Verificado

Você pode criar uma chave gerenciada pelo cliente usando o AWS Management Console ou APIs AWS KMS. Siga as etapas para criar uma chave simétrica gerenciada pelo cliente no Guia do AWS Key Management Service desenvolvedor.

Políticas de chaves

As principais políticas controlam o acesso à chave gerenciada pelo cliente. Cada chave gerenciada pelo cliente deve ter exatamente uma política de chaves, que contém declarações que determinam quem pode usar a chave e como pode usá-la. Ao criar a chave gerenciada pelo cliente, você pode especificar uma política de chaves. Para obter mais informações, consulte Gerenciar do acesso às chaves no AWS Key Management ServiceGuia do desenvolvedor.

Para usar a chave gerenciada pelo cliente com seus recursos de Acesso Verificado, as seguintes operações de API do devem ser permitidas na política de chaves:

- `kms:CreateGrant`— Adiciona uma concessão a uma chave gerenciada pelo cliente. Concede acesso de controle a uma chave KMS especificada, que permite o acesso às operações de concessão exigidas pelo Acesso Verificado. Para obter mais informações, consulte Uso de concessões no Guia do desenvolvedor do AWS Key Management Service.

  Isso permite que o Acesso Verificado faça o seguinte:

  - Ligue `GenerateDataKeyWithoutPlainText` para gerar uma chave de dados criptografada e armazená-la, porque a chave de dados não é usada imediatamente para criptografar.
  - Ligar para `Decrypt` para usar a chave de dados criptografada armazenada para acessar os dados criptografados.
  - Configure um diretor aposentado para permitir que o serviço `RetireGrant`.
- `kms:DescribeKey` – Fornece os principais detalhes gerenciados pelo cliente para permitir que o serviço valide a chave.
- `kms:GenerateDataKey`— Permite que o Acesso Verificado use a chave para criptografar dados.
- `kms:Decrypt`— Permita que o Acesso Verificado descriptografe as chaves de dados criptografadas.

Veja a seguir um exemplo de política de chaves que você pode usar para Acesso Verificado.

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

Para obter mais informações sobre Especificar permissões em uma política consulte o AWS Key Management ServiceGuia do desenvolvedor.

Para obter informações sobre acesso chave a solução de problemas , consulte AWS Key Management Service Guia do desenvolvedor.

Especificação de uma chave gerenciada pelo cliente para recursos de Acesso Verificado

Você pode especificar uma chave gerenciada pelo cliente para fornecer uma segunda camada de criptografia para os seguintes recursos:

- Grupo de Acesso Verificado
- Endpoint de Acesso Verificado
- Provedor confiável de Acesso Verificado

Ao criar qualquer um desses recursos usando o AWS Management Console, você pode especificar uma chave gerenciada pelo cliente na seção Criptografia adicional -- opcional. Durante o processo, marque a caixa de seleção Personalizar configurações de criptografia (avançadas) e insira a ID da AWS KMS chave que você deseja usar. Isso também pode ser feito ao modificar um recurso existente ou usando o AWS CLI.

> **Note**
>
> Se a chave gerenciada pelo cliente usada para adicionar criptografia adicional a qualquer um dos recursos acima for perdida, os valores de configuração dos recursos não estarão mais acessíveis. No entanto, os recursos podem ser modificados usando o AWS Management Console ouAWS CLI, para aplicar uma nova chave gerenciada pelo cliente e redefinir os valores de configuração.

AWS Contexto de criptografia de Acesso Verificado

Um contexto de criptografia é um conjunto opcional de pares de chave-valor que pode conter mais informações contextuais sobre os dados. O AWS KMS usa o contexto de criptografia como dados adicionais autenticados (AAD) para oferecer suporte à criptografia autenticada. Quando você inclui um contexto de criptografia em uma solicitação para criptografar dados, o AWS KMS vincula de forma criptográfica o contexto de criptografia aos dados criptografados. Para descriptografar os dados, você deve passar o mesmo contexto de criptografia na solicitação.

AWSContexto de criptografia de Acesso Verificado

O Acesso Verificado usa o mesmo contexto de criptografia em todas as operações AWS KMS criptográficas, onde a chave está `aws:verified-access:arn` e o valor é o nome do recurso da Amazon (ARN). Abaixo estão os contextos de criptografia dos recursos de Acesso Verificado.

Provedor confiável de Acesso Verificado

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

Grupo de Acesso Verificado

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

Endpoint de Acesso Verificado

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

Para obter mais informações sobre o contexto de criptografia, consulte Contexto de criptografia no Guia do Desenvolvedor AWS Key Management Service.

Monitorando suas chaves de criptografia para o AWS Acesso Verificado

Ao usar uma chave KMS gerenciada pelo cliente com seus recursos de AWS Acesso Verificado, você pode usar AWS CloudTrail para rastrear solicitações enviadas para as quais o Acesso Verificado envia AWS KMS.

Os exemplos a seguir são AWS CloudTrail eventos para `CreateGrant`, `RetireGrant`, `Decrypt`, `DescribeKey`, e `GenerateDataKey`, que monitoram as operações do KMS chamadas pelo Acesso Verificado para acessar dados criptografados pela chave KMS gerenciada pelo cliente:

CreateGrant

Quando você usa uma chave gerenciada pelo cliente para criptografar seus recursos, o Acesso Verificado envia uma `CreateGrant` solicitação em seu nome para acessar a chave em sua AWS conta. A concessão que o Acesso Verificado cria é específica para o recurso associado à chave gerenciada pelo cliente.

O evento de exemplo a seguir registra a `CreateGrant` operação:


```
{
    "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

O Acesso Verificado usa a `RetireGrant` operação para remover uma concessão quando você exclui um recurso.

O evento de exemplo a seguir registra a `RetireGrant` operação:


```
{
```

```
    "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

O Acesso Verificado chama a `Decrypt` operação para usar a chave de dados criptografada armazenada para acessar os dados criptografados.

O evento de exemplo a seguir registra a `Decrypt` operação:

```
{
    "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

O Acesso Verificado usa a `DescribeKey` operação para verificar se a chave gerenciada pelo cliente associada ao seu recurso existe na conta e na região.

O evento de exemplo a seguir registra a `DescribeKey` operação:

```
{
    "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

O evento de exemplo a seguir registra a `GenerateDataKey` operação:

```
{
    "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"
}
```


Gerenciamento de identidade e acesso para Acesso Verificado pelaAWS

O AWS Identity and Access Management (IAM) é um serviço da AWS service (Serviço da AWS) que ajuda a controlar o acesso aos recursos da AWS de forma segura. Os administradores do IAM controlam quem pode ser autenticado (fazer login) e autorizado (ter permissões) para usar recursos do Acesso Verificado. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

Tópicos

- Solução de problemas de identidade e acesso do Acesso Verificado pela AWS
- Usar funções vinculadas ao serviço para o Acesso Verificado
- Políticas da AWS gerenciadas para Acesso Verificado pela AWS

Público

O uso do AWS Identity and Access Management (IAM) varia dependendo do trabalho realizado no Acesso Verificado.

Usuário do serviço: se você usa o serviço Acesso Verificado para fazer o trabalho, o administrador fornece as credenciais e as permissões necessárias. À medida que usar mais recursos do Acesso Verificado para fazer seu trabalho, você poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um recurso no Acesso Verificado, consulte Solução de problemas de identidade e acesso do Acesso Verificado pela AWS.

Administrador do serviço: se você for o responsável pelos recursos do Acesso Verificado na empresa, provavelmente terá acesso total ao Acesso Verificado. Cabe a você determinar quais funcionalidades e recursos do Acesso Verificado os usuários do serviço devem acessar. Assim, é necessário enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os conceitos básicos do IAM. Para saber mais sobre como a empresa pode usar o IAM com o Acesso Verificado, consulte Como o Acesso Verificado pela AWS funciona com o IAM.

Administrador do IAM: se você for um administrador do IAM, talvez queira saber detalhes sobre como é possível criar políticas para gerenciar o acesso ao Acesso Verificado. Para visualizar exemplos de políticas baseadas em identidade do Acesso Verificado que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade para o Acesso Verificado pela AWS.

Como autenticar com identidades

A autenticação é a forma como você faz login na AWS usando suas credenciais de identidade. É necessário ser autenticado (fazer login na AWS) como o usuário raiz da Usuário raiz da conta da AWS, como usuário do IAM ou assumindo um perfil do IAM.

Você pode fazer login na AWS como uma identidade federada usando credenciais fornecidas por uma fonte de identidades. Os usuários do AWS IAM Identity Center (IAM Identity Center), a autenticação única da empresa e as suas credenciais do Google ou do Facebook são exemplos de

identidades federadas. Quando você faz login como uma identidade federada, o administrador já configurou anteriormente a federação de identidades utilizando perfis do IAM. Quando você acessa a AWS usando a federação, está indiretamente assumindo um perfil.

É possível fazer login no ou no portal de acesso da AWS Management Console dependendo do tipo de usuário que você é.AWS Para obter mais informações sobre como fazer login na AWS, consulte How to sign in to your Conta da AWS (Como fazer login na conta da) no Início de Sessão da AWS User Guide (Guia do usuário do).

Se você acessar a AWS programaticamente, a AWS fornecerá um kit de desenvolvimento de software (SDK) e uma interface da linha de comando (CLI) para você assinar criptograficamente as solicitações usando as suas credenciais. Se você não utilizar as ferramentas da AWS, deverá assinar as solicitações por conta própria. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulteAssinar AWSsolicitações de API da noGuia do usuário do IAM.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça mais informações de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte Autenticação multifator no Guia do usuário do AWS IAM Identity Center e Usar a autenticação multifator (MFA) naAWS no Guia do usuário do IAM.

Usuário raiz da Conta da AWS

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos os atributos e Serviços da AWS na conta. Essa identidade, denominada usuário raiz da Conta da AWS, e é acessada por login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não utilizar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários, inclusive os que precisam de acesso de administrador, usem a federação com um provedor de identidades para acessar Serviços da AWS usando credenciais temporárias.

Identidade federada é um usuário de seu diretório de usuários corporativos, um provedor de identidades da web AWS Directory Service, o , o diretório do Centro de Identidade ou qualquer

usuário que acesse os Serviços da AWS usando credenciais fornecidas por meio de uma fonte de identidade. Quando as identidades federadas acessam Contas da AWS, elas assumem perfis que fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o .AWS IAM Identity Center Você pode criar usuários e grupos no Centro de Identidade do IAM ou se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todas as suas Contas da AWS e aplicações. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no Guia do usuário do AWS IAM Identity Center.

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas para uma única pessoa ou aplicação. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de utilização específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível utilizar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e atribuir a esse grupo permissões para administrar atributos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de uma função) no Guia do usuário do IAM.

Perfis do IAM

Um perfil do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. É possível assumir temporariamente um perfil do IAM no AWS Management Console alternando perfis. É possível assumir um perfil chamando uma operação de API da AWS CLI ou da AWS, ou usando um

URL personalizado. Para obter mais informações sobre métodos para o uso de perfis, consulte Uso de funções do IAM no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar uma função para um provedor de identidade de terceiros no Guia do usuário do IAM. Se você usar o IAM Identity Center, deverá configurar um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no Guia do usuário do AWS IAM Identity Center.
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, alguns Serviços da AWS permitem que você anexe uma política diretamente a um atributo (em vez de usar um perfil como proxy). Para saber a diferença entre perfis e políticas baseadas em atributo para acesso entre contas, consulte Como os perfis do IAM diferem das políticas baseadas em atributo no Guia do usuário do IAM.
- Acesso entre serviços: alguns Serviços da AWS usam atributos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Encaminhamento de sessões de acesso (FAS): qualquer pessoa que utilizar uma função ou usuário do IAM para realizar ações na AWS é considerada uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações.

Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

- Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.
- Função vinculada ao serviço: uma função vinculada a serviço é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode assumir o perfil para executar uma ação em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode exibir, mas não pode editar as permissões para perfis vinculados ao serviço.

- Aplicações em execução no Amazon EC2: é possível usar um perfil do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir um perfil da AWS a uma instância do EC2 e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil de instância contém a perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar os perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Como gerenciar acesso usando políticas

Você controla o acesso na AWS criando políticas e anexando-as a identidades ou atributos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou atributo, define suas permissões. A AWS avalia essas políticas quando uma entidade principal (usuário, usuário raiz ou sessão de perfil) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas são armazenadas na AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar AWS as políticas JSON da para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a perfis, e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de perfil do AWS Management Console, da AWS CLI ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas embutidas ou políticas gerenciadas. As políticas embutidas são anexadas diretamente a um único usuário, grupo ou função. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e perfis na Conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recurso

Políticas baseadas em atributos são documentos de políticas JSON que você anexa a um atributo. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recurso, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse recurso e em que condições. Você precisa especificar uma entidade principal em uma política baseada em recurso. As entidades principais podem incluir contas, usuários, perfis, usuários federados ou Serviços da AWS.

Políticas baseadas em atributos são políticas em linha que estão localizadas nesse serviço. Não é possível usar as políticas gerenciadas da AWS do IAM em uma política baseada em atributos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou funções da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recurso, embora não usem o formato de documento de política JSON.

Amazon S3, AWS WAF e Amazon VPC são exemplos de serviços compatíveis com ACLs. Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

A AWS aceita tipos de política menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs): SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (UO) no AWS Organizations. O AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS pertencentes à sua empresa. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades em contas-membro, incluindo cada .Usuário raiz da conta da AWS Para obter mais informações sobre o Organizações e SCPs, consulte How SCPs work (Como os SCPs funcionam) noAWS Organizations Guia do usuário do .
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas

substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como a AWS determina se deve permitir uma solicitação quando há vários tipos de política envolvidos, consulte Lógica da avaliação de políticas no Guia do usuário do IAM.

Como o Acesso Verificado pela AWS funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Acesso Verificado, saiba quais recursos do IAM estão disponíveis para uso com o Acesso Verificado.

Recursos do IAM que você pode usar com o Acesso Verificado pela AWS

Recurso do IAM	Suporta Acesso Verificado
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
atributos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Sim

Para obter uma visão geral de como o acesso verificado e outros serviços da AWS funcionam com a maioria dos recursos do IAM, consulte AWS Serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para Acesso Verificado

Suporta políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou atributos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou função à qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos de política JSON do IAM no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para Acesso Verificado

Para visualizar exemplos de políticas baseadas em identidade do Acesso Verificado, consulte Exemplos de políticas baseadas em identidade para o Acesso Verificado pela AWS.

Políticas baseadas em recursos no Acesso Verificado

Oferece suporte a políticas baseadas em recurso	Não

Políticas baseadas em atributos são documentos de políticas JSON que você anexa a um atributo. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recurso, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico.

Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse recurso e em que condições. Você precisa especificar uma entidade principal em uma política baseada em recurso. As entidades principais podem incluir contas, usuários, perfis, usuários federados ou Serviços da AWS.

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando a entidade principal e o atributo estão em diferentes Contas da AWS, um administrador do IAM da conta confiável também deve conceder à entidade principal (usuário ou perfil) permissão para acessar o atributo. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma outra política baseada em identidade será necessária. Para obter mais informações, consulte Como as funções do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Ações políticas para Acesso Verificado

Oferece suporte a ações de políticas	Sim

Os administradores podem usar as políticas de JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome que a operação de API da AWS associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Inclua ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações de Acesso Verificado, consulte Ações definidas pelo Amazon EC2 na Referência de autorização do serviço.

As ações de políticas no Acesso Verificado usam o seguinte prefixo antes da ação:

```
ec2
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

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

Para visualizar exemplos de políticas baseadas em identidade do Acesso Verificado, consulte Exemplos de políticas baseadas em identidade para o Acesso Verificado pela AWS.

Recursos de política para Acesso Verificado

Oferece suporte a atributos de políticas	Sim

Os administradores podem usar as políticas de JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política `Resource` JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como prática recomendada, especifique um atributo usando seu Nome do atributo da Amazon (ARN). Isso pode ser feito para ações que oferecem suporte a um tipo de atributo específico, conhecido como permissões em nível de atributo.

Para ações que não oferecem suporte a permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para ver uma lista dos tipos de recursos do Acesso Verificado e seus ARNs, consulte Recursos definidos pelo Amazon EC2 na Referência de autorização do serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo Amazon EC2.

Para visualizar exemplos de políticas baseadas em identidade do Acesso Verificado, consulte Exemplos de políticas baseadas em identidade para o Acesso Verificado pela AWS.

Chaves de condição da política do Acesso Verificado

Suporta chaves de condição de política específicas de serviço	Sim

Os administradores podem usar as políticas de JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou `Condition` bloco de) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, a AWS avaliará a condição usando uma operação lógica `OR`. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode utilizar variáveis de espaço reservado ao especificar as condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos de política do IAM: variáveis e tags no Guia do usuário do IAM.

A AWS oferece suporte a chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição globais da AWS, consulte Chaves de contexto de condição globais da AWS no Guia do usuário do IAM.

Para ver uma lista de chaves de condição do Acesso Verificado, consulte Chaves de condição do Amazon EC2 na Referência de autorização do serviço. Para saber com quais ações e recursos você pode usar a chave de condição, consulte Ações definidas pelo Amazon EC2.

Para visualizar exemplos de políticas baseadas em identidade do Acesso Verificado, consulte Exemplos de políticas baseadas em identidade para o Acesso Verificado pela AWS.

ACLs em Acesso Verificado

Oferece suporte a ACLs	Não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com Acesso Verificado

Oferece suporte a ABAC (tags em políticas)	Parcial

O controle de acesso baseado em atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Na AWS, esses atributos são chamados de tags. É possível anexar tags a entidades do IAM (usuários ou perfis) e a muitos atributos da AWS. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do atributo que ela está tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys` chaves de condição.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial.

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Usar credenciais temporárias com Acesso Verificado

Oferece suporte a credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Você está usando credenciais temporárias se faz login no AWS Management Console usando qualquer método, exceto um nome de usuário e uma senha. Por exemplo, quando você acessa a AWS usando o link de autenticação única (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar perfis, consulte Alternar para um perfil (console) no Guia do usuário do IAM.

Você pode criar credenciais temporárias manualmente usando a AWS CLI ou a API da AWS. Em seguida, você pode usar essas credenciais temporárias para acessar aAWS .AWS A recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Permissões de entidade principal entre serviços para o Acesso Verificado

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou perfil do IAM para executar ações na AWS, você é considerado uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

Perfis de serviço para Acesso Verificado

Oferece suporte a perfis de serviço	Não

O perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.

Função vinculada ao serviço para acesso ao Acesso Verificado

Oferece suporte a perfis vinculados ao serviço	Sim

Um perfil vinculado ao serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode presumir a função de executar uma ação em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas ao serviço do Acesso Verificado, consulte Usar funções vinculadas ao serviço para o Acesso Verificado.

Exemplos de políticas baseadas em identidade para o Acesso Verificado pela AWS

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do ACM. Eles também não podem executar tarefas usando o AWS Management Console, a AWS Command Line Interface (AWS CLI) ou a AWS API. Para conceder aos usuários permissão para executar ações nos recursos de que precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis, e os usuários podem assumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recurso definidos pelo Acesso Verificado, por exemplo, o formato dos ARNs para cada um dos tipos de recurso, consulte Ações, recursos e chaves de condição do Amazon EC2 na Referência de autorização do serviço.

Tópicos

- Práticas recomendadas de políticas
- Política para criar instâncias de Acesso Verificado
- Permitir que usuários visualizem suas próprias permissões

Práticas recomendadas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Acesso Verificado em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com AWS as políticas gerenciadas pela e avance para as permissões de privilégio mínimo: para começar a conceder permissões a seus usuários e workloads, use as AWS políticas gerenciadas pela que concedem permissões para muitos casos de uso comuns. Elas estão disponíveis na sua Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da AWS específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e atributos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um AWS service (Serviço da AWS) específico, como o AWS CloudFormation. Para obter mais informações, consulte Elementos de política JSON do IAM: Condition no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM.
- Exigir autenticação multifator (MFA): se houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Política para criar instâncias de Acesso Verificado

Para criar uma instância de Acesso Verificado, os diretores do IAM precisam adicionar essa declaração adicional à política do IAM.

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

> **Note**
>
> `verified-access:AllowVerifiedAccess` é uma API virtual somente para ação. Ele não oferece suporte à autorização baseada em chave de recurso, tag ou condição. Use autorização baseada em recurso, tag ou chave de condição na ação da `ec2:CreateVerifiedAccessInstance` API.

Exemplo de política para criar uma instância do Acesso Verificado. Neste exemplo, `123456789012` é o número da AWS conta e `us-east-1` é a AWS região.

```
{
      "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": "*"
        }
    ]
}
```

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como é possível criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou de forma programática usando a AWS CLI ou a API da AWS.

```
{
    "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": "*"
        }
    ]
}
```

Solução de problemas de identidade e acesso do Acesso Verificado pela AWS

Use as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o Acesso Verificado e o IAM.

Problemas

- Não tenho autorização para executar uma ação no Acesso Verificado
- Não estou autorizado a executar iam:PassRole
- Quero permitir que as pessoas fora da minha Conta da AWS acessem meus recursos do Acesso Verificado

Não tenho autorização para executar uma ação no Acesso Verificado

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `ec2:`*`GetWidget`* fictícias.

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

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao atributo *`my-example-widget`* usando a ação `ec2:`*`GetWidget`*.

Se você precisar de ajuda, entre em contato com seu administrador AWS. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a executar iam:PassRole

Se você receber uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, as suas políticas deverão ser atualizadas para permitir a passagem de um perfil para o Acesso Verificado.

Alguns Serviços da AWS permitem que você transmita um perfil existente para o serviço, em vez de criar um perfil de serviço ou um perfil vinculado ao serviço. Para fazer isso, um usuário deve ter permissões para passar o perfil para o serviço.

O erro de exemplo a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta usar o console para executar uma ação no Acesso Verificado. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se você precisar de ajuda, entre em contato com seu administrador AWS. Seu administrador é a pessoa que forneceu a você suas credenciais de login.

Quero permitir que as pessoas fora da minha Conta da AWS acessem meus recursos do Acesso Verificado

Você pode criar uma função que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recurso ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte o seguinte:

- Para saber se o Acesso Verificado oferece suporte a esses recursos, consulte Como o Acesso Verificado pela AWS funciona com o IAM.
- Para saber como conceder acesso a seus recursos em todas as Contas da AWS pertencentes a você, consulte Fornecimento de acesso a um usuário do IAM em outra Conta da AWS pertencente a você no Guia de usuário do IAM.
- Para saber como conceder acesso a seus recursos para Contas da AWS terceirizadas, consulte Fornecimento de acesso a Contas da AWS pertencentes a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em atributos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em atributos no Guia do usuário do IAM.

Usar funções vinculadas ao serviço para o Acesso Verificado

AWSO Acesso Verificado usa AWS Identity and Access Management funções vinculadas ao serviço (IAM). A função vinculada ao produto é um tipo exclusivo de função do IAM vinculada diretamente ao Acesso Verificado. Os perfis vinculados ao serviço são definidos previamente pelo Acesso Verificado e incluem todas as permissões que o serviço requer para chamar outros Serviços da AWS em seu nome.

Uma função vinculada ao serviço facilita a configuração do Acesso Verificado porque não é preciso adicionar as permissões necessárias manualmente. O Acesso Verificado define as permissões das funções vinculadas ao serviço e, exceto se definido de outra forma, somente o Access Analyzer pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e esta política não pode ser anexada a nenhuma outra entidade do IAM.

Para obter informações sobre outros serviços compatíveis com funções vinculadas aos serviços, consulte serviços da AWS que funcionam com o IAM e procure os serviços que apresentam Sim na coluna Funções vinculadas aos serviços. Escolha um Sim com um link para visualizar a documentação da função vinculada a esse serviço.

Permissões de função vinculada ao serviço para detecção de conta do Acesso Verificado

O Acesso Verificado usa o perfil vinculado ao serviço chamado AWSServiceRoleForVPCVerifiedAccess para provisionar recursos em sua conta que são necessárias para usar o serviço.

O perfil vinculado ao serviço AWSServiceRoleForVPCVerifiedAccess confia nos seguintes serviços para assumir o perfil:

- `verified-access.amazonaws.com`

A política de permissões de perfil vinculado ao serviço AWSVPCVerifiedAccessServiceRolePolicy permite que o Acesso Verificado conclua as seguintes ações nos recursos especificados:

- Ação `ec2:CreateNetworkInterface` em todas as sub-redes e grupos de segurança, bem como em todas as interfaces de rede com a tag `VerifiedAccessManaged=true`
- Ação `ec2:CreateTags` em todas as interfaces de rede no momento da criação

- Ação `ec2:DeleteNetworkInterface` em todas as interfaces de rede com a tag `VerifiedAccessManaged=true`
- Ação `ec2:ModifyNetworkInterfaceAttribute` em todos os grupos de segurança e todas as interfaces de rede com a tag `VerifiedAccessManaged=true`

Você também pode ver as permissões dessa política na AWS Management Console AwsVPCVerifiedAccessServiceRolePolicy ou pode ver a política AwsVPCVerifiedAccessServiceRolePolicy no AWS Guia de Referência de Políticas Gerenciadas.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte Service-linked role permissions (Permissões de função vinculada a serviços) no Guia do usuário do IAM.

Criar uma função vinculada ao serviço para o Acesso Verificado

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você cria um grupo de nós gerenciados no CreateVerifiedAccessEndpoint ou AWS Management Console com AWS CLI a AWS API, o Acesso Verificado cria a função vinculada ao serviço para você.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você poderá usar esse mesmo processo para recriar a função em sua conta. Quando você chama o CreateVerifiedAccessEndpoint novamente, o Acesso Verificado cria a função vinculada ao serviço para você novamente.

Editar uma função vinculada ao serviço para o Acesso Verificado

O Acesso Verificado não permite editar a função vinculada ao serviço AWSServiceRoleForAccessAnalyzer. Depois que criar uma função vinculada ao serviço, você não poderá alterar o nome da função, pois várias entidades podem fazer referência a ela. No entanto, será possível editar a descrição da função usando o IAM. Para ter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para o Acesso Verificado

Não é necessário excluir manualmente a função AWSServiceRoleForVPCVerifiedAccess. Quando você usa Excluir endpoint de acesso verificado, no AWS Management Console ou na API da AWS CLI, o Acesso Verificado pela AWS limpa os recursos e exclui a função vinculada ao serviço para você.

Como excluir manualmente a função vinculada ao serviço usando o IAM

Use o console do IAM, a AWS CLI ou a API da AWS para excluir o perfil vinculado ao serviço WSServiceRoleForVPCVerifiedAccess. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Regiões compatíveis com funções vinculadas ao serviço do Acesso Verificado

O Acesso Verificado oferece suporte a funções vinculadas a serviços em todas as Regiões da AWS em que o serviço estiver disponível. Para obter mais informações, consulte AWS Regiões e endpoints.

Políticas da AWS gerenciadas para Acesso Verificado pela AWS

Uma política gerenciada pela AWS é uma política independente criada e administrada pela AWS. As políticas gerenciadas pela AWS são criadas para fornecer permissões a vários casos de uso comuns a fim de que você possa começar a atribuir permissões a usuários, grupos e perfis.

Lembre-se de que as políticas gerenciadas pela AWS podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para todos AWS os clientes da usarem. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da específicas para seus casos de uso.

Você não pode alterar as permissões definidas em políticas gerenciadas pela AWS. Se a AWS atualiza as permissões definidas em uma política gerenciada pela AWS, a atualização afeta todas as identidades de entidades principais (usuários, grupos e perfis) às quais a política está vinculada. É mais provável que a AWS atualize uma política gerenciada pela AWS quando um novo AWS service (Serviço da AWS) é lançado ou novas operações de API são disponibilizadas para os serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

AWS política gerenciada: AWSVPCVerifiedAccessServiceRolePolicy

Esta política está anexada a uma função vinculada ao serviço que permite ao acesso verificado executar ações em seu nome. Para obter mais informações, consulte Usar perfis vinculados a serviços. Para ver as permissões dessa política, você pode ver AwsVPCVerifiedAccessServiceRolePolicy no, AWS Management Console ou você pode ver

a política AwsVPCVerifiedAccessServiceRolePolicy no AWSGuia de Referência de Políticas Gerenciadas.

Atualizações de acesso verificado às políticas AWS gerenciadas

Visualize detalhes sobre atualizações em políticas gerenciadas para o Acesso Verificado pela AWS desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed de RSS na página Document History (Histórico do documento).

Alteração	Descrição	Data
AwsVPCVerifiedAccessServiceRolePolicy - Política atualizada	O Acesso Verificado atualizou sua política gerenciada para incluir as descrições de todas as ações no campo "sid".	17 de novembro de 2023
AwsVPCVerifiedAccessServiceRolePolicy - Política atualizada	O Acesso Verificado atualizou sua política gerenciada para adicionar recursos de grupo de segurança à `ec2:CreateNetworkInterface` permissão.	31 de maio de 2023
AwsVPCVerifiedAccessServiceRolePolicy - Nova política	O Acesso Verificado adicionou uma nova política para permitir provisionar recursos em sua conta que são necessários para usar o serviço.	29 de novembro de 2022
O Acesso Verificado começou a monitorar as alterações	O Acesso Verificado começou a rastrear alterações para suas AWS políticas gerenciadas.	29 de novembro de 2022

Validação de conformidade do Acesso Verificado pela AWS

Acesso Verificado pela AWS pode ser configurado para dar suporte à conformidade do Federal Information Processing Standards (FIPS). Para obter mais informações e detalhes sobre como configurar a conformidade com FIPS para Acesso Verificado, acesse Conformidade com FIPS para acesso verificado.

Para saber se um AWS service (Serviço da AWS) está no escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo por programa de conformidade e selecione o programa de conformidade em que você está interessado. Para obter informações gerais, consulteAWS Programas de conformidade.

É possível fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Downloading Reports inAWS Artifact.

Sua responsabilidade de conformidade ao usar o Serviços da AWS é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os seguintes atributos para ajudar com a conformidade:

- Guias de referência rápida de conformidade e segurança - estes guias de implantação discutem considerações sobre arquitetura e fornecem as etapas para a implantação de ambientes de linha de base focados em segurança e conformidade na AWS.
- Architecting for HIPAA Security and Compliance on Amazon Web Services (Arquitetura para segurança e conformidade com HIPAA no Amazon Web Services): esse estudo técnico descreve como as empresas podem usar a AWS para criar aplicações adequadas aos padrões HIPAA.

  > **Note**
  >
  > Nem todos os Serviços da AWS estão qualificados pela HIPAA. Para obter mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- atributos de conformidade da AWS: essa coleção de manuais e guias pode ser aplicada a seu setor e local.
- Guias de conformidade do cliente da AWS: entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as práticas recomendadas para proteção de Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões

de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).

- Avaliar atributos com regras no AWS Config Guia do desenvolvedor: o serviço AWS Config avalia como as configurações de atributos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub: este AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança na AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- AWS Audit Manager – Esse AWS service (Serviço da AWS) ajuda a auditar continuamente seu uso da AWS para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

Resiliência no Acesso Verificado pela AWS

A infraestrutura global da AWS se baseia em Regiões da AWS e zonas de disponibilidade. A Regiões da AWS oferece várias zonas de disponibilidade separadas e isoladas fisicamente que são conectadas com baixa latência, throughputs elevadas e em redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre Regiões da AWS e zonas de disponibilidade, consulte InfraestrututaglobalAWS.

Além da infraestrutura AWS global, o Acesso Verificado oferece o seguinte recurso para ajudar a dar suporte às suas necessidades de alta disponibilidade.

Várias sub-redes para alta disponibilidade

Ao criar um endpoint de Acesso Verificado do tipo balanceador de carga, você pode associar várias sub-redes ao endpoint. Cada sub-rede que você associa ao endpoint deve pertencer a uma zona de disponibilidade diferente. Ao associar várias sub-redes, você pode garantir alta disponibilidade usando várias zonas de disponibilidade.

Monitorando o Acesso Verificado pela AWS

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e a performance do Acesso Verificado pela AWS. A AWS fornece as ferramentas de monitoramento a seguir para observar o acesso verificado, informar quando algo está errado e realizar ações automaticamente quando apropriado:

- Registros de acesso: capture informações detalhadas sobre solicitações de acesso a aplicativos. Para obter mais informações, consulte the section called “Logs de Verified Acesss”.
- O AWS CloudTrail captura chamadas de API e eventos relacionados feitos por sua conta da Conta da AWS ou em nome dela e entrega os arquivos de log a um bucket do Amazon S3 que você especifica. Você pode identificar quais usuários e contas chamaram a AWS, o endereço IP de origem do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte the section called “Logs do CloudTrail”.

Logs de Verified Acesss

Depois que o Acesso AWS Verificado avalia cada solicitação de acesso, ele registra todas as tentativas de acesso. Isso fornece visibilidade centralizada do acesso aos aplicativos e ajuda você a responder rapidamente a incidentes de segurança e solicitações de auditoria. O Acesso Verificado suporta o formato de log do Open Cybersecurity Schema Framework (OCSF).

Ao ativar o log, você precisará configurar um destino para o envio dos logs. A entidade principal do IAM que está sendo usada para configurar o destino do log precisará ter certas permissões para que os logs funcionem corretamente. As permissões do IAM necessárias para cada destino de log podem ser vistas na seção Permissões de arquivo de log. O Acesso Verificado oferece suporte aos seguintes destinos para publicação de logs de acesso:

- Grupos CloudWatch de registros do Amazon Logs
- Buckets do Amazon S3
- Streams de entrega do Amazon Data Firehose

Conteúdo

- Ativar ou desativar logs
- Incluindo contexto de confiança
- Exemplo de entradas de registro para logs de Acesso Verificado

Versões de logs

Por padrão, o sistema de log de Acesso Verificado usa o Open Cybersecurity Schema Framework (OCSF) versão 0.1. Exemplos de logs usando a versão 0.1 podem ser vistos na seção Exemplos da versão 0.1 do OCSF.

A versão de log mais recente é compatível com a versão 1.0.0-rc.2 do OCSF. Detalhes específicos sobre o esquema podem ser encontrados aqui Esquema OCSF. Exemplos de logs usando a versão 1.0.0-rc.2 podem ser vistos na seção Exemplos da versão 1.0.0-rc.2 do OCSF.

Atualizar versão de log

Caso queira atualizar a versão de log que está sendo usada, siga o procedimento abaixo.

Para atualizar a versão de log usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do Acesso Verificado.
3. Selecione a instância de Acesso Verificado apropriada.
4. Na guia Configuração de log de instância de Acesso Verificado, escolha Modificar configuração de log de instância de Acesso Verificado.
5. Selecione ocsf-1.0.0-rc.2 na lista suspensa Versão do log de atualização.
6. Escolha Modificar configuração de log da instância de Acesso Verificado.

Para atualizar a versão de registro usando o AWS CLI

Use o comando modify-verified-access-instance-logging-configuration.

Permissões de arquivo de log

A entidade principal do IAM que está sendo usada para configurar o destino do log precisará ter certas permissões para que os logs funcionem corretamente. Abaixo, você pode ver as permissões necessárias para cada destino de log.

Para entrega ao CloudWatch Logs:

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration` na instância de Acesso Verificado
- `logs:CreateLogDelivery`, `logs:DeleteLogDelivery`, `logs:GetLogDelivery`, `logs:ListLogDeliveries` e `logs:UpdateLogDelivery` em todos os recursos
- `logs:DescribeLogGroups`, `logs:DescribeResourcePolicies`, e `logs:PutResourcePolicy` no grupo de logs de destino

Para entrega no Amazon S3:

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration` na instância de Acesso Verificado
- `logs:CreateLogDelivery`, `logs:DeleteLogDelivery`, `logs:GetLogDelivery`, `logs:ListLogDeliveries` e `logs:UpdateLogDelivery` em todos os recursos
- `s3:GetBucketPolicy` e `s3:PutBucketPolicy` no bucket de destino

Para entrega ao Firehose:

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration` na instância de Acesso Verificado
- `firehose:TagDeliveryStream` Para todos os recursos
- `iam:CreateServiceLinkedRole` Para todos os recursos
- `logs:CreateLogDelivery`, `logs:DeleteLogDelivery`, `logs:GetLogDelivery`, `logs:ListLogDeliveries` e `logs:UpdateLogDelivery` em todos os recursos

Ativar ou desativar logs

Ao ativar o log, você precisará configurar um destino para o envio dos logs. A entidade principal do IAM que está sendo usada para configurar o destino do log precisará ter certas permissões para que os logs funcionem corretamente. As permissões do IAM necessárias para cada destino de log podem ser vistas na seção Permissões de arquivo de log.

Conteúdo

- Desabilitar logs de acesso

Habilitar logs de acesso

Para habilitar logs de Acesso Verificado

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do Acesso Verificado.
3. Selecione a instância de Acesso Verificado.
4. Na guia Configuração de log de instância de Acesso Verificado, escolha Modificar configuração de log de instância de Acesso Verificado.
5. (Opcional) Para incluir dados de confiança enviados de provedores confiáveis nos logs, faça o seguinte:
   a. Selecione ocsf-1.0.0-rc.2 na lista suspensa Versão do log de atualização.
   b. Escolha Incluir contexto de confiança.
6. Faça um dos seguintes procedimentos:
   - Ative a opção Entregar para Amazon CloudWatch Logs. Escolha o grupo de logs de destino.
   - Ative a opção Entregar para o Amazon S3. Insira o nome, o proprietário e o prefixo do bucket de destino.
   - Ative o Deliver to Firehose. Escolha o fluxo de entrega de destino.
7. Escolha Modificar configuração de log da instância de Acesso Verificado.

Para ativar os registros de acesso verificado usando o AWS CLI

Use o comando modify-verified-access-instance-logging-configuration.

Desabilitar logs de acesso

Você pode desativar os logs de acesso da sua instância de Acesso Verificado a qualquer momento. Depois que os logs de acesso forem desabilitados, seus dados permanecerão no destino até que você os exclua.

Para desabilitar os logs de Acesso Verificado

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.

2. No painel de navegação, selecione Instâncias do Acesso Verificado.
3. Selecione a instância de Acesso Verificado.
4. Na guia Configuração de log de instância de Acesso Verificado, escolha Modificar configuração de log de instância de Acesso Verificado.
5. Desative a entrega de logs.
6. Escolha Modificar configuração de log da instância de Acesso Verificado.

Para desativar os registros de acesso verificado usando o AWS CLI

Use o comando modify-verified-access-instance-logging-configuration.

Incluindo contexto de confiança

O contexto de confiança enviado pelo seu provedor de confiança pode, opcionalmente, ser incluído nos seus logs de Acesso Verificado. Isso pode ser muito útil ao definir políticas que permitam ou neguem acesso aos aplicativos. Depois de ativado, o contexto de confiança será encontrado no log abaixo do campo `data`. Se desativado, o `data` campo será definido como `null`. Para configurar o Acesso Verificado para incluir contexto de confiança nos logs, siga o procedimento abaixo.

> **Note**
>
> A inclusão do contexto de confiança em seus logs de Acesso Verificado exige a atualização para a versão `ocsf-1.0.0-rc.2` mais recente do log. O procedimento abaixo pressupõe que você já tenha o log ativado. Se isso não for verdade, consulte Habilitar logs de acesso o procedimento completo.

Conteúdo

Habilitar contexto de confiança

Para incluir contexto de confiança nos logs de Acesso Verificado usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do Acesso Verificado.

3. Selecione a instância de Acesso Verificado apropriada.
4. Na guia Configuração de log de instância de Acesso Verificado, escolha Modificar configuração de log de instância de Acesso Verificado.
5. Selecione ocsf-1.0.0-rc.2 na lista suspensa Versão do log de atualização.
6. Ative a opção Incluir contexto de confiança.
7. Escolha Modificar configuração de log da instância de Acesso Verificado.

Para incluir contexto de confiança nos registros de acesso verificado usando o AWS CLI

Use o comando modify-verified-access-instance-logging-configuration.

Desabilitar contexto de confiança

Se você não quiser mais incluir o contexto de confiança nos logs, poderá removê-lo com o procedimento abaixo.

Para remover o contexto de confiança dos logs de Acesso Verificado usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do Acesso Verificado.
3. Selecione a instância de Acesso Verificado apropriada.
4. Na guia Configuração de log de instância de Acesso Verificado, escolha Modificar configuração de log de instância de Acesso Verificado.
5. Desative a opção Incluir contexto de confiança.
6. Escolha Modificar configuração de log da instância de Acesso Verificado.

Para remover o contexto de confiança dos registros de acesso verificado usando o AWS CLI

Use o comando modify-verified-access-instance-logging-configuration.

Exemplo de entradas de registro para logs de Acesso Verificado

A seguir estão exemplo de entradas de log.

Conteúdo

Exemplos da versão 0.1 do OCSF

Veja a seguir exemplos de logs usando a versão 0.1 do OCSF de log padrão.

Exemplos

- Acesso concedido com o OIDC
- Acesso concedido com OIDC e JAMF
- Acesso concedido com o OIDC e CrowdStrike
- Acesso negado devido à falta de um cookie
- Acesso negado pela política
- Entrada de log desconhecida

Acesso concedido com o OIDC

Neste exemplo de entrada de log, o Acesso Verificado permite acesso a um endpoint com um provedor confiável de usuários do OIDC.


```
{
    "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
}
```


Acesso concedido com OIDC e JAMF

Neste exemplo de entrada de log, o Acesso Verificado permite acesso a um endpoint com provedores confiáveis de dispositivos OIDC e JAMF.


```
{
    "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
}
```


Acesso concedido com o OIDC e CrowdStrike

Neste exemplo de entrada de registro, o Acesso Verificado permite acesso a um endpoint com OIDC e provedores confiáveis de CrowdStrike dispositivos.


```
{
    "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
}
```


Acesso negado devido à falta de um cookie

Neste exemplo de entrada de log, o Acesso Verificado nega o acesso devido à falta de um cookie de autenticação.


```
{
    "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
}
```

Acesso negado pela política

Neste exemplo de entrada de log, o Acesso Verificado nega uma solicitação autenticada porque a solicitação não é permitida pelas políticas de acesso.

```
{
    "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
}
```

Entrada de log desconhecida

Neste exemplo de entrada de log, o Acesso Verificado não pode gerar uma entrada de log completa, então emite uma entrada de log desconhecida. Isso garante que todas as solicitações apareçam no log de acesso.

```
{
    "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
}
```


Exemplos da versão 1.0.0-rc.2 do OCSF

Conteúdo

Acesso concedido com contexto de confiança incluído


```
{
    "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"
            }
        }
    }
}
```

Acesso concedido com contexto de confiança omitido

```
{
    "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
}
```


Registre chamadas da API de acesso AWS verificado usando AWS CloudTrail

AWS O Acesso Verificado é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um AWS service (Serviço da AWS) no Acesso Verificado. O CloudTrail captura todas as chamadas de API para o Acesso Verificado como eventos. As chamadas capturadas incluem chamadas do console do Acesso Verificado e chamadas de código para as operações de API do Acesso Verificado. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o Acesso Verificado. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Com as informações coletadas pelo CloudTrail, determine a solicitação feita para o Acesso Verificado, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e os detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Acessar informações do Acesso Verificado no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando a atividade ocorre no Acesso Verificado, essa atividade é registrada em um evento do CloudTrail junto com outros eventos de produtos da AWS service (Serviço da AWS) no Histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Viewing events with CloudTrail Event history (Como visualizar eventos com o histórico de eventos do CloudTrail).

Para obter um registro contínuo de eventos em sua Conta da AWS, incluindo eventos para os planos do Acesso Verificado, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, você pode configurar outros Serviços da AWS para analisar mais ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte as informações a seguir:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e Receber arquivos de log do CloudTrail de várias contas

Todas as ações do Acesso Verificado são registradas em log pelo CloudTrail e são documentados na Amazon EC2 API Reference. Por exemplo, as chamadas para as ações `CreateVerifiedAccessInstance`, `DeleteVerifiedAccessInstance` e `ModifyVerifiedAccessInstance` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou de AWS Identity and Access Management usuário do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro AWS service (Serviço da AWS).

Para obter mais informações, consulte Elemento userIdentity do CloudTrail.

Compreenda as Entradas dos arquivos de log do Acesso Verificado

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma solicitação única de qualquer fonte. Isso inclui informações sobre a ação

solicitada, a data e hora da ação, os parâmetros de solicitação, e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log do CloudTrail para a ação `CreateVerifiedAccessInstance`.


```
{
    "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"
}
```

Cotas para o Acesso Verificado pela AWS

Você Conta da AWS tem cotas padrão, anteriormente chamadas de limites, para cada serviço AWS service (Serviço da AWS). A menos que especificado de outra forma, cada cota é específica da região.

Conta da AWScotas de nível

Sua conta Conta da AWS tem as seguintes cotas relacionadas ao Acesso Verificado.

Nome	Padrão	Ajustável	Descrição
Instâncias de acesso verificado	5	Sim	O número máximo de instâncias de acesso verificado que podem ser criadas pelos clientes na região atual.
Grupos de acesso verificado	10	Sim	O número máximo de grupos de acesso verificado que podem ser criados pelos clientes na região atual.
Provedores de confiança de acesso verificado	15	Sim	O número máximo de provedores confiáveis de acesso verificado que podem ser criados pelos clientes na região atual.
Endpoints de acesso verificado	50	Sim	O número máximo de endpoints de acesso verificado que podem ser criados pelos clientes na região atual.

Cabeçalhos HTTP

Os cabeçalhos HTTP têm os seguintes limites de tamanho.

Nome	Padrão	Ajustável
Linha de solicitação	16 K	Não
Cabeçalho único	16 K	Não
Cabeçalho de resposta inteiro	32 K	Não
Cabeçalho da solicitação inteira	64 K	Não

O tamanho da reclamação OIDC

A seguir está o limite de tamanho da reivindicação do OIDC.

Nome	Padrão	Ajustável
O tamanho da reclamação OIDC	11 K	Não

Histórico do documento para o guia do usuário do Acesso Verificado

A tabela a seguir descreve as versões de documentação para o Acesso Verificado.

Alteração	Descrição	Data
AWS Atualização da política gerenciada	Atualização feita na política do IAM AWS gerenciada do Acesso Verificado.	17 de novembro de 2023
Criptografia de dados em repouso	Por padrão, o Acesso Verificado pela AWS criptografa dados em repouso, usando chaves KMS de propriedade da AWS.	28 de setembro de 2023
Compatibilidade com conformidade com FIPS	Configure o Acesso Verificado para conformidade com o FIPS.	26 de setembro de 2023
Registro em log aprimorado	Adição do recurso de registro que adiciona contextos de confiança aos registros.	19 de junho de 2023
AWS Atualização da política gerenciada	Atualização feita na política do IAM AWS gerenciada do Acesso Verificado.	31 de maio de 2023
Lançamento do GA	Versão GA do Guia do Usuário do Acesso Verificado. Inclui a AWS WAF integração.	27 de abril de 2023
Versão de visualização	Versão prévia do Guia do usuário do Acesso Verificado	29 de novembro de 2022

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.