Guida per l'utente

AWS Accesso verificato

AWS Accesso verificato: Guida per l’utente

Table of Contents

Che cos'è Accesso verificato da AWS?

Con Accesso verificato da AWS, puoi fornire un accesso sicuro alle tue applicazioni senza richiedere l'uso di una rete privata virtuale (VPN). Verified Access valuta ogni richiesta di applicazione e aiuta a garantire che gli utenti possano accedere a ciascuna applicazione solo quando soddisfano i requisiti di sicurezza specificati.

Vantaggi dell'accesso verificato

- Livello di sicurezza migliorato: un modello di sicurezza tradizionale valuta l'accesso una sola volta e garantisce all'utente l'accesso a tutte le applicazioni. Verified Access valuta ogni richiesta di accesso alle applicazioni in tempo reale. Ciò rende difficile per i malintenzionati passare da un'applicazione all'altra.
- Integrazione con i servizi di sicurezza: Verified Access si integra con i servizi di gestione delle identità e dei dispositivi, inclusi servizi sia AWS di terze parti. Utilizzando i dati di questi servizi, Verified Access verifica l'affidabilità di utenti e dispositivi rispetto a una serie di requisiti di sicurezza e determina se l'utente debba avere accesso a un'applicazione.
- Esperienza utente migliorata: l'accesso verificato elimina la necessità per gli utenti di utilizzare una VPN per accedere alle applicazioni. Questo aiuta a ridurre il numero di casi di assistenza derivanti da problemi relativi alla VPN.
- Risoluzione dei problemi e controlli semplificati: Verified Access registra tutti i tentativi di accesso, fornendo visibilità centralizzata sull'accesso alle applicazioni, per aiutarvi a rispondere rapidamente agli incidenti di sicurezza e alle richieste di audit.

Accesso a Verified Access

Puoi utilizzare una delle seguenti interfacce per lavorare con Verified Access:

- Console di gestione AWS— Fornisce un'interfaccia web che è possibile utilizzare per creare e gestire risorse di accesso verificato. Accedi Console di gestione AWS e apri la console Amazon VPC all'indirizzo. https://console.aws.amazon.com/vpc/
- AWS Command Line Interface (AWS CLI) — Fornisce comandi per un'ampia gamma di Servizi AWS, tra cui Accesso verificato da AWS. AWS CLI È supportato su Windows, macOS e Linux. Per ottenere il AWS CLI, vedi AWS Command Line Interface.

- AWS SDKs— Fornisci informazioni specifiche per la lingua APIs. AWS SDKs Si occupano di molti dettagli di connessione, come il calcolo delle firme e la gestione dei tentativi di richiesta e degli errori. Per ulteriori informazioni, consulta AWS SDKs.
- API di query: forniscono operazioni API di basso livello accessibili tramite richieste HTTPS. L'utilizzo dell'API Query è il modo più diretto per accedere a Verified Access. Tuttavia, richiede che l'applicazione gestisca dettagli di basso livello, come la generazione dell'hash per firmare la richiesta e la gestione degli errori. Per ulteriori informazioni, consulta le azioni di accesso verificato nell'Amazon EC2 API Reference.

Questa guida descrive come utilizzare le risorse di accesso verificato Console di gestione AWS per creare, accedere e gestire le risorse di accesso verificato.

Prezzi

Ti viene addebitato ogni ora per ogni applicazione su Verified Access e ti viene addebitata la quantità di dati elaborati da Verified Access. Per ulteriori informazioni, consulta Prezzi di Accesso verificato da AWS.

Come funziona l'accesso verificato

Accesso verificato da AWS valuta ogni richiesta di applicazione da parte degli utenti e consente l'accesso in base a:

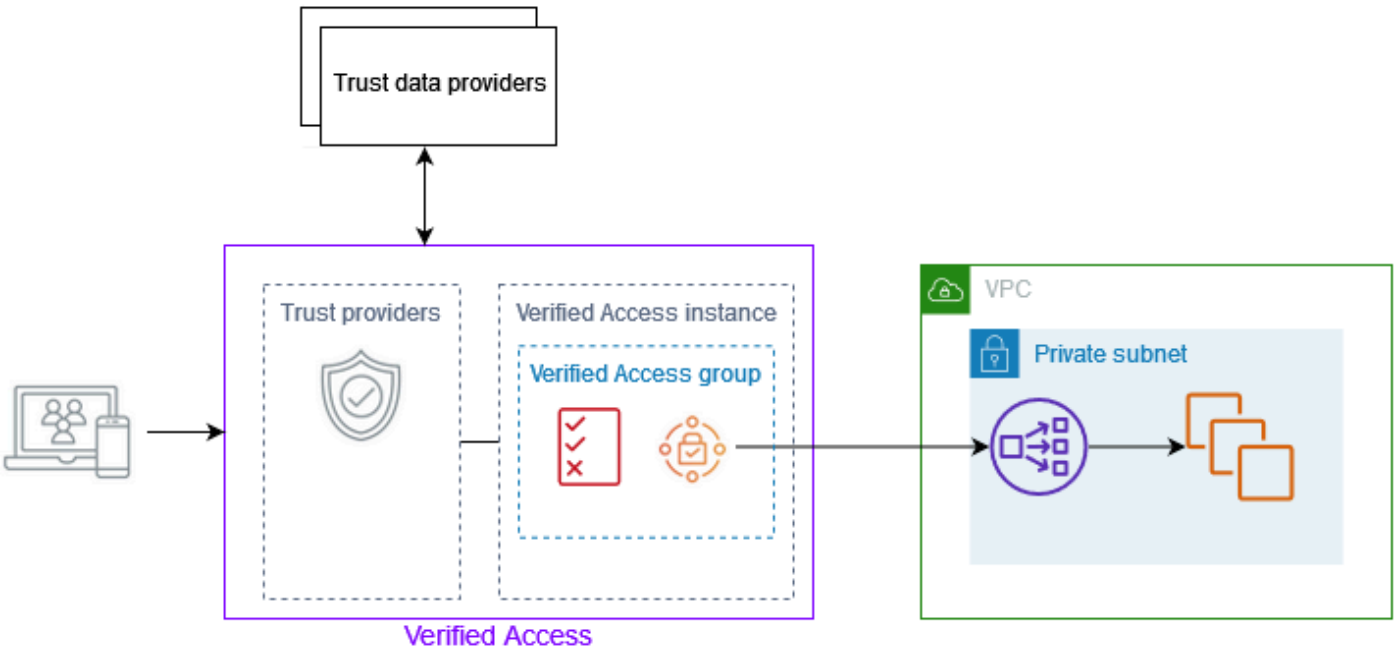
- Dati attendibili inviati dal fornitore fiduciario prescelto (da AWS o da una terza parte).
- Politiche di accesso che crei in Accesso verificato.

Quando un utente tenta di accedere a un'applicazione, Verified Access ottiene i dati dal trust provider e li valuta in base alle politiche impostate per l'applicazione. Verified Access concede l'accesso all'applicazione richiesta solo se l'utente soddisfa i requisiti di sicurezza specificati. Tutte le richieste di applicazione vengono rifiutate per impostazione predefinita, fino a quando non viene definita una policy.

Inoltre, Verified Access registra ogni tentativo di accesso, per aiutarvi a rispondere rapidamente agli incidenti di sicurezza e alle richieste di controllo.

Componenti chiave di Verified Access

Il diagramma seguente fornisce una panoramica di alto livello dell'accesso verificato. Gli utenti inviano richieste di accesso a un'applicazione. Verified Access valuta la richiesta in base alla politica di accesso del gruppo e a qualsiasi politica degli endpoint specifica dell'applicazione. Se l'accesso è consentito, la richiesta viene inviata all'applicazione tramite l'endpoint.



- Istanze di accesso verificato: un'istanza valuta le richieste dell'applicazione e concede l'accesso solo quando i requisiti di sicurezza sono soddisfatti.
- Endpoint ad accesso verificato: ogni endpoint rappresenta un'applicazione. Nel diagramma precedente, l'applicazione è ospitata su EC2 istanze che sono destinazioni di un sistema di bilanciamento del carico.
- Gruppo Verified Access: una raccolta di endpoint Verified Access. Ti consigliamo di raggruppare gli endpoint per applicazioni con requisiti di sicurezza simili per semplificare l'amministrazione delle policy. Ad esempio, puoi raggruppare gli endpoint per tutte le tue applicazioni di vendita.
- Criteri di accesso: un insieme di regole definite dall'utente che determinano se consentire o negare l'accesso a un'applicazione. È possibile specificare una combinazione di fattori, tra cui l'identità dell'utente e lo stato di sicurezza del dispositivo. Si crea una politica di accesso di gruppo per ogni gruppo di accesso verificato, che viene ereditata da tutti gli endpoint del gruppo. Facoltativamente, puoi creare policy specifiche per l'applicazione e collegarle a endpoint specifici.
- Trust provider: un servizio che gestisce le identità degli utenti o lo stato di sicurezza dei dispositivi. Verified Access funziona sia AWS con fornitori di fiducia che con fornitori di fiducia di terze parti. È necessario collegare almeno un provider fiduciario a ciascuna istanza di Verified Access. Puoi collegare un singolo provider di fiducia di identità e più provider di fiducia per dispositivi a ciascuna istanza di Verified Access.
- Dati attendibili: i dati relativi alla sicurezza per utenti o dispositivi che il tuo provider fiduciario invia a Verified Access. Detti anche affermazioni degli utenti o contesto di fiducia. Ad esempio, l'indirizzo

e-mail di un utente o la versione del sistema operativo di un dispositivo. Verified Access valuta questi dati rispetto alle politiche di accesso dell'utente quando riceve ogni richiesta di accesso a un'applicazione.

Tutorial: Inizia a usare Verified Access

Usa questo tutorial per iniziare Accesso verificato da AWS. Imparerai come creare e configurare risorse di accesso verificato.

Come parte di questo tutorial, aggiungerai un'applicazione a Verified Access. Alla fine del tutorial, utenti specifici possono accedere a quell'applicazione su Internet, senza utilizzare una VPN. Invece, lo utilizzerai AWS IAM Identity Center come provider di fiducia in materia di identità. Tieni presente che questo tutorial non utilizza anche un provider di fiducia per i dispositivi.

Processi

Prerequisiti del tutorial Verified Access

Di seguito sono riportati i prerequisiti per il completamento di questo tutorial:

- AWS IAM Identity Center abilitato nel Regione AWS sistema in cui stai lavorando. Puoi quindi utilizzare IAM Identity Center come fornitore di fiducia con accesso verificato. Per ulteriori informazioni, consulta Enable AWS IAM Identity Center nella Guida AWS IAM Identity Center per l'utente.
- Un gruppo di sicurezza per controllare l'accesso all'applicazione. Consenti tutto il traffico in entrata dal CIDR VPC e tutto il traffico in uscita.
- Un'applicazione in esecuzione con un sistema di bilanciamento del carico interno di Elastic Load Balancing. Associa il tuo gruppo di sicurezza al load balancer.

- Un certificato TLS autofirmato o pubblico in. AWS Certificate Manager Utilizza un certificato RSA con una lunghezza di chiave di 1.024 o 2.048.
- Un dominio ospitato pubblico e le autorizzazioni necessarie per aggiornare i record DNS per il dominio.
- Una policy IAM con le autorizzazioni necessarie per creare un'istanza. Accesso verificato da AWS Per ulteriori informazioni, consulta Politica per la creazione di istanze di accesso verificato.

Fase 1: Creare un provider fiduciario Verified Access

Utilizza la procedura seguente per configurarti AWS IAM Identity Center come fornitore di servizi fiduciari.

Per creare un provider fiduciario IAM Identity Center

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli fornitori di fiducia ad accesso verificato.
3. Scegli Crea un provider fiduciario di accesso verificato.
4. (Facoltativo) In Tag e Descrizione, inserisci un nome e una descrizione per il provider fiduciario Verified Access.
5. Inserisci un identificatore personalizzato da utilizzare in seguito quando lavori con le regole delle politiche per il nome di riferimento della politica. Ad esempio, puoi inserire**`idc`**.
6. Per il tipo di provider fiduciario, scegli User trust provider.
7. Per il tipo di User Trust Provider, scegli IAM Identity Center.
8. Scegli Create Verified Access Trust Provider.

Passaggio 2: creare un'istanza di accesso verificato

Utilizza la procedura seguente per creare un'istanza di accesso verificato.

Come creare un'istanza di accesso verificato

1. Nel riquadro di navigazione, scegli Istanze di accesso verificato.
2. Scegli Crea istanza di accesso verificato.
3. (Facoltativo) In Nome e descrizione, inserisci un nome e una descrizione per l'istanza di accesso verificato.

4. Per il provider fiduciario Verified Access, scegli il tuo provider fiduciario.
5. Scegli Crea istanza di accesso verificato.

Passaggio 3: creare un gruppo con accesso verificato

Utilizzare la procedura seguente per creare un gruppo con accesso verificato.

Come creare un gruppo di accesso verificato

1. Nel riquadro di navigazione, scegli Gruppi di accesso verificato.
2. Scegli Crea gruppo di accesso verificato.
3. (Facoltativo) In Tag e Descrizione, inserisci un nome e una descrizione per il gruppo.
4. Per l'istanza di accesso verificato, scegli la tua istanza di accesso verificato.
5. Mantieni vuota la definizione della politica. Aggiungerai una politica a livello di gruppo in un passaggio successivo.
6. Scegli Crea gruppo di accesso verificato.

Fase 4: Creare un endpoint con accesso verificato

Utilizzare la procedura seguente per creare un endpoint di accesso verificato. Questo passaggio presuppone che l'applicazione sia in esecuzione con un sistema di bilanciamento del carico interno di Elastic Load Balancing e che sia inserito un certificato di dominio pubblico. AWS Certificate Manager

Come creare un endpoint di accesso verificato

1. Nel riquadro di navigazione, scegli Endpoints ad accesso verificato.
2. Scegli Crea endpoint di accesso verificato.
3. (Facoltativo) Per Tag nome e Descrizione, inserisci un nome e una descrizione per l'endpoint.
4. Per il gruppo di accesso verificato, scegli il tuo gruppo di accesso verificato.
5. Per i dettagli sull'endpoint, procedi come segue:
    a. Per Protocollo, seleziona HTTPS o HTTP, a seconda della configurazione del tuo sistema di bilanciamento del carico.
    b. In Attachment type (Tipo collegamento), selezionare VPC.

c. Per il tipo di endpoint, scegli Load balancer.

d. In Porta, inserisci il numero di porta utilizzato dal tuo listener di load balancer. Ad esempio, 443 per HTTPS o 80 per HTTP.

e. Per Load balancer ARN, scegli il tuo load balancer.

f. Per Subnet, seleziona le sottoreti associate al tuo load balancer.

g. Per i gruppi di sicurezza, seleziona il tuo gruppo di sicurezza. L'utilizzo dello stesso gruppo di sicurezza per il sistema di bilanciamento del carico e l'endpoint consente il traffico tra di essi. Se preferisci non utilizzare lo stesso gruppo di sicurezza, assicurati di fare riferimento al gruppo di sicurezza degli endpoint del tuo sistema di bilanciamento del carico in modo che accetti il traffico dall'endpoint.

h. Per il prefisso del dominio Endpoint, inserisci un identificatore personalizzato. Ad esempio, **`my-ava-app`**. Questo prefisso viene aggiunto al nome DNS generato da Verified Access.

6. Per i dettagli dell'applicazione, procedi come segue:

   a. Per Dominio dell'applicazione, inserisci il nome DNS dell'applicazione. Questo dominio deve corrispondere a quello del certificato di dominio.

   b. Per Certificato di dominio ARN, seleziona l'Amazon Resource Name (ARN) del certificato di dominio in. AWS Certificate Manager

7. Lascia vuoti i dettagli della policy. Aggiungerai una politica di accesso a livello di gruppo in un passaggio successivo.

8. Scegli Crea endpoint di accesso verificato.

Passaggio 5: configurare il DNS per l'endpoint di accesso verificato

Per questo passaggio, mappi il nome di dominio dell'applicazione (ad esempio, www.myapp.example.com) al nome di dominio dell'endpoint Verified Access. Per completare la mappatura DNS, crea un Canonical Name Record (CNAME) con il tuo provider DNS. Dopo aver creato il record CNAME, tutte le richieste degli utenti alla tua applicazione verranno inviate a Verified Access.

Per ottenere il nome di dominio del tuo endpoint

1. Nel riquadro di navigazione, scegli Endpoints ad accesso verificato.
2. Seleziona il tuo endpoint.
3. Seleziona la scheda Details (Dettagli).

4. Copia il dominio dal dominio Endpoint. Di seguito è riportato un esempio di nome di dominio endpoint:. `my-ava-app.edge-1a2b3c4d5e6f7g.vai-1a2b3c4d5e6f7g.prod.verified-access.us-west-2.amazonaws.com`

Segui le istruzioni fornite dal tuo provider DNS per creare un record CNAME. Usa il nome di dominio dell'applicazione come nome del record e il nome di dominio dell'endpoint di accesso verificato come valore del record.

Fase 6: Verifica della connettività all'applicazione

Ora puoi testare la connettività alla tua applicazione. Inserisci il nome di dominio dell'applicazione nel tuo browser web. Il comportamento predefinito di Verified Access consiste nel rifiutare tutte le richieste. Poiché non abbiamo aggiunto una politica di accesso verificato al gruppo o all'endpoint, tutte le richieste vengono rifiutate.

Passaggio 7: aggiungere una politica di accesso a livello di gruppo con accesso verificato

Utilizza la seguente procedura per modificare il gruppo di accesso verificato e configurare una politica di accesso che consenta la connettività all'applicazione. I dettagli della policy dipenderanno dagli utenti e dai gruppi configurati in IAM Identity Center. Per informazioni, consulta Politiche di accesso verificato.

Per modificare un gruppo di accesso verificato

1. Nel riquadro di navigazione, scegli Gruppi di accesso verificato.
2. Seleziona il gruppo .
3. Scegli Azioni, Modifica la politica di gruppo di accesso verificato.
4. Attiva Abilita politica.
5. Inserisci una policy che consenta agli utenti del tuo IAM Identity Center di accedere alla tua applicazione. Per alcuni esempi, consulta the section called "Policy di esempio".
6. Scegli Modifica la politica di gruppo di accesso verificato.
7. Ora che la politica di gruppo è in vigore, ripeti il test del passaggio precedente per verificare che la richiesta sia consentita. Se la richiesta è consentita, ti viene richiesto di accedere tramite la

pagina di accesso di IAM Identity Center. Dopo aver fornito il nome utente e la password, puoi accedere all'applicazione.

Pulisci le tue risorse di accesso verificato

Al termine di questo tutorial, utilizza la seguente procedura per eliminare le risorse di accesso verificato.

Per eliminare le tue risorse di accesso verificato

1. Nel riquadro di navigazione, scegli Endpoint di accesso verificato. Seleziona l'endpoint e scegli Azioni, Elimina endpoint di accesso verificato.
2. Nel riquadro di navigazione, scegli Gruppi di accesso verificato. Seleziona il gruppo e scegli Azioni, Elimina gruppo con accesso verificato. Potrebbe essere necessario attendere il completamento del processo di eliminazione dell'endpoint.
3. Nel riquadro di navigazione, scegli Istanze di accesso verificato. Seleziona la tua istanza e scegli Actions, Detach Verified Access trust provider. Seleziona il fornitore di fiducia e scegli Detach Verified Access trust provider.
4. Nel riquadro di navigazione, scegli Provider fiduciari di accesso verificato. Seleziona il tuo fornitore di fiducia e scegli Azioni, Elimina fornitore di fiducia con accesso verificato.
5. Nel riquadro di navigazione, scegli Istanze di accesso verificato. Seleziona la tua istanza e scegli Azioni, Elimina istanza di accesso verificato.

Istanze di accesso verificato

Un' Accesso verificato da AWS istanza è una AWS risorsa che ti aiuta a organizzare i tuoi provider fiduciari e i gruppi di accesso verificato. Un'istanza valuta le richieste delle applicazioni e concede l'accesso solo quando i requisiti di sicurezza sono soddisfatti.

Processi

- Crea e gestisci un'istanza di accesso verificato
- Eliminare un'istanza di accesso verificato
- Integra Verified Access con AWS WAF
- Conformità FIPS per l'accesso verificato

Crea e gestisci un'istanza di accesso verificato

Utilizzi un'istanza di accesso verificato per organizzare i fornitori di fiducia e i gruppi di accesso verificato. Utilizza le seguenti procedure per creare un'istanza di accesso verificato, quindi collegare un provider fiduciario a Verified Access o scollegare un provider fiduciario da Verified Access.

Processi

- Crea un'istanza di accesso verificato
- Collegare un provider fiduciario a un'istanza di accesso verificato
- Scollega un fornitore di fiducia da un'istanza di accesso verificato
- Aggiungi un sottodominio personalizzato

Crea un'istanza di accesso verificato

Utilizza la procedura seguente per creare un'istanza di accesso verificato.

Per creare un'istanza di accesso verificato utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Istanze di accesso verificato, quindi Crea istanza di accesso verificato.
3. (Facoltativo) In Nome e Descrizione, inserisci un nome e una descrizione per l'istanza di accesso verificato.

4. (Endpoint CIDR di rete) Per il sottodominio personalizzato per l'endpoint CIDR di rete, inserisci un sottodominio personalizzato.
5. (Facoltativo) Scegliete Enable for Federal Information Process Standards (FIPS) se desiderate che Verified Access sia conforme allo standard FIPS.
6. (Facoltativo) Per il provider fiduciario Verified Access, scegli un provider fiduciario da collegare all'istanza di Verified Access.
7. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
8. Scegli Crea istanza di accesso verificato.

Per creare un'istanza di accesso verificato utilizzando il AWS CLI

Utilizza il comando create-verified-access-instance.

Collegare un provider fiduciario a un'istanza di accesso verificato

Utilizzare la procedura seguente per collegare un provider fiduciario a un'istanza di accesso verificato.

Per collegare un provider fiduciario a un'istanza di accesso verificato utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Istanze di accesso verificato.
3. Selezionare l'istanza.
4. Scegli Azioni, collega un provider fiduciario di accesso verificato.
5. Per un provider fiduciario ad accesso verificato, scegli un fornitore di fiducia.
6. Scegli Attach Verified Access Trust Provider.

Per collegare un provider fiduciario a un'istanza di accesso verificato utilizzando il AWS CLI

Utilizzate il comando attach-verified-access-trust-provider.

Scollega un fornitore di fiducia da un'istanza di accesso verificato

Utilizzare la procedura seguente per scollegare un provider fiduciario da un'istanza di accesso verificato.

Per scollegare un provider fiduciario da un'istanza di accesso verificato utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Istanze di accesso verificato.
3. Selezionare l'istanza.
4. Scegli Azioni, Scollega provider fiduciario di accesso verificato.
5. Per Verified Access Trust Provider, scegli il provider fiduciario.
6. Scegli Detach Verified Access trust provider.

Per scollegare un provider fiduciario da un'istanza di accesso verificato utilizzando il AWS CLI

Utilizzate il comando detach-verified-access-trust-provider.

Aggiungi un sottodominio personalizzato

Utilizza la procedura seguente per aggiungere o aggiornare un sottodominio personalizzato. Questo sottodominio viene utilizzato solo quando si crea un endpoint CIDR di rete.

Per aggiungere un sottodominio personalizzato utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Istanze di accesso verificato.
3. Selezionare l'istanza.
4. Scegli Azioni, Modifica istanza di accesso verificato.
5. Per Sottodominio personalizzato per endpoint CIDR di rete, inserisci un sottodominio personalizzato.
6. Scegli Modifica istanza di accesso verificato.
7. Aggiorna i nameserver per il tuo sottodominio, inserendo i nameserver forniti da Verified Access. Questo elenco è disponibile in Nameservers nella scheda Dettagli dell'istanza.

Per aggiungere un sottodominio personalizzato utilizzando AWS CLI

Utilizza il comando modify-verified-access-instance.

Eliminare un'istanza di accesso verificato

Quando hai finito con un'istanza di accesso verificato, puoi eliminarla. Prima di poter eliminare un'istanza, è necessario rimuovere tutti i provider fiduciari o i gruppi di accesso verificato associati.

Per eliminare un'istanza di accesso verificato utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Istanze di accesso verificato.
3. Seleziona l'istanza di accesso verificato.
4. Scegli Azioni, Elimina istanza di accesso verificato.
5. Quando viene richiesta la conferma, inserisci **`delete`** e scegli Delete (Elimina).

Per eliminare un'istanza di accesso verificato utilizzando il AWS CLI

Utilizza il comando delete-verified-access-instance.

Integra Verified Access con AWS WAF

Oltre alle regole di autenticazione e autorizzazione applicate da Verified Access, potresti voler applicare anche la protezione perimetrale. Questo può aiutarti a proteggere le tue applicazioni da minacce aggiuntive. Puoi farlo integrandoti AWS WAF nella tua implementazione di Verified Access. AWS WAF è un firewall per applicazioni Web che consente di monitorare le richieste HTTP inoltrate alle risorse protette delle applicazioni Web. Per ulteriori informazioni, consulta la Guida per gli sviluppatori di AWS WAF.

È possibile effettuare l'integrazione AWS WAF con Verified Access associando una lista di controllo degli accessi AWS WAF Web (ACL) a un'istanza di accesso verificato. Un ACL web è una AWS WAF risorsa che offre un controllo dettagliato su tutte le richieste Web HTTP a cui risponde la risorsa protetta. Durante l'elaborazione della richiesta di AWS WAF associazione o disassociazione, lo stato di tutti gli endpoint di accesso verificato collegati all'istanza viene visualizzato come. `updating` Una volta completata la richiesta, lo stato torna a. `active` È possibile visualizzare lo stato in Console di gestione AWS o descrivendo l'endpoint con. AWS CLI

Il provider di fiducia per l'identità dell'utente determina quando AWS WAF ispeziona il traffico. Se utilizzi IAM Identity Center, AWS WAF ispeziona il traffico prima dell'autenticazione dell'utente. Se si utilizza OpenID Connect (OIDC), AWS WAF ispeziona il traffico dopo l'autenticazione dell'utente.

Indice

Autorizzazioni IAM richieste

L'integrazione AWS WAF con Verified Access include azioni di sola autorizzazione che non corrispondono direttamente a un'operazione API. Queste azioni sono indicate nel AWS Identity and Access Management Service Authorization Reference con. `[permission only]` Consulta Azioni, risorse e chiavi di condizione per Amazon EC2 nel Service Authorization Reference.

Per lavorare con un ACL web, il AWS Identity and Access Management principale deve disporre delle seguenti autorizzazioni.

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

Associa un ACL web AWS WAF

I passaggi seguenti mostrano come associare una lista di controllo degli accessi AWS WAF Web (ACL) a un'istanza di accesso verificato utilizzando la console Verified Access.

Prerequisito

Prima di iniziare, crea un ACL AWS WAF web. Per ulteriori informazioni, consulta Creare un ACL web nella Guida per gli AWS WAF sviluppatori.

Per associare un ACL AWS WAF Web a un'istanza di accesso verificato

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Istanze di accesso verificato.
3. Seleziona l'istanza di accesso verificato.

4. Seleziona la scheda Integrazioni.
5. Scegli Azioni, quindi Associa Web ACL.
6. Per Web ACL, scegli un ACL Web esistente, quindi scegli Associa ACL Web.

In alternativa, puoi usare la console. AWS WAF Se utilizzi la AWS WAF console o l'API, hai bisogno dell'Amazon Resource Name (ARN) della tua istanza Verified Access. Un ARN AVA ha il seguente formato:. `arn:${Partition}:ec2:${Region}:${Account}:verified-access-instance/${VerifiedAccessInstanceId}` Per maggiori informazioni, consulta Associare un ACL web a una AWS risorsa nella AWS WAF Developer Guide.

Verificate lo stato dell'associazione

È possibile verificare se una lista di controllo degli accessi AWS WAF Web (ACL) è associata o meno a un'istanza di accesso verificato utilizzando la console Verified Access.

Per visualizzare lo stato dell' AWS WAF integrazione con un'istanza di accesso verificato

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Istanze di accesso verificato.
3. Seleziona l'istanza di accesso verificato.
4. Seleziona la scheda Integrazioni.
5. Controlla i dettagli elencati nella sezione Stato dell'integrazione WAF. Lo stato verrà visualizzato come Associato o Non associato, insieme all'identificatore web ACL, se si trova nello stato Associato.

Dissocia un ACL web AWS WAF

I passaggi seguenti mostrano come dissociare una lista di controllo degli accessi AWS WAF Web (ACL) da un'istanza di accesso verificato utilizzando la console Verified Access.

Per dissociare un ACL AWS WAF Web da un'istanza di accesso verificato

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Istanze di accesso verificato.
3. Seleziona l'istanza di accesso verificato.
4. Seleziona la scheda Integrazioni.

5. Scegli Azioni, quindi Disassocia Web ACL.
6. Confermate scegliendo Dissocia Web ACL.

In alternativa, puoi usare la AWS WAF console. Per ulteriori informazioni, consulta Dissociare un ACL Web da una AWS risorsa nella Guida per gli AWS WAF sviluppatori.

Conformità FIPS per l'accesso verificato

Il Federal Information Processing Standard (FIPS) è uno standard governativo statunitense e canadese che specifica i requisiti di sicurezza per i moduli crittografici che proteggono le informazioni sensibili. Accesso verificato da AWS offre la possibilità di configurare l'ambiente in modo che aderisca alla pubblicazione FIPS 140-2. La conformità FIPS per l'accesso verificato è disponibile nelle seguenti regioni: AWS

- Stati Uniti orientali (Ohio)
- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti occidentali (California settentrionale)
- Stati Uniti occidentali (Oregon)
- Canada (Centrale)
- AWS GovCloud (US) Ovest
- AWS GovCloud (US) Est

Questa pagina mostra come configurare un ambiente di accesso verificato nuovo o esistente in modo che sia conforme allo standard FIPS.

Indice

Configura un ambiente di accesso verificato esistente per la conformità FIPS

Se disponi di un ambiente di accesso verificato esistente e desideri configurarlo in modo che sia conforme a FIPS, alcune risorse dovranno essere eliminate e ricreate per attivare la conformità FIPS.

Per riconfigurare un Accesso verificato da AWS ambiente esistente in modo che sia conforme a FIPS, procedi nel seguente modo.

1. Elimina gli endpoint, i gruppi e l'istanza originali di Verified Access. I provider fiduciari configurati possono essere riutilizzati.
2. Crea un'istanza di accesso verificato, assicurandoti di abilitare i Federal Information Process Standards (FIPS) durante la creazione. Inoltre, durante la creazione, collega il provider fiduciario Verified Access che desideri utilizzare, selezionandolo dall'elenco a discesa.
3. Crea un gruppo di accesso verificato. Durante la creazione del gruppo, lo associ all'istanza di accesso verificato appena creata.
4. Creane uno o piùEndpoint con accesso verificato. Durante la creazione dei tuoi endpoint, li associ al gruppo creato nel passaggio precedente.

Configura un nuovo ambiente di accesso verificato per la conformità FIPS

Per configurare un nuovo Accesso verificato da AWS ambiente conforme a FIPS, procedi nel seguente modo.

1. Configura un fornitore di fiducia. Dovrai creare un provider di fiducia per l'identità degli utenti e (facoltativamente) un provider di fiducia basato sui dispositivi, a seconda delle tue esigenze.
2. Crea un'istanza di accesso verificato, assicurandoti di abilitare i Federal Information Process Standards (FIPS) durante il processo. Inoltre, durante la creazione, collega il provider fiduciario Verified Access che hai creato nel passaggio precedente, selezionandolo dall'elenco a discesa.
3. Crea un gruppo di accesso verificato. Durante la creazione del gruppo, lo associ all'istanza di accesso verificato appena creata.
4. Creane uno o piùEndpoint con accesso verificato. Durante la creazione dei tuoi endpoint, li associ al gruppo creato nel passaggio precedente.

Fornitori di fiducia per l'accesso verificato

Un provider fiduciario è un servizio che invia informazioni su utenti e dispositivi a Accesso verificato da AWS. Queste informazioni sono denominate contesto di fiducia. Può includere attributi basati sull'identità dell'utente, come un indirizzo e-mail o l'appartenenza all'organizzazione «vendita», o informazioni sul dispositivo come le patch di sicurezza installate o la versione del software antivirus.

Verified Access supporta le seguenti categorie di provider fiduciari:

- Identità utente: un servizio di provider di identità (IdP) che archivia e gestisce le identità digitali degli utenti.
- Gestione dei dispositivi: un sistema di gestione dei dispositivi per dispositivi come laptop, tablet e smartphone.

Indice

Provider affidabili per l'identità degli utenti per l'accesso verificato

Puoi scegliere di utilizzare uno dei due AWS IAM Identity Center o un provider fiduciario di identità utente compatibile con OpenID Connect.

Indice

Utilizzo di IAM Identity Center come fornitore di fiducia

Puoi utilizzarlo AWS IAM Identity Center come provider fiduciario per l'identità utente con AWS Verified Access.

Prerequisiti e considerazioni

- La tua istanza IAM Identity Center deve essere un' AWS Organizations istanza. Un'istanza IAM Identity Center con AWS account autonomo non funzionerà.

- L'istanza IAM Identity Center deve essere abilitata nella stessa AWS regione in cui desideri creare il provider fiduciario Verified Access.
- Verified Access può fornire l'accesso agli utenti di IAM Identity Center assegnati a un massimo di 1.000 gruppi.

Consulta Gestire le istanze dell'organizzazione e dell'account di IAM Identity Center nella Guida per l'AWS IAM Identity Center utente per i dettagli sui diversi tipi di istanze.

Crea un provider fiduciario IAM Identity Center

Dopo aver abilitato IAM Identity Center sul tuo AWS account, puoi utilizzare la seguente procedura per configurare IAM Identity Center come provider di fiducia per l'accesso verificato.

Per creare un provider di fiducia IAM Identity Center (AWS console)

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Provider fiduciari di accesso verificato, quindi Crea provider fiduciario di accesso verificato.
3. (Facoltativo) In Tag e Descrizione, inserisci un nome e una descrizione per il fornitore di fiducia.
4. Per il nome di riferimento della politica, inserisci un identificatore da utilizzare in seguito quando lavori con le regole delle politiche.
5. In Tipo di provider fiduciario, seleziona User trust provider.
6. In User trust provider type, seleziona IAM Identity Center.
7. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
8. Scegli Create Verified Access Trust Provider.

Per creare un provider di fiducia (AWS CLI) di IAM Identity Center

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

Elimina un provider fiduciario IAM Identity Center

Prima di poter eliminare un trust provider, devi rimuovere tutte le configurazioni di endpoint e gruppi dall'istanza a cui è collegato il trust provider.

Per eliminare un provider di fiducia IAM Identity Center (AWS console)

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Provider fiduciari di accesso verificato, quindi seleziona il provider di fiducia che desideri eliminare nella sezione Provider fiduciari di accesso verificato.
3. Scegli Azioni, quindi Elimina provider fiduciario di accesso verificato.
4. Conferma l'eliminazione `delete` inserendo nella casella di testo.
5. Scegli Elimina.

Per eliminare un provider fiduciario (AWS CLI) di IAM Identity Center

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

Usa un provider di fiducia OpenID Connect

Accesso verificato da AWS supporta provider di identità che utilizzano metodi OpenID Connect (OIDC) standard. È possibile utilizzare provider compatibili con OIDC come provider fiduciari di identità utente con accesso verificato. Tuttavia, a causa dell'ampia gamma di potenziali fornitori OIDC, non AWS è in grado di testare ogni integrazione OIDC con Verified Access.

Verified Access ottiene i dati di fiducia che valuta dal provider OIDC. `UserInfo Endpoint` Il `Scope` parametro viene utilizzato per determinare quali set di dati di attendibilità verranno recuperati. Dopo aver ricevuto i dati di attendibilità, la politica di accesso verificato viene valutata in base a tali dati.

Con i provider fiduciari creati il 24 febbraio 2025, le dichiarazioni relative al token ID del provider fiduciario OIDC sono incluse nella chiave. `addition_user_context`

Con i provider fiduciari creati prima del 24 febbraio 2025, Verified Access non utilizza i dati attendibili `ID token` inviati dal provider OIDC. Solo i dati attendibili di `UserInfo Endpoint` vengono valutati rispetto alla politica.

Con i provider di fiducia creati a partire dal 24 febbraio 2025, la durata della sessione predefinita è di un giorno. Con i provider fiduciari creati prima del 24 febbraio 2025, la durata predefinita della sessione è di sette giorni.

Se viene specificato un token di aggiornamento, Verified Access utilizza la scadenza del token di aggiornamento come durata della sessione. Se non è presente alcun token di aggiornamento, viene utilizzata la durata della sessione predefinita.

Indice

Prerequisiti per la creazione di un provider fiduciario OIDC

Dovrai raccogliere le seguenti informazioni direttamente dal tuo fornitore di fiducia:

- Emittente
- Endpoint di autorizzazione
- Endpoint Token
- UserInfo endpoint
- ID client
- Client secret
- Scope

Crea un provider fiduciario OIDC

Utilizza la procedura seguente per creare un OIDC come provider fiduciario.

Per creare un provider di fiducia OIDC (console)AWS

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Provider fiduciari di accesso verificato, quindi Crea provider fiduciario di accesso verificato.
3. (Facoltativo) In Tag e Descrizione, inserisci un nome e una descrizione per il fornitore di fiducia.
4. Per il nome di riferimento della politica, inserisci un identificatore da utilizzare in seguito quando lavori con le regole delle politiche.
5. In Tipo di provider fiduciario, seleziona User trust provider.
6. In User trust provider type, seleziona OIDC (OpenID Connect).
7. Per OIDC (OpenID Connect), scegli il provider di fiducia.
8. Per Emittente, inserisci l'identificativo dell'emittente OIDC.

9. Per Endpoint di autorizzazione, inserisci l'URL completo dell'endpoint di autorizzazione.
10. Per Token endpoint, inserisci l'URL completo dell'endpoint token.
11. Per User endpoint, inserisci l'URL completo dell'endpoint utente.
12. (Native Application OIDC) Per l'URL della chiave di firma pubblica, inserisci l'URL completo dell'endpoint della chiave di firma pubblica.
13. Immettete l'identificatore client OAuth 2.0 per Client ID.
14. Inserisci il segreto del client OAuth 2.0 per il segreto del cliente.
15. Inserisci un elenco di ambiti delimitato da spazi definiti con il tuo provider di identità. Come minimo, l'openidambito è obbligatorio per Scope.
16. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
17. Scegli Create Verified Access Trust Provider.
18. Devi aggiungere un URI di reindirizzamento all'elenco degli indirizzi consentiti per il tuo provider OIDC.
    - Applicazioni HTTP: utilizza il seguente URI:. **`https://application_domain/oauth2/idpresponse`** Nella console, puoi trovare il dominio dell'applicazione nella scheda Dettagli per l'endpoint Verified Access. Utilizzando l'SDK AWS CLI o un AWS SDK, il dominio dell'applicazione viene incluso nell'output quando si descrive l'endpoint Verified Access.
    - Applicazioni TCP: utilizza il seguente URI:. **`http://localhost:8000`**

Per creare un provider di fiducia OIDC (CLI AWS)

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

Modifica un provider fiduciario OIDC

Dopo aver creato un provider fiduciario, puoi aggiornarne la configurazione.

Per modificare un provider di fiducia OIDC (console)AWS

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Provider fiduciari di accesso verificato, quindi seleziona il provider fiduciario che desideri modificare in Provider fiduciari di accesso verificato.
3. Scegli Azioni, quindi Modifica provider fiduciario di accesso verificato.

4. Modifica le opzioni che desideri modificare.
5. Scegli Modify Verified Access Trust Provider.

Per modificare un provider di fiducia OIDC (CLI AWS)

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

Eliminare un provider fiduciario OIDC

Prima di poter eliminare un provider di fiducia utente, è necessario rimuovere tutte le configurazioni di endpoint e gruppi dall'istanza a cui è collegato il trust provider.

Per eliminare un provider di fiducia OIDC (console)AWS

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Provider fiduciari con accesso verificato, quindi seleziona il provider fiduciario che desideri eliminare in Provider fiduciari ad accesso verificato.
3. Scegli Azioni, quindi Elimina provider fiduciario di accesso verificato.
4. Conferma l'eliminazione `delete` inserendo nella casella di testo.
5. Scegli Elimina.

Per eliminare un provider di fiducia OIDC (CLI AWS)

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

Provider affidabili basati su dispositivi per l'accesso verificato

Puoi utilizzare provider affidabili per dispositivi con AWS accesso verificato. Puoi utilizzare uno o più provider affidabili per dispositivi con la tua istanza di accesso verificato.

Indice

Provider affidabili per dispositivi supportati

I seguenti provider di fiducia per i dispositivi possono essere integrati con Verified Access:

- CrowdStrike — Protezione delle applicazioni private con CrowdStrike accesso AWS verificato
- Jamf: integrazione dell'accesso verificato con Jamf Device Identity
- JumpCloud — JumpCloud Integrazione e accesso verificato AWS

Crea un provider di fiducia basato su dispositivi

Segui questi passaggi per creare e configurare un provider affidabile per dispositivi da utilizzare con Verified Access.

Per creare un provider affidabile per dispositivi con accesso verificato (AWS console)

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Provider affidabili di accesso verificato, quindi Crea provider fiduciario di accesso verificato.
3. (Facoltativo) In Tag e Descrizione, inserisci un nome e una descrizione per il fornitore di fiducia.
4. Immettete un identificatore da utilizzare in seguito quando lavorate con le regole dei criteri per il nome di riferimento della politica.
5. Per il tipo di provider fiduciario, seleziona Identità del dispositivo.
6. Per Tipo di identità del dispositivo, scegli Jamf o JumpCloud. CrowdStrike
7. Per ID tenant, inserisci l'identificatore dell'applicazione tenant.
8. (Facoltativo) Per l'URL della chiave di firma pubblica, inserisci l'URL della chiave univoca condiviso dal provider di fiducia del dispositivo. (Questo parametro non è obbligatorio per Jamf CrowdStrike o Jumpcloud.)
9. Scegli Create Verified Access Trust Provider.

> **Note**
>
> Dovrai aggiungere un URI di reindirizzamento alla lista delle autorizzazioni del tuo provider OIDC. Ti consigliamo di utilizzare l'endpoint `DeviceValidationDomain` di accesso verificato per questo scopo. È possibile trovarlo nella Console di gestione AWS scheda Dettagli dell'endpoint di accesso verificato o utilizzando la per AWS CLI descrivere l'endpoint.

Aggiungi quanto segue alla lista delle autorizzazioni del tuo provider OIDC: https:///oauth2/idpresponse `DeviceValidationDomain`

Per creare un provider di fiducia per dispositivi ad accesso verificato (AWS CLI)

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

Modifica un provider di fiducia basato su dispositivi

Dopo aver creato un trust provider, è possibile aggiornarne la configurazione.

Per modificare un provider affidabile di dispositivi con accesso verificato (AWS console)

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Provider affidabili di accesso verificato.
3. Seleziona il fornitore di fiducia.
4. Scegli Azioni, quindi seleziona Modifica provider fiduciario di accesso verificato.
5. Modifica la descrizione in base alle esigenze.
6. (Facoltativo) Per l'URL della chiave di firma pubblica, modifica l'URL della chiave univoca condiviso dal provider di fiducia del dispositivo. (Questo parametro non è richiesto se il provider di fiducia del dispositivo è Jamf CrowdStrike o Jumpcloud.)
7. Scegli Modify Verified Access Trust Provider.

Per modificare un provider di fiducia per dispositivi ad accesso verificato (AWS CLI)

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

Elimina un provider di fiducia basato su dispositivi

Quando hai finito con un fornitore di fiducia, puoi eliminarlo.

Per eliminare un provider affidabile di dispositivi con accesso verificato (AWS console)

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Provider affidabili di accesso verificato.

3. Seleziona il fornitore di fiducia che desideri eliminare nella sezione Provider fiduciari con accesso verificato.
4. Scegli Azioni, quindi seleziona Elimina fornitore di fiducia con accesso verificato.
5. Quando viene richiesta la conferma, inserisci **`delete`** e scegli Delete (Elimina).

Per eliminare un provider di fiducia per dispositivi ad accesso verificato (AWS CLI)

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

Gruppi di accesso verificato

Un gruppo di accesso verificato è costituito da endpoint di accesso verificato e da una politica di accesso verificato che si applica a tutti gli endpoint del gruppo. Raggruppando gli endpoint che hanno requisiti di sicurezza comuni, è possibile definire una singola policy di gruppo che soddisfi i requisiti minimi di sicurezza di più endpoint. Pertanto, non è necessario creare e mantenere una policy per ogni endpoint.

Ad esempio, puoi raggruppare tutte le applicazioni di vendita e impostare una politica di accesso a livello di gruppo. È quindi possibile utilizzare questa politica per definire un set comune di requisiti minimi di sicurezza per tutte le applicazioni di vendita. Questo approccio aiuta a semplificare l'amministrazione delle politiche.

Quando si crea un gruppo, è necessario associare il gruppo a un'istanza di accesso verificato. Durante il processo di creazione di un endpoint, assocerai l'endpoint a un gruppo.

Un'altra funzionalità dei gruppi ad accesso verificato è la possibilità di condividerli con altri AWS account utilizzando. AWS RAM Ciò consente di creare e gestire gruppi centralmente in un unico account, quindi condividerli con più account.

Processi

- Crea e gestisci un gruppo con accesso verificato
- Modificare una politica di gruppo con accesso verificato
- Condividi un gruppo ad accesso verificato con un altro Account AWS
- Elimina un gruppo con accesso verificato

Crea e gestisci un gruppo con accesso verificato

Utilizzi i gruppi di accesso verificato per organizzare gli endpoint in base ai rispettivi requisiti di sicurezza. Quando crei un endpoint Verified Access, associ l'endpoint a un gruppo.

Processi

- Crea un gruppo con accesso verificato
- Modificare un gruppo con accesso verificato

Crea un gruppo con accesso verificato

Utilizza le seguenti procedure per creare un gruppo con accesso verificato. Prima di creare un gruppo con accesso verificato, è necessario creare un'istanza di accesso verificato. Per ulteriori informazioni, consulta the section called "Crea un'istanza di accesso verificato".

Per creare un gruppo con accesso verificato utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Gruppi con accesso verificato, quindi Crea gruppo con accesso verificato.
3. (Facoltativo) In Tag nome e Descrizione, inserisci un nome e una descrizione per il gruppo.
4. Per l'istanza di accesso verificato, seleziona un'istanza di accesso verificato da associare al gruppo.
5. (Facoltativo) Per la definizione della politica, inserisci una politica di accesso verificato da applicare al gruppo.
6. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
7. Scegli Crea gruppo di accesso verificato.

Per creare un gruppo con accesso verificato utilizzando il AWS CLI

Utilizza il comando create-verified-access-group.

Modificare un gruppo con accesso verificato

Utilizzare la procedura seguente per modificare un gruppo di accesso verificato.

Per modificare un gruppo con accesso verificato utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Gruppi con accesso verificato, quindi Crea gruppo con accesso verificato.
3. Seleziona il gruppo, quindi scegli Azioni, Modifica gruppo di accesso verificato.
4. (Facoltativo) Aggiorna la descrizione.
5. Scegli Crea gruppo di accesso verificato.

6. Scegli l'istanza di accesso verificato da associare al gruppo.

Per modificare un gruppo con accesso verificato utilizzando il AWS CLI

Utilizza il comando modify-verified-access-group.

Modificare una politica di gruppo con accesso verificato

Accesso verificato da AWSconsente l'accesso alle applicazioni in base alle politiche di accesso create. La politica di accesso verificato associata a un gruppo viene ereditata da tutti gli endpoint del gruppo. Facoltativamente, puoi allegare policy specifiche dell'applicazione a endpoint specifici.

Utilizzare la procedura seguente per modificare la politica per un gruppo di accesso verificato. Dopo aver apportato le modifiche, occorrono alcuni minuti prima che abbiano effetto.

Per modificare una politica di gruppo con accesso verificato utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Gruppi di accesso verificato.
3. Selezionare il gruppo .
4. Scegli Azioni, Modifica la politica di gruppo di accesso verificato.
5. (Facoltativo) Attiva o disattiva la politica di attivazione in base alle esigenze.
6. (Facoltativo) Per Policy, inserisci la politica di accesso verificato da applicare al gruppo.
7. Scegli Modifica la politica di gruppo di accesso verificato.

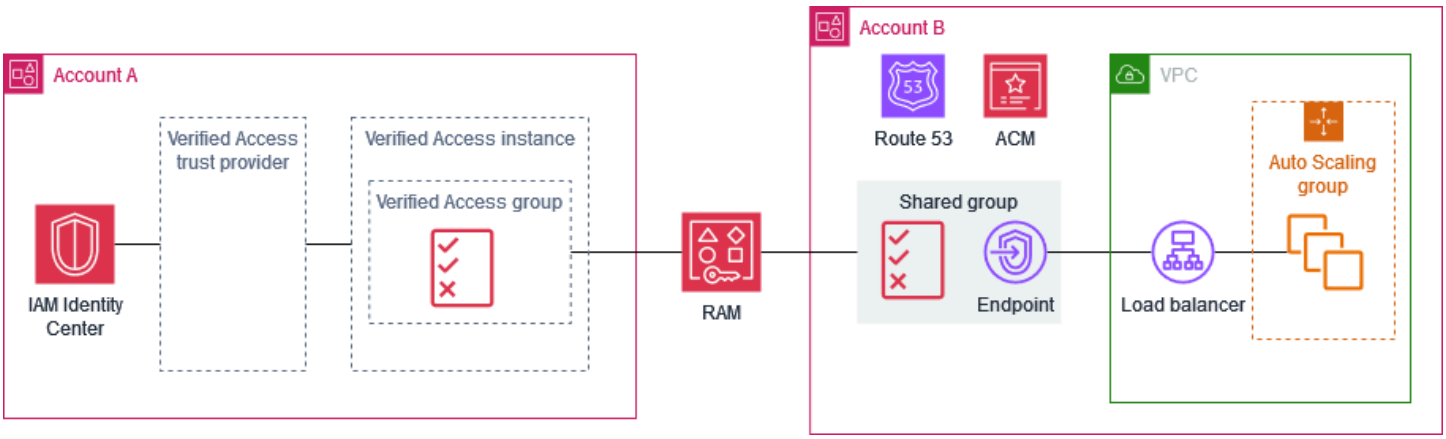
Per modificare una politica di gruppo ad accesso verificato utilizzando il AWS CLI

Utilizzare il comando modify-verified-access-group-policy.

Condividi un gruppo ad accesso verificato con un altro Account AWS

Quando condividi un gruppo ad accesso verificato di tua proprietà con altri AWS account, consenti a tali account di creare endpoint di accesso verificato nel tuo gruppo. L'account che ha creato il gruppo di accesso verificato in viene definito account del proprietario. L'account che utilizza un gruppo condiviso viene denominato account consumatore.

Il diagramma seguente illustra i vantaggi della condivisione di un gruppo con accesso verificato. Il team di sicurezza centrale è proprietario dell'Account A. Gestisce utenti e gruppi e gestisce le risorse di accesso verificato necessarie per fornire l'accesso alle applicazioni interne, come i provider fiduciari di accesso verificato, le istanze di accesso verificato, i gruppi di accesso verificato e le politiche di accesso verificato. AWS IAM Identity Center Il team dell'applicazione possiede l'Account B. Gestisce le risorse necessarie per eseguire l'applicazione interna, come il load balancer, il gruppo Auto Scaling, la configurazione DNS in Amazon Route 53 e i certificati AWS Certificate Manager TLS di (ACM). Dopo che il team di sicurezza centrale ha condiviso un gruppo di accesso verificato con l'Account B, il team dell'applicazione può creare endpoint di accesso verificato utilizzando il gruppo condiviso. L'accesso all'applicazione è consentito o negato in base alle politiche create dal team di sicurezza centrale per il gruppo di accesso verificato.



Considerazioni

Le seguenti considerazioni si applicano ai gruppi condivisi con accesso verificato.

Proprietari

- Per condividere un gruppo con accesso verificato, gli utenti devono disporre delle seguenti autorizzazioni: `ec2:PutResourcePolicy` e. `ec2:DeleteResourcePolicy`
- Per condividere un gruppo con accesso verificato, devi possederlo. Non puoi condividere un gruppo con accesso verificato che è stato condiviso con te.
- Se abiliti la condivisione con gli account della tua organizzazione, puoi condividere risorse, come i gruppi con accesso verificato, senza usare inviti. In caso contrario, il consumatore riceve un invito e deve accettarlo per accedere al gruppo condiviso. Per abilitare la condivisione, dall'account di gestione dell'organizzazione, apri la pagina Impostazioni nella AWS RAM console e scegli Abilita condivisione con AWS Organizations.

- Non puoi eliminare un gruppo se sono associati endpoint di accesso verificato. Puoi visualizzare gli endpoint creati dagli account consumer nella pagina degli endpoint con accesso verificato del tuo account. L'ID account del proprietario di un endpoint si riflette nell'Amazon Resource Name (ARN) del certificato per l'endpoint.

Consumatori

- Per visualizzare i gruppi con accesso verificato condivisi con te, apri la pagina dei gruppi con accesso verificato nella console o chiama describe-verified-access-groups. L'ID account del proprietario si riflette nel campo Owner e nell'Amazon Resource Name (ARN) del gruppo.
- Quando crei un endpoint di accesso verificato, puoi specificare tutti i gruppi di accesso verificato che sono stati condivisi con te.
- Non puoi visualizzare gli endpoint associati al gruppo condiviso ma non di tua proprietà.
- Se il proprietario del gruppo Verified Access elimina la condivisione di risorse, non puoi creare un nuovo endpoint di accesso verificato nel gruppo. Tutti gli endpoint di accesso verificato creati prima dell'eliminazione della condivisione di risorse non sono interessati dall'eliminazione della condivisione di risorse. Tuttavia, il proprietario del gruppo condiviso può eliminare i tuoi endpoint.

Condivisione delle risorse

Per condividere un gruppo con accesso verificato, è necessario aggiungerlo a una condivisione di risorse. Una condivisione di risorse specifica le risorse da condividere e i consumatori che possono utilizzare le risorse condivise.

Per condividere un gruppo con accesso verificato utilizzando la console

1. Apri la AWS RAM console a https://console.aws.amazon.com/ram/casa.
2. Se non disponi di una condivisione di risorse per la tua organizzazione, creane una. Per il responsabile, puoi scegliere l'intera organizzazione, un'unità organizzativa o AWS account specifici.
3. Seleziona la tua condivisione di risorse e scegli Modifica.
4. Per`Resources`, scegli Gruppi di accesso verificati come tipo di risorsa, quindi seleziona il gruppo di risorse da condividere.
5. Scegli Salta a: Rivedi e aggiorna.
6. Scegli Aggiorna condivisione risorse.

Per ulteriori informazioni, consulta l'argomento relativo alla creazione di una condivisione di risorse nella Guida per l'utente di AWS RAM.

Elimina un gruppo con accesso verificato

Quando hai finito con un gruppo con accesso verificato, puoi eliminarlo. Non puoi eliminare un gruppo se sono presenti endpoint di accesso verificato associati.

Per eliminare un gruppo con accesso verificato utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Gruppi di accesso verificato.
3. Selezionare il gruppo .
4. Scegli Azioni, Elimina il gruppo di accesso verificato.
5. Quando viene richiesta la conferma, inserisci **`delete`** e scegli Delete (Elimina).

Per eliminare un gruppo con accesso verificato utilizzando il AWS CLI

Utilizza il comando delete-verified-access-group.

Endpoint con accesso verificato

Un endpoint Verified Access rappresenta un'applicazione. Ogni endpoint è associato a un gruppo di Accesso verificato ed eredita la policy di accesso per il gruppo. Facoltativamente, puoi allegare una policy per gli endpoint specifica dell'applicazione a ciascun endpoint.

Indice

Tipi di endpoint Verified Access

I seguenti sono i possibili tipi di endpoint Verified Access:

- Load balancer: le richieste delle applicazioni vengono inviate a un load balancer per essere distribuite all'applicazione. Per ulteriori informazioni, consulta Crea un endpoint di bilanciamento del carico.
- Interfaccia di rete: le richieste di applicazione vengono inviate a un'interfaccia di rete utilizzando il protocollo e la porta specificati. Per ulteriori informazioni, consulta Crea un endpoint di interfaccia di rete.
- Rete CIDR: le richieste di applicazione vengono inviate al blocco CIDR specificato. Per ulteriori informazioni, consulta Crea un endpoint CIDR di rete.
- Amazon Relational Database Service (RDS): le richieste di applicazione vengono inviate a un'istanza RDS, un cluster RDS o un proxy RDS DB. Per ulteriori informazioni, consulta Crea un endpoint Amazon Relational Database Service.

Come funziona Verified Access con reti condivise e sottoreti VPCs

Di seguito sono riportati i comportamenti relativi alle sottoreti VPC condivise:

- Gli endpoint Verified Access sono supportati dalla condivisione di sottoreti VPC. Un partecipante può creare un endpoint Verified Access in una sottorete condivisa.
- Il partecipante che ha creato l'endpoint sarà il proprietario dell'endpoint e l'unica parte autorizzata a modificare l'endpoint. Al proprietario del VPC non sarà consentito modificare l'endpoint.
- Gli endpoint Verified Access non possono essere creati in una AWS Local Zone e pertanto la condivisione tramite Local Zones non è possibile.

Per ulteriori informazioni, consulta Condivisione del VPC con altri account nella Guida per l'utente di Amazon VPC.

Crea un endpoint di bilanciamento del carico per Verified Access

Utilizza la procedura seguente per creare un endpoint di bilanciamento del carico per Verified Access. Per ulteriori informazioni sui sistemi di bilanciamento del carico, consulta la Elastic Load Balancing User Guide.

Requisiti

- È supportato solo IPv4 il traffico.
- Le connessioni HTTPS di lunga durata, come WebSocket le connessioni, sono supportate solo tramite TCP.
- Il load balancer deve essere un Application Load Balancer o un Network Load Balancer e deve essere un load balancer interno.
- Il sistema di bilanciamento del carico e le sottoreti devono appartenere allo stesso cloud privato virtuale (VPC).
- I sistemi di bilanciamento del carico HTTPS possono utilizzare certificati TLS autofirmati o pubblici. Utilizza un certificato RSA con una lunghezza di chiave di 1.024 o 2.048.
- Prima di creare un endpoint di accesso verificato, è necessario creare un gruppo di accesso verificato. Per ulteriori informazioni, consulta the section called "Crea un gruppo con accesso verificato".
- È necessario fornire un nome di dominio per l'applicazione. Questo è il nome DNS pubblico che gli utenti utilizzeranno per accedere all'applicazione. Dovrai inoltre fornire un certificato SSL pubblico

con un CN che corrisponda a questo nome di dominio. È possibile creare o importare il certificato utilizzando AWS Certificate Manager.

Per creare un endpoint di bilanciamento del carico utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Endpoints di accesso verificato.
3. Scegli Crea endpoint di accesso verificato.
4. (Facoltativo) Per Tag nome e Descrizione, inserisci un nome e una descrizione per l'endpoint.
5. Per il gruppo di accesso verificato, scegli un gruppo di accesso verificato.
6. Per i dettagli sull'endpoint, procedi come segue:
   a. Per Protocollo, scegli un protocollo.
   b. In Attachment type (Tipo collegamento), selezionare VPC.
   c. Per il tipo di endpoint, scegli Load balancer.
   d. (HTTP/HTTPS) Per Porta, inserisci il numero di porta. (TCP) Per gli intervalli di porte, inserite un intervallo di porte e scegliete Aggiungi porta.
   e. Per Load balancer ARN, scegli un load balancer.
   f. Per Subnet, scegli le sottoreti. Puoi specificare una sola sottorete per ogni zona di disponibilità.
   g. Per i gruppi di sicurezza, scegli i gruppi di sicurezza per l'endpoint. Questi gruppi di sicurezza controllano il traffico in entrata e in uscita per l'endpoint Verified Access.
   h. Per il prefisso del dominio Endpoint, inserisci un identificatore personalizzato da anteporre al nome DNS generato da Verified Access per l'endpoint.
7. (HTTP/HTTPS) Per i dettagli dell'applicazione, procedi come segue:
   a. Per Dominio dell'applicazione, inserite un nome DNS per l'applicazione.
   b. In Certificato di dominio ARN, scegli un certificato TLS pubblico.
8. (Facoltativo) Per la definizione della policy, inserisci una policy di accesso verificato per l'endpoint.
9. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
10. Scegli Crea endpoint di accesso verificato.

Per creare un endpoint di accesso verificato utilizzando il AWS CLI

Utilizza il comando create-verified-access-endpoint.

Creare un endpoint di interfaccia di rete per Verified Access

Utilizzare la procedura seguente per creare un endpoint di interfaccia di rete.

Requisiti

- È supportato solo il IPv4 traffico.
- L'interfaccia di rete deve appartenere allo stesso cloud privato virtuale (VPC) dei gruppi di sicurezza.
- Utilizziamo l'IP privato sull'interfaccia di rete per inoltrare il traffico.
- Prima di creare un endpoint di accesso verificato, è necessario creare un gruppo di accesso verificato. Per ulteriori informazioni, consulta the section called "Crea un gruppo con accesso verificato".
- È necessario fornire un nome di dominio per l'applicazione. Questo è il nome DNS pubblico che gli utenti utilizzeranno per accedere all'applicazione. Dovrai inoltre fornire un certificato SSL pubblico con un CN che corrisponda a questo nome di dominio. È possibile creare o importare il certificato utilizzando AWS Certificate Manager.

Per creare un endpoint di interfaccia di rete utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Endpoints ad accesso verificato.
3. Scegli Crea endpoint di accesso verificato.
4. (Facoltativo) Per Tag nome e Descrizione, inserisci un nome e una descrizione per l'endpoint.
5. Per il gruppo di accesso verificato, scegli un gruppo di accesso verificato.
6. Per i dettagli sull'endpoint, procedi come segue:

    a. Per Protocollo, scegli un protocollo.
    b. In Attachment type (Tipo collegamento), selezionare VPC.
    c. Per Tipo di endpoint, scegli Interfaccia di rete.
    d. (HTTP/HTTPS) Per Porta, inserisci il numero di porta. (TCP) Per gli intervalli di porte, inserite un intervallo di porte e scegliete Aggiungi porta.

e. Per Interfaccia di rete, scegli un'interfaccia di rete.

f. Per Gruppi di sicurezza, scegli i gruppi di sicurezza per l'endpoint. Questi gruppi di sicurezza controllano il traffico in entrata e in uscita per l'endpoint Verified Access.

g. Per il prefisso del dominio Endpoint, inserisci un identificatore personalizzato da anteporre al nome DNS generato da Verified Access per l'endpoint.

7. (HTTP/HTTPS) Per i dettagli dell'applicazione, procedi come segue:

   a. Per Dominio dell'applicazione, inserite un nome DNS per l'applicazione.

   b. In Certificato di dominio ARN, scegli un certificato TLS pubblico.

8. (Facoltativo) Per la definizione della policy, inserisci una policy di accesso verificato per l'endpoint.

9. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.

10. Scegli Crea endpoint di accesso verificato.

Per creare un endpoint di accesso verificato utilizzando il AWS CLI

Utilizza il comando create-verified-access-endpoint.

Creare un endpoint CIDR di rete per Verified Access

Utilizzare la procedura seguente per creare un endpoint CIDR di rete. Ad esempio, puoi utilizzare un endpoint CIDR di rete per abilitare l'accesso alle istanze EC2 in una sottorete specifica tramite la porta 22 (SSH).

Requisiti

- È supportato solo il protocollo TCP.
- Verified Access fornisce un record DNS per ogni indirizzo IP nell'intervallo CIDR utilizzato da una risorsa. Se elimini una risorsa, il suo indirizzo IP non è più in uso e Verified Access elimina il record DNS corrispondente.
- Se specifichi un sottodominio personalizzato, Verified Access fornisce un record DNS per ogni indirizzo IP nelle sottoreti degli endpoint che si trova nell'intervallo CIDR specificato e utilizzato nel sottodominio, e fornisce gli indirizzi IP dei relativi server DNS. Puoi configurare una regola di inoltro per il tuo sottodominio in modo che punti ai server DNS ad accesso verificato. Qualsiasi richiesta

effettuata a un record nel dominio viene risolta dai server DNS ad accesso verificato all'indirizzo IP della risorsa richiesta.

- Prima di creare un endpoint di accesso verificato, è necessario creare un gruppo di accesso verificato. Per ulteriori informazioni, consulta the section called "Crea un gruppo con accesso verificato".
- Crea l'endpoint e poi connettiti all'applicazione utilizzando. Client di connettività

Per creare un endpoint CIDR di rete utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Endpoints di accesso verificato.
3. Scegli Crea endpoint di accesso verificato.
4. (Facoltativo) Per Tag nome e Descrizione, inserisci un nome e una descrizione per l'endpoint.
5. Per il gruppo di accesso verificato, scegli un gruppo di accesso verificato per l'endpoint.
6. Per i dettagli sull'endpoint, procedi come segue:
   a. Per Protocol (Protocollo), selezionare TCP.
   b. In Attachment type (Tipo collegamento), selezionare VPC.
   c. Per il tipo di endpoint, scegli Network CIDR.
   d. Per Intervalli di porte, inserisci un intervallo di porte e scegli Aggiungi porta.
   e. Per Subnet, scegli le sottoreti.
   f. Per i gruppi di sicurezza, scegli i gruppi di sicurezza per l'endpoint. Questi gruppi di sicurezza controllano il traffico in entrata e in uscita per l'endpoint Verified Access.
   g. (Facoltativo) Per il prefisso del dominio Endpoint, inserisci un identificatore personalizzato da anteporre al nome DNS generato da Verified Access per l'endpoint.
7. (Facoltativo) Per la definizione della policy, inserisci una policy di accesso verificato per l'endpoint.
8. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
9. Scegli Crea endpoint di accesso verificato.

Per creare un endpoint di accesso verificato utilizzando il AWS CLI

Utilizza il comando create-verified-access-endpoint.

Crea un endpoint Amazon Relational Database Service per un accesso verificato

Utilizza la seguente procedura per creare un endpoint Amazon Relational Database Service (RDS).

Requisiti

- È supportato solo il protocollo TCP.
- Crea un'istanza RDS, un cluster RDS o un proxy RDS DB.
- Prima di creare un endpoint Verified Access, è necessario creare un gruppo Verified Access. Per ulteriori informazioni, consulta the section called "Crea un gruppo con accesso verificato".
- Crea l'endpoint e poi connettiti all'applicazione utilizzando. Client di connettività

Per creare un endpoint Amazon Relational Database Service utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Verified Access Endpoints.
3. Scegli Crea endpoint di accesso verificato.
4. (Facoltativo) Per Tag nome e Descrizione, inserisci un nome e una descrizione per l'endpoint.
5. Per il gruppo di accesso verificato, scegli un gruppo di accesso verificato per l'endpoint.
6. Per i dettagli sull'endpoint, procedi come segue:

    a. Per Protocol (Protocollo), selezionare TCP.
    b. In Attachment type (Tipo collegamento), selezionare VPC.
    c. Per il tipo di endpoint, scegli Amazon Relational Database Service (RDS).
    d. Per il tipo di destinazione RDS, esegui una delle seguenti operazioni:
        - Scegli un'istanza RDS, quindi scegli un'istanza RDS dall'istanza RDS.
        - Scegli un cluster RDS, quindi scegli un cluster RDS dal cluster RDS.
        - Scegli il proxy RDS DB, quindi scegli un proxy RDS DB dal proxy RDS DB.
    e. Per l'endpoint RDS, scegli un endpoint RDS correlato alla risorsa RDS che hai scelto nel passaggio precedente.
    f. Per Port (Porta) inserire il numero di porta.
    g. Per Subnet, scegli le sottoreti. Puoi specificare una sola sottorete per ogni zona di disponibilità.

h. Per i gruppi di sicurezza, scegli i gruppi di sicurezza per l'endpoint. Questi gruppi di sicurezza controllano il traffico in entrata e in uscita per l'endpoint Verified Access.

i. (Facoltativo) Per il prefisso del dominio Endpoint, inserisci un identificatore personalizzato da anteporre al nome DNS generato da Verified Access per l'endpoint.

7. (Facoltativo) Per la definizione della policy, inserisci una policy di accesso verificato per l'endpoint.
8. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
9. Scegli Crea endpoint di accesso verificato.

Per creare un endpoint di accesso verificato utilizzando il AWS CLI

Utilizza il comando create-verified-access-endpoint.

Consenti il traffico proveniente dal tuo endpoint di accesso verificato

Puoi configurare i gruppi di sicurezza per le tue applicazioni in modo che consentano il traffico proveniente dall'endpoint di accesso verificato. A tale scopo, aggiungi una regola in entrata che specifica il gruppo di sicurezza per l'endpoint come origine. Ti consigliamo di rimuovere eventuali regole in entrata aggiuntive, in modo che l'applicazione riceva traffico solo dall'endpoint di accesso verificato.

Ti consigliamo di mantenere le regole in uscita esistenti.

Per aggiornare le regole dei gruppi di sicurezza per l'applicazione utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Endpoints di accesso verificato.
3. Scegli l'endpoint di accesso verificato, trova il gruppo IDs di sicurezza nella scheda Dettagli e copia l'ID del gruppo di sicurezza per l'endpoint.
4. Nel pannello di navigazione, seleziona Gruppi di sicurezza.
5. Seleziona la casella di controllo relativa al gruppo di sicurezza associato al target, quindi scegli Azioni, Modifica regole in entrata.

6. Per aggiungere una regola del gruppo di sicurezza che consenta il traffico proveniente dall'endpoint di accesso verificato, procedi come segue:
   a. Scegli Aggiungi regola.
   b. Per Tipo, scegli Tutto il traffico o il traffico specifico da consentire.
   c. Per Origine, scegli Personalizzato e incolla l'ID del gruppo di sicurezza per il tuo endpoint.
7. (Facoltativo) Per richiedere che il traffico provenga solo dall'endpoint di accesso verificato, elimina qualsiasi altra regola del gruppo di sicurezza in entrata.
8. Scegliere Salva regole.

Per aggiornare le regole del gruppo di sicurezza per l'applicazione utilizzando il AWS CLI

Utilizzate il describe-verified-access-endpointscomando per ottenere l'ID del gruppo di sicurezza, quindi utilizzate il authorize-security-group-ingresscomando per aggiungere una regola in entrata.

Modifica un endpoint di accesso verificato

Utilizzare la procedura seguente per modificare un endpoint Verified Access.

Per modificare un endpoint di accesso verificato utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Endpoint di accesso verificato.
3. Seleziona l'endpoint.
4. Scegli Azioni, Modifica endpoint di accesso verificato.
5. Modifica i dettagli dell'endpoint secondo necessità.
6. Scegli Modifica endpoint di accesso verificato.

Per modificare un endpoint di accesso verificato utilizzando il AWS CLI

Utilizza il comando modify-verified-access-endpoint.

Modificare una policy per gli endpoint di accesso verificato

Utilizza le seguenti procedure per modificare la policy per un endpoint Verified Access. Dopo aver apportato le modifiche, occorrono alcuni minuti prima che abbiano effetto.

Per modificare una policy sugli endpoint di accesso verificato utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Endpoints di accesso verificato.
3. Seleziona l'endpoint.
4. Scegli Azioni, Modifica la politica degli endpoint di accesso verificato.
5. (Facoltativo) Attiva o disattiva la politica di attivazione in base alle esigenze.
6. (Facoltativo) Per Policy, inserisci la policy di accesso verificato da applicare all'endpoint.
7. Scegli Modifica la politica degli endpoint di accesso verificato.

Per modificare una policy sugli endpoint di accesso verificato utilizzando il AWS CLI

Utilizzare il comando modify-verified-access-endpoint-policy.

Eliminare un endpoint con accesso verificato

Quando hai finito con un endpoint Verified Access, puoi eliminarlo.

Per eliminare un endpoint con accesso verificato utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Endpoint di accesso verificato.
3. Seleziona l'endpoint.
4. Scegli Azioni, Elimina endpoint di accesso verificato.
5. Quando viene richiesta la conferma, immettere **`delete`** e quindi scegliere Elimina.

Per eliminare un endpoint di accesso verificato utilizzando il AWS CLI

Utilizza il comando delete-verified-access-endpoint.

Dati attendibili inviati a Verified Access dai fornitori di servizi fiduciari

I dati attendibili sono dati inviati Accesso verificato da AWS da un provider fiduciario. I dati sulla fiducia vengono anche chiamati «affermazioni degli utenti» o «contesto di fiducia». I dati generalmente includono informazioni su un utente o su un dispositivo. Esempi di dati attendibili includono l'e-mail degli utenti, l'appartenenza ai gruppi, la versione del sistema operativo del dispositivo, lo stato di sicurezza del dispositivo e così via. Le informazioni inviate variano a seconda del fornitore di fiducia, quindi è necessario fare riferimento alla documentazione del fornitore di fiducia per un elenco completo e aggiornato dei dati sulla fiducia.

Tuttavia, utilizzando le funzionalità di registrazione dell'accesso verificato, puoi anche vedere quali dati attendibili vengono inviati dal tuo provider fiduciario. Ciò può essere utile quando si definiscono politiche che consentono o negano l'accesso alle applicazioni. Per informazioni sull'inclusione del contesto di fiducia nei log, consulta. Abilita o disabilita il contesto di fiducia di accesso verificato

Questa sezione contiene esempi di dati sulla fiducia ed esempi per aiutarti a iniziare a scrivere le politiche. Le informazioni qui fornite sono solo a scopo illustrativo e non come riferimento ufficiale.

Indice

Contesto predefinito per i dati attendibili di Verified Access

Accesso verificato da AWS include alcuni elementi sulla richiesta corrente per impostazione predefinita in tutte le valutazioni Cedar indipendentemente dai provider di fiducia configurati. Se lo desideri, puoi scrivere una politica che valuti i dati.

Di seguito sono riportati alcuni esempi dei dati inclusi nella valutazione.

Esempi

Richiesta HTTP

Quando viene valutata una politica, Verified Access include i dati sulla richiesta HTTP corrente nel contesto Cedar sotto la `context.http_request` chiave.

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

Esempio di policy

Di seguito è riportato un esempio di politica Cedar che utilizza i dati della richiesta HTTP.

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

Flusso TCP

Quando viene valutata una policy, Verified Access include i dati sul flusso TCP corrente nel contesto Cedar sotto la chiave. `context.tcp_flow`

```
{
    "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 contesto per i dati attendibili di Verified Access

Quando viene valutata una policy, se la definisci AWS IAM Identity Center come trust provider, Accesso verificato da AWS include i dati sulla fiducia nel contesto Cedar nella chiave specificata come «Policy Reference Name» nella configurazione del trust provider. Se lo desideri, puoi scrivere una politica che valuti i dati sulla fiducia.

> **Note**
>
> La chiave di contesto per il provider fiduciario deriva dal nome di riferimento della politica configurato al momento della creazione del provider fiduciario. Ad esempio, se configurate il nome di riferimento della policy come «idp123", la chiave di contesto sarà «context.idp123". Verificate di utilizzare la chiave contestuale corretta quando create la policy.

Lo schema JSON seguente mostra quali dati sono inclusi nella valutazione.

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

Di seguito è riportato un esempio di policy che valuta in base ai dati di attendibilità forniti da. 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**
>
> Poiché i nomi dei gruppi possono essere modificati, IAM Identity Center fa riferimento ai gruppi utilizzando il loro ID di gruppo. Questo aiuta a evitare di violare una dichiarazione politica quando si cambia il nome di un gruppo.

Contesto di fornitori di fiducia di terze parti per i dati attendibili ad accesso verificato

Questa sezione descrive i dati sulla fiducia forniti Accesso verificato da AWS da fornitori di fiducia di terze parti.

> **Note**
>
> La chiave di contesto per il provider fiduciario deriva dal nome di riferimento della politica che si configura al momento della creazione del provider fiduciario. Ad esempio, se configurate il nome di riferimento della policy come «idp123", la chiave di contesto sarà «context.idp123". Assicurati di utilizzare la chiave contestuale corretta quando crei la policy.

Indice

Estensione del browser

Se prevedi di incorporare il contesto di attendibilità del dispositivo nelle tue politiche di accesso, avrai bisogno dell'estensione del browser AWS Verified Access o dell'estensione del browser di un altro partner. Verified Access attualmente supporta i browser Google Chrome e Mozilla Firefox.

Attualmente supportiamo tre provider affidabili per dispositivi: Jamf (che supporta i dispositivi macOS) CrowdStrike , (che supporta i dispositivi Windows 11 e Windows 10) JumpCloud e (che supporta sia Windows che macOS).

- Se utilizzi Jamf Trust Data nelle tue norme, gli utenti devono scaricare e installare l'estensione del Accesso verificato da AWS browser dal Chrome web store o dal sito aggiuntivo per Firefox sui propri dispositivi.
- Se utilizzi dati CrowdStrikeattendibili nelle tue politiche, per prima cosa gli utenti devono installare l'host di messaggistica Accesso verificato da AWS nativo (link per il download diretto). Questo componente è necessario per ottenere i dati di attendibilità dall' CrowdStrike agente in esecuzione sui dispositivi degli utenti. Quindi, dopo aver installato questo componente, gli utenti devono installare l'estensione Accesso verificato da AWS del browser dal Chrome Web Store o dal sito aggiuntivo di Firefox sui propri dispositivi.
- Se lo utilizzi JumpCloud, i tuoi utenti devono avere l'estensione JumpCloud del browser del Chrome web store o del sito aggiuntivo per Firefox installata sui loro dispositivi.

Jamf

Jamf è un fornitore di servizi fiduciari di terze parti. Quando viene valutata una politica, se definisci Jamf come fornitore di fiducia, Verified Access include i dati sulla fiducia nel contesto Cedar nella chiave specificata come «Nome di riferimento della politica» nella configurazione del provider fiduciario. Se lo desideri, puoi scrivere una politica che valuti i dati sulla fiducia. Lo schema JSON seguente mostra quali dati sono inclusi nella valutazione.

Per ulteriori informazioni sull'utilizzo di Jamf con Verified Access, consulta Integrating AWS Verified Access with Jamf Device Identity sul sito Web 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)"
        }
    }
}
```

Di seguito è riportato un esempio di policy che valuta i dati di fiducia forniti da Jamf.

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

Cedar fornisce una `.contains()` funzione utile per aiutare con enumerazioni come il punteggio di rischio di Jamf.

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

CrowdStrike

CrowdStrike è un fornitore di fiducia di terze parti. Quando viene valutata una politica, se la definisci CrowdStrike come fornitore di fiducia, Verified Access include i dati sulla fiducia nel contesto Cedar nella chiave specificata come «Nome di riferimento della politica» nella configurazione del provider fiduciario. Se lo desideri, puoi scrivere una politica che valuti i dati sulla fiducia. Lo schema JSON seguente mostra quali dati sono inclusi nella valutazione.

Per ulteriori informazioni sull'utilizzo CrowdStrike con Verified Access, consulta Proteggere le applicazioni private con CrowdStrike e Accesso verificato da AWS sul GitHub sito 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"
    }
  }
}
```

Di seguito è riportato un esempio di policy che valuta i dati di attendibilità forniti da. CrowdStrike

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

JumpCloud

JumpCloud è un fornitore di servizi fiduciari di terze parti. Quando viene valutata una politica, se la definisci JumpCloud come fornitore di fiducia, Verified Access include i dati sulla fiducia nel contesto Cedar nella chiave specificata come «Nome di riferimento della politica» nella configurazione del provider fiduciario. Se lo desideri, puoi scrivere una politica che valuti i dati sulla fiducia. Lo schema JSON seguente mostra quali dati sono inclusi nella valutazione.

Per ulteriori informazioni sull'utilizzo JumpCloud con AWS Verified Access, consulta Integrazione JumpCloud e accesso AWS verificato sul JumpCloud sito 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"
    }
  }
}
```

Di seguito è riportato un esempio di policy che valuta in base al contesto di fiducia fornito da. JumpCloud

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

L'utente dichiara il superamento e la verifica della firma in Verified Access

Dopo che un' Accesso verificato da AWS istanza ha autenticato correttamente un utente, invia le dichiarazioni utente ricevute dall'IdP all'endpoint Verified Access. Le dichiarazioni degli utenti sono firmate in modo che le applicazioni possano verificare le firme e verificare anche che le attestazioni siano state inviate da Verified Access. Durante questo processo, viene aggiunta la seguente intestazione HTTP:

`x-amzn-ava-user-context`

Questa intestazione contiene le affermazioni degli utenti in formato token web JSON (JWT). Il formato JWT include un'intestazione, un carico utile e una firma con codifica URL base64. Verified Access

utilizza ES384 (algoritmo di firma ECDSA che utilizza l'algoritmo hash SHA-384) per generare la firma JWT.

Le applicazioni possono utilizzare queste dichiarazioni per la personalizzazione o altre esperienze specifiche dell'utente. Gli sviluppatori di applicazioni devono informarsi sul livello di unicità e verifica di ogni affermazione fornita dal fornitore di identità prima dell'uso. In generale, l'`sub`affermazione è il modo migliore per identificare un determinato utente.

Indice

Esempio: dichiarazioni utente firmate JWT for OIDC

Gli esempi seguenti mostrano come appariranno l'intestazione e il payload per le dichiarazioni degli utenti OIDC nel formato JWT.

Intestazione di esempio:

```
{
   "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)
}
```

Esempio di payload:

```
{
   "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"
   }
}
```

Esempio: dichiarazioni utente firmate JWT for IAM Identity Center

Gli esempi seguenti mostrano come appariranno l'intestazione e il payload per le dichiarazioni degli utenti di IAM Identity Center nel formato JWT.

> **Note**
>
> Per IAM Identity Center, nelle dichiarazioni verranno incluse solo le informazioni sull'utente.

Intestazione di esempio:

```
{
   "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)
}
```

Esempio di payload:

```
{
    "user": {
```

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

Chiavi pubbliche

Poiché le istanze di accesso verificato non crittografano le dichiarazioni degli utenti, ti consigliamo di configurare gli endpoint di accesso verificato per utilizzare HTTPS. Se configuri il tuo endpoint di accesso verificato per utilizzare HTTP, assicurati di limitare il traffico verso l'endpoint utilizzando i gruppi di sicurezza.

Per garantire la sicurezza, è necessario verificare la firma prima di eseguire qualsiasi autorizzazione in base alle affermazioni e verificare che il `signer` campo nell'intestazione JWT contenga l'ARN dell'istanza Verified Access previsto.

Per ottenere la chiave pubblica, ottenere la chiave ID dall'intestazione JWT e utilizzarla per cercare la chiave pubblica dall'endpoint.

L'endpoint per ciascuno è il seguente: Regione AWS

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

Esempio: recupero e decodifica di JWT

Il seguente esempio di codice mostra come ottenere l'ID della chiave, la chiave pubblica e il payload in 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'])
```

Politiche di accesso verificato

Accesso verificato da AWS le politiche consentono di definire regole per l'accesso alle applicazioni ospitate in AWS. Sono scritte in Cedar, un linguaggio AWS politico. Utilizzando Cedar, è possibile creare politiche che vengono valutate in base ai dati di attendibilità inviati dai provider di fiducia basati sull'identità o sui dispositivi che configuri per l'utilizzo con Verified Access.

Per informazioni più dettagliate sul linguaggio delle politiche Cedar, consulta la Cedar Reference Guide.

Quando crei un gruppo di accesso verificato o crei un endpoint di accesso verificato, hai la possibilità di definire la politica di accesso verificato. Puoi creare un gruppo o un endpoint senza definire la politica di accesso verificato, ma tutte le richieste di accesso verranno bloccate finché non definirai una politica. In alternativa, puoi aggiungere o modificare una policy su un gruppo o endpoint di accesso verificato esistente dopo la sua creazione.

Indice

Struttura della dichiarazione sulla politica di accesso verificato

La tabella seguente mostra la struttura di una politica di accesso verificato.

Componente	Sintassi
effetto	`permit | forbid`
scope	`(principal, action, resource)`
clausola condizionale	`when {`

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

Componenti della politica

Una politica di accesso verificato contiene i seguenti componenti:

- Effetto: `permit` (consentire) o `forbid` (negare) l'accesso.
- Ambito: i principi, le azioni e le risorse a cui si applica l'effetto. È possibile lasciare indefinito l'ambito in Cedar non identificando principi, azioni o risorse specifici. In questo caso, la politica si applica a tutti i possibili principi, azioni e risorse.
- Clausola condizionale: il contesto in cui si applica l'effetto.

> **Important**
>
> Per Verified Access, le politiche sono espresse integralmente facendo riferimento ai dati attendibili nella clausola condizionale. L'ambito della politica deve essere sempre mantenuto indefinito. È quindi possibile specificare l'accesso utilizzando il contesto di identità e fiducia del dispositivo nella clausola condizionale.

Commenti

Puoi includere commenti nelle tue Accesso verificato da AWS politiche. I commenti sono definiti come una riga che inizia `//` e termina con un carattere di nuova riga.

L'esempio seguente mostra i commenti in una politica.

```
// 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)
};
```

Clausole multiple

È possibile utilizzare più di una clausola condizionale in una dichiarazione di politica utilizzando l'operatore. &&

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

Per ulteriori esempi, consulta Esempi di politiche di accesso verificato.

Personaggi riservati

L'esempio seguente mostra come scrivere una politica se una proprietà di contesto utilizza un `:` (punto e virgola), che è un carattere riservato nel linguaggio delle politiche.

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

Operatori integrati per le politiche di accesso verificato

Quando si crea il contesto di una Accesso verificato da AWS politica utilizzando varie condizioni, come discusso inStruttura della dichiarazione sulla politica di accesso verificato, è possibile utilizzare l'&&operatore per aggiungere condizioni aggiuntive. Esistono anche molti altri operatori integrati che è possibile utilizzare per aggiungere ulteriore potenza espressiva alle condizioni della politica. La tabella seguente contiene tutti gli operatori incorporati come riferimento.

Operatore	Tipi e sovraccarichi	Descrizione
!	Booleano → Booleano	Logico no.

Operatore	Tipi e sovraccarichi	Descrizione
==	qualsiasi → qualsiasi	Uguaglianza. Funziona su argomenti di qualsiasi tipo, anche se i tipi non corrispon dono. I valori di tipi diversi non sono mai uguali tra loro.
!=	qualsiasi → qualsiasi	Disuguaglianza; l'esatto inverso dell'uguaglianza (vedi sopra).
<	(long, long) → Booleano	Intero lungo minore di.
<=	(lungo, lungo) → Booleano	Numero intero less-than-or-equal lungo -to.
>	(lungo, lungo) → Booleano	Intero lungo maggiore di.
>=	(lungo, lungo) → Booleano	Numero intero greater-than-or-equal lungo -to.
in	(entità, entità) → Booleano	Appartenenza alla gerarchia (riflessiva: A in A è sempre vera).
	(entity, set (entity)) → Booleano	Appartenenza alla gerarchia : A in [B, C,...] è vera se (A e B) || (A in C) ||... errore se l'insieme contiene una non-entità.
&&	(Booleano, Booleano) → Booleano	Logico e (cortocircuito).
||	(Booleano, Booleano) → Booleano	Logico o (cortocircuito).
.esiste ()	entità → Booleano	esistenza di un'entità.

Operatore	Tipi e sovraccarichi	Descrizione
ha	(entità, attributo) → Booleano	Operatore Infix. `e has f`verifica se il record o l'entità `e` ha un'associazione per l'attributo`f`. `e`Restituisce `false` se non esiste o se `e` esiste ma non ha l'attributo`f`. Gli attributi possono essere espressi come identificatori o stringhe letterali.
like	(stringa, stringa) → Booleano	Operatore Infix. `t like p`controlla se il testo `t` corrisponde allo schema`p`, che può includere caratteri jolly `*` che corrispondono a 0 o più caratteri di qualsiasi carattere. Per far corrispon dere un personaggio stellare letterale `at`, puoi usare la speciale sequenza di caratteri con escape in. `\* p`
.contiene ()	(set, qualsiasi) → Booleano	Appartenenza al set (se B è un elemento di A).
. contiene tutto ()	(set, set) → Booleano	Verifica se il set A contiene tutti gli elementi del set B.
. contiene Any ()	(set, set) → Booleano	Verifica se il set A contiene uno qualsiasi degli elementi del set B.

Valutazione della politica di accesso verificata

Un documento politico è un insieme di una o più dichiarazioni politiche (`permito` `forbid` dichiarazioni). La politica si applica se la clausola condizionale (la `when` dichiarazione) è vera. Affinché un documento di policy consenta l'accesso, deve essere applicata almeno una politica di autorizzazione nel documento e non può essere applicata alcuna politica di divieto. Se non si applica alcuna politica di autorizzazione, si applicano and/or una o più politiche di divieto, il documento di policy nega l'accesso. Se sono stati definiti documenti di policy sia per il gruppo Verified Access che per l'endpoint Verified Access, entrambi i documenti devono consentire l'accesso. Se non è stato definito un documento di policy per l'endpoint Verified Access, è necessario accedere solo alla politica di gruppo Verified Access.

Accesso verificato da AWS convalida la sintassi quando si crea la policy, ma non convalida i dati inseriti nella clausola condizionale.

Cortocircuito logico della politica di accesso verificato

Potresti voler scrivere una Accesso verificato da AWS policy che valuti i dati che possono o meno essere presenti in un determinato contesto. Se si fa riferimento ai dati in un contesto che non esiste, Cedar genererà un errore e valuterà la politica per negare l'accesso, indipendentemente dall'intenzione dell'utente. Ad esempio, ciò comporterebbe una negazione, poiché in questo contesto non esistono `fake_provider` e `bogus_key` non esistono.

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

Per evitare questa situazione, è possibile verificare se è presente una chiave utilizzando l'`has`operatore. Se l'`has`operatore restituisce false, l'ulteriore valutazione dell'istruzione concatenata si interrompe e Cedar non produce un errore nel tentativo di fare riferimento a un elemento che non esiste.

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

Ciò è particolarmente utile quando si specifica una politica che fa riferimento a due diversi fornitori di fiducia.

```
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)
    )
  )
};
```

Esempi di politiche di accesso verificato

Puoi utilizzare le politiche di accesso verificato per concedere l'accesso alle tue applicazioni a utenti e dispositivi specifici.

Policy di esempio

- Esempio 1: concedere l'accesso a un gruppo in IAM Identity Center
- Esempio 2: concedere l'accesso a un gruppo in un provider di terze parti
- Esempio 3: concedere l'accesso utilizzando CrowdStrike
- Esempio 4: consentire o negare un indirizzo IP specifico

Esempio 1: concedere l'accesso a un gruppo in IAM Identity Center

Quando si utilizza AWS IAM Identity Center, è meglio fare riferimento ai gruppi utilizzando i loro IDs. Ciò consente di evitare di violare una dichiarazione politica se si modifica il nome del gruppo.

La seguente politica di esempio consente l'accesso solo agli utenti del gruppo specificato con un indirizzo e-mail verificato. L'ID del gruppo èc242c5b0-6081-1845-6fa8-6e0d9513c107.

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

```
when {
    context.policy-reference-name.groups has "c242c5b0-6081-1845-6fa8-6e0d9513c107"
    && context.policy-reference-name.user.email.verified == true
};
```

La seguente politica di esempio consente l'accesso solo quando l'utente fa parte del gruppo specificato, ha un indirizzo e-mail verificato e il punteggio di rischio del dispositivo Jamf è`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"
};
```

Per ulteriori informazioni sui dati sulla fiducia, vederethe section called "AWS IAM Identity Center contesto".

Esempio 2: concedere l'accesso a un gruppo in un provider di terze parti

La seguente politica di esempio consente l'accesso solo quando l'utente fa parte del gruppo specificato, ha un indirizzo e-mail verificato e il punteggio di rischio del dispositivo Jamf è BASSO. Il nome del gruppo è «finanza».

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

Per ulteriori informazioni sui dati sulla fiducia, vederethe section called "Contesto di terze parti".

Esempio 3: concedere l'accesso utilizzando CrowdStrike

La seguente politica di esempio consente l'accesso quando il punteggio di valutazione complessivo è superiore a 50.

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

```
};
```

Esempio 4: consentire o negare un indirizzo IP specifico

La seguente politica di esempio consente le richieste HTTP dall'indirizzo IP specificato.

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

La seguente politica di esempio nega le richieste HTTP dall'indirizzo IP specificato.

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

La seguente politica di esempio consente le richieste TCP dall'indirizzo IP specificato.

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

Assistente alle politiche di accesso verificato

L'assistente alle politiche di accesso verificato è uno strumento della console Verified Access che puoi utilizzare per testare e sviluppare le tue politiche. Presenta la policy degli endpoint, la policy di gruppo e il contesto di fiducia in un'unica schermata, dove puoi testare e modificare le policy.

I formati dei contesti di fiducia variano tra i diversi provider di servizi fiduciari e talvolta l'amministratore di Verified Access potrebbe non conoscere il formato esatto utilizzato da un determinato provider di fiducia. Ecco perché può essere molto utile vedere il contesto di fiducia e le policy di gruppo ed endpoint in un unico posto per scopi di test e sviluppo.

Le sezioni seguenti descrivono le nozioni di base sull'utilizzo dell'editor delle politiche.

Attività

Fase 1: Specificate le vostre risorse

Nella prima pagina dell'assistente alle politiche, si specifica l'endpoint di accesso verificato con cui si desidera lavorare. Specificherai anche un utente (identificato tramite indirizzo e-mail) e, facoltativamente, il nome and/or dell'utente come identificatore del dispositivo. Per impostazione predefinita, la decisione di autorizzazione più recente viene estratta dai registri di accesso verificato per l'utente specificato. Facoltativamente, puoi scegliere in modo specifico la decisione di autorizzazione o rifiuto più recente.

Infine, il contesto di fiducia, la decisione di autorizzazione, la politica dell'endpoint e la politica di gruppo vengono tutti visualizzati nella schermata successiva.

Per aprire l'assistente alle politiche e specificare le risorse

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Istanze di accesso verificato, quindi fai clic sull'ID dell'istanza di accesso verificato per l'istanza con cui desideri lavorare.
3. Scegli Launch policy assistant.
4. Per Indirizzo e-mail utente, inserisci l'indirizzo e-mail dell'utente.
5. Per l'endpoint ad accesso verificato, seleziona l'endpoint per il quale desideri modificare e testare le politiche.
6. (Facoltativo) Per Nome, fornisci il nome dell'utente.
7. (Facoltativo) In Identificatore del dispositivo, inserisci l'identificatore univoco del dispositivo.
8. (Facoltativo) Per Risultato dell'autorizzazione, scegli il tipo di risultato di autorizzazione recente che desideri utilizzare. Per impostazione predefinita, verrà utilizzato il risultato dell'autorizzazione più recente.
9. Scegli Next (Successivo).

Fase 2: Verificare e modificare le politiche

In questa pagina ti verranno presentate le seguenti informazioni su cui lavorare:

- Il contesto di fiducia inviato dal provider di fiducia per l'utente e (facoltativamente) il dispositivo specificato nel passaggio precedente.
- La policy Cedar per l'endpoint Verified Access specificata nel passaggio precedente.
- La policy Cedar per il gruppo Verified Access a cui appartiene l'endpoint.

Le politiche Cedar per l'endpoint e il gruppo Verified Access possono essere modificate in questa pagina, ma il contesto di fiducia è statico. È ora possibile utilizzare questa pagina per visualizzare il contesto di fiducia insieme alle politiche Cedar.

Verifica le politiche rispetto al contesto di fiducia scegliendo il pulsante Test policies e il risultato dell'autorizzazione verrà visualizzato sullo schermo. Puoi apportare modifiche alle politiche e testare nuovamente le modifiche, ripetendo il processo secondo necessità.

Dopo essere soddisfatto delle modifiche apportate alle politiche, scegli Avanti per passare alla schermata successiva dell'assistente alle politiche.

Fase 3: Rivedere e applicare le modifiche

Nell'ultima pagina dell'assistente alle politiche, vedrai evidenziate le modifiche apportate alle politiche per facilitarne la revisione. Ora puoi esaminarle un'ultima volta e scegliere Applica modifiche per confermare le modifiche.

Hai anche la possibilità di tornare alla pagina precedente scegliendo Precedente o di annullare completamente l'assistente alle politiche scegliendo Annulla.

Client di connettività per Accesso verificato da AWS

Accesso verificato da AWS fornisce il Connectivity Client in modo da consentire la connettività tra i dispositivi utente e le applicazioni non HTTP. Il client crittografa in modo sicuro il traffico degli utenti, aggiunge le informazioni sull'identità dell'utente e il contesto del dispositivo e lo indirizza a Verified Access per l'applicazione delle policy. Se le politiche di accesso consentono l'accesso, l'utente è connesso all'applicazione. L'accesso dell'utente è continuamente autorizzato per tutto il tempo in cui il Connectivity Client è connesso.

Il client funziona come un servizio di sistema ed è resistente agli arresti anomali. Se la connessione diventa instabile, il client ristabilisce la connessione.

Il client utilizza token di OAuth accesso temporanei per stabilire il tunnel sicuro. Il tunnel viene disconnesso quando l'utente si disconnette dal client.

I token di accesso e aggiornamento vengono archiviati localmente sul dispositivo dell'utente, in un database crittografato. SQLite

Indice

Prerequisiti

Prima di iniziare, completa i seguenti prerequisiti:

- Crea un'istanza di accesso verificato con un provider affidabile.
- Crea un endpoint TCP per la tua applicazione.
- Disconnetti il computer da qualsiasi client VPN per evitare problemi di routing.

- Abilita IPv6 sul tuo computer. Per istruzioni, consulta la documentazione del sistema operativo in esecuzione sul tuo computer.
- Su un computer Windows, verifica che il Trusted Platform Module (TPM) sia supportato e installa il runtime WebView2.

Scaricate il Connectivity Client

Disinstalla qualsiasi versione precedente del client. Scarica il client, verifica che il programma di installazione sia firmato ed esegui il programma di installazione. Non installate il client utilizzando un programma di installazione non firmato.

- Connectivity Client per Mac con Apple Silicon versione 1.0.4
- Client di connettività per Mac con Intel versione 1.0.4
- Client di connettività per Windows con versione x64 1.0.5

Esportazione del file di configurazione del client

Utilizza la procedura seguente per esportare le informazioni di configurazione richieste dal client dall'istanza di Verified Access.

Per esportare il file di configurazione del client utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Istanze di accesso verificato.
3. Seleziona l'istanza di accesso verificato.
4. Scegli Azioni, Esporta il file di configurazione del client.

Per esportare il file di configurazione del client utilizzando AWS CLI

Utilizzare il comando export-verified-access-instance-client-configuration. Salva l'output in un file.json. Il nome del file deve iniziare con il `ClientConfig-` prefisso.

Connect all'applicazione

Utilizzare la procedura seguente per connettersi a un'applicazione tramite il client.

Per connettersi a un'applicazione utilizzando il client

1. Distribuisci i file di configurazione del client sui dispositivi degli utenti nella seguente posizione:
   - Windows — `C:\ProgramData\Connectivity Client`
   - macOS — `/Library/Application\ Support/Connectivity\ Client`
2. Assicurati che i file di configurazione del client siano di proprietà di root (macOS) o Admin (Windows).
3. Avvia il Connectivity Client.
4. Dopo aver caricato il Connectivity Client, l'utente viene autenticato dall'IdP.
5. Dopo l'autenticazione, gli utenti possono accedere all'applicazione utilizzando il nome DNS fornito da Verified Access, utilizzando il client di loro scelta.

Disinstalla il client

Quando hai finito di usare il Connectivity Client, puoi disinstallarlo.

macOS

Versione 1.0.1 e successive

Passa a `/Applications/Connectivity Client` ed esegui `Connectivity Client Uninstaller.app`.

Versione 1.0.0

Scarica lo `connectivity_client_cleanup.sh` script per Mac con Apple Silicon o Mac con Intel, imposta le autorizzazioni di esecuzione sullo script ed esegui lo script come segue.

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

Windows

Per disinstallare il client su Windows, esegui il programma di installazione e scegli Rimuovi.

Best practice

Prendi in considerazione le seguenti best practice:

- Installa la versione più recente del client.
- Non installare il client utilizzando un programma di installazione non firmato.
- Gli utenti non devono utilizzare una configurazione a meno che non si tratti di una configurazione affidabile fornita da un amministratore IT. Una configurazione non attendibile potrebbe reindirizzare a una pagina di phishing.
- Gli utenti devono disconnettersi dal client prima di lasciare le postazioni di lavoro inattive.
- Aggiungi l'`offline_access`ambito alla tua configurazione OIDC. Ciò consente di richiedere token di aggiornamento, che vengono utilizzati per ottenere più token di accesso senza richiedere all'utente di effettuare nuovamente l'autenticazione.

Risoluzione dei problemi

Le seguenti informazioni possono aiutarti a risolvere i problemi con il client.

Problemi

- Al momento dell'accesso, il browser non si apre per completare l'autenticazione da parte dell'IdP
- Dopo l'autenticazione, lo stato del client è «non connesso»
- Impossibile connettersi utilizzando un browser Chrome o Edge

Al momento dell'accesso, il browser non si apre per completare l'autenticazione da parte dell'IdP

Possibile causa: il file di configurazione è mancante o non valido.

Soluzione: contattare l'amministratore di sistema e richiedere un file di configurazione aggiornato.

Dopo l'autenticazione, lo stato del client è «non connesso»

Possibile causa: esecuzione di altri software VPN AWS Client VPN, come Cisco AnyConnect o OpenVPN Connect.

Soluzione: disconnettiti da qualsiasi altro software VPN. Se non riesci ancora a connetterti, genera un rapporto diagnostico e condividilo con l'amministratore di sistema.

Possibile causa: sulle piattaforme Windows, il client utilizza HTTP sulla porta 80 per la comunicazione sul piano di controllo. Una regola firewall che blocca la porta TCP 80 impedisce la comunicazione sul piano di controllo.

Soluzione: verifica se nelle regole di Windows Firewall è presente una regola in uscita esplicita che blocchi il protocollo TCP sulla porta 80 e disattivala.

Impossibile connettersi utilizzando un browser Chrome o Edge

Possibile causa: quando ci si connette a un'applicazione Web utilizzando un browser Chrome o Edge, il browser non riesce a risolvere il nome di IPv6 dominio.

Soluzione: contatto Supporto AWS.

Cronologia delle versioni

La tabella seguente contiene la cronologia delle versioni del client.

Versione	Modifiche	Scarica	Data
1.0.5	Windows • Correzioni di bug minori	• Windows con x64	20 aprile 2026
1.0.4	macOS • Correzioni di bug minori	• Mac con Apple Silicon • Mac con Intel	9 aprile 2026
1.0.4	Windows • Correzioni di bug minori	• Windows con x64	10 febbraio 2026
1.0.3	macOS • Correzioni di bug minori	• Mac con Apple Silicon • Mac con Intel	29 gennaio 2026
1.0.3	Windows • Correzioni di bug minori e miglioramento del livello di sicurezza	• Windows con x64	11 dicembre 2025

Versione	Modifiche	Scarica	Data
1.0.2	macOS • Correzioni di bug e miglioramenti dell'affidabilità • Miglioramenti dell'interfaccia utente Windows • Correzioni di bug e miglioramenti dell'affidabilità • Miglioramenti dell'interfaccia utente	• Mac con Apple Silicon • Mac con Intel • Windows con x64	9 giugno 2025
1.0.1	macOS • Miglioramenti della stabilità • Applicazione di disinstal lazione Windows • Miglioramenti della stabilità	• Mac con Apple Silicon • Mac con Intel • Windows con x64	5 febbraio 2025
1.0.0	Anteprima pubblica	• Mac con Apple Silicon • Mac con Intel • Windows con x64	1 dicembre 2024

Sicurezza nell'accesso verificato

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità che si applicano all'accesso AWS verificato, consulta AWS Servizi nell'ambito del programma di conformitàAWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza Verified Access. I seguenti argomenti mostrano come configurare l'accesso verificato per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse di accesso verificato.

Indice

Protezione dei dati in Verified Access

Il modello di responsabilità AWS condivisa (modello di) si applica alla protezione dei dati in AWS Verified Access. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei

contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, consulta Domande frequenti sulla privacy dei dati . Per informazioni sulla protezione dei dati in Europa, consulta il General Data Protection Regulation (GDPR) Center.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e di configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Verified Access o altro Servizi AWS utilizzando la console, l'API o gli SDK. AWS CLI AWS I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando si fornisce un URL a un server esterno, suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Crittografia dei dati in transito

Verified Access crittografa tutti i dati in transito dagli utenti finali agli endpoint Verified Access su Internet utilizzando Transport Layer Security (TLS) 1.2 o versione successiva.

Inter-network privacy del traffico

Puoi configurare l'accesso verificato per limitare l'accesso a risorse specifiche nel tuo VPC. Per l'autenticazione basata sull'utente, puoi anche limitare l'accesso a parti della rete, in base al gruppo di utenti che accede agli endpoint. Per ulteriori informazioni, consulta Politiche di accesso verificato.

Crittografia dei dati a riposo per AWS Accesso verificato

AWS Per impostazione predefinita, Verified Access crittografa i dati inattivi, utilizzando chiavi KMS AWS di proprietà. Quando la crittografia dei dati inattivi avviene per impostazione predefinita, aiuta a ridurre il sovraccarico operativo e la complessità associati alla protezione dei dati sensibili. Allo stesso tempo, consente di creare applicazioni sicure che soddisfano i rigorosi requisiti normativi e di conformità alla crittografia. Le sezioni seguenti forniscono i dettagli su come Verified Access utilizza le chiavi KMS per la crittografia dei dati inattivi.

Indice

Accesso verificato e chiavi KMS

AWS chiavi possedute

Verified Access utilizza le chiavi KMS per crittografare automaticamente le informazioni di identificazione personale (PII). Ciò avviene per impostazione predefinita e non puoi visualizzare, gestire, utilizzare o controllare personalmente l'uso delle chiavi di proprietà di AWS. Tuttavia, non è necessario effettuare alcuna operazione o modificare programmi per proteggere le chiavi che eseguono la crittografia dei dati. Per ulteriori informazioni, consulta la pagina chiavi di proprietàAWS nella Guida per gli sviluppatori di AWS Key Management Service .

Sebbene non sia possibile disabilitare questo livello di crittografia o selezionare un tipo di crittografia alternativo, è possibile aggiungere un secondo livello di crittografia alle chiavi di crittografia di AWS

proprietà esistenti scegliendo una chiave gestita dal cliente al momento della creazione delle risorse Verified Access.

Chiavi gestite dal cliente

Verified Access supporta l'uso di chiavi simmetriche gestite dal cliente, create e gestite dall'utente, per aggiungere un secondo livello di crittografia rispetto alla crittografia predefinita esistente. Avendo il pieno controllo di questo livello di crittografia, è possibile eseguire operazioni quali:

- Stabilire e mantenere le policy delle chiavi
- Stabilire e mantenere le policy e le sovvenzioni IAM
- Abilitare e disabilitare le policy delle chiavi
- Ruotare i materiali crittografici delle chiavi
- Aggiungere tag
- Creare alias delle chiavi
- Pianificare l'eliminazione delle chiavi

Per ulteriori informazioni, consulta Customer managed keys nella Guida per sviluppatori AWS Key Management Service .

> **Note**
>
> Verified Access abilita automaticamente la crittografia inattiva utilizzando chiavi AWS proprietarie per proteggere gratuitamente i dati di identificazione personale.
> Tuttavia, verranno AWS KMS applicati dei costi quando si utilizza una chiave gestita dal cliente. Per ulteriori informazioni sui prezzi, consulta i AWS Key Management Service prezzi.

Informazioni che consentono l'identificazione personale

La tabella seguente riassume le informazioni di identificazione personale (PII) utilizzate da Verified Access e il modo in cui vengono crittografate.

Tipo di dati	AWS crittografia a chiave proprietaria	Crittografia con chiavi gestite dal cliente (opzionale)
`Trust provider (user-type)` User-type i provider fiduciari contengono opzioni OIDC come AuthorizationEndpo int,, UserInfoEndpoint ClientId ClientSecret, e così via, che sono considerate informazioni personali.	Abilitato	Abilitato
`Trust provider (device-type)` Device-type i fornitori di servizi fiduciari contengono un TenantId, che è considerato PII.	Abilitato	Abilitato
`Group policy` Fornito durante la creazione o la modifica del gruppo Verified Access. Contiene regole per l'autorizzazione delle richieste di accesso. Potrebbe contenere informazi oni personali come nome utente e indirizzo e-mail e così via.	Abilitato	Abilitato
`Endpoint policy` Fornito durante la creazione o la modifica dell'endpoint	Abilitato	Abilitato

Tipo di dati	AWS crittografia a chiave proprietaria	Crittografia con chiavi gestite dal cliente (opzionale)
Verified Access. Contiene regole per l'autorizzazione delle richieste di accesso. Potrebbe contenere informazioni personali come nome utente e indirizzo e-mail e così via.		

In che modo AWS Verified Access utilizza le sovvenzioni in AWS KMS

Verified Access richiede una concessione per utilizzare la chiave gestita dal cliente.

Quando crei risorse di accesso verificato crittografate con una chiave gestita dal cliente, Verified Access crea una concessione per tuo conto inviando una CreateGrantrichiesta a AWS KMS. Le concessioni AWS KMS vengono utilizzate per consentire a Verified Access l'accesso a una chiave gestita dal cliente nel tuo account.

Verified Access richiede la concessione dell'utilizzo della chiave gestita dal cliente per le seguenti operazioni interne:

- Invia richieste Decrypt a AWS KMS per decrittografare le chiavi di dati crittografate in modo che possano essere utilizzate per decrittografare i dati.
- Invia RetireGrantrichieste a per eliminare una sovvenzione. AWS KMS

Puoi revocare l'accesso alla concessione o rimuovere l'accesso del servizio alla chiave gestita dal cliente in qualsiasi momento. In tal caso, Verified Access non sarà in grado di accedere a nessuno dei dati crittografati dalla chiave gestita dal cliente, il che influirà sulle operazioni che dipendono da tali dati.

Utilizzo di chiavi gestite dal cliente con Verified Access

Puoi creare una chiave simmetrica gestita dal cliente utilizzando o Console di gestione AWS le AWS KMS API. Segui i passaggi per la creazione di una chiave di crittografia simmetrica nella Guida per gli sviluppatori.AWS Key Management Service

Politiche chiave

Le policy della chiave controllano l'accesso alla chiave gestita dal cliente. Ogni chiave gestita dal cliente deve avere esattamente una policy della chiave, che contiene istruzioni che determinano chi può usare la chiave e come la possono usare. Quando crei la chiave gestita dal cliente, è possibile specificare una policy della chiave. Per ulteriori informazioni, consulta le politiche chiave nella Guida per gli AWS Key Management Service sviluppatori.

Per utilizzare la chiave gestita dal cliente con le risorse di accesso verificato, nella policy chiave devono essere consentite le seguenti operazioni API:

- `kms:CreateGrant`: aggiunge una concessione a una chiave gestita dal cliente. Concede l'accesso di controllo a una chiave KMS specificata, che consente l'accesso alle operazioni di concessione richieste da Verified Access. Per ulteriori informazioni, consulta Grants, nella Developer Guide.AWS Key Management Service

  Ciò consente a Verified Access di effettuare le seguenti operazioni:

  - Chiama `GenerateDataKeyWithoutPlainText` per generare una chiave dati crittografata e archiviarla, poiché la chiave dati non viene utilizzata immediatamente per crittografare.
  - Chiama `Decrypt` per utilizzare la chiave dati crittografata memorizzata per accedere ai dati crittografati.
  - Configurare un principale ritirato per consentire al servizio di `RetireGrant`.
- `kms:DescribeKey`— Fornisce i dettagli chiave gestiti dal cliente per consentire a Verified Access di convalidare la chiave.
- `kms:GenerateDataKey`— Consente a Verified Access di utilizzare la chiave per crittografare i dati.
- `kms:Decrypt`— Consenti a Verified Access di decrittografare le chiavi di dati crittografate.

Di seguito è riportato un esempio di policy chiave che è possibile utilizzare per l'accesso verificato.

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

Per ulteriori informazioni, consulta Creazione di una politica chiave e risoluzione dei problemi di accesso tramite chiave nella Guida per gli AWS Key Management Service sviluppatori.

Specificazione di una chiave gestita dal cliente per le risorse di accesso verificato

È possibile specificare una chiave gestita dal cliente per fornire una crittografia di secondo livello per le seguenti risorse:

- Gruppo di accesso verificato
- Endpoint di accesso verificato
- Provider fiduciario Verified Access

Quando si crea una di queste risorse utilizzando il Console di gestione AWS, è possibile specificare una chiave gestita dal cliente nella sezione Crittografia aggiuntiva - opzionale. Durante il processo, seleziona la casella di controllo Personalizza le impostazioni di crittografia (avanzate), quindi inserisci l'ID della AWS KMS chiave che desideri utilizzare. Questa operazione può essere eseguita anche quando si modifica una risorsa esistente o si utilizza il AWS CLI.

> **Note**
>
> Se la chiave gestita dal cliente utilizzata per aggiungere ulteriore crittografia a una delle risorse di cui sopra viene persa, i valori di configurazione delle risorse non saranno più accessibili. Tuttavia, le risorse possono essere modificate utilizzando Console di gestione AWS o AWS CLI, per applicare una nuova chiave gestita dal cliente e reimpostare i valori di configurazione.

AWS Contesto di crittografia Verified Access

Un contesto di crittografia è un insieme opzionale di coppie chiave-valore che contengono informazioni contestuali aggiuntive sui dati. AWS KMS utilizza il contesto di crittografia come dati autenticati aggiuntivi per supportare la crittografia autenticata. Quando includi un contesto di crittografia in una richiesta di crittografia dei dati, AWS KMS associa il contesto di crittografia ai dati crittografati. Per decrittografare i dati, nella richiesta deve essere incluso lo stesso contesto di crittografia.

AWS Contesto di crittografia Verified Access

Verified Access utilizza lo stesso contesto di crittografia in tutte le operazioni AWS KMS crittografiche, in cui la chiave è `aws:verified-access:arn` e il valore è la risorsa Amazon Resource Name (ARN). Di seguito sono riportati i contesti di crittografia per le risorse Verified Access.

Provider fiduciario Verified Access

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

Gruppo Verified Access

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

Endpoint di accesso verificato

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

Monitoraggio delle chiavi di crittografia per AWS Accesso verificato

Quando utilizzi una chiave KMS gestita dal cliente con le tue risorse di accesso AWS verificato, puoi utilizzarla AWS CloudTrailper tenere traccia delle richieste a cui Verified Access invia. AWS KMS

Gli esempi seguenti sono AWS CloudTrail eventi per`CreateGrant`,, e `RetireGrant` `Decrypt` `DescribeKey``GenerateDataKey`, che monitorano le operazioni KMS richiamate da Verified Access per accedere ai dati crittografati dalla chiave KMS gestita dal cliente:

CreateGrant

Quando utilizzi una chiave gestita dal cliente per crittografare le tue risorse, Verified Access invia una `CreateGrant` richiesta per tuo conto per accedere alla chiave del tuo account. AWS La concessione creata da Verified Access è specifica per la risorsa associata alla chiave gestita dal cliente.

L'evento di esempio seguente registra l'operazione `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

Verified Access utilizza l'`RetireGrant`operazione per rimuovere una concessione quando si elimina una risorsa.

L'evento di esempio seguente registra l'operazione `RetireGrant`:

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

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

Decrypt

Verified Access richiama l'`Decrypt`operazione per utilizzare la chiave dati crittografata memorizzata per accedere ai dati crittografati.

L'evento di esempio seguente registra l'operazione `Decrypt`:


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T17:19:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T17:47:05Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e",
        "encryptionContext": {
            "aws:verified-access:arn": "arn:aws:ec2:ca-
central-1:111122223333:verified-access-trust-provider/vatp-00f20a4e455e9340f",
```

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

DescribeKey

Verified Access utilizza l'`DescribeKey`operazione per verificare se la chiave gestita dal cliente associata alla risorsa esiste nell'account e nella regione.

L'evento di esempio seguente registra l'operazione `DescribeKey`:

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

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


GenerateDataKey

L'evento di esempio seguente registra l'operazione `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"
}
```


Gestione delle identità e degli accessi per Verified Access

AWS Identity and Access Management (IAM) è un sistema Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Verified Access. IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta Risoluzione dei problemi relativi all'identità e all'accesso Verified Access)

- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta Come funziona Verified Access con IAM)
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta Esempi di policy basate sull'identità per Verified Access)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/ Facebook Per ulteriori informazioni sull'accesso, consulta Come accedere all' Account AWS nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta AWS Signature Version 4 per le richieste API nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. Per ulteriori informazioni, consulta Che cos'è il Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee nella Guida per l'utente IAM.

Un gruppo IAM specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo passando da un ruolo utente a un ruolo IAM (console) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta Metodi per assumere un ruolo nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per maggiori informazioni, consultare Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere policy in linea (con embedding direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scegliere tra policy gestite e policy in linea nella Guida per l'utente di IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio specificare un'entità principale.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in. AWS Organizations Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta Politiche di controllo delle risorse (RCPs) nella Guida per l'AWS Organizations utente.

- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona Verified Access con IAM

Prima di utilizzare IAM per gestire l'accesso a Verified Access, scopri quali funzionalità IAM sono disponibili per l'uso con Verified Access.

Funzionalità IAM	Supporto Verified Access
Policy basate sull'identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
ACLs	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per avere una visione di alto livello di come Verified Access e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per l'accesso verificato

Supporta le policy basate sull'identità: sì

Le policy basate sull'identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente di IAM.

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Esempi di politiche basate sull'identità per l'accesso verificato

Per visualizzare esempi di politiche basate sull'identità di accesso verificato, consulta. Esempi di policy basate sull'identità per Verified Access

Politiche basate sulle risorse all'interno di Verified Access

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio specificare un'entità principale. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Azioni politiche per l'accesso verificato

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di azioni di accesso verificato, consulta Azioni definite da Amazon EC2 nel Service Authorization Reference.

Le azioni politiche in Verified Access utilizzano il seguente prefisso prima dell'azione:

```
ec2
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

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

Per visualizzare esempi di politiche basate sull'identità di Verified Access, consulta. Esempi di policy basate sull'identità per Verified Access

Risorse relative alle politiche per l'accesso verificato

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon

(ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di risorse Verified Access e relativi ARNs, consulta Resources Defined by Amazon EC2 nel Service Authorization Reference. Per sapere con quali azioni puoi specificare l'ARN di ogni risorsa, consulta Actions Defined by Amazon EC2.

Per visualizzare esempi di politiche basate sull'identità di Verified Access, consulta. Esempi di policy basate sull'identità per Verified Access

Chiavi relative alle condizioni delle policy per Verified Access

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco delle chiavi delle condizioni di accesso verificato, consulta Condition Keys for Amazon EC2 nel Service Authorization Reference. Per informazioni su operazioni e risorse con cui è possibile utilizzare una chiave di condizione, consulta Operazioni definite da Amazon Ec2.

Per visualizzare esempi di politiche basate sull'identità di Verified Access, consulta. Esempi di policy basate sull'identità per Verified Access

ACLs in Accesso verificato

Supporti ACLs: no

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con accesso verificato

Supporta ABAC (tag nelle policy): parzialmente

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con Verified Access

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono un accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee in IAM e Servizi AWS compatibili con IAM nella Guida per l'utente IAM.

Autorizzazioni principali multiservizio per Verified Access

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Le sessioni di accesso diretto (FAS) utilizzano le autorizzazioni del principale chiamante e, in combinazione con la richiesta Servizio AWS, di effettuare richieste Servizio AWS ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per Verified Access

Supporta i ruoli di servizio: no

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

Ruoli collegati ai servizi per Verified Access

Supporta i ruoli collegati ai servizi: sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Per informazioni dettagliate sulla creazione o la gestione dei ruoli collegati al servizio Verified Access, consulta. Usa ruoli collegati ai servizi per l'accesso verificato

Esempi di policy basate sull'identità per Verified Access

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse di accesso verificato. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM (console) nella Guida per l'utente di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da Verified Access, incluso il formato di ARNs per ogni tipo di risorsa, consulta Actions, Resources and Condition Keys for Amazon EC2 nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Politica per la creazione di istanze di accesso verificato
- Consentire agli utenti di visualizzare le loro autorizzazioni

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse di accesso verificato nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.
- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare Protezione dell'accesso API con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Politica per la creazione di istanze di accesso verificato

Per creare un'istanza Verified Access, i responsabili IAM devono aggiungere questa dichiarazione aggiuntiva alla propria policy IAM.

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

> **Note**
>
> `verified-access:AllowVerifiedAccess`è un'API virtuale di sola azione. Non supporta l'autorizzazione basata su risorse, tag o condizioni. Utilizza l'autorizzazione basata su risorse, tag o condizioni per l'azione API. `ec2:CreateVerifiedAccessInstance`

Esempio di politica per la creazione di un'istanza di accesso verificato. In questo esempio, `123456789012` è il numero di AWS account e `us-east-1` la AWS regione.

JSON

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

```
}
```

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono collegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI 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": "*"
        }
    ]
}
```

Risoluzione dei problemi relativi all'identità e all'accesso Verified Access

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Verified Access e IAM.

Problemi

Non sono autorizzato a eseguire un'azione in Verified Access

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `ec2:`*`GetWidget`* fittizie.

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

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `ec2:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo a Verified Access.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Verified Access. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

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

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse di accesso verificato

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se Verified Access supporta queste funzionalità, consulta. Come funziona Verified Access con IAM
- Per scoprire come fornire l'accesso alle tue risorse su tutto Account AWS ciò che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Usa ruoli collegati ai servizi per l'accesso verificato

Accesso verificato da AWS utilizza un ruolo collegato ai servizi IAM, che è un tipo di ruolo IAM collegato direttamente a un servizio. AWS I ruoli collegati ai servizi per Verified Access sono definiti da Verified Access e includono tutte le autorizzazioni richieste dal servizio per chiamare altri utenti per tuo conto. Servizi AWS

Un ruolo collegato al servizio semplifica la configurazione di Verified Access perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Verified Access definisce le autorizzazioni dei suoi ruoli collegati al servizio e, se non diversamente definito, solo Verified Access può assumerne i ruoli. Le autorizzazioni definite includono la politica di fiducia e la politica di autorizzazione e questa politica di autorizzazione non può essere associata a nessun'altra entità IAM.

Autorizzazioni di ruolo collegate al servizio per Verified Access

Verified Access utilizza il ruolo collegato al servizio denominato AWSServiceRoleForVPCVerifiedAccess per fornire le risorse necessarie per utilizzare il servizio nell'account dell'utente.

Il ruolo collegato AWSServiceRoleForVPCVerifiedal servizio di Access prevede che i seguenti servizi assumano il ruolo:

- `verified-access.amazonaws.com`

La politica di autorizzazione dei ruoli, denominata AWSVPCVerifiedAccessServiceRolePolicy, consente a Verified Access di completare le seguenti azioni sulle risorse specificate:

- Azione `ec2:CreateNetworkInterface` su tutte le sottoreti e i gruppi di sicurezza, nonché su tutte le interfacce di rete con il tag `VerifiedAccessManaged=true`
- Azione `ec2:CreateTags` su tutte le interfacce di rete al momento della creazione
- Azione `ec2:DeleteNetworkInterface` su tutte le interfacce di rete con il tag `VerifiedAccessManaged=true`
- Azione `ec2:ModifyNetworkInterfaceAttribute` su tutti i gruppi di sicurezza e tutte le interfacce di rete con il tag `VerifiedAccessManaged=true`

È inoltre possibile visualizzare le autorizzazioni per questa politica nella AWS Managed Policy Reference Guide; vedere. AWSVPCVerifiedAccessServiceRolePolicy

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Crea un ruolo collegato al servizio per Verified Access

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando CreateVerifiedAccessEndpointrichiami la Console di gestione AWS, la o l' AWS API AWS CLI, Verified Access crea automaticamente il ruolo collegato al servizio.

Se elimini questo ruolo collegato ai servizi, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando chiami ancora CreateVerifiedAccessEndpointuna volta, Verified Access crea nuovamente il ruolo collegato al servizio per te.

Modifica un ruolo collegato al servizio per Verified Access

Verified Access non consente di modificare il ruolo collegato al servizio di AWSServiceRoleForVPCVerifiedAccess. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modificare la descrizione di un ruolo collegato al servizio nella Guida per l'utente IAM.

Elimina un ruolo collegato al servizio per Verified Access

Non è necessario eliminare manualmente il ruolo AWSServiceRoleForVPCVerifiedAccess. Quando DeleteVerifiedAccessEndpointrichiami il Console di gestione AWS, il o l' AWS API AWS CLI, Verified Access pulisce le risorse ed elimina automaticamente il ruolo collegato al servizio.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, l'o l' AWS API per eliminare il ruolo collegato al servizio di Access. AWSService RoleFor VPCVerified Per ulteriori informazioni, consulta Eliminare un ruolo collegato al servizio nella Guida per l'utente IAM.

Regioni supportate per i ruoli collegati ai servizi Verified Access

Verified Access supporta l'utilizzo di ruoli collegati al servizio in tutti i paesi in Regioni AWS cui il servizio è disponibile. Per ulteriori informazioni, consulta AWS Regioni ed endpoint.

AWS politiche gestite per l'accesso verificato

Una policy AWS gestita è una policy autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWS nella Guida per l'utente di IAM.

AWS politica gestita: AWSVPCVerified AccessServiceRolePolicy

Questa policy è associata a un ruolo collegato al servizio che consente a Verified Access di eseguire azioni per conto dell'utente. Per ulteriori informazioni, consulta Utilizzo dei ruoli collegati ai servizi. Per visualizzare le autorizzazioni per questa politica, puoi consultare la oppure puoi visualizzare la Console di gestione AWS politica AWSVPCVerifiedAccessServiceRolePolicynella AWS Managed AWSVPCVerifiedAccessServiceRolePolicyPolicy Reference Guide.

Verified Access: aggiornamenti alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti alle politiche AWS gestite per Verified Access da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei documenti di accesso verificato.

Modifica	Descrizione	Data
AWSVPCVerifiedAccessServiceRolePolicy- Politica aggiornata	Verified Access ha aggiornato la sua politica di gestione per	17 novembre 2023

Modifica	Descrizione	Data
	includere le descrizioni di tutte le azioni nel campo «sid».	
AWSVPCVerifiedAccessServiceRolePolicy- Politica aggiornata	Verified Access ha aggiornato la sua politica di gestione per aggiungere risorse del gruppo di sicurezza all'`ec2:CreateNetworkInterface` autorizzazione.	31 maggio 2023
AWSVPCVerifiedAccessServiceRolePolicy: nuova policy	Verified Access ha aggiunto una nuova politica per consentirgli di fornire le risorse necessarie per utilizzare il servizio nell'account.	29 novembre 2022
Verified Access ha iniziato a tenere traccia delle modifiche	Verified Access ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	29 novembre 2022

Convalida della conformità per Verified Access

Accesso verificato da AWS può essere configurato per supportare la conformità agli standard federali di elaborazione delle informazioni (FIPS). Per maggiori informazioni e dettagli sulla configurazione della conformità FIPS per l'accesso verificato, vai a. Conformità FIPS per l'accesso verificato

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. Per ulteriori informazioni sulla responsabilità di conformità durante l'utilizzo Servizi AWS, consulta AWS la documentazione sulla sicurezza.

Resilienza nell'accesso verificato

L'infrastruttura AWS globale è costruita attorno a zone Regioni AWS di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS

Oltre all'infrastruttura AWS globale, Verified Access offre le seguenti funzionalità per aiutarti a supportare le tue esigenze di alta disponibilità.

Più sottoreti per un'elevata disponibilità

Quando crei un endpoint ad accesso verificato di tipo Load Balancer, puoi associare più sottoreti all'endpoint. Ogni sottorete associata all'endpoint deve appartenere a una zona di disponibilità diversa. Associando più sottoreti è possibile garantire un'elevata disponibilità utilizzando più zone di disponibilità.

Monitoraggio Accesso verificato da AWS

Il monitoraggio è una parte importante del mantenimento dell'affidabilità, della disponibilità e delle prestazioni di Accesso verificato da AWS. AWS fornisce i seguenti strumenti di monitoraggio per monitorare Verified Access, segnalare quando qualcosa non va e intraprendere azioni automatiche se necessario:

- Registri di accesso: acquisiscono informazioni dettagliate sulle richieste di accesso alle applicazioni. Per ulteriori informazioni, consulta the section called "Log di accesso verificati".
- AWS CloudTrail— Acquisisce le chiamate API e gli eventi correlati effettuati da o per conto dell'utente Account AWS e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta the section called "CloudTrail registri".

Log di accesso verificati

Dopo aver Accesso verificato da AWS valutato ogni richiesta di accesso, registra tutti i tentativi di accesso. Ciò offre una visibilità centralizzata sull'accesso alle applicazioni e aiuta a rispondere rapidamente agli incidenti di sicurezza e alle richieste di controllo. Verified Access supporta il formato di registrazione Open Cybersecurity Schema Framework (OCSF).

Quando si abilita la registrazione, è necessario configurare una destinazione per l'invio dei log. Il principale IAM utilizzato per configurare la destinazione di registrazione deve disporre di determinate autorizzazioni affinché la registrazione funzioni correttamente. Le autorizzazioni IAM richieste per ogni destinazione di registrazione possono essere visualizzate nella sezione. Autorizzazioni di registrazione degli accessi verificate Verified Access supporta le seguenti destinazioni per la pubblicazione dei log di accesso:

- Gruppi di CloudWatch log di Amazon Logs
- Bucket Amazon S3
- Flussi di distribuzione di Amazon Data Firehose

Indice

- Autorizzazioni di registrazione degli accessi verificate
- Abilita o disabilita i registri di accesso verificato
- Abilita o disabilita il contesto di fiducia di accesso verificato
- Esempi di log OCSF versione 0.1 per Verified Access
- Esempi di log OCSF versione 1.0.0-rc.2 per Verified Access

Versioni di registrazione degli accessi verificate

Per impostazione predefinita, il sistema di registrazione Verified Access utilizza Open Cybersecurity Schema Framework (OCSF) versione 0.1. Per i log di esempio che utilizzano la versione 0.1, vedere. Esempi di log OCSF versione 0.1 per Verified Access

L'ultima versione di registrazione è compatibile con la versione OCSF 1.0.0-rc.2. Per ulteriori informazioni sullo schema, vedere Schema OCSF. Per i log di esempio che utilizzano la versione 1.0.0-rc.2, vedere. Esempi di log OCSF versione 1.0.0-rc.2 per Verified Access

Tieni presente che non puoi utilizzare la versione 0.1 di OCSF se l'endpoint Verified Access utilizza il protocollo TCP.

Per aggiornare la versione di registrazione utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Istanze di accesso verificato.
3. Seleziona l'istanza di accesso verificato appropriata.
4. Nella scheda di configurazione della registrazione dell'istanza di accesso verificato, scegli Modifica la configurazione di registrazione dell'istanza di accesso verificato.
5. Seleziona ocsf-1.0.0-rc.2 dall'elenco a discesa della versione del registro degli aggiornamenti.
6. Scegli Modifica la configurazione di registrazione delle istanze di accesso verificato.

Per aggiornare la versione di registrazione utilizzando il AWS CLI

Utilizzare il comando modify-verified-access-instance-logging-configuration.

Autorizzazioni di registrazione degli accessi verificate

Il principale IAM utilizzato per configurare la destinazione di registrazione deve disporre di determinate autorizzazioni affinché la registrazione funzioni correttamente. Le sezioni seguenti mostrano le autorizzazioni richieste per ogni destinazione di registrazione.

Per la consegna ai registri CloudWatch :

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration`sull'istanza Verified Access
- `logs:CreateLogDelivery`,`logs:DeleteLogDelivery`, `logs:GetLogDeliverylogs:ListLogDeliveries`, e `logs:UpdateLogDelivery` su tutte le risorse
- `logs:DescribeLogGroupse` nel gruppo `logs:PutResourcePolicy` di log di destinazione `logs:DescribeResourcePolicies`

Per la consegna ad Amazon S3:

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration`sull'istanza Verified Access
- `logs:CreateLogDelivery`,`logs:DeleteLogDelivery`, `logs:GetLogDeliverylogs:ListLogDeliveries`, e `logs:UpdateLogDelivery` su tutte le risorse
- `s3:GetBucketPolicye` `s3:PutBucketPolicy` nel bucket di destinazione

Per la consegna a Firehose:

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration`sull'istanza Verified Access
- `firehose:TagDeliveryStream`su tutte le risorse
- `iam:CreateServiceLinkedRole`su tutte le risorse
- `logs:CreateLogDelivery`,`logs:DeleteLogDelivery`, `logs:GetLogDeliverylogs:ListLogDeliveries`, e `logs:UpdateLogDelivery` su tutte le risorse

Abilita o disabilita i registri di accesso verificato

È possibile utilizzare le procedure descritte in questa sezione per abilitare o disabilitare la registrazione. Quando si abilita la registrazione, è necessario configurare una destinazione per l'invio

dei log. Il principio IAM utilizzato per configurare la destinazione di registrazione deve disporre di determinate autorizzazioni affinché la registrazione funzioni correttamente. Le autorizzazioni IAM richieste per ogni destinazione di registrazione sono disponibili nella sezione. Autorizzazioni di registrazione degli accessi verificate

Indice

Abilitare log di accesso

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Istanze di accesso verificato.
3. Seleziona l'istanza di accesso verificato.
4. Nella scheda di configurazione della registrazione dell'istanza di accesso verificato, scegli Modifica la configurazione di registrazione dell'istanza di accesso verificato.
5. (Facoltativo) Per includere i dati di attendibilità inviati dai provider di fiducia nei log, procedi come segue:
   a. Seleziona ocsf-1.0.0-rc.2 dall'elenco a discesa della versione del registro degli aggiornamenti.
   b. Scegli Includi contesto di fiducia.
6. Esegui una delle seguenti operazioni:
   - Attiva Deliver to Amazon CloudWatch Logs. Scegli il gruppo di log di destinazione.
   - Attiva Delivery to Amazon S3. Inserisci il nome, il proprietario e il prefisso del bucket di destinazione.
   - Attiva Deliver to Firehose. Scegli il flusso di consegna di destinazione.
7. Scegli Modifica la configurazione di registrazione delle istanze di accesso verificato.

Per abilitare i registri di accesso verificato utilizzando il AWS CLI

Utilizzare il comando modify-verified-access-instance-logging-configuration.

Disabilitazione dei log di accesso

Puoi disabilitare i log di accesso per la tua istanza di accesso verificato in qualsiasi momento. Dopo aver disabilitato i log di accesso, i dati di registro rimangono nella destinazione del registro fino a quando non vengono eliminati.

Per disabilitare i registri di accesso verificato

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Istanze di accesso verificato.
3. Seleziona l'istanza di accesso verificato.
4. Nella scheda di configurazione della registrazione dell'istanza di accesso verificato, scegli Modifica la configurazione di registrazione dell'istanza di accesso verificato.
5. Disattiva la consegna dei log.
6. Scegli Modifica la configurazione di registrazione delle istanze di accesso verificato.

Per disabilitare i registri di accesso verificato utilizzando il AWS CLI

Utilizzare il comando modify-verified-access-instance-logging-configuration.

Abilita o disabilita il contesto di fiducia di accesso verificato

Il contesto di fiducia inviato dal tuo provider di fiducia può essere facoltativamente abilitato per l'inclusione nei registri di accesso verificato. Ciò può essere utile quando si definiscono politiche che consentono o negano l'accesso alle applicazioni. Dopo averlo abilitato, il contesto di fiducia viene trovato nel registro sotto il `data` campo. Se il contesto di fiducia è disabilitato, il `data` campo è impostato su`null`. Per configurare l'accesso verificato in modo che includa il contesto di fiducia nei log, esegui la procedura seguente.

> **Note**
>
> L'inclusione del contesto di attendibilità nei registri di accesso verificato richiede l'aggiornamento alla versione di registrazione più recente. `ocsf-1.0.0-rc.2` La procedura seguente presuppone che la registrazione sia già abilitata. Se ciò non è vero, vedere Abilitare log di accesso la procedura completa.

Indice

- Abilita il contesto di fiducia
- Disabilita il contesto di fiducia

Abilita il contesto di fiducia

Per includere il contesto di fiducia nei log di accesso verificato utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Istanze di accesso verificato.
3. Seleziona l'istanza di accesso verificato appropriata.
4. Nella scheda di configurazione della registrazione dell'istanza di accesso verificato, scegli Modifica la configurazione di registrazione dell'istanza di accesso verificato.
5. Seleziona ocsf-1.0.0-rc.2 dall'elenco a discesa della versione del registro degli aggiornamenti.
6. Attiva Include trust context.
7. Scegli Modifica la configurazione di registrazione delle istanze di accesso verificato.

Per includere il contesto di fiducia nei log di accesso verificato utilizzando il AWS CLI

Utilizzare il comando modify-verified-access-instance-logging-configuration.

Disabilita il contesto di fiducia

Se non si desidera più includere il contesto di fiducia nei log, è possibile rimuoverlo eseguendo la procedura seguente.

Per rimuovere il contesto di attendibilità dai log di accesso verificato utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Istanze di accesso verificato.
3. Seleziona l'istanza di accesso verificato appropriata.
4. Nella scheda di configurazione della registrazione dell'istanza di accesso verificato, scegli Modifica la configurazione di registrazione dell'istanza di accesso verificato.
5. Disattiva Include trust context.
6. Scegli Modifica la configurazione di registrazione delle istanze di accesso verificato.

Per rimuovere il contesto di attendibilità dai log di accesso verificato utilizzando il AWS CLI

Utilizzare il comando modify-verified-access-instance-logging-configuration.

Esempi di log OCSF versione 0.1 per Verified Access

Di seguito sono riportati alcuni log di esempio che utilizzano la versione 0.1 di OCSF.

Esempi

- Accesso concesso con OIDC
- Accesso concesso con OIDC e JAMF
- Accesso concesso con OIDC e CrowdStrike
- Accesso negato a causa di un cookie mancante
- Accesso negato dalla policy
- Voce di registro sconosciuta

Accesso concesso con OIDC

In questo esempio di registrazione, Verified Access consente l'accesso a un endpoint con un provider di fiducia per utenti 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
}
```

Accesso concesso con OIDC e JAMF

In questo esempio di registrazione, Verified Access consente l'accesso a un endpoint con provider affidabili di dispositivi OIDC e JAMF.

```
{
    "activity": "Access Granted",
    "activity_id": "1",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": {
        "ip": "10.2.7.68",
        "type": "Unknown",
        "type_id": 0,
        "uid": "41b07859-4222-4f41-f3b9-97dc1EXAMPLE"
    },
    "duration": "0.347",
    "end_time": "1668804944086",
    "time": "1668804944086",
    "http_request": {
        "http_method": "GET",
```

```
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "h2",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36",
        "version": "HTTP/2.0"
    },
    "http_response": {
        "code": 304
    },
    "identity": {
        "authorizations": [
            {
                "decision": "Allow",
                "policy": {
                    "name": "inline"
                }
            }
        ],
        "idp": {
            "name": "oidc",
            "uid": "vatp-9778003bc2EXAMPLE"
        },
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "4f040d0f96becEXAMPLE"
        }
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-321318ce-6100d340adf4fb29dEXAMPLE",
        "logged_time": 1668805278555,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
```

```
    "ref_time": "2022-11-18T20:55:44.086480Z",
    "proxy": {
        "ip": "10.5.192.96",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-3598f66575EXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "192.168.20.246",
        "port": 61769
    },
    "start_time": "1668804943739",
    "status_code": "100",
    "status_details": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "20800101",
    "type_name": "AccessLogs: Access Granted",
    "unmapped": null
}
```


Accesso concesso con OIDC e CrowdStrike

In questo esempio di registrazione, Verified Access consente l'accesso a un endpoint con OIDC e Device Trust Provider. 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
}
```

Accesso negato a causa di un cookie mancante

In questo esempio di registrazione, Verified Access nega l'accesso a causa della mancanza di un cookie di autenticazione.

```
{
    "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
}
```

Accesso negato dalla policy

In questa voce di registro di esempio, Verified Access nega una richiesta autenticata perché la richiesta non è consentita dalle politiche di accesso.

```
{
    "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
}
```

Voce di registro sconosciuta

In questa voce di registro di esempio, Verified Access non può generare una voce di registro completa, quindi emette una voce di registro sconosciuta. Ciò garantisce che ogni richiesta venga visualizzata nel registro degli accessi.

```
{
    "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
}
```


Esempi di log OCSF versione 1.0.0-rc.2 per Verified Access

Di seguito sono riportati alcuni log di esempio che utilizzano la versione OCSF 1.0.0-rc.2.

Esempi

- Accesso concesso con contesto di fiducia incluso
- Accesso concesso con contesto di fiducia omesso
- Assegna i privilegi con l'endpoint CIDR di rete

Accesso concesso con contesto di fiducia incluso


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

Accesso concesso con contesto di fiducia omesso

```
{
    "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
}
```


Assegna i privilegi con l'endpoint CIDR di rete


```
{
    "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"
    }
}
```

Registra le chiamate API ad accesso verificato utilizzando AWS CloudTrail

AWS Verified Access è integrato con AWS CloudTrail un servizio che fornisce una registrazione delle azioni intraprese da un utente, da un ruolo o da un utente Servizio AWS in Accesso verificato. CloudTrail acquisisce le chiamate API per Verified Access come eventi. Le chiamate acquisite includono chiamate dalla console Verified Access e chiamate in codice alle operazioni dell'API Verified Access. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a Verified Access, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e ulteriori dettagli.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente root o utente.
- Se la richiesta è stata effettuata per conto di un utente del Centro identità IAM.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro Servizio AWS.

CloudTrail è attivo nel tuo account Account AWS quando crei l'account e hai automaticamente accesso alla cronologia degli CloudTrail eventi. La cronologia CloudTrail degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni di eventi di gestione registrati in un. Regione AWSPer ulteriori informazioni, consulta Lavorare con la cronologia degli CloudTrail eventi nella Guida per l'utente.AWS CloudTrail Non sono CloudTrail previsti costi per la visualizzazione della cronologia degli eventi.

Per una registrazione continua degli eventi degli Account AWS ultimi 90 giorni, crea un trail o un data store di eventi CloudTrailLake.

CloudTrail sentieri

Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Tutti i percorsi creati utilizzando il Console di gestione AWS sono multiregionali. È possibile creare un trail per una singola Regione o per più Regioni tramite AWS CLI. La creazione di un percorso multiregionale è consigliata in quanto consente di registrare l'intera attività del proprio Regioni AWS account. Se si crea un trail per una singola Regione, è possibile visualizzare solo gli eventi registrati nella Regione AWS del trail. Per ulteriori informazioni sui trail, consulta Creating a trail for your Account AWS e Creating a trail for an organization nella Guida per l'utente di AWS CloudTrail .

Puoi inviare gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket Amazon S3 CloudTrail creando un percorso, tuttavia ci sono costi di storage di Amazon S3. Per ulteriori informazioni sui CloudTrail prezzi, consulta la pagina Prezzi.AWS CloudTrail Per informazioni sui prezzi di Amazon S3, consulta Prezzi di Amazon S3.

CloudTrail Archivi di dati sugli eventi di Lake

CloudTrail Lake ti consente di eseguire query basate su SQL sui tuoi eventi. CloudTrail Lake converte gli eventi esistenti in formato JSON basato su righe in formato Apache ORC. ORC è un formato di archiviazione a colonne ottimizzato per il recupero rapido dei dati. Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili basate sui criteri selezionati applicando i selettori di eventi avanzati. I selettori applicati a un archivio di dati degli eventi controllano quali eventi persistono e sono disponibili per l'esecuzione della query. Per ulteriori informazioni su CloudTrail Lake, consulta Working with AWS CloudTrail Lake nella Guida per l'utente.AWS CloudTrail

CloudTrail Gli archivi e le richieste di dati sugli eventi di Lake comportano dei costi. Quando crei un datastore di eventi, scegli l'opzione di prezzo da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. Per ulteriori informazioni sui CloudTrail prezzi, consulta Prezzi.AWS CloudTrail

Eventi di gestione degli accessi verificati

Gli eventi di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse di Account AWS. Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

Verified Access registra le operazioni del piano di controllo come eventi di gestione. Per un elenco, consulta Amazon EC2 API Reference.

Esempi di eventi Verified Access

L'esempio seguente mostra un CloudTrail evento che dimostra l'`CreateVerifiedAccessInstance`azione.


```
{
    "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"
}
```

Per informazioni sul contenuto dei CloudTrail record, consultate il contenuto dei CloudTrail record nella Guida per l'AWS CloudTrail utente.

Quote per Accesso verificato da AWS

Hai Account AWS delle quote predefinite, precedentemente denominate limiti, per ciascuna di esse. Servizio AWS Salvo diversa indicazione, ogni quota è. Region-specific

Account AWS quote a livello 2

Hai Account AWS le seguenti quote relative all'accesso verificato.

Nome	Predefinita	Adattabile	Description
Istanze di accesso verificato	5	Sì	Il numero massimo di istanze di accesso verificato che i clienti possono creare nella regione corrente.
Gruppi di accesso verificato	10	Sì	Il numero massimo di gruppi di accesso verificati che i clienti possono creare nella regione corrente.
Fornitori fiduciari di accesso verificato	15	Sì	Il numero massimo di fornitori fiduciari di accesso verificato che i clienti possono creare nella regione corrente.
Endpoint di accesso verificato	50	Sì	Il numero massimo di endpoint di accesso verificato che i clienti possono creare nella regione corrente.

Intestazioni HTTP

Di seguito sono elencati i limiti di dimensione per le intestazioni HTTP.

Nome	Predefinita	Adattabile
Riga della richiesta	16 K	No
Intestazione singola	16 K	No
Intestazione della risposta intera	32 K	No
Intestazione della richiesta intera	64 K	No

Traffico HTTP

Il timeout di inattività della connessione è di 60 secondi. Se un'applicazione impiega più di 60 secondi per rispondere a una richiesta HTTP, il client riceve un errore di timeout del gateway HTTP 504. Se i log di accesso verificato sono abilitati, registriamo tutti gli errori HTTP 504.

Dimensione della dichiarazione OIDC

Di seguito è riportato il limite di dimensione delle richieste OIDC.

Nome	Predefinita	Adattabile
Dimensione della dichiarazione OIDC	11 KG	No

Centro identità IAM

Verified Access può fornire l'accesso agli utenti di IAM Identity Center assegnati a un massimo di 1.000 gruppi.

Client di connettività

Il Connectivity Client ha il seguente limite.

Nome	Predefinita	Adattabile
Connessioni simultanee di istanze Verified Access per dispositivo	5	No

Cronologia dei documenti per la Verified Access User Guide

La tabella seguente descrive le versioni della documentazione per Verified Access.

Modifica	Descrizione	Data
Support per i token di accesso nel contesto della fiducia	Aggiornamento da aggiunger e `additional_user_co ntext` alle dichiarazioni degli utenti OIDC.	24 febbraio 2025
Support per risorse su protocolli non HTTP	Rilascio dell'accesso alle risorse tramite protocolli non HTTP.	5 febbraio 2025
Versione di anteprima	Versione di anteprima dell'accesso alle risorse tramite protocolli non HTTP.	1 dicembre 2024
AWS politica gestita aggiornat a	Aggiornamento apportato alla policy IAM AWS gestita per l'accesso verificato.	17 novembre 2023
Crittografia dei dati a riposo	AWS Per impostazione predefinita, Verified Access crittografa i dati inattivi, utilizzando chiavi KMS AWS di proprietà.	28 settembre 2023
Supporto per la conformità a FIPS	Configura l'accesso verificato per la conformità FIPS.	26 settembre 2023
Registrazione avanzata	Aggiunta della funzionalità di registrazione che aggiunge contesti di fiducia ai log.	19 giugno 2023

AWS politica gestita aggiornata	Aggiornamento apportato alla policy IAM AWS gestita per l'accesso verificato.	31 maggio 2023
Versione GA	Versione GA della Verified Access User Guide. Include AWS WAF l'integrazione.	27 aprile 2023
Versione di anteprima	Versione di anteprima della Verified Access User Guide	29 novembre 2022

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.