Guía del usuario

AWS Acceso verificado

AWS Acceso verificado: Guía del usuario

Table of Contents

¿Qué es Acceso verificado de AWS?

Con Acceso verificado de AWSél, puede proporcionar un acceso seguro a sus aplicaciones sin necesidad de utilizar una red privada virtual (VPN). Acceso verificado evalúa cada solicitud de aplicación y ayuda a garantizar que los usuarios puedan acceder a cada aplicación solo cuando cumplan los requisitos de seguridad especificados.

Beneficios de Acceso verificado

- Mejora de la postura de seguridad: un modelo de seguridad tradicional evalúa el acceso una vez y concede al usuario acceso a todas las aplicaciones. Acceso verificado evalúa cada solicitud de acceso a la aplicación en tiempo real. Esto dificulta que los delincuentes pasen de una aplicación a otra.
- Integración con los servicios de seguridad: Verified Access se integra con los servicios de administración de identidades y dispositivos, incluidos los servicios de terceros AWS y los de terceros. Con los datos de estos servicios, Acceso verificado verifica la fiabilidad de los usuarios y los dispositivos en función de una serie de requisitos de seguridad y determina si el usuario debe tener acceso a una aplicación.
- Experiencia de usuario mejorada: Acceso verificado elimina la necesidad de que los usuarios usen una VPN para acceder a sus aplicaciones. Esto ayuda a reducir el número de casos de asistencia relacionados con problemas relacionados con la VPN.
- Resolución de problemas y auditorías simplificadas: Acceso verificado registra todos los intentos de acceso, lo que proporciona una visibilidad centralizada del acceso a la aplicación para ayudar a responder rápidamente a los incidentes de seguridad y las solicitudes de auditoría.

Acceso a Acceso verificado de

Puede trabajar con Acceso verificado usando cualquiera de las siguientes interfaces:

- AWS Management Console: proporciona una interfaz web que puede utilizar para crear y administrar sus recursos de Acceso verificado. Inicie sesión en la consola de Amazon VPC AWS Management Console y ábrala en. https://console.aws.amazon.com/vpc/
- AWS Command Line Interface (AWS CLI): proporciona comandos para un amplio conjunto de Servicios de AWS, incluidos Acceso verificado de AWS. AWS CLI Es compatible con Windows, macOS y Linux. Para obtener el AWS CLI, consulte AWS Command Line Interface.

- AWS SDKs— Proporcione un idioma específico APIs. Se AWS SDKs ocupan de muchos de los detalles de la conexión, como el cálculo de las firmas y la gestión de los reintentos y errores de las solicitudes. Para obtener más información, consulte AWS SDKs.
- API de consulta: proporciona acciones de API de nivel bajo a las que se llama mediante solicitudes HTTPS. Utilizar la API de consulta es la forma más directa de obtener acceso a Acceso verificado. Sin embargo, requiere que la aplicación gestione detalles de nivel inferior, como, por ejemplo, la generación del hash para firmar la solicitud y la gestión de errores. Para obtener más información, consulta las acciones de acceso verificado en la referencia de las EC2 API de Amazon.

En esta guía se describe cómo utilizarlos AWS Management Console para crear, acceder y gestionar los recursos de acceso verificado.

Precios

Se le cobrará por hora por cada aplicación en Acceso verificado y se le cobrará la cantidad de datos procesados por Acceso verificado. Para obtener más información, consulte Precios de Acceso verificado de AWS.

Cómo funciona Acceso verificado

Acceso verificado de AWS evalúa cada solicitud de aplicación de sus usuarios y permite el acceso en función de:

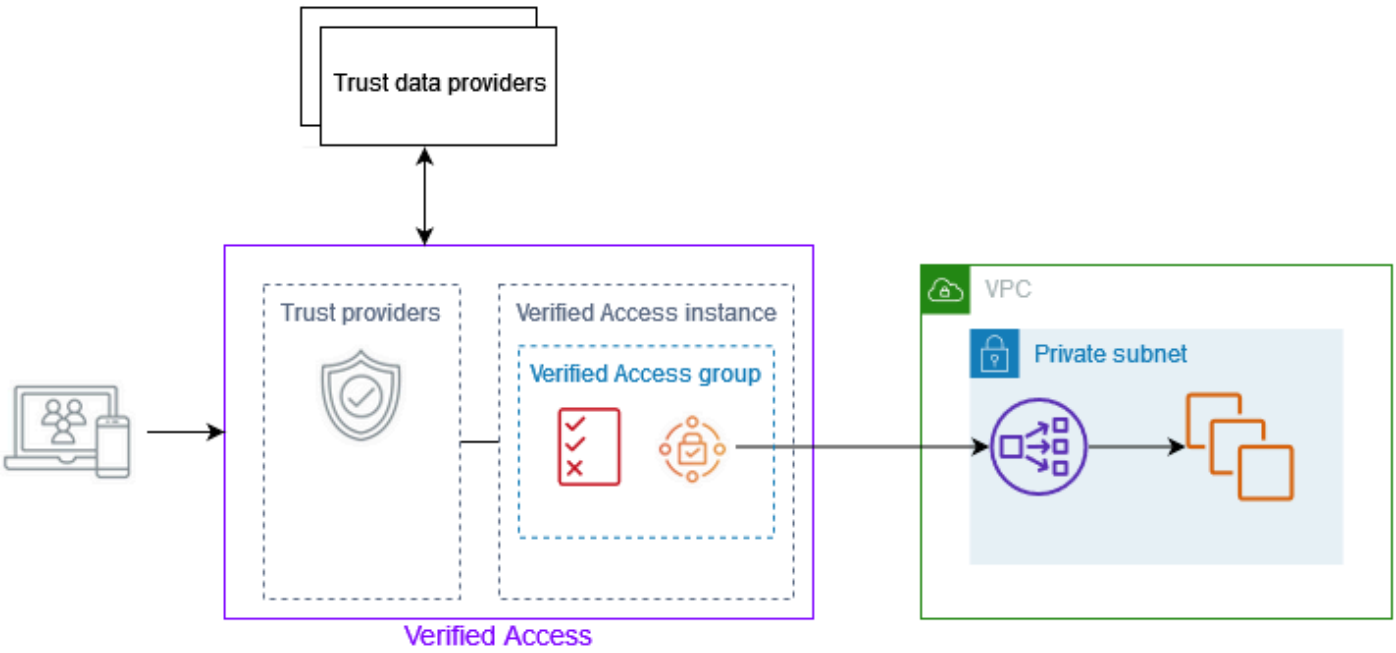
- Datos de confianza enviados por el proveedor de confianza que haya elegido (de AWS o de un tercero).
- Políticas de acceso que usted cree en Acceso verificado.

Cuando un usuario intenta acceder a una aplicación, Acceso verificado obtiene sus datos del proveedor de confianza y los compara con las políticas que usted establezca para la aplicación. Acceso verificado permite el acceso a la aplicación solicitada solo si el usuario cumple los requisitos de seguridad especificados. Todas las solicitudes de aplicaciones se rechazan de forma predeterminada, hasta que se defina una política.

Además, Acceso verificado registra todos los intentos de acceso para ayudarle a responder rápidamente a los incidentes de seguridad y a las solicitudes de auditoría.

Componentes clave de Acceso verificado

El siguiente diagrama brinda información general de alto nivel sobre Acceso verificado. Los usuarios envían solicitudes para acceder a una aplicación. Acceso verificado evalúa la solicitud en función de la política de acceso del grupo y de cualquier política de punto de conexión específica de la aplicación. Si se permite el acceso, la solicitud se envía a la aplicación a través del punto de conexión.



- Instancias de Acceso verificado: una instancia evalúa las solicitudes de aplicación y concede el acceso solo cuando se cumplen los requisitos de seguridad.
- Puntos de conexión de Acceso verificado: cada punto de conexión representa una aplicación. En el diagrama anterior, la aplicación está alojada en EC2 instancias que son el destino de un balanceador de cargas.
- Grupo de Acceso verificado: conjunto de puntos de conexión de Acceso verificado. Se recomienda agrupar los puntos de conexión de las aplicaciones con requisitos de seguridad similares a fin de simplificar la administración de las políticas. Por ejemplo, puede agrupar los puntos de conexión de todas sus aplicaciones de ventas.
- Políticas de acceso: conjunto de reglas definidas por el usuario que determinan si se debe permitir o denegar el acceso a una aplicación. Puede especificar una combinación de factores, como la identidad del usuario y el estado de seguridad del dispositivo. Puede crear una política de acceso grupal para cada grupo de Acceso verificado, heredada por todos los puntos de conexión del grupo. Si lo desea, puede crear políticas específicas para la aplicación y adjuntarlas a puntos de conexión específicos.
- Proveedores de confianza: un servicio que administra las identidades de los usuarios o el estado de seguridad de los dispositivos. Verified Access funciona tanto AWS con proveedores de confianza como con proveedores de confianza externos. Debe adjuntar al menos un proveedor de confianza a cada instancia de Acceso verificado. Puede adjuntar un único proveedor de confianza de identidades y varios proveedores de confianza de dispositivos a cada instancia de Acceso verificado.

- Datos de confianza: los datos relacionados con la seguridad de los usuarios o dispositivos que su proveedor de confianza envía a Acceso verificado. También se conocen como notificaciones de usuario o contexto de confianza. Por ejemplo, la dirección de correo electrónico de un usuario o la versión del sistema operativo de un dispositivo. Acceso verificado compara estos datos con sus políticas de acceso cuando recibe cada solicitud de acceso a una aplicación.

Tutorial: Introducción a Acceso verificado

Usa este tutorial para empezar Acceso verificado de AWS. Aprenderá a crear y Configurar recursos de Acceso verificado.

Como parte de este tutorial, agregará una aplicación a Acceso verificado. Al final de este tutorial, usuarios específicos podrán acceder a la misma aplicación a través de Internet, sin usar una VPN. En su lugar, la utilizarás AWS IAM Identity Center como proveedor de confianza en la identidad. Tenga en cuenta que este tutorial no utiliza además un proveedor de confianza de dispositivos.

Tareas

Requisitos previos del tutorial de Acceso verificado

Los siguientes son requisitos previos para completar este tutorial:

- AWS IAM Identity Center habilitado en el Región de AWS lugar en el que estás trabajando. A continuación, puede utilizar el IAM Identity Center como proveedor de confianza con Acceso verificado. Para obtener más información, consulte Habilitar AWS IAM Identity Center en la Guía AWS IAM Identity Center del usuario.
- Un grupo de seguridad para controlar el acceso a la aplicación. Permitir todo el tráfico entrante de CIDR de VPC y todo el tráfico saliente.
- Una aplicación ejecutándose detrás de un equilibrador de carga interno de Elastic Load Balancing. Asociación de su grupo de seguridad con el equilibrador de carga.

- Un certificado TLS público o autofirmado en. AWS Certificate Manager Utilice un certificado RSA con una longitud de clave de 1024 o 2048.
- Un dominio hospedado público y los permisos necesarios para actualizar los registros DNS del dominio.
- Una política de IAM con los permisos necesarios para crear una instancia. Acceso verificado de AWS Para obtener más información, consulte Política para crear instancias de Acceso verificado.

Paso 1: Creación de un proveedor de confianza de Acceso verificado

Utilice el siguiente procedimiento para configurarlo AWS IAM Identity Center como su proveedor de confianza.

Creación de un proveedor de confianza de IAM Identity Center

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Proveedores de confianza de Acceso verificado.
3. Seleccione Crear un proveedor de confianza de Acceso verificado.
4. (Opcional) En la Etiqueta de nombre y la Descripción, introduzca un nombre y una descripción para el proveedor de confianza de Acceso verificado.
5. Introduzca un identificador personalizado para usarlo más adelante cuando trabaje con las reglas de política para el Nombre de referencia de la política. Por ejemplo, puede introducir **`idc`**.
6. En Tipo de proveedor de confianza, seleccione Proveedor de confianza de usuarios.
7. En Tipo de proveedor de confianza de usuarios, seleccione IAM Identity Center.
8. Seleccione Crear un proveedor de confianza de Acceso verificado.

Paso 2: Creación de una instancia de Acceso verificado

Utilice el siguiente procedimiento para crear una instancia de Acceso verificado.

Creación de una instancia de Acceso verificado

1. En el panel de navegación, seleccione Instancias de Acceso verificado.
2. Seleccione Crear instancia de Acceso verificado.

3. (Opcional) En Nombre y Descripción, introduzca un nombre y una descripción para la instancia de Acceso verificado.
4. En Proveedor de confianza de Acceso verificado, seleccione su proveedor de confianza.
5. Seleccione Crear instancia de Acceso verificado.

Paso 3: Creación de un grupo de Acceso verificado

Utilice el siguiente procedimiento para crear un grupo de Acceso verificado.

Creación de un grupo de Acceso verificado

1. En el panel de navegación, seleccione grupos de Acceso verificado.
2. Seleccione Crear grupo de Acceso verificado.
3. (Opcional) En Etiqueta de nombre y Descripción, introduzca un nombre y una descripción para el grupo.
4. En Instancia de Acceso verificado, seleccione su instancia de Acceso verificado.
5. Deje Definición de la política en blanco. Agregará una política a nivel de grupo en un paso posterior.
6. Seleccione Crear grupo de Acceso verificado.

Paso 4: Creación de un punto de conexión de Acceso verificado

Utilice el siguiente procedimiento para crear un punto de conexión de Acceso verificado. En este paso, se supone que tiene una aplicación que se ejecuta detrás de un equilibrador de carga interno de Elastic Load Balancing y un certificado de dominio público en AWS Certificate Manager.

Para crear un punto de conexión de Acceso verificado

1. En el panel de navegación, seleccione Puntos de conexión de Acceso verificado.
2. Seleccione Crear punto de conexión de Acceso verificado.
3. (Opcional) En Etiqueta de nombre y Descripción, introduzca un nombre y una descripción para el punto de conexión.
4. En Grupo de Acceso verificado, seleccione su grupo de Acceso verificado.
5. En Detalles del punto de conexión, haga lo siguiente:

a. En Protocolo, seleccione HTTPS o HTTP, según la configuración del equilibrador de carga.

b. En Tipo de vinculación, elija VPC.

c. En Tipo de punto de conexión, elija Equilibrador de carga.

d. En Puerto, introduzca el número de puerto utilizado por el oyente del equilibrador de carga. Por ejemplo, 443 en HTTPS u 80 en HTTP.

e. En ARN del equilibrador de carga, elija su equilibrador de carga.

f. En Subredes, seleccione las subredes asociadas a su equilibrador de carga.

g. En Grupos de seguridad, seleccione su grupo de seguridad. El uso del mismo grupo de seguridad para el equilibrador de carga y el punto de conexión permite el tráfico entre ellos. Si prefiere no usar el mismo grupo de seguridad, asegúrese de hacer referencia al grupo de seguridad de punto de conexión desde su equilibrador de carga para que acepte el tráfico procedente del punto de conexión.

h. En Prefijo de dominio del punto de conexión, introduzca un identificador personalizado. Por ejemplo, **`my-ava-app`**. El prefijo se añadirá al nombre DNS que genere Acceso verificado.

6. En Detalles de la aplicación, haga lo siguiente:

   a. En Dominio de la aplicación, introduzca el nombre DNS de la aplicación. Este dominio debe coincidir con el de su certificado de dominio.

   b. En ARN de certificado de dominio, seleccione el nombre de recurso de Amazon (ARN) de su certificado de dominio en AWS Certificate Manager.

7. Deje Detalles de la política en blanco. Agregará una política de acceso a nivel de grupo en un paso posterior.

8. Seleccione Crear punto de conexión de Acceso verificado.

Paso 5: Configuración de DNS para el punto de conexión de Acceso verificado

Para este paso, asigne el nombre de dominio de su aplicación (por ejemplo, www.myapp.example.com) al nombre de dominio de su punto de conexión de Acceso verificado. Para completar la asignación de DNS, cree un registro de nombre canónico (CNAME) con su proveedor de DNS. Tras crear el registro CNAME, todas las solicitudes de los usuarios para su aplicación se enviarán a Acceso verificado.

Obtención del nombre de dominio de su punto de conexión

1. En el panel de navegación, seleccione Puntos de conexión de Acceso verificado.
2. Seleccione el punto de conexión.
3. Elija la pestaña Detalles.
4. Copie el dominio de Dominio de punto de conexión. El siguiente es un ejemplo de nombre de dominio de punto de conexión: `my-ava-app.edge-1a2b3c4d5e6f7g.vai-1a2b3c4d5e6f7g.prod.verified-access.us-west-2.amazonaws.com`.

Siga las instrucciones de su proveedor de DNS para crear un registro CNAME. Use el nombre de dominio de su aplicación como nombre de registro y el nombre de dominio del punto de conexión de Acceso verificado como valor de registro.

Paso 6: Probar la conectividad con la aplicación

Ahora puede probar la conectividad con su aplicación. Introduzca el nombre de dominio de su aplicación en su navegador web. El comportamiento predeterminado de Acceso verificado es denegar todas las solicitudes. Como no agregamos una política de Acceso verificado al grupo o al punto de conexión, se deniegan todas las solicitudes.

Paso 7: Agregar una política de acceso a nivel de grupo de Acceso verificado

Utilice el siguiente procedimiento para modificar el grupo de Acceso verificado y configurar una política de acceso que permita la conectividad con la aplicación. Los detalles de la política dependerán de los usuarios y grupos que estén configurados en el IAM Identity Center. Para obtener más información, consulte Políticas de Acceso verificado.

Modificación de un grupo de Acceso verificado

1. En el panel de navegación, seleccione grupos de Acceso verificado.
2. Seleccione su grupo de .
3. Seleccione Acciones y Modificar la política de grupo de Acceso verificado.
4. Active Habilitar política.

5. Introduzca una política que permita a los usuarios de su IAM Identity Center acceder a su aplicación. Para ver ejemplos, consulta the section called “Ejemplos de políticas”.
6. Seleccione Modificar la política de grupo de Acceso verificado.
7. Ahora que la política de grupo está establecida, repita la prueba del paso anterior para comprobar que se permite la solicitud. Si la solicitud se permite, se le pedirá que inicie sesión en la página de inicio de sesión de IAM Identity Center. Después de proporcionar el nombre de usuario y la contraseña, podrá acceder a la aplicación.

Limpieza de los recursos de Acceso verificado

Cuando acabe este tutorial, utilice el siguiente procedimiento para eliminar los recursos de Acceso verificado.

Eliminación de los recursos de Acceso verificado

1. En el panel de navegación, seleccione Puntos de conexión de Acceso verificado. Seleccione el punto de conexión y elija Acciones, Eliminar punto de conexión de acceso verificado.
2. En el panel de navegación, seleccione grupos de Acceso verificado. Seleccione el grupo y seleccione Acciones, Eliminar grupo de Acceso verificado. Es posible que deba esperar hasta que se complete el proceso de eliminación del punto de conexión.
3. En el panel de navegación, seleccione Instancias de Acceso verificado. Seleccione su instancia y seleccione Acciones, Desasociar proveedor de confianza de acceso verificado. Seleccione el proveedor de confianza y seleccione Desasociar proveedor de confianza de acceso verificado.
4. En el panel de navegación, seleccione Proveedores de confianza de Acceso verificado. Seleccione su proveedor de confianza y elija Acciones, Eliminar proveedor de confianza de acceso verificado.
5. En el panel de navegación, seleccione Instancias de Acceso verificado. Seleccione su instancia y elija Acciones, Eliminar instancia de acceso verificado.

Instancias de Acceso verificado

Una Acceso verificado de AWS instancia es un AWS recurso que le ayuda a organizar sus proveedores de confianza y grupos de acceso verificado. Una instancia evalúa las solicitudes de aplicación y concede el acceso solo cuando se cumplen los requisitos de seguridad.

Tareas

- Creación y administración de una instancia de Acceso verificado
- Eliminación de una instancia de Acceso verificado
- Integre Verified Access con AWS WAF
- Conformidad con las normas FIPS para Acceso verificado

Creación y administración de una instancia de Acceso verificado

Puede usar una instancia de Acceso verificado para organizar sus proveedores de confianza y grupos de Acceso verificado. Utilice los siguientes procedimientos para crear una instancia de Acceso verificado y, a continuación, asociar un proveedor de confianza a Acceso verificado o desasociar un proveedor de confianza de Acceso verificado.

Tareas

- Creación de una instancia de Acceso verificado
- Asociar un proveedor de confianza a una instancia de Acceso verificado
- Desasociar un proveedor de confianza de una instancia de Acceso verificado
- Agrega un subdominio personalizado

Creación de una instancia de Acceso verificado

Utilice el siguiente procedimiento para crear una instancia de Acceso verificado.

Para crear una instancia de acceso verificado mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione instancias de Acceso verificado y, a continuación, Crear instancia de Acceso verificado.

3. (Opcional) En Nombre y Descripción, introduzca un nombre y una descripción para la instancia de Acceso verificado.
4. (Puntos de conexión CIDR de red) En el caso de un subdominio personalizado para un punto de conexión CIDR de red, introduzca un subdominio personalizado.
5. (Opcional) Seleccione Activar los estándares federales de procesos de información (FIPS) si necesita que el acceso verificado cumpla con las normas FIPS.
6. (Opcional) En el caso del proveedor de confianza de Verified Access, elija un proveedor de confianza para adjuntarlo a la instancia de Verified Access.
7. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
8. Seleccione Crear instancia de Acceso verificado.

Para crear una instancia de acceso verificado mediante AWS CLI

Utilice el comando create-verified-access-instance.

Asociar un proveedor de confianza a una instancia de Acceso verificado

Utilice el siguiente procedimiento para asociar un proveedor de confianza a una instancia de Acceso verificado.

Para adjuntar un proveedor de confianza a una instancia de acceso verificado mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Instancias de Acceso verificado.
3. Seleccione la instancia.
4. Seleccione Acciones y Asociar proveedor de confianza de Acceso verificado.
5. Para el Proveedor de confianza de Acceso verificado, seleccione un proveedor de confianza.
6. Seleccione Asociar proveedor de confianza de Acceso verificado.

Para adjuntar un proveedor de confianza a una instancia de acceso verificado mediante AWS CLI

Utilice el comando attach-verified-access-trust-provider.

Desasociar un proveedor de confianza de una instancia de Acceso verificado

Utilice el siguiente procedimiento para desvincular un proveedor de confianza de una instancia de Acceso verificado.

Para separar un proveedor de confianza de una instancia de acceso verificado mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Instancias de Acceso verificado.
3. Seleccione la instancia.
4. Seleccione Acciones y Desvincular proveedor de confianza de Acceso verificado.
5. En el caso del Proveedor de confianza de Acceso verificado, seleccione el proveedor de confianza.
6. Seleccione Desvincular proveedor de confianza de Acceso verificado.

Para separar un proveedor de confianza de una instancia de acceso verificado mediante AWS CLI

Utilice el comando detach-verified-access-trust-provider.

Agrega un subdominio personalizado

Utilice el siguiente procedimiento para añadir o actualizar un subdominio personalizado. Este subdominio solo se usa cuando se crea un punto final CIDR de red.

Para añadir un subdominio personalizado mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Instancias de Acceso verificado.
3. Seleccione la instancia.
4. Elija Acciones, modifique la instancia de acceso verificado.
5. En Subdominio personalizado para punto final CIDR de red, introduzca un subdominio personalizado.
6. Elija Modificar instancia de acceso verificado.

7. Actualice los servidores de nombres de su subdominio e introduzca los servidores de nombres proporcionados por Verified Access. Esta lista está disponible en Servidores de nombres, en la pestaña Detalles de la instancia.

Para añadir un subdominio personalizado mediante AWS CLI

Utilice el comando modify-verified-access-instance.

Eliminación de una instancia de Acceso verificado

Cuando ya no necesite una instancia de Acceso verificado, puede eliminarla. Antes de poder eliminar una instancia, debe eliminar todos los proveedores de confianza o grupos de Acceso verificado asociados.

Para eliminar una instancia de acceso verificado mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Instancias de Acceso verificado.
3. Seleccione la instancia de Acceso verificado.
4. Seleccione Acciones y Eliminar la instancia de Acceso verificado.
5. Cuando se le pida confirmación, ingrese **`delete`** y elija Eliminar.

Para eliminar una instancia de acceso verificado mediante AWS CLI

Utilice el comando delete-verified-access-instance.

Integre Verified Access con AWS WAF

Además de las reglas de autenticación y autorización que impone Acceso verificado, es posible que también desee aplicar protección perimetral. Esto puede ayudarle a proteger sus aplicaciones de amenazas adicionales. Puede lograrlo AWS WAF integrándolo en su implementación de Verified Access. AWS WAF es un firewall de aplicaciones web que le permite supervisar las solicitudes HTTP que se reenvían a los recursos de sus aplicaciones web protegidas. Para obtener más información, consulte la Guía para desarrolladores de AWS WAF.

Puede integrarse AWS WAF con Verified Access asociando una lista de control de acceso AWS WAF web (ACL) a una instancia de Verified Access. Una ACL web es un AWS WAF recurso que

le brinda un control detallado sobre todas las solicitudes web HTTP a las que responde su recurso protegido. Mientras se procesa la solicitud de AWS WAF asociación o disociación, el estado de todos los puntos finales de Verified Access adjuntos a la instancia se muestra como. `updating` Una vez completada la solicitud, el estado vuelve a `active`. Puede ver el estado en el AWS Management Console o describiendo el punto final con el. AWS CLI

El proveedor de confianza de la identidad del usuario determina cuándo AWS WAF inspecciona el tráfico. Si utiliza el Centro de identidad de IAM, AWS WAF inspecciona el tráfico antes de la autenticación del usuario. Si utiliza OpenID Connect (OIDC), AWS WAF inspecciona el tráfico tras la autenticación del usuario.

Contenido

Permisos de IAM necesarios

La integración AWS WAF con Verified Access incluye acciones que solo requieren permisos y que no se corresponden directamente con una operación de API. Estas acciones se indican en la AWS Identity and Access Management Referencia de autorización de servicio con `[permission only]`. Consulta Acciones, recursos y claves de condición de Amazon EC2 en la Referencia de autorización de servicio.

Para trabajar con una ACL web, su AWS Identity and Access Management director debe tener los siguientes permisos.

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

Asocie una ACL AWS WAF web

Los siguientes pasos muestran cómo asociar una lista de control de acceso (ACL) AWS WAF web a una instancia de Verified Access mediante la consola de Verified Access.

Requisito previo

Antes de empezar, cree una ACL AWS WAF web. Para obtener más información, consulte Creación de una ACL web en la Guía para desarrolladores de AWS WAF .

Para asociar una ACL AWS WAF web a una instancia de acceso verificado

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Instancias de Acceso verificado.
3. Seleccione la instancia de Acceso verificado.
4. Elija la pestaña Integraciones.
5. A continuación, elija Acciones y Asociar dirección.
6. Para ACL web, seleccione una ACL web existente y, a continuación, seleccione Asociar ACL web.

Como alternativa, puede utilizar la AWS WAF consola. Si utilizas la AWS WAF consola o la API, necesitas el nombre de recurso de Amazon (ARN) de tu instancia de acceso verificado. El ARN de AVA tiene el siguiente formato: `arn:${Partition}:ec2:${Region}:${Account}:verified-access-instance/${VerifiedAccessInstanceId}`. Para obtener más información, consulte Asociar una ACL web a un AWS recurso en la Guía para AWS WAF desarrolladores.

Comprobación del estado de la asociación

Puede comprobar si una lista de control de acceso (ACL) AWS WAF web está asociada a una instancia de Verified Access o no mediante la consola de Verified Access.

Para ver el estado de la AWS WAF integración con una instancia de acceso verificado

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Instancias de Acceso verificado.
3. Seleccione la instancia de Acceso verificado.
4. Elija la pestaña Integraciones.

5. Compruebe los detalles que figuran en el estado de integración de WAF. El estado se mostrará como Asociado o No asociado, junto con el identificador de ACL web, si está en el estado Asociado.

Desasociar una ACL AWS WAF web

Los siguientes pasos muestran cómo desasociar una lista de control de acceso (ACL) AWS WAF web de una instancia de Verified Access mediante la consola de Verified Access.

Para desasociar una ACL AWS WAF web de una instancia de acceso verificado

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Instancias de Acceso verificado.
3. Seleccione la instancia de Acceso verificado.
4. Elija la pestaña Integraciones.
5. Seleccione Acciones y, a continuación, Desasociar ACL web.
6. Confirme seleccionando Desasociar ACL web.

Como alternativa, puede utilizar la AWS WAF consola. Para obtener más información, consulte Desasociar una ACL web de un AWS recurso en la Guía para AWS WAF desarrolladores.

Conformidad con las normas FIPS para Acceso verificado

El Estándar Federal de Procesamiento de la Información (FIPS) es un estándar gubernamental de EE. UU. y Canadá que especifica los requisitos de seguridad de los módulos criptográficos que protegen la información confidencial. Acceso verificado de AWS ofrece la opción de configurar su entorno para que cumpla con la publicación 140-2 de la FIPS. La conformidad con las normas FIPS para el acceso verificado está disponible en las siguientes regiones: AWS

- Este de EE. UU. (Ohio)
- Este de EE. UU. (Norte de Virginia)
- Oeste de EE. UU. (Norte de California)
- Oeste de EE. UU. (Oregón)
- Canadá (centro)
- AWS GovCloud (US) Oeste

- AWS GovCloud (US) Este

En esta página, se muestra cómo configurar un entorno de Acceso verificado nuevo o existente para que cumpla con las norma FIPS.

Contenido

Configuración de un entorno de Acceso verificado existente para cumplir con las normas FIPS

Si ya tiene un entorno de Acceso verificado y desea configurarlo para que sea compatible con FIPS, será necesario eliminar y volver a crear algunos de los recursos para activar la conformidad con FIPS.

Para volver a configurar un Acceso verificado de AWS entorno existente para que sea compatible con FIPS, siga los pasos que se indican a continuación.

1. Elimine los puntos de conexión, los grupos y la instancia originales de Acceso verificado. Los proveedores de confianza configurados se pueden reutilizar.
2. Cree una instancia de Acceso verificado y asegúrese de habilitar los Estándares federales de procesamiento de la información (FIPS) durante la creación. Además, durante la creación, adjunte el proveedor de confianza de Acceso verificado que desee utilizar seleccionándolo en la lista desplegable.
3. Crear un grupo de Acceso verificado. Durante la creación del grupo, debe asociarlo a la instancia de Acceso verificado que se acaba de crear.
4. Cree uno o más Puntos de conexión de Acceso verificado. Durante la creación de sus puntos de conexión, asócielos al grupo creado en el paso anterior.

Configuración de un nuevo entorno de Acceso verificado para cumplir con las normas FIPS

Para configurar un nuevo Acceso verificado de AWS entorno que sea compatible con FIPS, siga los pasos que se indican a continuación.

1. Configure un proveedor de confianza. Deberá crear un proveedor de confianza de identidad de usuario y (opcionalmente) un proveedor de confianza basado en dispositivos, en función de sus necesidades.
2. Cree una instancia de Acceso verificado y asegúrese de habilitar los Estándares federales de procesamiento de la información (FIPS) durante el proceso. Además, durante la creación, adjunte el proveedor de confianza de Acceso verificado que creó en el paso anterior seleccionándolo en la lista desplegable.
3. Crear un grupo de Acceso verificado. Durante la creación del grupo, debe asociarlo a la instancia de Acceso verificado que se acaba de crear.
4. Cree uno o más Puntos de conexión de Acceso verificado. Durante la creación de sus puntos de conexión, asócielos al grupo creado en el paso anterior.

Proveedores de confianza para Acceso verificado

Un proveedor de confianza es un servicio que envía información sobre los usuarios y los dispositivos a Acceso verificado de AWS. Esta información se denomina contexto de confianza. Pueden incluir atributos basados en la identidad del usuario, como una dirección de correo electrónico o la pertenencia a la organización de ventas, o información del dispositivo, como los parches de seguridad instalados o la versión del software antivirus.

Acceso verificado es compatible con las siguientes categorías de proveedores de confianza:

- Identidad de usuario: servicio de proveedor de identidades (IdP) que almacena y administra las identidades digitales de los usuarios.
- Administración de dispositivos: sistema de administración de dispositivos para dispositivos como ordenadores portátiles, tabletas y teléfonos inteligentes.

Contenido

Proveedores de confianza de identidad de usuarios para Acceso verificado

Puede optar por utilizar un proveedor de confianza de identidad de usuario compatible con OpenID Connect AWS IAM Identity Center o uno compatible.

Contenido

Uso de IAM Identity Center como proveedor de confianza

Puede usarlo AWS IAM Identity Center como su proveedor de confianza de identidad de usuario con Verified Access. AWS

Requisitos y consideraciones previos

- Su instancia de IAM Identity Center debe ser una AWS Organizations instancia. Una instancia de IAM Identity Center con una AWS cuenta independiente no funcionará.
- Su instancia de IAM Identity Center debe estar habilitada en la misma AWS región en la que desea crear el proveedor de confianza de acceso verificado.
- Acceso verificado puede proporcionar acceso a los usuarios de IAM Identity Center que estén asignados a un máximo de 1000 grupos.

Consulte Administrar las instancias de organización y cuenta de IAM Identity Center en la Guía del usuario de AWS IAM Identity Center para obtener más información sobre los distintos tipos de instancias.

Creación de un proveedor de confianza de IAM Identity Center

Una vez que el Centro de Identidad de IAM esté habilitado en su AWS cuenta, puede utilizar el siguiente procedimiento para configurar el Centro de Identidad de IAM como su proveedor de confianza para el acceso verificado.

Para crear un proveedor de confianza del IAM Identity Center (consola)AWS

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione proveedores de confianza de Acceso verificado y, a continuación, Crear proveedor de confianza de Acceso verificado.
3. (Opcional) En Etiqueta de nombre y Descripción, introduzca un nombre y una descripción para el proveedor de confianza.
4. En Nombre de referencia de la política, introduzca un identificador para usarlo más adelante cuando trabaje con las reglas de la política.
5. En Tipo de proveedor de confianza, seleccione Proveedor de confianza de usuarios.
6. En Tipo de proveedor de confianza de usuarios, seleccione IAM Identity Center.
7. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
8. Seleccione Crear un proveedor de confianza de Acceso verificado.

Para crear un proveedor de confianza (AWS CLI) del Centro de Identidad de IAM

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

Eliminación de un proveedor de confianza de IAM Identity Center

Antes de poder eliminar un proveedor de confianza, debe eliminar toda la configuración de punto de conexión y grupo de la instancia a la que está conectado el proveedor de confianza.

Para eliminar un proveedor de confianza del IAM Identity Center (consola)AWS

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione los proveedores de confianza de Acceso verificado y, a continuación, seleccione el proveedor de confianza que desea eliminar en la sección Proveedores de confianza de Acceso verificado.
3. Seleccione Acciones y, a continuación, Eliminar proveedor de confianza de Acceso verificado.
4. Para confirmar la eliminación, ingrese `delete` en el cuadro de texto.
5. Elija Eliminar.

Para eliminar un proveedor de confianza (AWS CLI) de IAM Identity Center

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

Uso de un proveedor de confianza de OpenID Connect

Acceso verificado de AWS admite proveedores de identidad que utilizan métodos estándar de OpenID Connect (OIDC). Con Acceso verificado, puede utilizar proveedores compatibles con OIDC como proveedores de confianza de identidades de usuarios. Sin embargo, debido a la amplia gama de posibles proveedores de OIDC, no puede probar cada AWS integración del OIDC con Verified Access.

Acceso verificado obtiene los datos de confianza que evalúa de los proveedores de OIDC `UserInfo Endpoint`. El parámetro `Scope` se utiliza para determinar qué conjuntos de datos de confianza se recuperarán. Una vez recibidos los datos de confianza, se evalúa la política de Acceso verificado en función de dichos datos.

En el caso de los proveedores de confianza creados después del 24 de febrero de 2025, se incluyen en la `addition_user_context` clave las declaraciones sobre el token de identidad del proveedor de confianza del OIDC.

Dado que los proveedores de confianza se crearon el 24 de febrero de 2025 o antes, Verified Access no utiliza los datos de confianza `ID token` enviados por el proveedor del OIDC. Solo los datos de confianza de `UserInfo Endpoint` se evalúan con respecto a la política.

La duración de la sesión de un proveedor de confianza del OIDC es de 1 día o el tiempo de caducidad indicado en el token de acceso, lo que sea menor. En el caso de los proveedores de confianza creados antes del 24 de febrero de 2025, la duración de la sesión es de 7 días.

Contenido

Requisitos previos para crear un proveedor de confianza de OIDC

Deberá recopilar la siguiente información directamente de su servicio de proveedores de confianza:

- Emisor
- Punto de conexión de autorización
- Punto de conexión de token
- UserInfo endpoint
- ID de cliente
- Secreto del cliente
- Alcance

Creación de un proveedor de confianza de OIDC

Utilice el siguiente procedimiento para crear un OIDC como proveedor de confianza.

Para crear un proveedor de confianza OIDC (consola)AWS

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.

2. En el panel de navegación, seleccione proveedores de confianza de Acceso verificado y, a continuación, Crear proveedor de confianza de Acceso verificado.
3. (Opcional) En Etiqueta de nombre y Descripción, introduzca un nombre y una descripción para el proveedor de confianza.
4. En Nombre de referencia de la política, introduzca un identificador para usarlo más adelante cuando trabaje con las reglas de la política.
5. En Tipo de proveedor de confianza, seleccione Proveedor de confianza de usuarios.
6. En Tipo de proveedor de confianza de usuarios, seleccione OIDC (OpenID Connect).
7. Para OIDC (OpenID Connect), elija el proveedor de confianza.
8. En Emisor, introduzca el identificador del emisor de OIDC.
9. En Punto de conexión de autorización, introduzca la URL completa del punto de conexión de autorización.
10. En Punto de conexión del token, introduzca la URL completa del punto de conexión del token.
11. En Punto de conexión del usuario, introduzca la URL completa del punto de conexión del usuario.
12. (Aplicación nativa OIDC) En el caso de la URL de la clave de firma pública, introduzca la URL completa del punto final de la clave de firma pública.
13. Introduzca el identificador de cliente OAuth 2.0 para el ID de cliente.
14. Introduzca el secreto de cliente OAuth 2.0 como Secreto de cliente.
15. Introduzca una lista de ámbitos delimitados por espacios definidos con su proveedor de identidad. Como mínimo, el openid alcance es obligatorio para Scope.
16. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
17. Seleccione Crear un proveedor de confianza de Acceso verificado.
18. Debe añadir un URI de redireccionamiento a la lista de direcciones permitidas de su proveedor de OIDC.
    - Aplicaciones HTTP: utilice la siguiente URI:. **`https://application_domain/oauth2/idpresponse`** En la consola, puede encontrar el dominio de la aplicación en la pestaña Detalles del punto final de acceso verificado. Al usar el AWS CLI o un AWS SDK, el dominio de la aplicación se incluye en el resultado cuando se describe el punto final de Verified Access.
    - Aplicaciones TCP: utilice el siguiente URI:**`http://localhost:8000`**.

Para crear un proveedor de confianza (CLI AWS) de OIDC

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

Modificación de un proveedor de confianza de OIDC

Después de crear un proveedor de confianza, puede actualizar su configuración.

Para modificar un proveedor de confianza del OIDC (consola)AWS

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Proveedores de confianza de Acceso verificado y, a continuación, seleccione el proveedor de confianza que desee modificar en Proveedores de confianza de Acceso verificado.
3. Seleccione Acciones y, a continuación, Modificar proveedor de confianza de Acceso verificado.
4. Cambie las opciones que desee modificar.
5. Seleccione Modificar proveedor de confianza de Acceso verificado.

Para modificar un proveedor de confianza (CLI AWS) de OIDC

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

Eliminación de un proveedor de confianza de OIDC

Para poder eliminar un proveedor de confianza de usuarios, primero debe eliminar toda la configuración de puntos de conexión y grupos de la instancia a la que está conectado el proveedor de confianza.

Para eliminar un proveedor de confianza del OIDC (consola)AWS

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione los proveedores de confianza de Acceso verificado y, a continuación, seleccione el proveedor de confianza que desea eliminar en la sección Proveedores de confianza de Acceso verificado.
3. Seleccione Acciones y, a continuación, Eliminar proveedor de confianza de Acceso verificado.
4. Para confirmar la eliminación, ingrese `delete` en el cuadro de texto.

5. Elija Eliminar.

Para eliminar un proveedor de confianza (CLI AWS) de OIDC

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

Proveedores de confianza basados en dispositivo para Acceso verificado

Puedes usar proveedores de confianza para dispositivos con acceso AWS verificado. Puede usar uno o varios proveedores de confianza para dispositivos con su instancia de Acceso verificado.

Contenido

Proveedores de confianza de dispositivos compatibles

Los siguientes proveedores de confianza de dispositivos pueden integrarse con Acceso verificado:

- CrowdStrike — Proteger las aplicaciones privadas con CrowdStrike un acceso AWS verificado
- Jamf: Integrar Acceso verificado con Jamf Device Identity
- JumpCloud — Acceso integrado JumpCloud y AWS verificado

Creación de un proveedor de confianza basado en dispositivos

Siga estos pasos para crear y configurar un proveedor de confianza de dispositivos para usarlo con Acceso verificado.

Para crear un proveedor de confianza de dispositivos de acceso verificado (AWS consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.

2. En el panel de navegación, seleccione proveedores de confianza de Acceso verificado y, a continuación, Crear proveedor de confianza de Acceso verificado.
3. (Opcional) En Etiqueta de nombre y Descripción, introduzca un nombre y una descripción para el proveedor de confianza.
4. Introduzca un identificador para usarlo más adelante cuando trabaje con reglas de políticas para el Nombre de referencia de la política.
5. En Tipo de proveedor de confianza, seleccione Identidad de dispositivo.
6. En el tipo de identidad del dispositivo, selecciona Jamf CrowdStrike, o JumpCloud.
7. En Tenant ID, introduzca el identificador de la solicitud de inquilino.
8. (Opcional) En URL de la clave de firma pública, ingrese la URL de clave única compartida por el proveedor de confianza de su dispositivo. (Este parámetro no es obligatorio para Jamf CrowdStrike o Jumpcloud).
9. Seleccione Crear un proveedor de confianza de Acceso verificado.

> **Note**
>
> Deberá añadir un URI de redireccionamiento a la lista de permisos de su proveedor de OIDC. Para ello, querrá utilizar el `DeviceValidationDomain` del punto de conexión de Acceso verificado. Puedes encontrarlo en la AWS Management Console pestaña Detalles de tu terminal de acceso verificado o utilizándola AWS CLI para describir el punto final. Añada lo siguiente a su lista de permitidos de su proveedor de OIDC: https://`DeviceValidationDomain`/oauth2/idpresponse

Para crear un proveedor de confianza de dispositivos (AWS CLI) de acceso verificado

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

Modificación de un proveedor de confianza basado en dispositivos

Después de crear un proveedor de confianza, puede actualizar su configuración.

Para modificar el proveedor de confianza de un dispositivo de acceso verificado (AWS consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.

2. En el panel de navegación, seleccione Proveedores de confianza de Acceso verificado.
3. Seleccione el proveedor de confianza.
4. Seleccione Acciones y, a continuación, seleccione Modificar el proveedor de confianza de Acceso verificado.
5. Modifique la descripción según sea necesario.
6. (Opcional) En URL de la clave de firma pública, modifique la URL de clave única compartida por el proveedor de confianza de su dispositivo. (Este parámetro no es obligatorio si el proveedor de confianza de tu dispositivo es Jamf CrowdStrike o Jumpcloud).
7. Seleccione Modificar proveedor de confianza de Acceso verificado.

Para modificar un proveedor de confianza de dispositivos (AWS CLI) de acceso verificado

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

Eliminación de un proveedor de confianza basado en un dispositivo

Cuando ya no necesite un proveedor de confianza, puede eliminarlo.

Para eliminar un proveedor de confianza de dispositivos de acceso verificado (AWS consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Proveedores de confianza de Acceso verificado.
3. Seleccione el proveedor de confianza que desee eliminar en Proveedores de confianza de Acceso verificado.
4. Seleccione Acciones y, a continuación, seleccione Eliminar el proveedor de confianza de Acceso verificado.
5. Cuando se le pida confirmación, ingrese **`delete`** y elija Eliminar.

Para eliminar un proveedor de confianza de dispositivos (AWS CLI) de acceso verificado

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

Grupos de Acceso verificado

Un grupo de Acceso verificado se compone de puntos de conexión de Acceso verificado y una política de Acceso verificado que se aplica a todos los puntos de conexión del grupo. Al agrupar los puntos de conexión que tienen requisitos de seguridad comunes, puede definir una política de grupo única que cumpla los requisitos de seguridad mínimos de varios puntos de conexión. De este modo, no necesita crear ni mantener una política para cada punto de conexión.

Por ejemplo, puede agrupar todas las aplicaciones de ventas y establecer una política de acceso para todo el grupo. A continuación, puede utilizar esta política para definir un conjunto común de requisitos mínimos de seguridad para todas las aplicaciones de ventas. Este enfoque ayuda a simplificar la administración de políticas.

Cuando crea un grupo, debe asociarlo a una instancia de Acceso verificado. Durante el proceso de creación de un punto de conexión, asociará el punto de conexión a un grupo.

Otra característica de los grupos de acceso verificado es la posibilidad de compartirlos con otras AWS cuentas mediante AWS RAM. Esto le permite crear y administrar grupos de forma centralizada en una cuenta y luego compartirlos con varias cuentas.

Tareas

- Cree y administre un grupo de acceso verificado
- Modificación de una política de grupo de Acceso verificado
- Comparta un grupo de acceso verificado con otro Cuenta de AWS
- Eliminación de un grupo de Acceso verificado

Cree y administre un grupo de acceso verificado

Los grupos de acceso verificado se utilizan para organizar los puntos finales según sus requisitos de seguridad. Al crear un punto final de acceso verificado, lo asocia a un grupo.

Tareas

- Creación de un grupo de Acceso verificado
- Modificar un grupo de acceso verificado

Creación de un grupo de Acceso verificado

Utilice los siguientes procedimientos para crear un grupo de acceso verificado. Antes de crear un grupo de acceso verificado, debe crear una instancia de acceso verificado. Para obtener más información, consulte the section called “ Creación de una instancia de Acceso verificado”.

Para crear un grupo de acceso verificado mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Grupos de Acceso verificado y, a continuación, Crear grupo de Acceso verificado.
3. (Opcional) En Etiqueta de nombre y Descripción, introduzca un nombre y una descripción para el grupo.
4. Para la instancia de Acceso verificado, seleccione una instancia de Acceso verificado para asociarla al grupo.
5. (Opcional) En Definición de la política, introduzca una política de Acceso verificado para aplicarla al grupo.
6. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
7. Seleccione Crear grupo de Acceso verificado.

Para crear un grupo de acceso verificado mediante AWS CLI

Utilice el comando create-verified-access-group.

Modificar un grupo de acceso verificado

Utilice el siguiente procedimiento para modificar un grupo de acceso verificado.

Para modificar un grupo de acceso verificado mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Grupos de Acceso verificado y, a continuación, Crear grupo de Acceso verificado.
3. Seleccione el grupo y, a continuación, elija Acciones, modificar el grupo de acceso verificado.
4. (Opcional) Actualice la descripción.

5. Seleccione Crear grupo de Acceso verificado.
6. Elija la instancia de acceso verificado que desee asociar al grupo.

Para modificar un grupo de acceso verificado mediante el AWS CLI

Utilice el comando modify-verified-access-group.

Modificación de una política de grupo de Acceso verificado

Acceso verificado de AWS permite el acceso a sus aplicaciones en función de las políticas de acceso que cree. Todos los puntos finales del grupo heredan la política de acceso verificado que se adjunta a un grupo. Si lo desea, puede adjuntar políticas específicas de la aplicación a puntos finales específicos.

Utilice el siguiente procedimiento para modificar la política de un grupo de Acceso verificado. Una vez realizados los cambios, pasarán varios minutos antes de que surtan efecto.

Para modificar una política de grupo de acceso verificado mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Grupos de Acceso verificado.
3. Seleccione el grupo de .
4. Seleccione Acciones y Modificar la política de grupo de Acceso verificado.
5. (Opcional) Active o desactive Habilitar política según sea necesario.
6. (Opcional) En Política, introduzca una política de Acceso verificado para aplicarla al grupo.
7. Seleccione Modificar la política de grupo de Acceso verificado.

Para modificar una política de grupo de acceso verificado mediante el AWS CLI

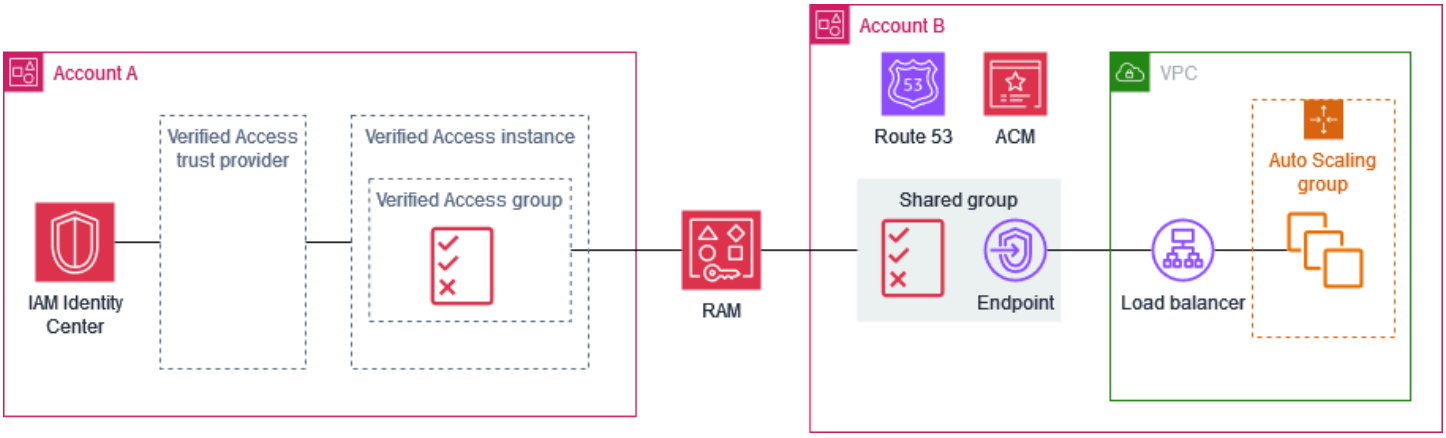
Utilice el comando modify-verified-access-group-policy.

Comparta un grupo de acceso verificado con otro Cuenta de AWS

Cuando compartes un grupo de acceso verificado de tu propiedad con otras AWS cuentas, permites que esas cuentas creen puntos de conexión de acceso verificado en tu grupo. La cuenta en la que se

creó el grupo de Acceso verificado se denomina cuenta de propietario. La cuenta que usa un grupo compartido se denomina cuenta de consumidor.

En el siguiente diagrama, se muestran las ventajas de compartir un grupo de Acceso verificado. El equipo de seguridad central es propietario de la cuenta A. Administra los usuarios y grupos y administra los recursos de acceso verificado necesarios para proporcionar acceso a las aplicaciones internas, como los proveedores de confianza de acceso verificado, las instancias de acceso verificado, los grupos de acceso verificado y las políticas de acceso verificado. AWS IAM Identity Center El equipo de aplicaciones es propietario de la cuenta B. Administra los recursos necesarios para ejecutar su aplicación interna, como el balanceador de carga, el grupo Auto Scaling, la configuración de DNS en Amazon Route 53 y los certificados TLS de AWS Certificate Manager (ACM). Una vez que el equipo de seguridad central comparte un grupo de Acceso verificado con la cuenta B, el equipo de aplicaciones puede crear puntos de conexión de Acceso verificado mediante el grupo compartido. El acceso a la aplicación se permite o deniega en función de las políticas que el equipo de seguridad central haya creado para el grupo de Acceso verificado.



Consideraciones

Las siguientes consideraciones se aplican a los grupos de Acceso verificado compartidos.

Propietarios

- Para compartir un grupo de Acceso verificado, los usuarios deben tener los siguientes permisos: `ec2:PutResourcePolicy` y `ec2:DeleteResourcePolicy`.
- Para compartir un grupo de Acceso verificado, usted debe ser propietario. No puede compartir un grupo de Acceso verificado que se ha compartido con usted.
- Si habilita el uso compartido con las cuentas de su organización, puede compartir recursos, como los grupos de Acceso verificado, sin usar invitaciones. De lo contrario, el consumidor recibirá una

invitación y debe aceptarla para acceder al grupo compartido. Para habilitar el uso compartido, desde la cuenta de administración de su organización, abra la página de configuración de la AWS RAM consola y seleccione Habilitar el uso compartido con. AWS Organizations

- No puede eliminar un grupo si hay puntos de conexión de Acceso verificado asociados. Puede ver los puntos de conexión creados por las cuentas de consumidor en la página Puntos de conexión de Acceso verificado de su cuenta. El ID de cuenta del propietario de un punto de conexión se refleja en el nombre de recurso de Amazon (ARN) del certificado del punto de conexión.

Consumidores

- Para ver los grupos de acceso verificado que se comparten contigo, abre la página de grupos de acceso verificado en la consola o llama describe-verified-access-groups. El ID de cuenta del propietario se refleja en el campo Propietario y en el nombre de recurso de Amazon (ARN) del grupo.
- Al crear un punto de conexión de Acceso verificado, puede especificar cualquier grupo de Acceso verificado que se haya compartido con usted.
- No puede ver los puntos de conexión asociados al grupo compartido de los que usted no es propietario.
- Si el propietario del grupo de Acceso verificado elimina el recurso compartido, no podrá crear un nuevo punto de conexión de Acceso verificado en el grupo. Los puntos de conexión de Acceso verificado que haya creado antes de la eliminación del recurso compartido no se verán afectados por la eliminación. Sin embargo, el propietario del grupo compartido puede eliminar sus puntos de conexión.

Uso compartido de recursos

Para compartir un grupo de Acceso verificado, debe agregarlo a un recurso compartido. Un uso compartido de recursos especifica los recursos que se van a compartir y los consumidores con quienes se comparten.

Para compartir un grupo de acceso verificado mediante la consola

1. Abre la AWS RAM consola en https://console.aws.amazon.com/ram/casa.
2. Si no dispone de un recurso compartido en su organización, cree uno. Para el director, puedes elegir toda la organización, una unidad organizativa o AWS cuentas específicas.
3. Seleccione el recurso compartido y elija Modificar.

4. En `Resources`, elija Grupos de acceso verificado como el tipo de recurso y, a continuación, seleccione el grupo de recursos que desee compartir.
5. Elija Saltar a: Revisar y actualizar.
6. Elija Actualizar recurso compartido.

Para obtener más información, consulte Crear un recurso compartido en la Guía del usuario de AWS RAM .

Eliminación de un grupo de Acceso verificado

Cuando ya no necesite un grupo de Acceso verificado, puede eliminarlo. No puede eliminar un grupo si hay puntos de conexión de Acceso verificado asociados.

Para eliminar un grupo de acceso verificado mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Grupos de Acceso verificado.
3. Seleccione el grupo de .
4. Seleccione Acciones y Eliminar grupo de Acceso verificado.
5. Cuando se le pida confirmación, ingrese **`delete`** y elija Delete (Eliminar).

Para eliminar un grupo de acceso verificado mediante AWS CLI

Utilice el comando delete-verified-access-group.

Puntos de conexión de Acceso verificado

Un punto de conexión de Acceso verificado representa una aplicación. Cada punto de conexión está asociado a un grupo de Acceso verificado y hereda la política de acceso del grupo. Si lo desea, puede adjuntar una política de punto de conexión específica para cada aplicación a cada punto de conexión.

Contenido

Tipos de puntos de conexión de Acceso verificado

Los tipos de puntos de conexión de Acceso verificado posibles son los siguientes:

- Equilibrador de carga: las solicitudes de aplicación se envían a un equilibrador de carga para distribuirlas en su aplicación. Para obtener más información, consulte Creación de un punto de conexión del equilibrador de carga.
- Interfaz de red: las solicitudes de aplicación se envían a una interfaz de red mediante el protocolo y el puerto especificados. Para obtener más información, consulte Creación de un punto de conexión de interfaz de red.
- CIDR de red: las solicitudes de aplicación se envían al bloque CIDR especificado. Para obtener más información, consulte Cree un punto final CIDR de red.
- Amazon Relational Database Service (RDS): las solicitudes de aplicación se envían a una instancia de RDS, un clúster de RDS o un proxy de base de datos de RDS. Para obtener más información, consulte Creación de un punto final de Amazon Relational Database Service.

Cómo funciona Verified Access con redes compartidas y subredes VPCs

Los siguientes son los comportamientos relacionados con las subredes de VPC compartidas:

- Los puntos de conexión de Acceso verificado son compatibles con el uso compartido de subredes de VPC. Un participante puede crear un punto de conexión de Acceso verificado en una subred compartida.
- El participante que creó el punto de conexión será el propietario del punto de conexión y el único autorizado a modificarlo. El propietario de la VPC no podrá modificar el punto de conexión.
- Los puntos finales de acceso verificado no se pueden crear en una zona AWS local y, por lo tanto, no es posible compartirlos a través de zonas locales.

Para obtener más información, consulte Compartir su VPC con otras cuentas en la Guía del usuario de Amazon VPC.

Creación de un punto de conexión del equilibrador de carga para Acceso verificado

Utilice el siguiente procedimiento para crear un punto de conexión del equilibrador de carga para Acceso verificado. Para obtener más información sobre los equilibradores de carga, consulte la Guía del usuario de Elastic Load Balancing.

Requisitos

- Solo se admite el IPv4 tráfico.
- Las conexiones HTTPS de larga duración, como WebSocket las conexiones, solo se admiten a través de TCP.
- El equilibrador de carga debe ser un equilibrador de carga de aplicación o un equilibrador de carga de red y debe ser un equilibrador de carga interno.
- El equilibrador de carga y las subredes deben pertenecer a la misma nube privada virtual (VPC).
- Los equilibradores de carga HTTPS pueden usar certificados TLS públicos o autofirmados. Utilice un certificado RSA con una longitud de clave de 1024 o 2048.
- Antes de crear un punto final de acceso verificado, debe crear un grupo de acceso verificado. Para obtener más información, consulte the section called “Creación de un grupo de Acceso verificado”.

- Debe proporcionar un nombre de dominio para su aplicación. Se trata del nombre DNS público que utilizarán los usuarios para acceder a su aplicación. También tendrá que proporcionar un certificado SSL público con una CN que coincida con este nombre de dominio. Puede crear o importar el certificado utilizando AWS Certificate Manager.

Para crear un punto final del equilibrador de carga mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Puntos de conexión de Acceso verificado.
3. Seleccione Crear punto de conexión de Acceso verificado.
4. (Opcional) En Etiqueta de nombre y Descripción, introduzca un nombre y una descripción para el punto de conexión.
5. Para el grupo de acceso verificado, elija un grupo de acceso verificado.
6. En Detalles del punto de conexión, haga lo siguiente:
   a. En Protocolo, elija un protocolo.
   b. En Tipo de vinculación, elija VPC.
   c. En Tipo de punto de conexión, elija Equilibrador de carga.
   d. (HTTP/HTTPS) En Puerto, introduzca el número de puerto. (TCP) Para los rangos de puertos, introduzca un rango de puertos y elija Agregar puerto.
   e. Para el ARN del balanceador de carga, elige un balanceador de carga.
   f. En Subred, elija las subredes. Puede especificar solo una subred por zona de disponibilidad.
   g. En Grupos de seguridad, elija los grupos de seguridad para el punto de conexión. Estos grupos de seguridad controlan el tráfico entrante y saliente del punto final de acceso verificado.
   h. En Prefijo del dominio del punto de conexión, introduzca un identificador personalizado que se anteponga al nombre DNS que Acceso verificado genera para el punto de conexión.
7. (HTTP/HTTPS) Para obtener los detalles de la aplicación, haga lo siguiente:
   a. En Dominio de la aplicación, introduzca un nombre DNS para la aplicación.
   b. En Certificado de dominio ARN, elige un certificado TLS público.
8. (Opcional) En Definición de la política, introduzca una política de Acceso verificado para el punto de conexión.

9. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
10. Seleccione Crear punto de conexión de Acceso verificado.

Para crear un punto final de acceso verificado mediante el AWS CLI

Utilice el comando create-verified-access-endpoint.

Creación de un punto de conexión de la interfaz de red para Acceso verificado

Utilice el siguiente procedimiento para crear un punto de conexión de interfaz de red.

Requisitos

- Solo se admite el IPv4 tráfico.
- La interfaz de red debe pertenecer a la misma nube privada virtual (VPC) que los grupos de seguridad.
- Usamos la IP privada de la interfaz de red para reenviar el tráfico.
- Antes de crear un punto final de acceso verificado, debe crear un grupo de acceso verificado. Para obtener más información, consulte the section called “Creación de un grupo de Acceso verificado”.
- Debe proporcionar un nombre de dominio para su aplicación. Se trata del nombre DNS público que utilizarán los usuarios para acceder a su aplicación. También tendrá que proporcionar un certificado SSL público con una CN que coincida con este nombre de dominio. Puede crear o importar el certificado utilizando AWS Certificate Manager.

Para crear un punto final de interfaz de red mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Puntos de conexión de Acceso verificado.
3. Seleccione Crear punto de conexión de Acceso verificado.
4. (Opcional) En Etiqueta de nombre y Descripción, introduzca un nombre y una descripción para el punto de conexión.
5. Para el grupo de acceso verificado, elija un grupo de acceso verificado.

6. En Detalles del punto de conexión, haga lo siguiente:
   a. En Protocolo, elija un protocolo.
   b. En Tipo de vinculación, elija VPC.
   c. En Tipo de punto de conexión, elija Interfaz de red.
   d. (HTTP/HTTPS) En Puerto, introduzca el número de puerto. (TCP) Para los rangos de puertos, introduzca un rango de puertos y elija Agregar puerto.
   e. En Interfaz de red, elija una interfaz de red.
   f. En Grupos de seguridad, elija los grupos de seguridad para el punto de conexión. Estos grupos de seguridad controlan el tráfico entrante y saliente del punto final de acceso verificado.
   g. En Prefijo del dominio del punto de conexión, introduzca un identificador personalizado que se anteponga al nombre DNS que Acceso verificado genera para el punto de conexión.
7. (HTTP/HTTPS) Para obtener los detalles de la aplicación, haga lo siguiente:
   a. En Dominio de la aplicación, introduzca un nombre DNS para la aplicación.
   b. En Certificado de dominio ARN, elige un certificado TLS público.
8. (Opcional) En Definición de la política, introduzca una política de Acceso verificado para el punto de conexión.
9. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
10. Seleccione Crear punto de conexión de Acceso verificado.

Para crear un punto final de acceso verificado mediante el AWS CLI

Utilice el comando create-verified-access-endpoint.

Cree un punto final CIDR de red para el acceso verificado

Utilice el siguiente procedimiento para crear un punto final CIDR de red. Por ejemplo, puede usar un punto final CIDR de red para permitir el acceso a las EC2 instancias de una subred específica a través del puerto 22 (SSH).

Requisitos

- Solo se admite el protocolo TCP.

- El acceso verificado proporciona un registro DNS para cada dirección IP del rango CIDR que utilice un recurso. Si eliminas un recurso, su dirección IP deja de estar en uso y Verified Access elimina el registro DNS correspondiente.
- Si especificas un subdominio personalizado, Verified Access proporciona registros DNS para cada dirección IP utilizada en el subdominio y te proporciona las direcciones IP de sus servidores DNS. Puede configurar una regla de reenvío para que su subdominio apunte a los servidores DNS de Verified Access. Los servidores DNS de Verified Access resuelven cualquier solicitud realizada a un registro del dominio en la dirección IP del recurso solicitado.
- Antes de crear un punto final de acceso verificado, debe crear un grupo de acceso verificado. Para obtener más información, consulte the section called “Creación de un grupo de Acceso verificado”.
- Cree el punto final y, a continuación, conéctese a la aplicación medianteCliente de conectividad.

Para crear un punto final CIDR de red mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Puntos de conexión de Acceso verificado.
3. Seleccione Crear punto de conexión de Acceso verificado.
4. (Opcional) En Etiqueta de nombre y Descripción, introduzca un nombre y una descripción para el punto de conexión.
5. En Grupo de Acceso verificado, seleccione un grupo de Acceso verificado para el punto de conexión.
6. En Detalles del punto de conexión, haga lo siguiente:
    a. En Protocol, seleccione TCP.
    b. En Tipo de vinculación, elija VPC.
    c. Para el tipo de punto final, elija CIDR de red.
    d. Para los rangos de puertos, introduzca un rango de puertos y elija Agregar puerto.
    e. En Subred, elija las subredes.
    f. En Grupos de seguridad, elija los grupos de seguridad para el punto de conexión. Estos grupos de seguridad controlan el tráfico entrante y saliente del punto final de acceso verificado.
    g. (Opcional) En el prefijo de dominio del punto final, introduzca un identificador personalizado que se anteponga al nombre DNS que Verified Access genera para el punto final.

7. (Opcional) En Definición de la política, introduzca una política de Acceso verificado para el punto de conexión.
8. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
9. Seleccione Crear punto de conexión de Acceso verificado.

Para crear un punto final de acceso verificado mediante el AWS CLI

Utilice el comando create-verified-access-endpoint.

Cree un punto final de Amazon Relational Database Service para el acceso verificado

Utilice el siguiente procedimiento para crear un punto final de Amazon Relational Database Service (RDS) (RDS).

Requisitos

- Solo se admite el protocolo TCP.
- Cree una instancia de RDS, un clúster de RDS o un proxy de base de datos de RDS.
- Antes de crear un punto final de acceso verificado, debe crear un grupo de acceso verificado. Para obtener más información, consulte the section called “Creación de un grupo de Acceso verificado”.
- Cree el punto final y, a continuación, conéctese a la aplicación mediante Cliente de conectividad.

Para crear un punto final de Amazon Relational Database Service mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Puntos de conexión de Acceso verificado.
3. Seleccione Crear punto de conexión de Acceso verificado.
4. (Opcional) En Etiqueta de nombre y Descripción, introduzca un nombre y una descripción para el punto de conexión.
5. En Grupo de Acceso verificado, seleccione un grupo de Acceso verificado para el punto de conexión.
6. En Detalles del punto de conexión, haga lo siguiente:

a. En Protocol, seleccione TCP.

b. En Tipo de vinculación, elija VPC.

c. Para el tipo de punto final, elija Amazon Relational Database Service (RDS).

d. Para el tipo de destino RDS, realice una de las siguientes acciones:

   - Elija una instancia de RDS y, a continuación, elija una instancia de RDS de una instancia de RDS.
   - Elija un clúster de RDS y, a continuación, elija un clúster de RDS del clúster de RDS.
   - Elija el proxy de base de datos RDS y, a continuación, elija un proxy de base de datos RDS del proxy de base de datos RDS.

e. Para el punto final de RDS, elija un punto final de RDS relacionado con el recurso de RDS que eligió en el paso anterior.

f. En Puerto, escriba el número de puerto.

g. En Subred, elija las subredes. Puede especificar solo una subred por zona de disponibilidad.

h. En Grupos de seguridad, elija los grupos de seguridad para el punto de conexión. Estos grupos de seguridad controlan el tráfico entrante y saliente del punto final de acceso verificado.

i. (Opcional) En el prefijo de dominio del punto final, introduzca un identificador personalizado que se anteponga al nombre DNS que Verified Access genera para el punto final.

7. (Opcional) En Definición de la política, introduzca una política de Acceso verificado para el punto de conexión.
8. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
9. Seleccione Crear punto de conexión de Acceso verificado.

Para crear un punto final de acceso verificado mediante el AWS CLI

Utilice el comando create-verified-access-endpoint.

Cómo permitir el tráfico que se origina en su punto de conexión de Acceso verificado

Puede configurar los grupos de seguridad de sus aplicaciones para que permitan el tráfico que se origine en su punto de conexión de Acceso verificado. Para ello, agregue una regla de entrada que especifique el grupo de seguridad del punto de conexión como origen. Le recomendamos que elimine cualquier regla de entrada adicional para que su aplicación reciba tráfico únicamente desde su punto de conexión de Acceso verificado.

Le recomendamos que utilice las reglas de salida existentes.

Para actualizar las reglas del grupo de seguridad de su aplicación mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Puntos de conexión de Acceso verificado.
3. Elija el punto de acceso verificado, busque el grupo de seguridad IDs en la pestaña Detalles y copie el ID del grupo de seguridad de su punto final.
4. En el panel de navegación, selecciona Grupos de seguridad.
5. Seleccione la casilla de verificación del grupo de seguridad asociado a su objetivo y, a continuación, seleccioneAcciones, Editar reglas de entrada.
6. Para añadir una regla de grupo de seguridad que permita el tráfico que se origine en su punto de conexión de Acceso verificado, haga lo siguiente:
    a. Seleccione Agregar regla.
    b. En Tipo, elija Todo el tráfico o un tráfico específico que desee permitir.
    c. En Fuente, elija Personalizada y pegue el ID del grupo de seguridad de su punto de conexión.
7. (Opcional) Para exigir que el tráfico se origine únicamente en su punto de conexión de Acceso verificado, elimine cualquier otra regla de grupo de seguridad entrante.
8. Seleccione Guardar reglas.

Para actualizar las reglas de los grupos de seguridad de su aplicación mediante el AWS CLI

Utilice el describe-verified-access-endpointscomando para obtener el ID del grupo de seguridad y, a continuación, utilice el authorize-security-group-ingresscomando para añadir una regla de entrada.

Modificación de un punto de conexión de Acceso verificado

Utilice el siguiente procedimiento para modificar un punto de conexión de Acceso verificado.

Para modificar un punto final de acceso verificado mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Puntos de conexión de Acceso verificado.
3. Seleccione el punto de conexión.
4. Seleccione Acciones, Modificar el punto de conexión de Acceso verificado.
5. Modifique los detalles del punto de conexión según sea necesario.
6. Seleccione Modificar el punto de conexión de Acceso verificado.

Para modificar un punto final de acceso verificado mediante el AWS CLI

Utilice el comando modify-verified-access-endpoint.

Modificación de una política de punto de conexión de Acceso verificado

Utilice los siguientes procedimientos para modificar la política de un punto de conexión de Acceso verificado. Una vez realizados los cambios, pasarán varios minutos antes de que surtan efecto.

Para modificar una política de puntos finales de acceso verificado mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Puntos de conexión de Acceso verificado.
3. Seleccione el punto de conexión.
4. Seleccione Acciones y Modificar la política de puntos de conexión de Acceso verificado.
5. (Opcional) Active o desactive Habilitar política según sea necesario.
6. (Opcional) En Política, introduzca una política de Acceso verificado para aplicarla al punto de conexión.
7. Seleccione Modificar la política de puntos de conexión de Acceso verificado.

Para modificar una política de puntos finales de acceso verificado mediante el AWS CLI

Utilice el comando modify-verified-access-endpoint-policy.

Eliminación de un punto de conexión de Acceso verificado

Cuando ya no necesite un punto de conexión de Acceso verificado, puede eliminarlo.

Para eliminar un punto final de acceso verificado mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Puntos de conexión de Acceso verificado.
3. Seleccione el punto de conexión.
4. Seleccione Acciones, Eliminar punto de conexión de Acceso verificado.
5. Cuando se le pida confirmación, ingrese **`delete`** y elija Eliminar.

Para eliminar un punto final de acceso verificado mediante el AWS CLI

Utilice el comando delete-verified-access-endpoint.

Datos de confianza enviados a Acceso verificado desde proveedores de confianza

Los datos de confianza son datos que se envían Acceso verificado de AWS desde un proveedor de confianza. Los datos de confianza también se conocen como “notificaciones de usuario” o “contexto de confianza”. Los datos generalmente incluyen información sobre un usuario o un dispositivo. Algunos ejemplos de datos de confianza son el correo electrónico del usuario, la pertenencia a un grupo, la versión del sistema operativo del dispositivo, el estado de seguridad del dispositivo, etc. La información que se envía varía en función del proveedor de confianza, por lo que debe consultar la documentación del proveedor de confianza para obtener una lista completa y actualizada de los datos de confianza.

Sin embargo, al utilizar las funciones de registro de Acceso verificado, también puede ver qué datos de confianza envía su proveedor de confianza. Esto puede resultar útil al definir políticas que permitan o denieguen el acceso a las aplicaciones. Para obtener información sobre cómo incluir el contexto de confianza en sus registros, consulte Habilitación o deshabilitación del contexto de confianza de Acceso verificado.

Esta sección contiene una muestra de datos de confianza y ejemplos para ayudarle a empezar a redactar políticas. La información que se proporciona aquí tiene únicamente fines ilustrativos y no es una referencia oficial.

Contenido

Contexto predeterminado para datos de confianza de Acceso verificado

Acceso verificado de AWS incluye algunos elementos sobre la solicitud actual de forma predeterminada en todas las evaluaciones de Cedar, independientemente de los proveedores de confianza configurados. Si lo desea, puede escribir una política que evalúe en función de los datos que usted seleccione.

Los siguientes son ejemplos de los datos que se incluyen en la evaluación.

Ejemplos

- Solicitud HTTP
- Flujo TCP

Solicitud HTTP

Cuando se evalúa una política, Verified Access incluye datos sobre la solicitud HTTP actual en el contexto de Cedar bajo la `context.http_request` clave.

```
{
    "title": "HTTP Request data included by Verified Access",
    "type": "object",
    "properties": {
        "http_method": {
            "type": "string",
            "description": "The HTTP method",
            "example": "GET"
        },
        "hostname": {
            "type": "string",
            "description": "The host subcomponent of the authority component of the
 URI",
            "example": "example.com"
        },
        "path": {
            "type": "string",
            "description": "The path component of the URI",
            "example": "app/images"
        },
        "query": {
            "type": "string",
            "description": "The query component of the URI",
            "example": "value1=1&value2=2"
        },
        "x_forwarded_for": {
            "type": "string",
            "description": "The value of the X-Forwarded-For request header",
            "example": "17.7.7.1"
        },
```

```
        "port": {
           "type": "integer",
           "description": "The endpoint port",
           "example": 443
        },
        "user_agent": {
            "type": "string",
            "description": "The value of the User-Agent request header",
            "example": "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0)
 Gecko/20100101 Firefox/47.0"
        },
        "client_ip": {
            "type": "string",
            "description": "The IP address connecting to the endpoint",
            "example": "15.248.6.6"
        }
    }
}
```

Ejemplo de política

El siguiente es un ejemplo de una política de Cedar que utiliza los datos de la solicitud HTTP.

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

Flujo TCP

Cuando se evalúa una política, Verified Access incluye datos sobre el flujo TCP actual en el contexto de Cedar bajo la `context.tcp_flow` clave.

```
{
    "title": "TCP flow data included by Verified Access",
    "type": "object",
    "properties": {
        "destination_ip": {
            "type": "string",
            "description": "The IP address of the target",
            "example": "192.100.1.3"
        },
```

```
        "destination_port": {
            "type": "string",
            "description": "The target port",
            "example": 22
        },
        "client_ip": {
            "type": "string",
            "description": "The IP address connecting to the endpoint",
            "example": "172.154.16.9"
        }
    }
}
```

AWS IAM Identity Center contexto para los datos de confianza de Verified Access

Cuando se evalúa una política, si la define AWS IAM Identity Center como un proveedor de confianza, Acceso verificado de AWS incluye los datos de confianza del contexto de Cedar bajo la clave que especifique como «nombre de referencia de la política» en la configuración del proveedor de confianza. Si lo desea, puede escribir una política que evalúe los datos de confianza.

> **Note**
>
> La clave de contexto de su proveedor de confianza proviene del nombre de referencia de la política que configuró al crear el proveedor de confianza. Por ejemplo, si configura el nombre de referencia de la política como «idp123», la clave de contexto será «context.idp123». Compruebe que está utilizando la clave de contexto correcta al crear la política.

El siguiente esquema JSON muestra los datos que se incluyen en la evaluación.

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

El siguiente es un ejemplo de política que se evalúa en función de los datos de confianza proporcionados por 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 los nombres de los grupos se pueden cambiar, IAM Identity Center hace referencia a los grupos utilizando su ID de grupo. Esto ayuda a evitar infringir una declaración de política al cambiar el nombre de un grupo.

Contexto de proveedor de confianza externo para datos de confianza de Acceso verificado

En esta sección se describen los datos de confianza proporcionados Acceso verificado de AWS por los proveedores de confianza externos.

> **Note**
>
> La clave de contexto de su proveedor de confianza proviene del nombre de referencia de la política que configuró al crear el proveedor de confianza. Por ejemplo, si configura el nombre de referencia de la política como «idp123», la clave de contexto será «context.idp123». Asegúrese de utilizar la clave de contexto correcta al crear la política.

Contenido

Extensión del navegador

Si planea incorporar el contexto de confianza de los dispositivos en sus políticas de acceso, necesitará la extensión de navegador AWS Verified Access o la extensión de navegador de otro socio. Actualmente, Acceso verificado es compatible con los navegadores Google Chrome y Mozilla Firefox.

Actualmente, admitimos tres proveedores de confianza de dispositivos: Jamf (que es compatible con dispositivos macOS), CrowdStrike (que es compatible con dispositivos con Windows 11 y Windows 10) y JumpCloud (que es compatible con Windows y macOS).

- Si utilizas los datos de confianza de Jamf en tus políticas, tus usuarios deberán descargar e instalar la extensión del Acceso verificado de AWS navegador desde la tienda web de Chrome o desde el sitio de complementos de Firefox en sus dispositivos.
- Si utilizas datos de CrowdStrikeconfianza en tus políticas, primero los usuarios deben instalar el servidor de mensajería Acceso verificado de AWS nativo (enlace de descarga directa). Este componente es necesario para obtener los datos de confianza del CrowdStrike agente que se ejecuta en los dispositivos de los usuarios. A continuación, tras instalar este componente, los usuarios deben instalar la extensión del Acceso verificado de AWS navegador desde la tienda web de Chrome o desde el sitio de complementos de Firefox en sus dispositivos.
- Si lo utilizas JumpCloud, tus usuarios deben tener instalada en sus dispositivos la extensión de JumpCloud navegador de la tienda web de Chrome o del sitio de complementos de Firefox.

Jamf

Jamf es un proveedor de confianza de terceros. Al evaluar una política, si define a Jamf como un proveedor de confianza, Acceso verificado incluirá los datos de confianza en el contexto de Cedar bajo la clave que especifique como «nombre de referencia de la política» en la configuración del proveedor de confianza. Si lo desea, puede escribir una política que evalúe los datos de confianza. El siguiente esquema JSON muestra los datos que se incluyen en la evaluación.

Para obtener más información sobre el uso de Jamf con Acceso verificado, consulte Integrar Acceso verificado de AWS con Jamf Device Identity en el sitio web de Jamf.

```
{
    "title": "Jamf device data specification",
    "type": "object",
    "properties": {
```

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

```
}
```

El siguiente es un ejemplo de política que se evalúa en función de los datos de confianza proporcionados por Jamf.

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

Cedar proporciona una función `.contains()` útil para ayudar con enumeraciones como la puntuación de riesgo de Jamf.

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

CrowdStrike

CrowdStrike es un proveedor de confianza externo. Cuando se evalúa una política, si la define CrowdStrike como un proveedor de confianza, Verified Access incluye los datos de confianza en el contexto de Cedar bajo la clave que especifique como «nombre de referencia de la política» en la configuración del proveedor de confianza. Si lo desea, puede escribir una política que evalúe los datos de confianza. El siguiente esquema JSON muestra los datos que se incluyen en la evaluación.

Para obtener más información sobre su uso CrowdStrike con Verified Access, consulte Proteger aplicaciones privadas con CrowdStrike y Acceso verificado de AWS en el GitHub sitio web.

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

```
          "type": "integer",
          "description": "A single metric, between 1-100, that accounts for the OS-
specific settings monitored on the host"
        },
        "sensor_config": {
          "type": "integer",
          "description": "A single metric, between 1-100, that accounts for the
 different sensor policies monitored on the host"
        },
        "version": {
          "type": "string",
          "description": "The version of the scoring algorithm being used"
        }
      }
    },
    "cid": {
      "type": "string",
      "description": "Customer ID (CID) unique to the customer's environment"
    },
    "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"
    }
  }
}
```

El siguiente es un ejemplo de política que se evalúa en función de los datos de confianza proporcionados por CrowdStrike.

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

JumpCloud

JumpCloud es un proveedor de confianza externo. Cuando se evalúa una política, si la define JumpCloud como un proveedor de confianza, Verified Access incluye los datos de confianza en el contexto de Cedar bajo la clave que especifique como «nombre de referencia de la política» en la configuración del proveedor de confianza. Si lo desea, puede escribir una política que evalúe los datos de confianza. El siguiente esquema JSON muestra los datos que se incluyen en la evaluación.

Para obtener más información sobre su uso JumpCloud con AWS Verified Access, consulte Integration JumpCloud and AWS Verified Access en el JumpCloud sitio web.

```
{
  "title": "JumpCloud device data specification",
  "type": "object",
  "properties": {
    "device": {
      "type": "object",
      "description": "Properties of the device",
      "properties": {
        "is_managed": {
          "type": "boolean",
          "description": "Boolean to indicate if the device is under management"
        }
      }
```

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

El siguiente es un ejemplo de una política que se evalúa en función del contexto de confianza proporcionado por JumpCloud.

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

Transferencia de las notificaciones de usuario y verificación de firmas en Acceso verificado

Una vez que una Acceso verificado de AWS instancia autentica a un usuario correctamente, envía las reclamaciones del usuario recibidas del IdP al punto final de Verified Access. Las notificaciones de usuario se firman para que las aplicaciones puedan verificar las firmas y confirmar que las notificaciones fueron enviadas por Acceso verificado. Durante este proceso, se agrega el siguiente encabezado HTTP:

`x-amzn-ava-user-context`

Este encabezado contiene las notificaciones de los usuarios en formato de token web JSON (JWT). El formato JWT incluye un encabezado, una carga y una firma que tienen codificación de URL en base64. Verified Access utiliza ES384 (el algoritmo de firma ECDSA que utiliza el algoritmo de hash SHA-384) para generar la firma JWT.

Las aplicaciones pueden usar estas notificaciones para personalizar o para realizar otras experiencias específicas del usuario. Los desarrolladores de aplicaciones deben informarse sobre el nivel de exclusividad y verificación de cada notificación proporcionada por el proveedor de identidad antes de utilizarla. En general, la reclamación `sub` es la mejor forma de identificar a un usuario determinado.

Contenido

Ejemplo: JWT firmado para las notificaciones de usuarios de OIDC

Los siguientes ejemplos muestran el aspecto que tendrán el encabezado y la carga útil de las notificaciones de los usuarios de OIDC en el formato JWT.

Encabezado de ejemplo:

```
{
   "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)
}
```

Ejemplo de carga:

```
{
   "sub": "xyzsubject",
   "email": "xxx@amazon.com",
   "email_verified": true,
   "groups": [
      "Engineering",
      "finance"
   ],
   "additional_user_context": {
      "aud": "xxx",
      "exp": 1000000000,
      "groups": [
         "group-id-1",
         "group-id-2"
      ],
      "iat": 1000000000,
      "iss": "https://oidc-tp.com/",
      "sub": "xyzsubject",
      "ver": "1.0"
   }
}
```

Ejemplo: JWT firmado para las notificaciones de los usuarios de IAM Identity Center

Los siguientes ejemplos muestran el aspecto que tendrán el encabezado y la carga útil de las notificaciones de los usuarios de IAM Identity Center en el formato JWT.

> **Note**
>
> En el caso de IAM Identity Center, en las notificaciones solo se incluirá la información del usuario.

Encabezado de ejemplo:

```
{
   "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)
}
```

Ejemplo de carga:

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

Claves públicas

Como las instancias de Acceso verificado no cifran las notificaciones de los usuarios, le recomendamos que configure los puntos de conexión de Acceso verificado para que usen HTTPS. Si configura el punto de conexión de Acceso verificado para que utilice HTTP, asegúrese de restringir el tráfico al punto de conexión mediante grupos de seguridad.

Para garantizar la seguridad, debe verificar la firma antes de realizar cualquier autorización basada en las notificaciones y validar que el campo `signer` del encabezado JWT contenga el ARN esperado de la instancia de Acceso verificado.

Para obtener la clave pública, obtenga el ID de clave del encabezado JWT y utilícelo para buscar la clave pública desde el siguiente punto de conexión regional.

El punto final de cada uno es el siguiente: Región de AWS

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

Ejemplo: recuperación y decodificación de JWT

El siguiente ejemplo de código muestra cómo obtener la identificación de clave, la clave pública y la carga en Python 3.9:

```
import jwt
import requests
import base64
import json

# Step 1: Validate the signer
expected_verified_access_instance_arn = 'arn:aws:ec2:region-code:account-id:verified-
access-instance/verified-access-instance-id'

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)
received_verified_access_instance_arn = decoded_json['signer']

assert expected_verified_access_instance_arn == received_verified_access_instance_arn,
 "Invalid Signer"

# Step 2: Get the key id from JWT headers (the kid field)
kid = decoded_json['kid']

# Step 3: 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 4: Get the payload
payload = jwt.decode(encoded_jwt, pub_key, algorithms=['ES384'])
```

Políticas de Acceso verificado

Acceso verificado de AWS las políticas le permiten definir reglas para acceder a las aplicaciones alojadas en ellas AWS. Están escritas en cedro, un lenguaje AWS de políticas. Con Cedar, puede crear políticas que se evalúen en función de los datos de confianza enviados desde los proveedores de confianza basados en identidades o dispositivos que configure para utilizar con Acceso verificado.

Para obtener información más detallada sobre el lenguaje de las políticas de Cedar, consulte la Guía de referencia de Cedar.

Al crear un grupo de Acceso verificado o un punto de conexión de Acceso verificado, tiene la opción de definir la política de Acceso verificado. Puede crear un grupo o un punto de conexión sin definir la política de Acceso verificado, pero todas las solicitudes de acceso se bloquearán hasta que defina una política. De forma alternativa, puede añadir o cambiar una política en un grupo o punto de conexión de Acceso verificado existente una vez creado.

Contenido

Estructura de declaración de política de Acceso verificado

En la siguiente tabla se muestra la estructura de una política de Acceso verificado.

Componente	Sintaxis
effect	`permit | forbid`
scope	`(principal, action, resource)`
cláusula de condición	`when {`

Componente	Sintaxis
	context.*policy-reference-name* .*attribute-name* };

Componentes de política

Una política de Acceso verificado contiene los siguientes componentes:

- Efecto: `permit` (permitir) o `forbid` (denegar) el acceso.
- Alcance: las entidades principales, las acciones y los recursos a los que se aplica el efecto. Puede dejar el alcance de Cedar sin definir si no identifica entidades principales, acciones o recursos específicos. En este caso, la política se aplica a todas las entidades principales, acciones y recursos posibles.
- Cláusula de condición: el contexto en el que se aplica el efecto.

> **Important**
>
> En el caso de Acceso verificado, las políticas se expresan en su totalidad haciendo referencia a los datos de confianza de la cláusula de condición. El alcance de la política debe mantenerse siempre indefinido. A continuación, puede especificar el acceso mediante el contexto de identidad y confianza del dispositivo en la cláusula de condición.

Comentarios

Puede incluir comentarios en sus Acceso verificado de AWS políticas. Los comentarios se definen como una línea que comienza por `//` y termina con un carácter de nueva línea.

En el siguiente ejemplo se muestran comentarios en una política.

```
// grants access to users in a specific domain using 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)
};
```

Cláusulas múltiples

Puede utilizar más de una cláusula de condición en una declaración de política mediante el operador &&.

```
permit(principal,action,resource)
when{
 context.policy-reference-name.attribute1 &&
 context.policy-reference-name.attribute2
};
```

Para ver otros ejemplos, consulte Ejemplos de políticas de Acceso verificado.

Caracteres reservados

El siguiente ejemplo muestra cómo escribir una política si una propiedad de contexto utiliza un : (punto y coma), que es un carácter reservado en el lenguaje de la política.

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

Operadores integrados para políticas de Acceso verificado

Al crear el contexto de una Acceso verificado de AWS política con varias condiciones, como se explica enEstructura de declaración de política de Acceso verificado, puede utilizar el && operador para añadir condiciones adicionales. También hay muchos otros operadores integrados que puede utilizar para añadir un poder de expresión adicional a las condiciones de su política. La siguiente tabla contiene todos los operadores integrados como referencia.

Operador	Tipos y sobrecargas	Descripción
!	Booleano → Booleano	Not lógico.

Operador	Tipos y sobrecargas	Descripción
==	any → any	Igualdad. Funciona con argumentos de cualquier tipo, incluso si los tipos no coinciden. Los valores de diferentes tipos nunca son iguales entre sí.
!=	any → any	Desigualdad; exactamente lo contrario de la igualdad (ver arriba).
<	(long, long) → Booleano	Entero largo menor que.
<=	(long, long) → Booleano	Entero largo less-than-or-equal -to.
>	(long, long) → Booleano	Entero largo mayor que.
>=	(long, long) → Booleano	Entero largo greater-than-or-equal -to.
in	(entity, entity) → Booleano	Pertenencia jerárquica (reflexiva: A en A siempre es verdadera).
	(entidad, conjunto (entidad)) → Booleano	Pertenencia jerárquica: A en [B, C, ...] es verdadero si (A y B) || (A en C) || ... es un error si el conjunto no contiene una entidad.
&&	(Boolean, Boolean) → Booleano	Lógico y (cortocircuito).
||	(Boolean, Boolean) → Booleano	Lógico o (cortocircuito).

Operador	Tipos y sobrecargas	Descripción
.exists()	entity → Booleano	Existencia de la entidad.
has	(entity, attribute) → Booleano	Operador de infijo. `e has f` comprueba si el registro o la entidad `e` tienen un enlace para el atributo `f`. Devuelve `false` si `e` no existe o si `e` existe pero no tiene el atributo `f`. Los atributos se pueden expresar como identificadores o cadenas literales.
like	(string, string) → Booleano	Operador de infijo. `t like p` comprueba si el texto `t` coincide con el patrón `p`, que puede incluir caractere s comodín `*` que coincidan con 0 o más caracteres. Para que coincida con un carácter estrella literal en `t`, puede utilizar la secuencia especial de caracteres de escape `\*` en `p`.
.contains()	(set, any) → Booleano	Establecer pertenencia (es B un elemento de A).
.containsAll()	(set, set) → Booleano	Comprueba si el conjunto A contiene todos los elementos del conjunto B.
.containsAny()	(set, set) → Booleano	Comprueba si el conjunto A contiene alguno de los elementos del conjunto B.

Evaluación de políticas de Acceso verificado

Un documento de política es un conjunto de una o más declaraciones de política (instrucciones de `permit` o `forbid`). La política se aplica si la cláusula condicional (la declaración `when`) es verdadera. Para que un documento de política permita el acceso, debe aplicarse al menos una política de permisos del documento y no puede aplicarse ninguna política de denegación. Si no se aplica ninguna política de permisos y/o se aplica una o más políticas de denegación, el documento de política deniega el acceso. Si ha definido documentos de política tanto para el grupo de Acceso verificado como para el punto de conexión de Acceso verificado, ambos documentos deben permitir el acceso. Si no ha definido un documento de política para el punto de conexión de Acceso verificado, solo necesita el acceso de la política de grupo de Acceso verificado.

Acceso verificado de AWS valida la sintaxis al crear la política, pero no valida los datos que se incluyen en la cláusula condicional.

Cortocircuito de lógica de política de Acceso verificado

Es posible que desee escribir una Acceso verificado de AWS política que evalúe los datos que pueden estar presentes o no en un contexto determinado. Si hace referencia a los datos en un contexto que no existe, Cedar generará un error y evaluará la política para denegarla, independientemente de su intención. Por ejemplo, esto daría lugar a una denegación, ya que `fake_provider` y `bogus_key` no existen en este contexto.

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

Para evitar esta situación, puede comprobar si hay una clave presente mediante el operador `has`. Si el operador `has` devuelve un valor falso, la evaluación de la declaración encadenada se detiene y Cedar no genera ningún error al intentar hacer referencia a un elemento que no existe.

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

Esto resulta especialmente útil cuando se especifica una política que hace referencia a dos proveedores de confianza 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)
    )
  )
};
```

Ejemplos de políticas de Acceso verificado

Puede utilizar las políticas de Acceso verificado para conceder acceso a sus aplicaciones a usuarios y dispositivos específicos.

Ejemplos de políticas

- Ejemplo 1: Conceder acceso a un grupo de IAM Identity Center
- Ejemplo 2: Conceder acceso a un grupo de un proveedor externo
- Ejemplo 3: conceder acceso mediante CrowdStrike
- Ejemplo 4: Permitir o rechazar una dirección IP específica

Ejemplo 1: Conceder acceso a un grupo de IAM Identity Center

Cuando se usa AWS IAM Identity Center, es mejor hacer referencia a los grupos usando sus IDs. Esto ayuda a que no se infrinja una declaración de política si cambia el nombre de un grupo.

El siguiente ejemplo de política permite el acceso solo a los usuarios del grupo especificado con una dirección de correo electrónico verificada. El identificador del grupo es c242c5b0-6081-1845-6fa8-6e0d9513c107.

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

El siguiente ejemplo de política permite el acceso solo cuando el usuario está en el grupo especificado, el usuario tiene una dirección de correo electrónico verificada y la puntuación de riesgo del dispositivo Jamf es 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"
};
```

Para obtener más información sobre los datos de confianza, consulte the section called “AWS IAM Identity Center contexto”.

Ejemplo 2: Conceder acceso a un grupo de un proveedor externo

El siguiente ejemplo de política permite el acceso solo cuando el usuario está en el grupo especificado, el usuario tiene una dirección de correo electrónico verificada y la puntuación de riesgo del dispositivo Jamf es BAJA. El nombre del grupo en es "finance".

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

Para obtener más información sobre los datos de confianza, consulte the section called “Contexto de proveedor externo”.

Ejemplo 3: conceder acceso mediante CrowdStrike

El siguiente ejemplo de política permite el acceso cuando la puntuación general de la evaluación es superior a 50.

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

Ejemplo 4: Permitir o rechazar una dirección IP específica

La siguiente política de ejemplo permite las solicitudes únicamente desde la dirección IP especificada.

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

La siguiente política de ejemplo rechaza las solicitudes únicamente desde la dirección IP especificada.

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

Asistente de políticas de Acceso verificado

El asistente de políticas de Acceso verificado es una herramienta de la consola de Acceso verificado que puede utilizar para probar y desarrollar sus políticas. Este presenta la política de puntos de conexión, la política de grupo y el contexto de confianza en una pantalla, donde puede probar las políticas y modificarlas.

Los formatos del contexto de confianza varían según los distintos proveedores de confianza y, en algunas ocasiones, es posible que el administrador de Acceso verificado no sepa el formato exacto que utiliza un determinado proveedor de confianza. Por lo tanto, puede resultar muy útil ver el contexto de confianza tanto como las políticas de grupo y punto de conexión en un mismo lugar para probarlas y desarrollarlas.

En las siguientes secciones, se describen los aspectos principales del uso del editor de políticas.

Tareas

Paso 1: Especifique los recursos

En la primera página del asistente de políticas, especifique el punto de conexión de Acceso verificado con el que desea trabajar. También especificará un usuario (identificado por la dirección de correo electrónico) y, de manera opcional, el nombre del usuario y/o un identificador de dispositivo. Por defecto, la decisión de autorización más reciente se extrae de los registros de Acceso verificado del usuario especificado. Si lo desea, puede elegir específicamente la decisión de permitir o denegar más reciente.

Por último, el contexto de confianza, la decisión de autorización, la política de puntos de conexión y la política de grupo se muestran en la siguiente pantalla.

Para abrir el asistente de políticas y especificar sus recursos

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Instancias de Acceso verificado y, a continuación, haga clic en el ID de instancia de Acceso verificado de la instancia con la que quiere trabajar.
3. Seleccione Lanzar asistente de políticas.
4. En Dirección de correo electrónico del usuario, escriba la dirección de correo electrónico del usuario raíz de la cuenta.
5. En el caso del punto de conexión de Acceso verificado, seleccione el punto de conexión para el que desee modificar y probar las políticas.
6. (Opcional) En Nombre, proporcione el nombre del usuario.
7. (Opcional) En Identificador del dispositivo, proporcione el identificador único del dispositivo.
8. (Opcional) En Resultado de autorización, elija el tipo de resultado de autorización reciente que desee usar. Por defecto, se utilizará el último resultado de la autorización.
9. Elija Next (Siguiente).

Paso 2: Pruebe y modifique las políticas

En esta página se le presentará la siguiente información con la que trabajar:

- El contexto de confianza enviado por su proveedor de confianza para el usuario y (opcionalmente) el dispositivo que especificó en el paso anterior.
- La política de Cedar para el punto de conexión de Acceso verificado especificada en el paso anterior.
- La política de Cedar para el grupo de Acceso verificado al que pertenece el punto de conexión.

En esta página pueden modificarse Las políticas de Cedar para el punto de conexión y el grupo de Acceso verificado, pero el contexto de confianza es estático. Ahora puede utilizar esta página para ver el contexto de confianza junto con las políticas de Cedar.

Pruebe las políticas en función del contexto de confianza al pulsar el botón Probar políticas y el resultado de la autorización aparecerá en la pantalla. Puede modificar las políticas y volver a probar los cambios, y repetir el proceso según sea necesario.

Cuando esté satisfecho con los cambios realizados en las políticas, seleccione Siguiente para pasar a la siguiente pantalla del asistente de políticas.

Paso 3: Revise y aplique los cambios

En la última página del asistente de políticas, verá resaltados los cambios que llevó a cabo en las políticas para así facilitar su revisión. Ahora puede revisarlos por última vez y seleccionar Aplicar cambios para confirmar los cambios.

Además, tiene la opción de volver a la página anterior al seleccionar Anterior o cancelar completamente el asistente de políticas tras elegir Cancelar.

Cliente de conectividad para Acceso verificado de AWS

Acceso verificado de AWS proporciona el cliente de conectividad para que pueda habilitar la conectividad entre los dispositivos de los usuarios y las aplicaciones que no son HTTP. El cliente cifra de forma segura el tráfico de los usuarios, añade la información sobre la identidad del usuario y el contexto del dispositivo y lo enruta a Verified Access para aplicar las políticas. Si las políticas de acceso permiten el acceso, el usuario está conectado a la aplicación. El acceso de los usuarios está autorizado de forma continua mientras el cliente de conectividad esté conectado.

El cliente funciona como un servicio del sistema y es resistente a los bloqueos. Si la conexión se vuelve inestable, el cliente la restablece.

El cliente usa tokens de OAuth acceso efímeros para establecer el túnel seguro. El túnel se desconecta cuando el usuario cierra sesión en el cliente.

Los identificadores de acceso y actualización se almacenan localmente en el dispositivo del usuario, en una SQLite base de datos cifrada.

Contenido

Requisitos previos

Antes de comenzar, complete los siguientes requisitos previos:

- Cree una instancia de acceso verificado con un proveedor de confianza.
- Cree un punto final TCP para su aplicación.

- Desconecte su ordenador de cualquier cliente VPN para evitar problemas de enrutamiento.
- IPv6 Actívalo en tu ordenador. Para obtener instrucciones, consulte la documentación del sistema operativo que se ejecuta en el equipo.
- En un equipo con Windows, compruebe que el Trusted Platform Module (TPM) es compatible e instale el motor de ejecución WebView2.

Descargue el cliente de conectividad

Desinstale cualquier versión anterior del cliente. Descargue el cliente, compruebe que el instalador esté firmado y ejecútelo. No instale el cliente con un instalador sin firma.

- Cliente de conectividad para Mac con Apple Silicon versión 1.0.2
- Cliente de conectividad para Mac con la versión 1.0.2 de Intel
- Cliente de conectividad para Windows con x64 versión 1.0.2

Exportación del archivo de configuración del cliente

Utilice el siguiente procedimiento para exportar la información de configuración requerida por el cliente desde su instancia de Verified Access.

Para exportar el archivo de configuración del cliente mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Instancias de Acceso verificado.
3. Seleccione la instancia de Acceso verificado.
4. Elija Acciones, Exportar el archivo de configuración del cliente.

Para exportar el archivo de configuración del cliente mediante AWS CLI

Utilice el comando export-verified-access-instance-client-configuration. Guarde el resultado en un archivo.json. El nombre del archivo debe empezar por el `ClientConfig-` prefijo.

Conéctese a la aplicación

Utilice el siguiente procedimiento para conectarse a una aplicación mediante el cliente.

Para conectarse a una aplicación mediante el cliente

1. Implemente los archivos de configuración del cliente en los dispositivos de los usuarios en la siguiente ubicación:
   - Windows: `C:\ProgramData\Connectivity Client`
   - macOS — `/Library/Application\ Support/Connectivity\ Client`
2. Asegúrese de que los archivos de configuración del cliente sean propiedad de root (macOS) o Admin (Windows).
3. Inicie el cliente de conectividad.
4. Una vez cargado el cliente de conectividad, el IdP autentica al usuario.
5. Tras la autenticación, los usuarios pueden acceder a la aplicación mediante el nombre DNS proporcionado por Verified Access, mediante el cliente que elijan.

Desinstale el cliente

Cuando termine de utilizar el cliente de conectividad, podrá desinstalarlo.

macOS

Versión 1.0.1 y versiones posteriores

Vaya a `/Applications/Connectivity Client` y ejecute `Connectivity Client Uninstaller.app`.

Versión 1.0.0

Descargue el `connectivity_client_cleanup.sh` script para Mac con Apple Silicon o Mac con Intel, establezca los permisos de ejecución en el script y ejecútelo de la siguiente manera.

```
sudo ./connectivity_client_cleanup.sh
```

Windows

Para desinstalar el cliente en Windows, ejecute el instalador y seleccione Eliminar.

Prácticas recomendadas

Tenga en cuenta las siguientes prácticas recomendadas:

- Instale la versión más reciente del cliente.
- No instale el cliente con un instalador sin firma.
- Los usuarios no deben usar una configuración a menos que sea una configuración de confianza proporcionada por un administrador de TI. Una configuración que no sea de confianza podría redirigir a una página de suplantación de identidad.
- Los usuarios deben cerrar sesión en el cliente antes de dejar sus estaciones de trabajo inactivas.
- Añada el `offline_access` ámbito a su configuración de OIDC. Esto permite solicitar tokens de actualización, que se utilizan para obtener más tokens de acceso sin necesidad de que el usuario se vuelva a autenticar.

Solución de problemas

La siguiente información puede ayudarle a solucionar problemas con el cliente.

Problemas

Al iniciar sesión, el navegador no se abre para completar la autenticación por parte del IdP

Causa posible: falta el archivo de configuración o tiene un formato incorrecto.

Solución: póngase en contacto con el administrador del sistema y solicite un archivo de configuración actualizado.

Tras la autenticación, el estado del cliente es «no conectado»

Causa posible: ejecutar otro software de VPN AWS Client VPN, como Cisco AnyConnect u OpenVPN Connect.

Solución: desconéctese de cualquier otro software de VPN. Si sigues sin poder conectarte, genera un informe de diagnóstico y compártelo con el administrador del sistema.

Causa posible: en las plataformas Windows, el cliente usa HTTP en el puerto 80 para la comunicación en el plano de control. Una regla de firewall que bloquea el puerto TCP 80 impide la comunicación en el plano de control.

Solución: compruebe las reglas del Firewall de Windows para ver si hay una regla de salida explícita que bloquee el TCP en el puerto 80 y deshabilítela.

¿No puedes conectarte mediante un navegador Chrome o Edge

Causa posible: al conectarse a una aplicación web mediante un navegador Chrome o Edge, el navegador no resuelve el nombre de IPv6 dominio.

Solución: contacto AWS Support.

Historial de versiones

La siguiente tabla contiene el historial de versiones del cliente.

Versión	Cambios	Descargar	Date
1.0.2	macOS • Correcciones de errores y mejoras de estabilidad • Mejoras en la interfaz Windows • Correcciones de errores y mejoras de estabilidad • Mejoras en la interfaz	• Mac con Apple Silicon • Mac con Intel • Windows con x64	9 de junio de 2025
1.0.1	macOS • Mejoras de estabilidad • Aplicación de desinstalación	• Mac con Apple Silicon • Mac con Intel • Windows con x64	5 de febrero de 2025

Versión	Cambios	Descargar	Date
	Windows • Mejoras de estabilidad		
1.0.0	Vista previa pública	• Mac con Apple Silicon • Mac con Intel • Windows con x64	1 de diciembre de 2024

Seguridad en Acceso verificado de

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de conformidad que se aplican a AWS Verified Access, consulte AWS Servicios incluidos en el ámbito de aplicación del programa de conformidad AWS .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Acceso verificado. En los siguientes temas, se le mostrará cómo configurar Acceso verificado para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a usar otros AWS servicios que le ayudan a monitorear y proteger sus recursos de Verified Access.

Contenido

Protección de los datos en Acceso verificado de

El modelo de se aplica a protección de datos en AWS Verified Access. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en

esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Verified Access u otro tipo de acceso Servicios de AWS mediante la consola, la API o AWS CLI AWS SDKs Cualquier dato que ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cifrado en tránsito

Acceso verificado cifra todos los datos en tránsito de los usuarios finales a los puntos de conexión de Acceso verificado a través de Internet mediante la seguridad de la capa de transporte (TLS) 1.2 o una versión posterior.

Privacidad del tráfico entre redes

Puede configurar Acceso verificado para restringir el acceso a recursos específicos de la VPC. Para la autenticación basada en usuarios, también puede restringir el acceso a partes de la red, en función del grupo de usuarios que accede a los puntos de conexión. Para obtener más información, consulte Políticas de Acceso verificado.

Cifrado de datos en reposo para AWS Verified Access

AWS Verified Access cifra los datos en reposo de forma predeterminada mediante claves KMS AWS propias. Cuando el cifrado de los datos en reposo se realiza de forma predeterminada, ayuda a reducir la sobrecarga operativa y la complejidad que implica la protección de los datos confidenciales. Al mismo tiempo, le permite crear aplicaciones seguras que cumplen con los estrictos requisitos normativos y de conformidad con el cifrado. En las siguientes secciones se proporciona información detallada sobre cómo Acceso verificado utiliza las claves KMS para el cifrado de datos en reposo.

Contenido

Acceso verificado y claves KMS

AWS claves propias

Acceso verificado utiliza claves KMS para cifrar automáticamente la información de identificación personal (PII). Esto ocurre de forma predeterminada y usted mismo no puede ver, administrar, usar ni auditar el uso de las claves propiedad de AWS. Sin embargo, no tiene que realizar ninguna acción ni cambiar ningún programa para proteger las claves que cifran sus datos. Para obtener más información, consulte las claves propiedad de AWS en la Guía para desarrolladores de AWS Key Management Service .

Si bien no puedes deshabilitar esta capa de cifrado ni seleccionar un tipo de cifrado alternativo, puedes añadir una segunda capa de cifrado sobre las claves de cifrado que ya AWS poseas si eliges una clave gestionada por el cliente al crear tus recursos de acceso verificado.

Claves administradas por el cliente

Acceso verificado admite el uso de claves simétricas administradas por el cliente que usted crea y administra, para agregar una segunda capa de cifrado sobre el cifrado predeterminado existente. Como usted tiene el control total de esta capa de cifrado, puede realizar tareas como las siguientes:

- Establecer y mantener políticas de claves
- Establecer y mantener concesiones y políticas de IAM
- Habilitar y deshabilitar políticas de claves
- Rotar el material criptográfico
- Agregar etiquetas.
- Crear alias de clave
- Programar la eliminación de claves

Para obtener más información, consulte las claves administradas por el cliente en la Guía para desarrolladores de AWS Key Management Service .

> **Note**
>
> Verified Access habilita automáticamente el cifrado en reposo mediante claves AWS propias para proteger los datos de identificación personal sin coste alguno.
> Sin embargo, se aplicarán AWS KMS cargos cuando utilices una clave gestionada por el cliente. Para obtener más información acerca de los precios, consulte Precios de AWS Key Management Service.

Información personalmente identificable

En la siguiente tabla se resume la información de identificación personal (PII) que utiliza Acceso verificado y cómo se cifra.

Tipo de datos:	AWS cifrado de clave propia	Cifrado de claves administradas por el cliente (opcional)
`Trust provider (user-type)` Los proveedores de confianza de tipo usuario contienen opciones de OIDC AuthorizationEndpoint, como, UserInfoEndpoint, ClientId, ClientSecret, etc., que se consideran PII.	Habilitado	Habilitado
`Trust provider (device-type)` Los proveedores de confianza de tipo dispositivo contienen una TenantId, que se considera PII.	Habilitado	Habilitado
`Group policy` Se proporciona durante la creación o modificación del grupo de Acceso verificado. Contiene reglas para autorizar las solicitudes de acceso. Puede contener información de identificación personal, como nombre de usuario y dirección de correo electrónico, etc.	Habilitado	Habilitado

Tipo de datos:	AWS cifrado de clave propia	Cifrado de claves administradas por el cliente (opcional)
`Endpoint policy` Se proporciona durante la creación o modificación del punto de conexión de Acceso verificado. Contiene reglas para autorizar las solicitudes de acceso. Puede contener información de identificación personal, como nombre de usuario y dirección de correo electrónico, etc.	Habilitado	Habilitado

Cómo utiliza AWS Verified Access las concesiones en AWS KMS

Acceso verificado requiere una concesión para utilizar su clave administrada por el cliente.

Cuando creas recursos de acceso verificado cifrados con una clave administrada por el cliente, Verified Access crea una concesión en tu nombre enviando una CreateGrantsolicitud a AWS KMS. Las concesiones se AWS KMS utilizan para conceder a Verified Access el acceso a una clave gestionada por el cliente en tu cuenta.

Acceso verificado necesita la concesión para utilizar la clave administrada por el cliente para las siguientes operaciones internas:

- Envíe solicitudes de descifrado AWS KMS a para descifrar las claves de datos cifrados para que puedan usarse para descifrar sus datos.
- Envíe RetireGrantsolicitudes para AWS KMS eliminar una subvención.

Puede revocar el acceso a la concesión o eliminar el acceso del servicio a la clave administrada por el cliente en cualquier momento. Si lo hace, Acceso verificado no podrá acceder a ninguno de los datos cifrados por la clave administrada por el cliente, lo que afectará a las operaciones que dependen de esos datos.

Uso de claves administradas por el cliente con Acceso verificado

Puede crear una clave simétrica gestionada por el cliente mediante el AWS Management Console, o el AWS KMS APIs. Siga los pasos para crear una clave de cifrado simétrica de la Guía para AWS Key Management Service desarrolladores.

Políticas de claves

Las políticas de clave controlan el acceso a la clave administrada por el cliente. Cada clave administrada por el cliente debe tener exactamente una política de clave, que contiene instrucciones que determinan quién puede usar la clave y cómo puede utilizarla. Cuando crea la clave administrada por el cliente, puede especificar una política de clave. Para obtener más información, consulte las políticas clave en la Guía para AWS Key Management Service desarrolladores.

Para utilizar la clave administrada por el cliente con sus recursos de Acceso verificado, se deben permitir las siguientes operaciones de API en la política de claves:

- `kms:CreateGrant`: añade una concesión a una clave administrada por el cliente. Otorga el acceso de control a una clave KMS específica, que permite acceder a las operaciones de concesión que requiere Acceso verificado. Para obtener más información, consulte Subvenciones en la Guía para AWS Key Management Service desarrolladores.

  Esto permite que Acceso verificado realice las siguientes tareas:

  - Llamar a `GenerateDataKeyWithoutPlainText` para generar una clave de datos cifrada y almacenarla, ya que la clave de datos no se utiliza inmediatamente para cifrar.
  - Llamar a `Decrypt` para usar la clave de datos cifrados almacenada para acceder a los datos cifrados.
  - Configurar una entidad principal que se retire para permitir que el servicio `RetireGrant`.
- `kms:DescribeKey`: proporciona los detalles de la clave administrada por el cliente para permitir que Acceso verificado valide la clave.
- `kms:GenerateDataKey`: permite que Acceso verificado utilice la clave para cifrar los datos.
- `kms:Decrypt`: permitir que Acceso verificado descifre las claves de datos cifradas.

El siguiente es un ejemplo de política de claves que puede usar para Acceso 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 obtener más información, consulte Creación de una política clave y solución de problemas de acceso a las claves en la Guía para AWS Key Management Service desarrolladores.

Especificación de una clave administrada por el cliente para los recursos de Acceso verificado

Puede especificar una clave administrada por el cliente para proporcionar un cifrado de segunda capa para los siguientes recursos:

- Grupo de Acceso verificado
- Punto de conexión de Acceso verificado
- Proveedor de confianza de Acceso verificado

Al crear cualquiera de estos recursos mediante el AWS Management Console, puede especificar una clave gestionada por el cliente en la sección Cifrado adicional (opcional). Durante el proceso, active la casilla de verificación Personalizar la configuración de cifrado (avanzada) y, a continuación, introduzca el ID de AWS KMS clave que desee utilizar. Esto también se puede hacer al modificar un recurso existente o mediante la AWS CLI.

> **Note**
>
> Si se pierde la clave administrada por el cliente que se utiliza para añadir cifrado adicional a cualquiera de los recursos anteriores, los valores de configuración de los recursos dejarán de ser accesibles. Sin embargo, los recursos se pueden modificar mediante las teclas AWS Management Console o AWS CLI, para aplicar una nueva clave gestionada por el cliente y restablecer los valores de configuración.

AWS Contexto de cifrado de Verified Access

Un contexto de cifrado es un conjunto opcional de pares clave-valor que contienen información contextual adicional sobre los datos. AWS KMS utiliza el contexto de cifrado como datos autenticados adicionales para respaldar el cifrado autenticado. Al incluir un contexto de cifrado en una solicitud de cifrado de datos, AWS KMS vincula el contexto de cifrado a los datos cifrados. Para descifrar los datos, debe incluir el mismo contexto de cifrado en la solicitud.

AWS Contexto de cifrado de Verified Access

Verified Access utiliza el mismo contexto de cifrado en todas las operaciones AWS KMS criptográficas, donde la clave es `aws:verified-access:arn` y el valor es el nombre de recurso de Amazon (ARN) del recurso. A continuación, se muestran los contextos de cifrado de los recursos de Acceso verificado.

Proveedor de confianza de Acceso verificado

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

Grupo de Acceso verificado

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

Punto de conexión de Acceso verificado

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

Supervisión de las claves de cifrado para AWS el acceso verificado

Cuando utilizas una clave KMS gestionada por el cliente con tus recursos de acceso AWS verificado, puedes utilizarla AWS CloudTrailpara realizar un seguimiento de las solicitudes que envía Verified Access AWS KMS.

Los siguientes ejemplos son AWS CloudTrail eventos para`CreateGrant`,, y `RetireGrant` `Decrypt` `DescribeKey``GenerateDataKey`, que supervisan las operaciones de KMS solicitadas por Verified Access para acceder a los datos cifrados por la clave de KMS administrada por el cliente:

CreateGrant

Cuando utiliza una clave administrada por el cliente para cifrar sus recursos, Acceso verificado envía una solicitud `CreateGrant` en su nombre para acceder a la clave de su cuenta de AWS .

La concesión que crea Acceso verificado es específica para el recurso asociado a la clave administrada por el cliente.

El siguiente evento de ejemplo registra la operación `CreateGrant`:


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T16:27:12Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T16:41:42Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "operations": [
            "Decrypt",
            "RetireGrant",
            "GenerateDataKey"
        ],
        "keyId": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae",
        "constraints": {
```

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


RetireGrant

Acceso verificado utiliza la operación `RetireGrant` para eliminar una concesión cuando se elimina un recurso.

El siguiente evento de ejemplo registra la operación `RetireGrant`:


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
```

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

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt

Acceso verificado llama a la operación `Decrypt` para que utilice la clave de datos cifrados almacenada para acceder a los datos cifrados.

El siguiente evento de ejemplo registra la operación `Decrypt`:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T17:19:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T17:47:05Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
```

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


DescribeKey

Acceso verificado utiliza la operación `DescribeKey` para comprobar si la clave administrada por el cliente que está asociada al recurso existe en la cuenta y la región.

El siguiente evento de ejemplo registra la operación `DescribeKey`:


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
```

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

GenerateDataKey

El siguiente ejemplo de evento registra la operación `GenerateDataKey`:


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T17:19:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T17:46:49Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:verified-access:arn": "arn:aws:ec2:ca-
central-1:111122223333:verified-access-trust-provider/vatp-00f20a4e455e9340f",
            "aws-crypto-public-key": "A/ATGxaYatPUlOtM+l/mfDndkzHUmX5Hav+29IlIm
+JRBKFuXf24ulztmOIsqFQliw=="
        },
        "numberOfBytes": 32,
        "keyId": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
```

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


Administración de identidades y accesos para Acceso verificado de

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Acceso verificado. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realices en Verified Access.

Usuario de servicio: si utiliza el servicio de Acceso verificado para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Acceso verificado para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en Acceso verificado, consulte Solución de problemas de identidades y accesos en Acceso verificado de .

Administrador de servicio: si está a cargo de los recursos de Acceso verificado en su empresa, es probable que tenga acceso completo a Acceso verificado. Su trabajo consiste en determinar a qué características y recursos de Acceso verificado deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su gestionador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con Acceso verificado, consulte Funcionamiento de Acceso verificado de con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a Acceso verificado. Para consultar ejemplos de políticas basadas en identidades de Acceso verificado que puede utilizar en IAM, consulte Ejemplos de políticas basadas en identidades para Acceso verificado de .

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su gestionador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre la firma de solicitudes, consulte AWS Signature Versión 4 para solicitudes API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Autenticación multifactor AWS en IAM en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utiliza el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulta Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios empresarial, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulta ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulta Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede cambiar de un rol de usuario a uno de IAM (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puedes crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué puedes acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puedes asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puedes utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en AWS ellas, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulta Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio

desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puedes asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puedes ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Usar un rol de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulta Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puedes crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utiliza para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción

`iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puedes asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades puedes clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios puedes utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puedes realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios compatibles. AWS WAF ACLs Para obtener más información ACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas puedes establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puedes conceder a una entidad de IAM (usuario o rol de IAM). Puedes establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulta Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): SCPs son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre Organizations SCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- Políticas de control de recursos (RCPs): RCPs son políticas de JSON que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las políticas de IAM asociadas a cada recurso que poseas. El RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades, incluidos los permisos Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de Servicios de AWS ese apoyo RCPs, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades

del rol y las políticas de la sesión. Los permisos también puedes proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulta Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Funcionamiento de Acceso verificado de con IAM

Antes de utilizar IAM para administrar el acceso a Acceso verificado, conozca qué características de IAM se pueden utilizar con Acceso verificado.

Característica de IAM	Asistencia técnica de Acceso verificado
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACLs	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo funcionan el acceso verificado y otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en identidades para Acceso verificado

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades para Acceso verificado

Para ver ejemplos de políticas basadas en identidades de Acceso verificado, consulte Ejemplos de políticas basadas en identidades para Acceso verificado de .

Políticas basadas en recursos de Acceso verificado

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios puedes utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puedes realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los directores pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Cross account resource access in IAM en la Guía del usuario de IAM.

Acciones políticas para Acceso verificado

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puedes utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de acciones de acceso verificado, consulta Acciones definidas por Amazon EC2 en la Referencia de autorización de servicio.

Las acciones de políticas de Acceso verificado utilizan el siguiente prefijo antes de la acción:

```
ec2
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

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

Para ver ejemplos de políticas basadas en identidades de Acceso verificado, consulte Ejemplos de políticas basadas en identidades para Acceso verificado de .

Recursos de políticas para Acceso verificado

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de recursos de acceso verificado y sus tipos ARNs, consulte Recursos definidos por Amazon EC2 en la Referencia de autorización de servicio. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por Amazon. EC2

Para ver ejemplos de políticas basadas en identidades de Acceso verificado, consulte Ejemplos de políticas basadas en identidades para Acceso verificado de .

Claves de condición de políticas para Acceso verificado

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones

condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de claves de condición de acceso verificado, consulta Claves de condición de Amazon EC2 en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por Amazon EC2.

Para ver ejemplos de políticas basadas en identidades de Acceso verificado, consulte Ejemplos de políticas basadas en identidades para Acceso verificado de .

ACLs en Verified Access

Soporta ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con Acceso verificado

Compatibilidad con ABAC (etiquetas en las políticas): parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de

entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulta Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con Acceso verificado

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Permisos de entidades principales entre servicios de Acceso verificado

Admite sesiones de acceso directo (FAS): sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulta Reenviar sesiones de acceso.

Roles de servicio para Acceso verificado

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

Roles vinculados a servicios para Acceso verificado

Admite roles vinculados a servicios: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puedes asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puedes ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información acerca de cómo crear o administrar roles vinculados a servicios de Acceso verificado, consulte Uso de roles vinculados a servicios para Acceso verificado.

Ejemplos de políticas basadas en identidades para Acceso verificado de

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de Acceso verificado. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la API. Un administrador de IAM puedes crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que

necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Verified Access, incluido el ARNs formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Amazon EC2 en la Referencia de autorización de servicio.

Temas

- Prácticas recomendadas sobre las políticas
- Política para crear instancias de Acceso verificado
- Cómo permitir a los usuarios consultar sus propios permisos

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear o eliminar los recursos de Acceso y acceder a ellos verificado en su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se puedes llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utiliza condiciones en las políticas de IAM para restringir aún más el acceso: puedes agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puedes

escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Política para crear instancias de Acceso verificado

Para crear una instancia de Acceso verificado, las entidades principales de IAM deben añadir esta declaración adicional a su política de IAM.

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

> **Note**
>
> `verified-access:AllowVerifiedAccess` es una API virtual de acción exclusiva. No admite la autorización basada en claves de recursos, etiquetas o condiciones. Utilice la autorización basada en claves de recursos, etiquetas o condiciones en la acción de la API `ec2:CreateVerifiedAccessInstance`.

Ejemplo de política para crear una instancia de Acceso verificado. En este ejemplo, `123456789012` es el número de AWS cuenta y `us-east-1` la región. AWS

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

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas gestionadas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o 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": "*"
        }
    ]
}
```

Solución de problemas de identidades y accesos en Acceso verificado de

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Acceso verificado e IAM.

Problemas

- No tengo autorización para realizar una acción en Acceso verificado
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de acceso verificado

No tengo autorización para realizar una acción en Acceso verificado

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `ec2:`*`GetWidget`*.

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

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `ec2:GetWidget`.

Si necesitas ayuda, ponte en contacto con tu administrador. AWS El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, se deben actualizar las políticas a fin de permitirle pasar un rol a Acceso verificado.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Acceso verificado. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de acceso verificado

Puedes crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puedes especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admiten políticas basadas en recursos o listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para obtener más información, consulte lo siguiente:

- Para obtener información acerca de si Acceso verificado admite estas características, consulte Funcionamiento de Acceso verificado de con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro de su propiedad en la Cuenta de AWS Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulta Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Uso de roles vinculados a servicios para Acceso verificado

Acceso verificado de AWS usa un rol vinculado a un servicio de IAM, que es un tipo de rol de IAM que está vinculado directamente a un servicio. AWS Verified Access define las funciones vinculadas al servicio para Verified Access e incluyen todos los permisos que el servicio necesita para llamar a otras personas en su nombre. Servicios de AWS

Un rol vinculado a un servicio simplifica la configuración de Acceso verificado porque ya no tendrá que agregar manualmente los permisos necesarios. Acceso verificado define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo Acceso verificado puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Permisos de roles vinculados al servicio de Acceso verificado

Verified Access utiliza la función vinculada al servicio denominada AWSServiceRoleForVPCVerifiedAccess para aprovisionar los recursos de su cuenta que son necesarios para utilizar el servicio.

El rol vinculado AWSServiceRoleForVPCVerifiedal servicio de Access confía en los siguientes servicios para asumir el rol:

- `verified-access.amazonaws.com`

La política de permisos del rol, denominada AWSVPCVerifiedAccessServiceRolePolicy, permite a Verified Access realizar las siguientes acciones en los recursos especificados:

- Acción `ec2:CreateNetworkInterface` en todas las subredes y grupos de seguridad, así como en todas las interfaces de red con la etiqueta `VerifiedAccessManaged=true`
- Acción `ec2:CreateTags` en todas las interfaces de red en el momento de la creación
- Acción `ec2:DeleteNetworkInterface` en todas las interfaces de red con la etiqueta `VerifiedAccessManaged=true`
- Acción `ec2:ModifyNetworkInterfaceAttribute` en todos los grupos de seguridad y en todas las interfaces de red con la etiqueta `VerifiedAccessManaged=true`

También puede ver los permisos de esta política en la Guía de referencia de políticas AWS gestionadas; consulte AWSVPCVerifiedAccessServiceRolePolicy.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a servicios para Acceso verificado

No necesita crear manualmente un rol vinculado a servicios. Cuando llamas a CreateVerifiedAccessEndpointla AWS Management Console, a la AWS CLI API o a la AWS API, Verified Access crea automáticamente el rol vinculado al servicio.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando vuelves a llamar, Verified Access CreateVerifiedAccessEndpointvuelve a crear el rol vinculado al servicio para ti.

Edición de un rol vinculado a servicios para Acceso verificado

Verified Access no le permite editar el rol vinculado al servicio de AWSServiceRoleForVPCVerifiedAccess. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte la Descripción sobre cómo editar un rol vinculado al servicio en la Guía del usuario de IAM.

Eliminación de un rol vinculado a servicios para Acceso verificado

No es necesario eliminar manualmente el rol de AWSServiceRoleForVPCVerifiedAccess. Cuando llamas a DeleteVerifiedAccessEndpointla AWS Management Console, a la AWS CLI API o a la AWS API, Verified Access limpia los recursos y elimina automáticamente la función vinculada al servicio.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Usa la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al servicio de Access. AWSService RoleFor VPCVerified Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a un servicio de Acceso verificado

Verified Access permite el uso de funciones vinculadas al servicio en todos los Regiones de AWS lugares en los que el servicio esté disponible. Para obtener más información, consulte Puntos de conexión y Regiones de AWS.

AWS políticas gestionadas para el acceso verificado

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AWS política gestionada: AWSVPCVerified AccessServiceRolePolicy

Esta política está adjunta a un rol vinculado a servicios que permite a Acceso verificado realizar acciones en su nombre. Para obtener más información, consulte Uso de roles vinculados a servicios. Para ver los permisos de esta política, puede consultarla AWSVPCVerifiedAccessServiceRolePolicyen la AWS Management ConsoleGuía de referencia de AWSVPCVerifiedAccessServiceRolePolicypolíticas AWS gestionadas o consultarla en la misma.

Verified Access actualiza las políticas AWS gestionadas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de Verified Access desde que este servicio comenzó a rastrear estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos de Acceso verificado.

Cambio	Descripción	Fecha
AWSVPCVerifiedAccessServiceRolePolicy- Política actualizada	Acceso verificado actualizó su política de administración para incluir descripciones de todas las acciones en el campo "sid".	17 de noviembre de 2023
AWSVPCVerifiedAccessServiceRolePolicy- Política actualizada	Acceso verificado actualizó su política administrada para añadir un recurso de grupo de seguridad al permiso `ec2:CreateNetworkInterface` .	31 de mayo de 2023
AWSVPCVerifiedAccessServiceRolePolicy: política nueva	Acceso verificado añadió una nueva política que le permite aprovisionar los recursos de su cuenta necesarios para usar el servicio.	29 de noviembre de 2022
Acceso verificado comenzó a realizar un seguimiento de los cambios	Verified Access comenzó a realizar un seguimiento de los	29 de noviembre de 2022

Cambio	Descripción	Fecha
	cambios en sus políticas AWS gestionadas.	

Validación de la conformidad de Acceso verificado de

Acceso verificado de AWS se puede configurar para respaldar el cumplimiento de los estándares federales de procesamiento de información (FIPS). Para obtener más información y datos sobre cómo configurar el cumplimiento de las normas FIPS para Acceso verificado, visite Conformidad con las normas FIPS para Acceso verificado.

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Cumplimiento de seguridad y gobernanza: en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- Referencia de servicios válidos de HIPAA: muestra una lista con los servicios válidos de HIPAA. No todos Servicios de AWS cumplen con los requisitos de la HIPAA.
- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).

- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulta la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en Acceso verificado de

La infraestructura AWS global se basa en zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Además de la infraestructura AWS global, Verified Access ofrece las siguientes funciones para satisfacer sus necesidades de alta disponibilidad.

Varias subredes para disfrutar de una alta disponibilidad

Al crear un punto de conexión de Acceso verificado del tipo equilibrador de carga, puede asociar varias subredes al punto de conexión. Cada una de las subredes que asocie con el punto de

conexión debe pertenecer a una zona de disponibilidad diferente. Al asociar varias subredes, puede garantizar una alta disponibilidad mediante el uso de varias zonas de disponibilidad.

Monitorización Acceso verificado de AWS

La supervisión es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de Acceso verificado de AWS. AWS proporciona las siguientes herramientas de supervisión para controlar el acceso verificado, informar cuando algo anda mal y tomar medidas automáticas cuando sea necesario:

- Registros de acceso: recopilan información detallada sobre las solicitudes de acceso a las aplicaciones. Para obtener más información, consulte the section called “Registros de Acceso verificado”.
- AWS CloudTrail— Captura las llamadas a la API y los eventos relacionados realizados por usted o en su nombre Cuenta de AWS y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. Para obtener más información, consulte the section called “CloudTrail registra”.

Registros de Acceso verificado

Tras Acceso verificado de AWS evaluar cada solicitud de acceso, registra todos los intentos de acceso. Esto le proporciona una visibilidad centralizada del acceso a las aplicaciones y le ayuda a responder rápidamente a los incidentes de seguridad y a las solicitudes de auditoría. Acceso verificado admite el formato de registro Open Cybersecurity Schema Framework (OCSF).

Cuando habilite el registro, debe configurar un destino para el envío de los registros. La entidad principal de IAM que se utiliza para configurar el destino del registro necesita tener ciertos permisos para que el registro funcione correctamente. Los permisos de IAM necesarios para cada destino de registro se pueden consultar en la sección Permisos de registro de Acceso verificado. Acceso verificado admite los siguientes destinos para publicar los registros de acceso:

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

Contenido

- Permisos de registro de Acceso verificado
- Habilitación o deshabilitación de registros de Acceso verificado
- Habilitación o deshabilitación del contexto de confianza de Acceso verificado
- Ejemplos de registro de la versión 0.1 de OCSF para Acceso verificado
- Ejemplos de registro de la versión 1.0.0-rc.2 de OCSF para Acceso verificado

Versiones de registro de Acceso verificado

De forma predeterminada, el sistema de registro de Acceso verificado utiliza la versión 0.1 de Open Cybersecurity Schema Framework (OCSF). Para ver ejemplos de registros que utilizan la versión 0.1, consulteEjemplos de registro de la versión 0.1 de OCSF para Acceso verificado.

La última versión de registro es compatible con la versión 1.0.0-rc.2 de OCSF. Para obtener más información sobre el esquema, consulte Esquema OCSF. Para ver ejemplos de registros que utilizan la versión 1.0.0-rc.2, consulte. Ejemplos de registro de la versión 1.0.0-rc.2 de OCSF para Acceso verificado

Tenga en cuenta que no puede usar la versión 0.1 de OCSF si el punto final de Verified Access usa el protocolo TCP.

Actualización de la versión de registro mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Instancias de Acceso verificado.
3. Seleccione la instancia de Acceso verificado adecuada.
4. En la pestaña Configuración del registro de instancias de Acceso verificado, seleccione Modificar la configuración de registro de instancias de Acceso verificado.
5. Seleccione ocsf-1.0.0-rc.2 en la lista desplegable Actualizar versión de registro.
6. Seleccione Modificar la configuración de registro de instancias de Acceso verificado.

Para actualizar la versión de registro mediante el AWS CLI

Utilice el comando modify-verified-access-instance-logging-configuration.

Permisos de registro de Acceso verificado

La entidad principal de IAM que se utiliza para configurar el destino del registro necesita tener ciertos permisos para que el registro funcione correctamente. Las siguientes secciones muestran los permisos necesarios para cada destino de registro.

Para la entrega a Logs: CloudWatch

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration` en la instancia de Acceso verificado
- `logs:CreateLogDelivery`, `logs:DeleteLogDelivery`, `logs:GetLogDelivery`, `logs:ListLogDeliveries` y `logs:UpdateLogDelivery` en todos los recursos
- `logs:DescribeLogGroups`, `logs:DescribeResourcePolicies` y `logs:PutResourcePolicy` en el grupo de registro de destino

Para la entrega en Amazon S3:

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration` en la instancia de Acceso verificado
- `logs:CreateLogDelivery`, `logs:DeleteLogDelivery`, `logs:GetLogDelivery`, `logs:ListLogDeliveries` y `logs:UpdateLogDelivery` en todos los recursos
- `s3:GetBucketPolicy` y `s3:PutBucketPolicy` en el bucket de destino

Para la entrega en Firehose:

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration` en la instancia de Acceso verificado
- `firehose:TagDeliveryStream` en todos los recursos
- `iam:CreateServiceLinkedRole` en todos los recursos
- `logs:CreateLogDelivery`, `logs:DeleteLogDelivery`, `logs:GetLogDelivery`, `logs:ListLogDeliveries` y `logs:UpdateLogDelivery` en todos los recursos

Habilitación o deshabilitación de registros de Acceso verificado

Puede utilizar los procedimientos de esta sección para habilitar o deshabilitar el registro. Cuando habilite el registro, debe configurar un destino para el envío de los registros. La entidad principal

de IAM que se utiliza para configurar el destino del registro debe tener ciertos permisos para que el registro funcione correctamente. Los permisos de IAM necesarios para cada destino de registro se pueden consultar en la sección Permisos de registro de Acceso verificado.

Contenido

Habilitación de registros de acceso

Habilitación de los registros de Acceso verificado

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Instancias de Acceso verificado.
3. Seleccione la instancia de Acceso verificado.
4. En la pestaña Configuración del registro de instancias de Acceso verificado, seleccione Modificar la configuración de registro de instancias de Acceso verificado.
5. (Opcional) Para incluir en los registros los datos de confianza enviados por los proveedores de confianza, haga lo siguiente:
   a. Seleccione ocsf-1.0.0-rc.2 en la lista desplegable Actualizar versión de registro.
   b. Seleccione Incluir contexto de confianza.
6. Realice una de las siguientes acciones:
   - Activa la opción Entregar a Amazon CloudWatch Logs. Seleccione el grupo de registro de destino.
   - Active la opción Entregar a Amazon S3. Introduzca el nombre, el propietario y el prefijo del bucket de destino.
   - Active la opción Entregar a Firehose. Elija el flujo de entrega de destino.
7. Seleccione Modificar la configuración de registro de instancias de Acceso verificado.

Para activar los registros de acceso verificado, utilice la AWS CLI

Utilice el comando modify-verified-access-instance-logging-configuration.

Desactivación de los registros de acceso

Puede deshabilitar los registros de acceso de su instancia de Acceso verificado en cualquier momento. Después de desactivar los registros de acceso, sus datos de registro permanecerán en su destino de registro hasta que los elimine.

Desactivación de los registros de Acceso verificado

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Instancias de Acceso verificado.
3. Seleccione la instancia de Acceso verificado.
4. En la pestaña Configuración del registro de instancias de Acceso verificado, seleccione Modificar la configuración de registro de instancias de Acceso verificado.
5. Desactive la entrega de registros.
6. Seleccione Modificar la configuración de registro de instancias de Acceso verificado.

Para deshabilitar los registros de acceso verificado mediante el AWS CLI

Utilice el comando modify-verified-access-instance-logging-configuration.

Habilitación o deshabilitación del contexto de confianza de Acceso verificado

El contexto de confianza enviado por su proveedor de confianza puede habilitarse opcionalmente para incluirse en sus registros de Acceso verificado. Esto puede resultar útil al definir políticas que permitan o denieguen el acceso a las aplicaciones. Una vez habilitado, el contexto de confianza se encontrará en el registro situado debajo del campo `data`. Si el contexto de confianza está deshabilitado, el campo `data` se establece en `null`. Si quiere configurar Acceso verificado para que incluya el contexto de confianza en los registros, siga el procedimiento que se indica a continuación.

> **Note**
>
> Para incluir el contexto de confianza en los registros de Acceso verificado, debe actualizar a la versión de registro más reciente `ocsf-1.0.0-rc.2`. En el siguiente procedimiento se presupone que ya tiene habilitado el registro. De no ser así, consulte Habilitación de registros de acceso para conocer el procedimiento completo.

Contenido

Habilitación del contexto de confianza

Inclusión del contexto de confianza en los registros de Acceso verificado mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Instancias de Acceso verificado.
3. Seleccione la instancia de Acceso verificado adecuada.
4. En la pestaña Configuración del registro de instancias de Acceso verificado, seleccione Modificar la configuración de registro de instancias de Acceso verificado.
5. Seleccione ocsf-1.0.0-rc.2 en la lista desplegable Actualizar versión de registro.
6. Active la opción Incluir contexto de confianza.
7. Seleccione Modificar la configuración de registro de instancias de Acceso verificado.

Para incluir el contexto de confianza en los registros de acceso verificado mediante el AWS CLI

Utilice el comando modify-verified-access-instance-logging-configuration.

Deshabilitación del contexto de confianza

Si ya no desea incluir el contexto de confianza en los registros, puede eliminarlo mediante el procedimiento que se indica a continuación.

Eliminación del contexto de confianza de los registros de Acceso verificado mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Instancias de Acceso verificado.
3. Seleccione la instancia de Acceso verificado adecuada.
4. En la pestaña Configuración del registro de instancias de Acceso verificado, seleccione Modificar la configuración de registro de instancias de Acceso verificado.
5. Desactive la opción Incluir contexto de confianza.
6. Seleccione Modificar la configuración de registro de instancias de Acceso verificado.

Para eliminar el contexto de confianza de los registros de acceso verificado mediante el AWS CLI

Utilice el comando modify-verified-access-instance-logging-configuration.

Ejemplos de registro de la versión 0.1 de OCSF para Acceso verificado

A continuación, se muestran ejemplos de registros que utilizan la versión 0.1 de OCSF.

Ejemplos

- Acceso concedido con OIDC
- Acceso concedido con OIDC y JAMF
- Acceso concedido con OIDC y CrowdStrike
- Acceso denegado debido a la falta de una cookie
- Acceso denegado por política
- Entrada de registro desconocida

Acceso concedido con OIDC

En este ejemplo de entrada de registro, Acceso verificado permite el acceso a un punto de conexión con un proveedor de confianza de usuarios de 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
}
```

Acceso concedido con OIDC y JAMF

En este ejemplo de entrada de registro, Acceso verificado permite el acceso a un punto de conexión con los proveedores de confianza de dispositivos OIDC y 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
}
```


Acceso concedido con OIDC y CrowdStrike

En este ejemplo de entrada de registro, el acceso verificado permite el acceso a un punto final tanto con el OIDC como con los proveedores de confianza de dispositivos. CrowdStrike


```
{
    "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
}
```

Acceso denegado debido a la falta de una cookie

En este ejemplo de entrada de registro, Acceso verificado deniega el acceso porque falta una cookie de autenticación.

```
{
    "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
}
```

Acceso denegado por política

En este ejemplo de entrada de registro, Acceso verificado deniega una solicitud autenticada porque las políticas de acceso no la permiten.

```
{
    "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 registro desconocida

En este ejemplo de entrada de registro, Acceso verificado no puede generar una entrada de registro completa, por lo que emite una entrada de registro desconocida. Esto garantiza que todas las solicitudes aparezcan en el registro de acceso.

```
{
    "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
}
```


Ejemplos de registro de la versión 1.0.0-rc.2 de OCSF para Acceso verificado

A continuación, se muestran ejemplos de registros que utilizan la versión 1.0.0-rc.2 de OCSF.

Ejemplos

- Acceso concedido con el contexto de confianza incluido
- Acceso concedido con el contexto de confianza omitido
- Asigne privilegios con el punto final CIDR de la red

Acceso concedido con el contexto de confianza incluido


```
{
    "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",
                "additional_user_context": {
                    "aud": "xxx",
                    "exp": 1000000000,
                    "groups": [
                        "group-id-1",
                        "group-id-2"
                    ],
                    "iat": 1000000000,
                    "iss": "https://oidc-tp.com/",
                    "sub": "xyzsubject",
                    "ver": "1.0"
                }
            },
            "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"
            }
        }
    }
}
```


Acceso concedido con el contexto de confianza 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
}
```


Asigne privilegios con el punto final CIDR de la red


```
{
    "activity_id": "1",
    "activity_name": "Assign Privileges",
    "category_name": "Audit Activity",
    "category_uid": "3",
```

```
    "class_name": "Authorization",
    "class_uid": "3003",
    "data": {
        "endpoint_type": "cidr",
        "protocol": "tcp",
        "access_path": "public",
        "idp": {
            "name": "my-oidc-instance",
            "uid": "vatp-09bc4cbce2EXAMPLE"
        },
        "authorizations": [{
            "decision": "Allow",
            "policy": {
                "name": "inline"
            }
        }],
        "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",
                "additional_user_context": {
                    "aud": "xxx",
                    "exp": 1000000000,
                    "groups": [
                        "group-id-1",
                        "group-id-2"
                    ],
                    "iat": 1000000000,
                    "iss": "https://oidc-tp.com/",
                    "sub": "xyzsubject",
                    "ver": "1.0"
                }
            },
```

```
            "tcp_flow": {
                "destination_ip": "10.0.0.1",
                "destination_port": 22,
                "client_ip": "10.2.7.68"
            }
        }
    },
    "device": {
        "ip":  "10.2.7.68",
        "port": 1002,
        "type": "Unknown",
        "type_id": 0
    },
    "duration": "0.004",
    "end_time": "1668580194344",
    "time": "1668580194344",
    "metadata": {
        "uid": "",
        "logged_time": 1668580281337,
        "version": "1.0.0-rc.2",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "severity": "Informational",
    "severity_id": "1",
    "start_time": "1668580194340",
    "status_code": "200",
    "status_id": "1",
    "status": "Success",
    "type_uid": "300301",
    "type_name": "Authorization: Assign Privileges",
    "count": 1,
    "dst_endpoint": {
        "ip": "107.22.231.155",
        "port": 22
    },
    "privileges": [
        "vae-12345cbce2EXAMPLE"
    ],
    "user": {
        "email_addr": "johndoe-user@test.com",
        "uid": "johndoe-user",
```

```
        "uuid": "9bcce02a-fc15-4091-a0b7-874d157c67b8"
    }
}
```

Registre las llamadas a la API de acceso verificado mediante AWS CloudTrail

AWS Verified Access está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o una persona Servicio de AWS en Verified Access. CloudTrail captura las llamadas a la API para el acceso verificado como eventos. Las llamadas capturadas incluyen las llamadas realizadas desde la consola de Acceso verificado y las llamadas de código a las operaciones de la API de Acceso verificado. Con la información recopilada CloudTrail, puede determinar la solicitud que se realizó a Verified Access, la dirección IP desde la que se realizó la solicitud, cuándo se realizó y detalles adicionales.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz o del usuario.
- Si la solicitud se realizó en nombre de un usuario de IAM Identity Center.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

CloudTrail está activa en tu cuenta Cuenta de AWS cuando creas la cuenta y tienes acceso automáticamente al historial de CloudTrail eventos. El historial de CloudTrail eventos proporciona un registro visible, consultable, descargable e inmutable de los últimos 90 días de eventos de gestión registrados en un. Región de AWSPara obtener más información, consulte Uso del historial de CloudTrail eventos en la Guía del usuario.AWS CloudTrail La visualización del historial de eventos no conlleva ningún CloudTrail cargo.

Para tener un registro continuo de los eventos de Cuenta de AWS los últimos 90 días, crea un almacén de datos de eventos de senderos o CloudTraillagos.

CloudTrail senderos

Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. Todos los senderos creados con él AWS Management Console son multirregionales. Puede crear un registro de seguimiento de una sola región o de varias regiones mediante la AWS CLI. Se recomienda crear un sendero multirregional, ya que puedes capturar toda la actividad de tu Regiones de AWS cuenta. Si crea un registro de seguimiento de una sola región, solo podrá ver los eventos registrados en la Región de AWS del registro de seguimiento. Para obtener más información acerca de los registros de seguimiento, consulte Creación de un registro de seguimiento para su Cuenta de AWS y Creación de un registro de seguimiento para una organización en la Guía del usuario de AWS CloudTrail .

Puede enviar una copia de sus eventos de administración en curso a su bucket de Amazon S3 sin coste alguno CloudTrail mediante la creación de una ruta; sin embargo, hay cargos por almacenamiento en Amazon S3. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios. Para obtener información acerca de los precios de Amazon S3, consulte Precios de Amazon S3.

CloudTrail Almacenes de datos de eventos en Lake

CloudTrail Lake le permite ejecutar consultas basadas en SQL en sus eventos. CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato Apache ORC. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida de datos. Los eventos se agregan en almacenes de datos de eventos, que son recopilaciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Los selectores que se aplican a un almacén de datos de eventos controlan los eventos que perduran y están disponibles para la consulta. Para obtener más información sobre CloudTrail Lake, consulte Cómo trabajar con AWS CloudTrail Lake en la Guía del AWS CloudTrail usuario.

CloudTrail Los almacenes de datos y las consultas sobre eventos de Lake conllevan costes. Cuando crea un almacén de datos de eventos, debe elegir la opción de precios que desee utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el período de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios.

Eventos de administración de Acceso verificado

Los eventos de administración proporcionan información sobre las operaciones de administración que se llevan a cabo en los recursos de su empresa Cuenta de AWS. Se denominan también operaciones del plano de control. De forma predeterminada, CloudTrail registra los eventos de administración.

Acceso verificado registra todas las operaciones de plano de control como eventos de administración. Para ver una lista, consulta la referencia de la EC2 API de Amazon.

Ejemplos de eventos de Acceso verificado

El siguiente ejemplo muestra un CloudTrail evento que demuestra la `CreateVerifiedAccessInstance` acción.


```
{
    "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"
}
```


Para obtener información sobre el contenido de los CloudTrail registros, consulte el contenido de los CloudTrail registros en la Guía del AWS CloudTrail usuario.

Cuotas para Acceso verificado de AWS

Cuenta de AWS Tiene cuotas predeterminadas, antes denominadas límites, para cada una de ellas Servicio de AWS. A menos que se indique lo contrario, cada cuota es específica de la región.

Cuotas de nivel Cuenta de AWS

Cuenta de AWS Tiene las siguientes cuotas relacionadas con el acceso verificado.

Nombre	Valor predeterminado	Ajustable	Descripción
Instancias de Acceso verificado	5	Sí	El número máximo de instancias de Acceso verificado que los clientes pueden crear en la región actual.
Grupos de Acceso verificado	10	Sí	El número máximo de grupos de Acceso verificado que los clientes pueden crear en la región actual.
Proveedores de confianza de Acceso verificado	15	Sí	El número máximo de proveedores de confianza de Acceso verificado que los clientes pueden crear en la región actual.
Puntos de conexión de Acceso verificado	50	Sí	El número máximo de puntos de conexión de Acceso verificado que los clientes pueden crear en la región actual.

Encabezados HTTP

A continuación se presentan los límites de tamaño para los encabezados HTTP.

Nombre	Valor predeterminado	Ajustable
Línea de solicitud	16 K	No
Encabezado único	16 K	No
Encabezado de respuesta completo	32 K	No
Encabezado de solicitud completo	64 K	No

Tráfico HTTP

El tiempo de espera de la conexión inactiva es de 60 segundos. Si una aplicación tarda más de 60 segundos en responder a una solicitud HTTP, el cliente recibe un error de tiempo de espera de la puerta de enlace HTTP 504. Si los registros de acceso verificado están habilitados, registramos cualquier error de HTTP 504.

Tamaño de la notificación de OIDC

El siguiente es el límite de tamaño de las notificaciones de OIDC.

Nombre	Valor predeterminado	Ajustable
Tamaño de la notificación de OIDC	11 K	No

IAM Identity Center

Acceso verificado puede proporcionar acceso a los usuarios de IAM Identity Center que estén asignados a un máximo de 1000 grupos.

Historial de revisión de la Guía del usuario de Acceso verificado

En la siguiente tabla se describen las versiones de la documentación de Acceso verificado.

Cambio	Descripción	Fecha
Support para los tokens de acceso en el contexto de la confianza	Actualización para añadirla a las reclamaciones `additional_user_context` de los usuarios de la OIDC.	24 de febrero de 2025
Support para recursos a través de protocolos que no son HTTP	Liberación del acceso a los recursos a través de protocolos que no son HTTP.	5 de febrero de 2025
Versión de prueba	Versión preliminar del acceso a los recursos a través de protocolos distintos de HTTP.	1 de diciembre de 2024
AWS política gestionada actualizada	Se ha realizado una actualización de la política de IAM AWS gestionada para el acceso verificado.	17 de noviembre de 2023
Cifrado de datos en reposo	AWS Verified Access cifra los datos en reposo de forma predeterminada mediante claves KMS AWS propias.	28 de septiembre de 2023
Compatibilidad con la conformidad con FIPS	Configure Acceso verificado para cumplir con las normas FIPS.	26 de septiembre de 2023
Registro optimizado	Se agregó una característica de registro que añade	19 de junio de 2023

	contextos de confianza a los registros.	
AWS política gestionada actualizada	Se ha realizado una actualización de la política de IAM AWS gestionada para el acceso verificado.	31 de mayo de 2023
Versión de GA	Versión general de la Guía del usuario de Acceso verificado. Incluye AWS WAF integración.	27 de abril de 2023
Versión de prueba	Versión de prueba de la Guía del usuario de Acceso verificado	29 de noviembre de 2022

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.