Guida per l'utente

AWS Accesso verificato

AWS Accesso verificato: Guida per l'utente

Table of Contents

Che cos'è l'accesso AWS verificato?

Con AWS Verified Access, 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 dell'accesso verificato

- Migliore livello di sicurezza: un modello di sicurezza tradizionale valuta l'accesso una 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 i AWS servizi 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 deve 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 richieste di assistenza derivanti da problemi relativi alla VPN.
- Risoluzione dei problemi e controlli semplificati: Verified Access registra tutti i tentativi di accesso, fornendo una visibilità centralizzata sull'accesso alle applicazioni, per aiutarti a rispondere rapidamente agli incidenti di sicurezza e alle richieste di controllo.

Accedere all'accesso AWS verificato

È possibile utilizzare una qualsiasi delle seguenti interfacce per utilizzare una qualsiasi delle seguenti interfacce per utilizzare una qualsiasi delle seguenti interfacce per lavorare con

- AWS Management Console: fornisce un'interfaccia Web utilizzare per creare e gestire risorse di accesso verificato per creare e gestire risorse di accesso verificato. Accedere ad AWS Management Console e aprire la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.

- AWS Command Line Interface(AWS CLI) — Fornisce comandi per un'ampia gamma diServizi AWS, incluso l'accesso AWS verificato. La AWS CLI è supportata su Windows, macOS e Linux. Per ottenere la AWS CLI, consulta AWS Command Line Interface.
- AWSSDK: forniscono API specifiche per le lingue. Gli AWS SDK di gestiscono molti dei dettagli della connessione, ad esempio il calcolo delle firme e la gestione degli errori e gestire molti degli SDK di gestiscono molti dei dettagli della connessione, ad esempio il calcolo delle firme e la gestione degli errori. Per ulteriori informazioni, consulta SDK di AWS.
- API di query: forniscono operazioni API di basso livello accessibili tramite richieste HTTPS. L'utilizzo dell'API di query è il modo più diretto di accedere a un tramite. Tuttavia, richiede che l'applicazione gestisca dettagli di basso livello, come la generazione dell'hash per gestire dettagli di basso livello, come la generazione dell'hash per gestire dettagli di basso livello, come la generazione dell'hash per gestire dettagli di basso livello Per ulteriori informazioni, consulta Azioni di accesso verificato nel riferimento API di Amazon EC2.

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

Prezzi

Ti verrà addebitata ogni ora per ogni richiesta su Verified Access e ti verrà addebitata la quantità di dati elaborata da Verified Access. Per ulteriori informazioni, consulta Prezzi di AWS Verified Access.

Come funziona l'accesso verificato

AWSVerified Access valuta ogni richiesta di applicazione da parte degli utenti e consente l'accesso in base a:

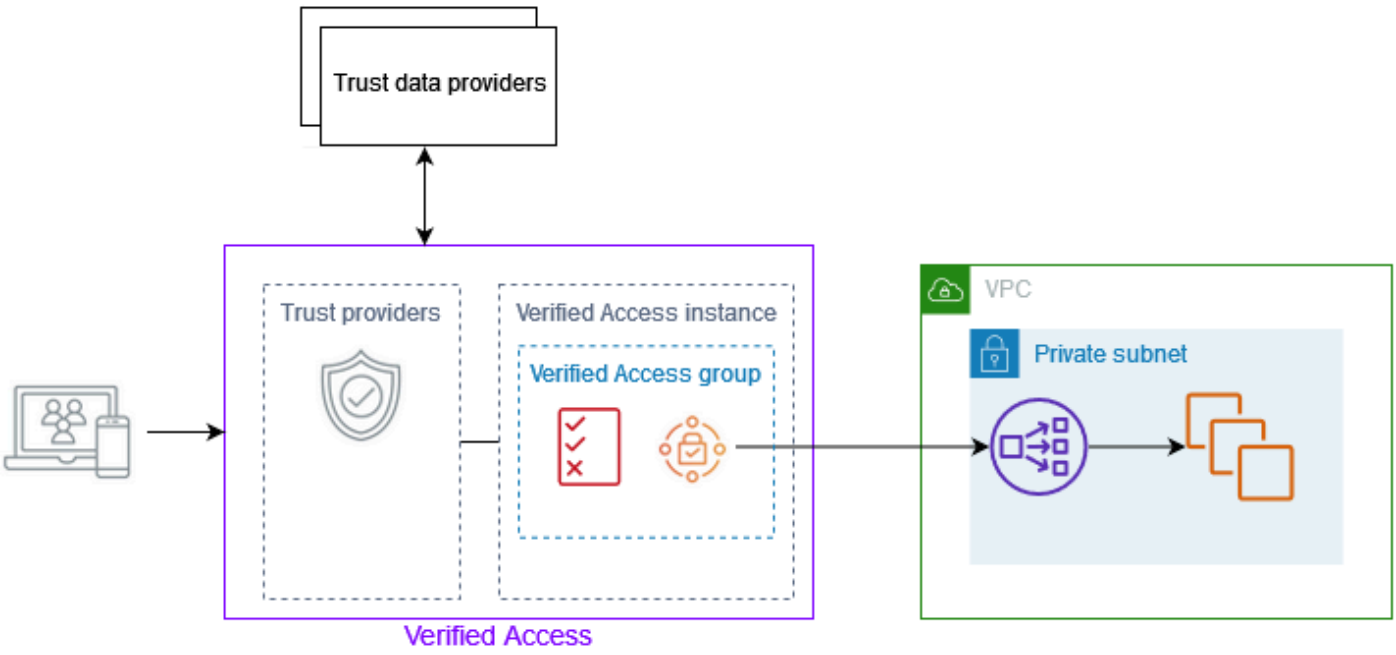
- Dati attendibili inviati dal fornitore fiduciario scelto (da AWS o da una terza parte).
- Politiche di accesso che crei in Accesso verificato.

Quando un utente tenta di accedere a un'applicazione, Verified Access ottiene i dati dal fornitore di fiducia e li valuta rispetto ai criteri impostati 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 politica.

Inoltre, Verified Access registra ogni tentativo di accesso, per aiutarti 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 per il gruppo e a qualsiasi politica dell'endpoint specifica dell'applicazione. Se l'accesso è consentito, la richiesta viene inviata all'applicazione tramite l'endpoint.



- Istanze di accesso verificate: un'istanza valuta le richieste delle applicazioni e concede l'accesso solo quando i requisiti di sicurezza sono soddisfatti.
- Endpoint di accesso verificati: ogni endpoint rappresenta un'applicazione. È possibile creare un endpoint di bilanciamento del carico o un endpoint di interfaccia di rete.
- Gruppo Verified Access: una raccolta di endpoint di accesso verificato. Ti consigliamo di raggruppare gli endpoint per le 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.
- Politiche 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 al 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.
- Provider fiduciari: un servizio che gestisce le identità degli utenti o lo stato di sicurezza dei dispositivi. Verified Access funziona con entrambi i fornitori di servizi fiduciari AWS e di terze parti. Devi collegare almeno un trust provider a ciascuna istanza di Verified Access. Puoi collegare un unico provider di trust delle identità e più provider di attendibilità dei dispositivi a ciascuna istanza di Verified Access.
- Dati attendibili: i dati relativi alla sicurezza per utenti o dispositivi che il tuo fornitore di fiducia invia a Verified Access. Denominato anche contesto di fiducia o affermazioni degli utenti. 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: Guida introduttiva all'accesso verificato

Usa questo tutorial per iniziare a usare AWS Verified Access. Imparerai come creare e configurare risorse di accesso verificato.

Prima di aggiungere questa applicazione a Verified Access, l'applicazione era accessibile solo tramite la rete privata. Alla fine di questo tutorial, utenti specifici possono accedere alla stessa applicazione su Internet, senza utilizzare una VPN.

> **Note**
>
> Questo esempio non dimostra l'integrazione con il tuo provider di fiducia basato su dispositivi. Per questo esempio, lavoriamo solo con un provider fiduciario basato sull'identità.

Attività

Prerequisiti

Di seguito sono riportati i prerequisiti per questo tutorial:

- Per dimostrare questo esempio di utilizzo dell'accesso verificato, ne useremo dueAccount AWS. Un account ospiterà l'applicazione di destinazione e le risorse di accesso verificato verranno create nell'altro account.
- AWS IAM Identity CenterAbilitalo in Regione AWS quello in cui stai lavorando. Puoi quindi utilizzare IAM Identity Center come fornitore di fiducia con accesso verificato. Per ulteriori informazioni, consulta Enable IAM Identity Center nella Guida AWS IAM Identity Center per l'utente.
- Un dominio pubblico ospitato e le autorizzazioni necessarie per aggiornare i record DNS per il dominio.
- Un'applicazione in esecuzione dietro un sistema di bilanciamento del carico interno in un. Account AWS Il nome di dominio dell'applicazione di esempio che useremo è`www.myapp.example.com`.
- Assicurati che la tua policy IAM disponga di tutte le autorizzazioni necessarie per creare un'istanza di accesso AWS verificato, elencate quiPolitica per la creazione di istanze di accesso verificato.

Passaggio 1: crea un'istanza di accesso verificato

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

Per creare un'istanza di accesso verificato

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione di Amazon VPC, 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 Verified Access.
4. Per Trust provider, mantieni l'opzione predefinita.
5. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
6. Scegli Crea istanza di accesso verificato.

Passaggio 2: configura un fornitore di fiducia

Puoi configurarti AWS IAM Identity Center come fornitore di fiducia.

Per creare un provider fiduciario IAM Identity Center

1. Nel pannello di navigazione di Amazon VPC, scegli fornitori di fiducia di accesso verificato, quindi Crea provider di fiducia di accesso verificato.
2. (Facoltativo) Per Targhetta e Descrizione, inserisci un nome e una descrizione per il provider fiduciario Verified Access.
3. 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`**.
4. In Tipo di provider fiduciario, seleziona User trust provider.
5. In User trust provider type, seleziona IAM Identity Center.
6. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
7. Scegli Create Verified Access Trust Provider.

Passaggio 3: collega il tuo provider fiduciario all'istanza

Utilizza la seguente procedura per collegare il provider fiduciario alla tua istanza di accesso verificato.

Per collegare un provider fiduciario alla tua istanza

1. Nel pannello di navigazione di Amazon VPC, scegli Istanze di accesso verificato.
2. Selezionare l'istanza.
3. Scegli Actions, Attach Verified Access Trust Provider.
4. Per il provider fiduciario Verified Access, scegli il tuo fornitore di fiducia.
5. Scegli Attach Verified Access Trust Provider.

Passaggio 4: creare un gruppo di accesso verificato

Creiamo un gruppo che puoi usare per l'endpoint che creerai nel passaggio successivo.

Per creare un gruppo con accesso verificato

1. Nel pannello di navigazione di Amazon VPC, scegli Gruppi di accesso verificato, quindi Crea gruppo di accesso verificato.
2. (Facoltativo) Per Tag e Descrizione, inserisci un nome e una descrizione per il gruppo.

3. Per l'istanza di accesso verificato, scegli la tua istanza di accesso verificato.
4. Per la definizione della politica, lascia vuoto questo campo. Creerai una politica più avanti in questo tutorial.
5. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
6. Scegli Crea gruppo di accesso verificato.

Passaggio 5: Condividi il tuo gruppo con accesso verificato tramite AWS Resource Access Manager

In questo passaggio, condividerai il gruppo appena creato con quello Account AWS in cui è in esecuzione l'applicazione di destinazione. Per condividere un gruppo ad accesso verificato, devi aggiungerlo a una condivisione di risorse. Se non disponi di una condivisione di risorse, devi prima crearne una.

Se fai parte di un'organizzazione e la condivisione all'interno dell'organizzazione è abilitata, ai consumatori dell'organizzazione viene automaticamente concesso l'accesso al gruppo condiviso di accesso verificato. AWS Organizations In caso contrario, i consumatori ricevono un invito a partecipare alla condivisione di risorse e ottengono l'accesso al gruppo condiviso con accesso verificato dopo aver accettato l'invito.

Segui la procedura descritta in Creazione di una condivisione di risorse nella Guida per l'utente di AWS RAM. Per Seleziona il tipo di risorsa, scegli il gruppo con accesso verificato, quindi seleziona la casella di controllo relativa al tuo gruppo di accesso verificato.

Per ulteriori informazioni, consulta Nozioni di base nella Guida per l'utente di AWS RAM.

Passaggio 6: aggiungi l'applicazione creando un endpoint

Utilizza le seguenti procedure per creare un endpoint. Questo passaggio presuppone che l'applicazione sia in esecuzione con un sistema di bilanciamento del carico interno di Elastic Load Balancing.

Per creare un endpoint con accesso verificato

1. Nel pannello di navigazione di Amazon VPC, scegli Endpoint di accesso verificato, quindi Crea endpoint di accesso verificato.

2. (Facoltativo) Per Tag e Descrizione, inserisci un nome e una descrizione per l'endpoint.
3. Per il gruppo di accesso verificato, scegli il tuo gruppo di accesso verificato.
4. Per i dettagli dell'applicazione, procedi come segue:
    a. Per Dominio dell'applicazione, inserisci un nome DNS per l'applicazione.
    b. In Certificato di dominio ARN, seleziona l'Amazon Resource Name (ARN) del tuo certificato TLS pubblico.
5. Per informazioni dettagliate sull'endpoint, procedi come segue:
    a. In Attachment type (Tipo collegamento), selezionare VPC.
    b. Per i gruppi di sicurezza, seleziona un gruppo di sicurezza da associare all'endpoint.
    c. Per il prefisso del dominio Endpoint, inserisci un identificatore personalizzato. Questo verrà aggiunto al nome DNS generato da Verified Access. Per questo esempio, possiamo usare. **`my-ava-app`**
    d. Per il tipo di endpoint, scegli Load balancer.
    e. Per Protocollo, seleziona HTTPS o HTTP. Dipende dalla configurazione del sistema di bilanciamento del carico.
    f. Per Port (Porta) inserire il numero di porta. Dipende dalla configurazione del sistema di bilanciamento del carico.
    g. Per Load balancer ARN, scegli il tuo load balancer.
    h. Per Subnet, seleziona le sottoreti associate al tuo load balancer.
6. Per la definizione della politica, non inserire una politica in questo momento. Ne parleremo più avanti nel tutorial.
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 endpoint di accesso verificato.

Passaggio 7: Configurare le impostazioni DNS

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 pannello di navigazione di Amazon VPC, scegli Endpoint Verified Access.
2. Seleziona l'endpoint che hai creato in precedenza.
3. Scegli la scheda Dettagli per l'endpoint.
4. Copia il dominio dell'endpoint da Dominio dell'endpoint.

Per questo tutorial, il nome di dominio dell'endpoint sarà. `my-ava-app.edge-1a2b3c4d5e6f7g.vai-1a2b3c4d5e6f7g.prod.verified-access.us-west-2.amazonaws.com`

Crea un record CNAME con il tuo provider DNS:

Nome record	Type	Valore
www.myapp.example.com	CNAME	my-ava-app.edge-1a 2b3c4d5e6f7g.vai-1 a2b3c4d5e6f7g.prod. verified-access.us-west-2.amazonaws. com

Fase 8: Verifica la connettività alla tua applicazione

Ora puoi testare la connettività alla tua applicazione. Inserisci il nome di dominio dell'applicazione nel tuo browser web. Il comportamento predefinito delle politiche di accesso verificato consiste nel rifiutare tutte le richieste. Poiché non abbiamo ancora adottato una politica che consenta l'accesso a chiunque, tutte le richieste devono essere rifiutate.

Fase 9: Configurazione della politica di accesso a livello di gruppo

Utilizza la procedura seguente per modificare il gruppo Verified Access 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 sulla creazione di una policy, consultaPolitiche di accesso verificato.

Per modificare un gruppo di accesso verificato

1. Nel pannello di navigazione di Amazon VPC, scegli Gruppi di accesso verificato.
2. Seleziona il gruppo .
3. Scegli Azioni, Modifica la politica di gruppo Verified Access.
4. Inserisci la politica.
5. Scegli Modifica politica di gruppo con accesso verificato.

Passaggio 10: ripetere il test della connettività

Ora che i criteri di gruppo sono stati definiti, puoi accedere all'applicazione. Inserisci il nome di dominio dell'applicazione nel tuo browser web. La richiesta dovrebbe essere consentita e dovresti essere reindirizzato all'applicazione.

Eliminazione

Al termine del test, procedi nel seguente modo per eliminare le risorse che sono state create.

Per eliminare le risorse di accesso verificato create con questo tutorial

1. Nel pannello di navigazione di Amazon VPC, scegli Endpoint Verified Access. Seleziona l'endpoint che desideri rimuovere. Scegli Azioni, Elimina l'endpoint di accesso verificato.
2. Nel riquadro di navigazione, scegli Gruppi di accesso verificato. Seleziona il gruppo che desideri rimuovere. Scegli Azioni, Elimina il gruppo di accesso verificato. Nota: potrebbe essere necessario attendere un paio di minuti fino al completamento del processo di eliminazione dell'endpoint.
3. Nel pannello di navigazione di Amazon VPC, scegli Istanze di accesso verificato. Seleziona l'istanza che hai creato per questo tutorial. Scegli Actions, Detach Verified Access Trust Provider. Seleziona il fornitore di fiducia dall'elenco a discesa, scegli Detach Verified Access trust provider.
4. Nel pannello di navigazione di Amazon VPC, scegli fornitori di fiducia ad accesso verificato. Seleziona il provider di fiducia che hai creato per questo tutorial. Scegli Azioni, Elimina il provider fiduciario di accesso verificato.
5. Nel pannello di navigazione di Amazon VPC, scegli Istanze di accesso verificato. Seleziona l'istanza che hai creato per questo tutorial. Scegli Azioni, Elimina istanza di accesso verificato.

Istanze di accesso verificato

Un'istanza di accesso AWS verificato è una AWS risorsa che ti aiuta a organizzare i tuoi provider fiduciari e i gruppi di accesso verificato.

Argomenti

Crea un'istanza di accesso verificato

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

Per creare un'istanza di accesso verificato

1. Accedi alla 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. (Facoltativo) Scegli abilita per gli standard FIPS (Federal Information Process Standards) se desideri che Verified Access sia conforme allo standard FIPS.
5. (Facoltativo) Per Trust provider, scegli un provider fiduciario da collegare all'istanza Verified Access.
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 istanza di accesso verificato.

Collega un provider fiduciario a un'istanza

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

1. Accedi alla 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.

Scollega un fornitore di fiducia da un'istanza

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

1. Accedi alla 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.

Elimina 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

1. Accedi alla 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).

Integrazione 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 WAFè un firewall per applicazioni Web che consente di monitorare le richieste HTTP (S) inoltrate alle risorse protette delle applicazioni Web. Per ulteriori informazioni su AWS WAF, consulta AWS WAF nella 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 (S) 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 AWS Management Console o descrivendo l'endpoint con. AWS CLI

> **Note**
>
> Puoi anche utilizzare la AWS WAF console o l'API per realizzare questa integrazione. Avrai bisogno dell'Amazon Resource Name (ARN) della tua istanza Verified Access. È possibile creare questo ARN utilizzando il seguente formato:. `arn:${Partition}:ec2:${Region}:${Account}:verified-access-instance/${VerifiedAccessInstanceId}`

Argomenti

- Autorizzazioni IAM necessarie per l'integrazione AWS WAF
- Associa un ACL web AWS WAF
- Verifica lo stato dell'integrazione AWS WAF
- Dissocia un ACL web AWS WAF

Autorizzazioni IAM necessarie per l'integrazione AWS WAF

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 il. AWS Management Console

> **Tip**
>
> È necessario disporre di un ACL AWS WAF Web esistente per completare la procedura seguente. Per ulteriori informazioni sugli ACL Web, consulta gli elenchi di controllo degli accessi Web nella Guida per gli AWS WAFsviluppatori.

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

1. Accedi alla 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.

Puoi anche usare il form AWS Management Console per AWS WAF eseguire questa operazione. Per ulteriori informazioni, consulta Associare o dissociare un ACL Web con una risorsa AWS nella Developer Guide. AWS WAF

Verifica lo stato dell'integrazione AWS WAF

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 ilAWS Management Console.

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

1. Accedi alla 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 il. AWS Management Console

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

1. Accedi alla 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.

È inoltre possibile utilizzare il form AWS Management Console per AWS WAF eseguire questa operazione. Per ulteriori informazioni, consulta Associare o dissociare un ACL Web con una risorsa AWS nella Developer Guide. AWS WAF

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 AWSoffre 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)

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

Argomenti

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 AWS Verified Access. Queste informazioni sono chiamate 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

Fornitori di servizi fiduciari per l'identità

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 Organizationsistanza. 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.

Consulta Gestire le istanze dell'organizzazione e dell'account di IAM Identity Center nella Guida per l'AWS IAM Identity Centerutente 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 (AWSconsole)

1. Apri alla 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 (AWSCLI) 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 (AWSconsole)

1. Apri alla 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 (AWSCLI) di IAM Identity Center

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

Utilizzo di un provider di fiducia OpenID Connect

AWSVerified Access supporta provider di identità che utilizzano metodi OpenID Connect (OIDC) standard. Puoi utilizzare provider compatibili con OIDC come provider fiduciari di identità utente con Verified Access. 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 fiducia verranno recuperati. Dopo aver ricevuto i dati di attendibilità, la politica di accesso verificato viene valutata rispetto a tali dati.

> **Note**
>
> Verified Access non utilizza i dati attendibili `ID token` inviati dal provider OIDC per la valutazione della politica di accesso verificato. Solo i dati attendibili di `UserInfo Endpoint` vengono valutati rispetto alla politica.

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
- Ambito

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 alla 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 Emittente, inserisci l'identificatore dell'emittente OIDC.
8. Per Endpoint di autorizzazione, inserisci l'URL completo dell'endpoint di autorizzazione.
9. Per Token endpoint, inserisci l'URL completo dell'endpoint token.
10. Per User endpoint, inserisci l'URL completo dell'endpoint utente.
11. Inserisci l'identificatore del client OAuth 2.0 per Client ID.
12. Inserisci il segreto del client OAuth 2.0 per il segreto del cliente.
13. Inserisci un elenco di ambiti delimitato da spazi definiti con il tuo provider di identità. Per Scope è richiesto almeno l'ambito «openid».

14. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
15. 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 `ApplicationDomain` di accesso verificato per questo scopo. È possibile trovarlo nella AWS Management Console 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 `ApplicationDomain`

Per creare un provider di fiducia OIDC (CLIAWS)

- 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 alla 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 (CLIAWS)

- 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 alla 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 (CLIAWS)

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

Provider fiduciari basati su dispositivi

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 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 (AWSconsole)

1. Apri alla 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 AWS Management Console 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 (AWSCLI)

- 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 (AWSconsole)

1. Apri alla 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 Modifica provider fiduciario di accesso verificato.

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

- 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 (AWSconsole)

1. Apri alla 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 in 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 (AWSCLI)

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

Gruppi di accesso verificati

Un gruppo di accesso AWS verificato è una raccolta di endpoint di accesso verificato e una politica di accesso verificato a livello di gruppo. Ogni endpoint all'interno di un gruppo condivide la politica di accesso verificato. È possibile utilizzare i gruppi per riunire endpoint con requisiti di sicurezza comuni. Questo può aiutare a semplificare l'amministrazione delle policy utilizzando un'unica policy per le esigenze di sicurezza di più applicazioni.

Ad esempio, puoi raggruppare tutte le richieste di vendita e impostare una politica di accesso a livello di gruppo. È quindi possibile utilizzare questa politica per definire una serie 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 associil gruppo a un'istanza di accesso Durante il processo di creazione di un endpoint, assocerai l'endpoint a un gruppo.

Processi

- Crea un gruppo un gruppo un gruppo di utenti
- Modifica una policy di gruppo di utenti
- Elimun gruppo un gruppo un gruppo di utenti

Crea un gruppo un gruppo un gruppo di utenti

Per creare un gruppo un gruppo un gruppo, utilizza la procedura seguente.

Per creare un gruppo un gruppo un gruppo un gruppo un gruppo,

1. Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Gruppi di accesso verificato, quindi Crea gruppo di accesso verificato.
3. (Facoltativo) In riquadro nome e Descrizione, inserun nome e una descrizione per il gruppo.
4. Per l'istanza Verified Access, seleziona un'istanza di accesso verificato da associare al gruppo.
5. (Facoltativo) Per la definizione dei criteri, inserisci un criterio 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.

Modifica una policy di gruppo di utenti

Per modificare una policy di gruppo, utilizza la procedura seguente seguente.

Per modificare una policy di gruppo di utenti, per modificare una policy di accesso

1. Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegliere Gruppi di utenti, quindi seleziona il gruppo di cui desideri modificare la policy.
3. Scegli Azioni, quindi Modifica politica del gruppo di accesso verificato.
4. (Facoltativo) Attiva o disattiva la politica in base all'obiettivo attuale.
5. (Facoltativo) In Politica, inserisci un criterio di accesso verificato da applicare al gruppo.
6. Scegli Modifica politica del gruppo Verified Access.

Elimun gruppo un gruppo un gruppo di utenti

Quando un gruppo un gruppo non è più necessario un gruppo, è più necessario, è possibile eliminarlo.

Per eliminare un gruppo un gruppo un gruppo un gruppo un gruppo,

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

Endpoint con accesso verificato

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

Indice

Tipi di endpoint Verified Access

Di seguito sono riportati i possibili tipi di endpoint:

- Load balancer: le richieste delle applicazioni vengono inviate a un load balancer per essere distribuite all'applicazione.
- Interfaccia di rete: le richieste di applicazione vengono inviate a un'interfaccia di rete utilizzando il protocollo e la porta specificati.

VPC e sottoreti condivise

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

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

Requisiti

- È supportato solo il traffico IPv4.
- Sono supportati solo i protocolli HTTP e HTTPS.
- 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.
- 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 utilizzandoAWS Certificate Manager.

Per creare un endpoint di bilanciamento del carico

1. Accedi alla 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 per l'endpoint.
6. Per i dettagli dell'applicazione, procedi come segue:

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

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

7. Per i dettagli sull'endpoint, procedi come segue:

   a. In Attachment type (Tipo collegamento), selezionare VPC.

   b. Per i gruppi di sicurezza, scegli i gruppi di sicurezza per l'endpoint. Il traffico proveniente dall'endpoint Verified Access che entra nel sistema di bilanciamento del carico verrà associato a questo gruppo di sicurezza.

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

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

   e. Per Protocollo, scegli HTTPS o HTTP.

   f. In Porta, inserisci il numero di porta.

   g. Per Load balancer ARN, scegli il load balancer.

   h. Per Subnet, scegli le sottoreti per il tuo load balancer.

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.

Crea 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 traffico IPv4.
- Sono supportati solo i protocolli HTTP e HTTPS.
- 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.
- 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 utilizzandoAWS Certificate Manager.

Per creare un endpoint di interfaccia di rete

1. Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Endpoint 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 per l'endpoint.
6. Per i dettagli dell'applicazione, procedi come segue:
   a. Per Dominio dell'applicazione, inserisci il nome DNS dell'applicazione.
   b. In Certificato di dominio ARN, scegli il certificato TLS pubblico.
7. Per i dettagli sull'endpoint, procedi come segue:
   a. In Attachment type (Tipo collegamento), selezionare VPC.
   b. Per i gruppi di sicurezza, scegli i gruppi di sicurezza per l'endpoint. Il traffico proveniente dall'endpoint Verified Access che entra nell'interfaccia di rete verrà associato a questo gruppo di sicurezza.
   c. Per il prefisso del dominio Endpoint, inserisci un identificatore personalizzato da anteporre al nome DNS generato da Verified Access per l'endpoint.
   d. Per il tipo di endpoint, scegli Interfaccia di rete.
   e. Per Protocollo, scegli HTTPS o HTTP.
   f. In Porta, inserisci il numero di porta.
   g. Per Interfaccia di rete, scegli l'interfaccia di rete.
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.

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 dal tuo 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

1. Accedi alla 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 Verified Access, trova gli ID del gruppo di sicurezza nella scheda Dettagli e copia l'ID del gruppo di sicurezza per il tuo 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.

Modifica un endpoint con accesso verificato

Dopo aver creato un endpoint con accesso verificato, puoi aggiornarne la configurazione.

Per modificare un endpoint di accesso verificato

1. Accedi alla 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.

Modifica una policy per gli endpoint di accesso verificato

Dopo aver creato un endpoint con accesso verificato, puoi modificarne la politica.

Per modificare una policy per gli endpoint di accesso verificato

1. Accedi alla 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 di cui desideri modificare la politica.
4. Scegli Azioni, Modifica la politica dell'endpoint di accesso verificato.
5. (Facoltativo) Attiva o disattiva la politica di attivazione in base all'obiettivo attuale.
6. (Facoltativo) Per Policy, inserisci una policy di accesso verificato da applicare all'endpoint.
7. Scegli Modifica la politica degli endpoint di accesso verificato.

Elimina un endpoint con accesso verificato

Quando hai finito con un endpoint con accesso verificato, puoi eliminarlo.

Per eliminare un endpoint di accesso verificato

1. Accedi alla 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.

Dati attendibili provenienti da fornitori di servizi fiduciari

I dati attendibili sono dati inviati a AWS Verified Access da un provider fiduciario. A volte 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 altro ancora. Le informazioni inviate variano in base al fornitore del trust, 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 con accesso verificato, puoi anche vedere quali dati attendibili vengono inviati dal tuo provider fiduciario. Ciò può essere molto utile quando si definiscono politiche che consentono o negano l'accesso alle applicazioni. Per informazioni sull'inclusione del contesto di fiducia nei log, consulta. Incluso il contesto di fiducia

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

Indice

Contesto predefinito di Verified Access

AWSVerified Access include alcuni elementi sulla richiesta HTTP corrente per impostazione predefinita in tutte le valutazioni Cedar indipendentemente dai provider di fiducia configurati. Quando viene valutata una policy, Verified Access include i dati sulla richiesta HTTP corrente nel contesto Cedar sotto. `context.http_request key` Se lo desideri, puoi scrivere una politica che valuti in base ai dati. Lo schema JSON seguente mostra quali dati sono inclusi nella valutazione.

```
{
     "title": "HTTP Request data included by Verified Access",
     "type": "object",
```

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

Di seguito è riportato un esempio di policy che valuta i dati della richiesta HTTP.

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

Centro identità AWS IAM

Quando viene valutata una politica, se la definisci AWS IAM Identity Center come provider di fiducia, AWS Verified Access include i dati sulla fiducia nel contesto Cedar nella chiave specificata come «Nome di riferimento della politica» nella configurazione del provider di fiducia. 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 i 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.

Fornitori di servizi fiduciari terzi

Questa sezione descrive i dati sulla fiducia forniti a AWS Verified Access da fornitori di fiducia di terze parti.

> **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". 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 politiche, i tuoi utenti devono scaricare e installare l'estensione del browser AWS Verified Access dal web store di Chrome 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 nativa ad accesso AWS verificato (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 del browser AWS Verified Access dal Web Store di Chrome 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 AWS 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 AWS Verified Access, consulta Proteggere le applicazioni private con CrowdStrike e AWS Verified Access 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 environemnt"
    },
    "exp": {
      "type": "integer",
      "description": "unixtime, The expiration time of the token"
    },
    "iat": {
      "type": "integer",
      "description": "unixtime, The issued time of the token"
    },
    "jwk_url": {
      "type": "string",
```

```
      "description": "URL that details the JWT signing"
    },
    "platform": {
      "type": "string",
      "enum": ["Windows 10", "Windows 11", "macOS"],
      "description": "Operating system of the endpoint"
    },
    "serial_number": {
      "type": "string",
      "description": "The serial number of the device derived by unique system
 information"
    },
    "sub": {
      "type": "string",
      "description": "Unique CrowdStrike Agent ID (AID) of machine"
    },
    "typ": {
      "type": "string",
      "enum": ["crowdstrike-zta+jwt"],
      "description": "Generic name for this JWT media. Client MUST reject any other
 type"
    }
  }
}
```

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_orgnaization_identifier'
};
```

L'utente dichiara il superamento e la verifica della firma

Dopo che un'istanza AWS Verified Access 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 sia le firme sia 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 attestazioni 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"
]
}
```

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 gruppi di sicurezza.

Ti consigliamo di verificare la firma prima di effettuare qualsiasi autorizzazione in base alle affermazioni. Per ottenere la chiave pubblica, ottenere la chiave ID dall'intestazione JWT e utilizzarla per cercare la chiave pubblica dall'endpoint. L'endpoint per ciascuna di esse Regione AWS è il seguente:

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

# Step 2: Get the public key from Regional endpoint
url = 'https://public-keys.prod.verified-access.' + region + '.amazonaws.com/' + kid
req = requests.get(url)
pub_key = req.text

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

Politiche di accesso verificato

AWSLe politiche di accesso verificato consentono di definire regole per l'accesso alle applicazioni ospitate inAWS. Sono scritte in Cedar, un linguaggio AWS politico. Utilizzando Cedar, è possibile creare politiche che vengono valutate in base al contesto di fiducia inviato dai provider di fiducia basati su identità o dispositivi che configuri per l'utilizzo con Verified Access.

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

Questa sezione descrive come sono strutturate le politiche di accesso verificato, cosa contengono, come definirle e fornisce alcuni esempi.

Indice

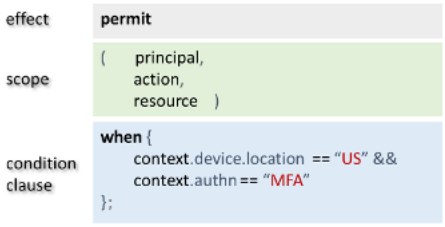
Utilizza le politiche per l'accesso verificato

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.

Per aggiungere o modificare una policy su un gruppo o endpoint di accesso verificato esistente dopo la sua creazione, consulta Modifica una policy di gruppo di utenti o. Modifica una policy per gli endpoint di accesso verificato

Struttura della dichiarazione politica

Questa sezione descrive la dichiarazione sulla politica di accesso AWS verificato e come viene valutata. È possibile avere più istruzioni in un'unica politica di accesso verificato. Il diagramma seguente mostra la struttura di una politica di accesso verificato.



La politica contiene le seguenti parti:

- Effetto: specifica se l'informativa è `permit` (`Allow`) o `forbid` (`Deny`).
- Ambito: specifica i principi, le azioni e le risorse a cui si applica l'effetto. È possibile lasciare indefinito l'ambito in Cedar evitando di identificare principi, azioni o risorse specifici (come mostrato nell'esempio precedente). In questo caso, la politica si applica a tutti i possibili principi, azioni e risorse.
- Clausola condizionale: specifica il contesto in cui si applica l'effetto.

> **Important**
>
> Per Verified Access, le politiche sono espresse completamente facendo riferimento al contesto di fiducia 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.

Semplice esempio di politica

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

Nell'esempio precedente, si noti che è possibile utilizzare più di una clausola condizionale in una dichiarazione di politica utilizzando l'&&operatore. Il linguaggio delle politiche Cedar offre il potere espressivo di creare dichiarazioni politiche personalizzate, dettagliate ed estese. Per ulteriori esempi, consulta Policy di esempio.

Valutazione delle politiche

Un documento politico è un insieme di una o più dichiarazioni politiche (o dichiarazioni). `permit` `forbid` 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 applicano politiche di autorizzazione e/o si applicano 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.

> **Note**
>
> AWSVerified Access convalida la sintassi quando si crea la policy, ma non convalida i dati inseriti nella clausola condizionale.

Operatori integrati

Quando crei il contesto di una politica di accesso AWS verificato utilizzando varie condizioni, come discusso inStruttura della dichiarazione politica, puoi 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 integrati come riferimento.

Operatore	Tipi e sovraccarichi	Description
!	Booleano → Booleano	Logico no.
==	qualsiasi → qualsiasi	Uguaglianza. Funziona su argomenti di qualsiasi tipo,

Operatore	Tipi e sovraccarichi	Description
		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	Description
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 corrispondere 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.

Commenti sulla politica

Puoi includere dichiarazioni relative ai commenti nelle tue politiche di accesso AWS verificato. I commenti sono definiti come una riga che inizia con `//` e termina con una nuova riga.

L'esempio seguente mostra le dichiarazioni di commento nella politica.

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

Cortocircuito logico delle politiche

Potresti voler scrivere una policy di accesso AWS verificato che valuti i dati che possono o meno essere presenti in un determinato contesto. Se fai 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)
    )
  )
};
```

Policy di esempio

Esempio 1: creazione di policy per IAM Identity Center

> **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.

La seguente politica di esempio consente l'accesso solo quando un utente appartiene al `finance` gruppo (che ha l'ID di gruppo di`c242c5b0-6081-1845-6fa8-6e0d9513c107`) e dispone di un indirizzo email verificato.

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

Esempio 1b: aggiunta di altre condizioni a una dichiarazione di policy per IAM Identity Center

La seguente policy di esempio consente l'accesso solo quando un utente appartiene al `finance` gruppo (che ha l'ID di gruppo di`c242c5b0-6081-1845-6fa8-6e0d9513c107`), ha un indirizzo email 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"
};
```

Esempio 2: la stessa politica per un provider OIDC di terze parti

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

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

Esempio 3: Utilizzo CrowdStrike

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

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

Esempio 4: Utilizzo di caratteri speciali

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")
};
```

Esempio 5: consentire un indirizzo IP specifico

L'esempio seguente mostra una politica che consente solo un indirizzo IP specifico.

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

Esempio 5a: blocca un indirizzo IP specifico

L'esempio seguente mostra una politica che bloccherà un indirizzo IP specifico.

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

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 politica degli endpoint, la politica di gruppo e il contesto di fiducia in un'unica schermata, in cui è possibile testare e apportare modifiche alle politiche.

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 e di 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
- Fase 2: Verificare e modificare le politiche

- Passaggio 3: rivedere e applicare le modifiche

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 dell'utente e/o un 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 alla 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. Seleziona Avanti.

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 ripetere il test delle modifiche, ripetendo il processo se necessario.

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

Passaggio 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.

Sicurezza nell'accesso AWS verificato

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, puoi trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle aziende più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra AWS e l'utente. Il modello di responsabilità condivisa fa riferimento ad una sicurezza del cloud e nel cloud:

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

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 AWS Verified Access

Il modello di responsabilità AWS condivisa modello si applica alla protezione dei dati in AWS Verified Access. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che esegue tutto l'Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su

questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS.

Per garantire la protezione dei dati, ti suggeriamo di proteggere le credenziali Account AWS e di configurare singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con le risorse AWS. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza predefiniti in 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 necessiti di moduli crittografici convalidati FIPS 140-2 quando accedi ad AWSattraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente 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 AWS gli SDK. AWS CLI 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 fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia 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.

Riservatezza del traffico Internet

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 accesso verificato AWS

AWSPer 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

Chiavi di proprietà di AWS

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 Chiavi gestite dal cliente (CMK) 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 Serviceprezzi.

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	AWScrittografia a chiave proprietaria	Crittografia con chiavi gestite dal cliente (opzionale)
`Trust provider (user-type)` I provider fiduciari di tipo utente contengono opzioni OIDC come AuthorizationEndpoint, UserInfoEndpoint ClientId, e così via ClientSecret, che sono considerate informazioni personali.	Abilitato	Abilitato
`Trust provider (device-type)` I provider fiduciari di tipo dispositivo contengono un, che è considerato PII. TenantId	Abilitato	Abilitato
`Group policy` Fornito durante la creazione o la modifica del gruppo Verified Access. Contiene le regole per l'autorizzazione delle richieste di accesso. Potrebbe contenere informazioni personali come nome utente e indirizzo e-mail e così via.	Abilitato	Abilitato
`Endpoint policy`	Abilitato	Abilitato

Tipo di dati	AWScrittografia a chiave proprietaria	Crittografia con chiavi gestite dal cliente (opzionale)
Fornito durante la creazione o la modifica dell'endpoint Verified Access. Contiene le 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 aAWS 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 la AWS Management Console o le API AWS KMS. Segui la procedura riportata in Creazione di una chiave simmetrica gestita dal cliente nella Guida per gli sviluppatori di AWS Key Management Service.

Politiche chiave

Le policy chiave controllano l'accesso alla chiave gestita dal cliente. Ogni chiave gestita dal cliente deve avere esattamente una policy delle chiavi, che contiene istruzioni che determinano chi può usare la chiave e come la possono usare. Quando crei la chiave gestita dal cliente, puoi specificare una policy chiave. Per ulteriori informazioni, consulta Gestione dell'accesso alle chiavi gestite dal cliente nella Guida per gli sviluppatori di AWS Key Management Service.

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 sull'utilizzo di Grants, consulta la AWS Key Management Service Guida per gli sviluppatori.

  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.
  - Imposta un preside in pensione per consentire al servizio di farlo`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 su come specificare le autorizzazioni in una policy, consulta la Guida per gli sviluppatori di AWS Key Management Service.

Per informazioni sulla Risoluzione dei problemi delle chiavi di accesso consulta la Guida per gli sviluppatori di AWS Key Management Service.

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 ilAWS Management Console, 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 ilAWS 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 AWS Management Console oAWS CLI, per applicare una nuova chiave gestita dal cliente e reimpostare i valori di configurazione.

AWSContesto di crittografia Verified Access

Un contesto di crittografia è un set opzionale di coppie chiave-valore che contiene ulteriori informazioni contestuali sui dati. AWS KMS utilizza il contesto di crittografia come dati autenticati aggiuntivi per supportare crittografia autenticata. Quando includi un contesto di crittografia in una

richiesta di crittografia dei dati, AWS KMS lega il contesto di crittografia ai dati crittografati. Per decrittografare i dati, nella richiesta deve essere incluso lo stesso contesto di crittografia.

AWSContesto 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"
}
```

Per ulteriori informazioni sull'utilizzo del contesto di crittografia per le concessioni o nelle politiche, consulta il contesto di crittografia nella Guida per gli AWS Key Management Servicesviluppatori.

Monitoraggio delle chiavi di crittografia per l'accesso AWS 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 AWS Verified Access

AWS Identity and Access Management (IAM) è un Servizio AWSche consente agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Verified Access. IAM è un Servizio AWS il cui uso non comporta costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Come funziona AWS Verified Access con IAM
- Esempi di policy basate sull'identità per Verified Access AWS
- Risoluzione dei problemi relativi all'identità e all'accesso AWS Verified Access
- Usa ruoli collegati ai servizi per l'accesso verificato

- AWSpolitiche gestite per l'accesso AWS verificato

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Verified Access.

Utente del servizio: se utilizzi il servizio Verified Access per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di accesso verificato per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Accesso verificato, consultaRisoluzione dei problemi relativi all'identità e all'accesso AWS Verified Access.

Amministratore del servizio: se sei responsabile delle risorse di accesso verificato presso la tua azienda, probabilmente hai pieno accesso a Verified Access. È tuo compito determinare a quali funzionalità e risorse di accesso verificato devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con Verified Access, consultaCome funziona AWS Verified Access con IAM.

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere politiche per gestire l'accesso a Verified Access. Per visualizzare esempi di policy basate sull'identità di Verified Access che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità per Verified Access AWS

Autenticazione con identità

L'autenticazione è la procedura di accesso ad AWScon le credenziali di identità. Devi essere autenticato (connesso a AWS) come utente root Utente root dell'account AWS, come utente IAM o assumere un ruolo IAM.

Puoi accedere ad AWScome identità federata utilizzando le credenziali fornite attraverso un'origine di identità. AWS IAM Identity Center Gli esempi di identità federate comprendono gli utenti del centro identità IAM, l'autenticazione Single Sign-On (SSO) dell'azienda e le credenziali di Google o Facebook. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Se accedi ad AWStramite la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere alla AWS Management Consoleo al portale di accesso AWS. Per ulteriori informazioni sull'accesso ad AWS, consulta la sezione Come accedere al tuo Account AWSnella Guida per l'utente di Accedi ad AWS.

Se accedi ad AWS in modo programmatico, AWS fornisce un Software Development Kit (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le richieste utilizzando le tue credenziali. Se non utilizzi gli strumenti AWS, devi firmare le richieste personalmente. Per ulteriori informazioni sulla firma delle richieste, consulta Firma delle richieste AWS nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. AWS consiglia ad esempio di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza dell'account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Utente root di un Account AWS

Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWSe le risorse nell'account. Tale identità è detta utente root Account AWSed è possibile accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conservare le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Identità federata

Come best practice, richiedere agli utenti umani, compresi quelli che richiedono l'accesso di amministratore, di utilizzare la federazione con un provider di identità per accedere a Servizi AWSutilizzando credenziali temporanee.

Un'identità federata è un utente della directory degli utenti aziendali, un provider di identità Web, AWS Directory Service, la directory Identity Center o qualsiasi utente che accede a Servizi AWS utilizzando le credenziali fornite tramite un'origine di identità. Quando le identità federate accedono a Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. È possibile creare utenti e gruppi in IAM Identity Center oppure connettersi e sincronizzarsi con un

gruppo di utenti e gruppi nell'origine di identità per utilizzarli in tutte le applicazioni e gli Account AWS. Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center.

Utenti e gruppi IAM

Un utente IAM è una identità all'interno del tuo Account AWSche dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità all'interno di Account AWSche dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un ruolo IAM nella AWS Management Consolemediante lo scambio di ruoli. È possibile assumere un ruolo chiamando un'operazione AWS CLIo API AWSoppure utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene

autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center.

- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, per alcuni dei Servizi AWS, è possibile collegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso multi-servizio: alcuni Servizi AWS utilizzano funzionalità in altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Inoltro delle sessioni di accesso (FAS): quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, tale utente o ruolo viene considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altri Servizi AWS o risorse per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
  - Ruolo collegato al servizio: 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 ai servizi sono visualizzati nell'account Account AWSe sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste di AWS CLIo dell'API AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWSa un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo dell'istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Per controllare l'accesso a AWS è possibile creare policy e collegarle a identità o risorse AWS. Una policy è un oggetto in AWSche, quando associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWSvaluta queste policy quando un principale IAM (utente, utente root o sessione ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene archiviata in AWSsotto forma di documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWSJSON per specificare l'accesso ai diversi elementi. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dalla AWS Management Console, la AWS CLIo l'API AWS.

Policy basate su identità

Le policy basate su 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 Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le policy gestite sono policy autonome che possono essere collegate a più utenti, gruppi e ruoli in Account AWS. Le policy gestite includono le policy gestite da AWSe le policy gestite dal cliente. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

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

Liste di controllo degli accessi (ACL)

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

Amazon S3, AWS WAFe Amazon VPC sono esempi di servizi che supportano le ACL. Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta altri tipi di policy meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Policy di controllo dei servizi (SCP): le SCP sono policy JSON che specificano il numero massimo di autorizzazioni per un'organizzazione o unità organizzativa (OU) in AWS Organizations. AWS Organizationsè un servizio per il raggruppamento e la gestione centralizzata degli Account AWSmultipli di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. La SCP limita le autorizzazioni per le entità negli account membri, compreso ogni Utente root dell'account AWS. Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella Guida per l'utente di IAM.

Come funziona AWS 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 che puoi utilizzare con AWS Verified Access

Funzionalità IAM	Supporto Verified Access
Policy basate su identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
Liste di controllo degli accessi	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 AWSi servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per l'accesso verificato

Supporta le policy basate su identità	Sì

Le policy basate su 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 Creazione di policy IAM nella Guida per l'utente di IAM.

Con le policy basate su 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. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. 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 di 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 AWS

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 allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando l'entità principale e la risorsa si trovano in diversi Account AWS, un amministratore IAM nell'account attendibile deve concedere all'entità principale (utente o ruolo) anche l'autorizzazione per accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non

sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Azioni politiche per l'accesso verificato

Supporta le operazioni di policy	Sì

Gli amministratori possono utilizzare le policy JSON AWSper specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni 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 a un criterio. Le operazioni di policy hanno spesso lo stesso nome dell'operazione API AWS. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi 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 AWS

Risorse politiche per l'accesso verificato

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy JSON AWSper specificare gli accessi ai diversi elementi. Cioè, quale 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. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, 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 dei relativi ARN, 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 accesso verificato, consulta. Esempi di policy basate sull'identità per Verified Access AWS

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 JSON AWSper specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi 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.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se specifichi più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione `OR` logica. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche per il servizio. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente di IAM.

Per visualizzare un elenco di chiavi di condizione 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 AWS

ACL in Verified Access

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con accesso verificato

Supporta ABAC (tag nelle policy)	Parziale

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, tali attributi sono denominati tag. È possibile collegare dei tag alle entità IAM (utenti o ruoli) e a numerose risorse AWS. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci 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 Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è 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 accesso verificato

Supporta le credenziali temporanee	Sì

Alcuni Servizi AWSnon funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, inclusi i Servizi AWS che funzionano con le credenziali temporanee, consulta Servizi AWS supportati da IAM nella Guida per l'utente IAM.

Le credenziali temporanee sono utilizzate se si accede alla AWS Management Consoleutilizzando qualsiasi metodo che non sia la combinazione di nome utente e password. Ad esempio, quando accedi ad AWS utilizzando il collegamento Single Sign-On (SSO) della tua azienda, tale processo crea in automatico credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando la AWS CLIo l'API AWS. È quindi possibile utilizzare tali credenziali temporanee per accedere ad AWS. AWSconsiglia di generare le

credenziali temporanee dinamicamente anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni principali multiservizio per Verified Access

Supporta sessioni di accesso diretto (FAS)	Sì

Quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, si viene considerati un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altri Servizi AWS o risorse per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina 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 la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

Ruoli collegati ai servizi per Verified Access

Supporta i ruoli collegati ai servizi	Sì

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

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

Esempi di policy basate sull'identità per Verified Access AWS

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse di accesso verificato. Inoltre, non sono in grado di eseguire attività utilizzando la AWS Management Console, l'AWS Command Line Interface (AWS CLI) o l'API AWS. Per concedere agli utenti l'autorizzazione per eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

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

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

Argomenti

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 operazioni possono comportare costi aggiuntivi per l'Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Nozioni di base sulle policy gestite da AWSe passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite da AWSche concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente di AWSspecifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.

- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori 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 a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi inoltre utilizzare le condizioni per concedere l'accesso alle operazioni di servizio, ma solo se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel tuo Account AWS, attiva MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto 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.

```
{
      "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 allegate alla relativa identità utente. La policy include le autorizzazioni per completare questa azione sulla console o a livello di programmazione utilizzando la AWS CLIo l'API 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 AWS 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
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse di accesso verificato

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`*.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. 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 AWSconsentono di trasmettere un ruolo esistente a tale servizio, invece di creare un nuovo ruolo di servizio o un ruolo collegato ai servizi. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio 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 passare 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`.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. 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 servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Verified Access supporta queste funzionalità, consultaCome funziona AWS Verified Access con IAM.
- Per informazioni su come garantire l'accesso alle risorse negli Account AWSche possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS in tuo possesso nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso alle risorse ad Account AWS di terze parti, consulta Fornire l'accesso agli 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 di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Usa ruoli collegati ai servizi per l'accesso verificato

AWSVerified Access utilizza AWS Identity and Access Management ruoli collegati ai servizi (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a Verified Access. I ruoli collegati al servizio sono predefiniti da Verified Access e includono tutte le autorizzazioni richieste dal servizio per chiamare altri Servizi AWS utenti per tuo conto.

Un ruolo collegato ai servizi semplifica la configurazione dell'accesso verificato perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Verified Access definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo Verified Access

può assumerne i ruoli. Le autorizzazioni definite includono la politica di fiducia e la politica delle autorizzazioni e questa politica di autorizzazioni non può essere associata a nessun'altra entità IAM.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta Servizi AWS che funzionano con IAM e cerca i servizi che riportano Yes (Sì) nella colonna Service-linked roles (Ruoli collegati ai servizi). Scegli Yes (Sì) in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate al servizio per l'accesso verificato

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

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi AWSServiceRoleForVPCVerifiedAccess considera attendibili i seguenti servizi:

- `verified-access.amazonaws.com`

La politica sulle autorizzazioni 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`

Puoi anche visualizzare le autorizzazioni per questa politica nella AWS Management Console AWSVPCVerifiedAccessServiceRolePolicy, oppure puoi visualizzare la AWSVPCVerifiedAccessServiceRolePolicypolitica nella AWSManaged Policy Reference Guide.

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 laAWS Management Console, la o l'AWSAPIAWS CLI, Verified Access crea automaticamente il ruolo collegato al servizio.

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando chiami CreateVerifiedAccessEndpointnuovamente, 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 AWSServiceRoleForVPCVerifiedAccesscollegato al servizio. Dopo aver creato un ruolo collegato ai servizi, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminare un ruolo collegato al servizio per Verified Access

Non è necessario eliminare manualmente il ruolo AWSServiceRoleForVPCVerifiedAccess. Quando DeleteVerifiedAccessEndpointrichiami laAWS Management Console, la o l'AWSAPIAWS CLI, Verified Access ripulisce le risorse ed elimina automaticamente il ruolo collegato al servizio.

Per eliminare manualmente il ruolo collegato ai servizi utilizzando IAM

Utilizza la console IAM, la AWS CLI o l'API AWS per eliminare il ruolo collegato ai servizi AWSServiceRoleForVPCVerifiedAccess. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per ruoli collegati al servizio Verified Access

Verified Access supporta l'utilizzo di ruoli collegati al servizio in tutte le aree in Regioni AWS cui il servizio è disponibile. Per ulteriori informazioni, consulta AWSRegioni ed endpoint.

AWSpolitiche gestite per l'accesso AWS verificato

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

Ricorda che le policy gestite da AWSpotrebbero non concedere autorizzazioni con privilegi minimi per i tuoi casi d'uso specifici perché possono essere utilizzate da tutti i clienti AWS. Consigliamo pertanto

di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle policy gestite da AWS. Se AWSaggiorna le autorizzazioni definite in una policy gestita da AWS, l'aggiornamento riguarda tutte le identità principali (utenti, gruppi e ruoli) a cui è collegata la policy. È molto probabile che AWSaggiorni una policy gestita da AWSquando viene lanciato un nuovo Servizio AWSo nuove operazioni API diventano disponibili per i servizi esistenti.

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

AWSPolicy gestita: AWSVPCVerifiedAccessServiceRolePolicy

Questa politica è associata a un ruolo collegato al servizio che consente a Verified Access di eseguire azioni per tuo conto. Per ulteriori informazioni, consulta Utilizzo dei ruoli collegati ai servizi. Per visualizzare le autorizzazioni per questa politica, puoi consultare la oppure puoi visualizzare la AWS Management Console politica AWSVPCVerifiedAccessServiceRolePolicynella AWSManaged 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	Description	Data
AWSVPCVerifiedAccessServiceRolePolicy- Politica aggiornata	Verified Access ha aggiornato la sua politica di gestione per includere le descrizioni di tutte le azioni nel campo «sid».	17 novembre 2023
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

Modifica	Description	Data
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 AWS 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. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

> **Note**
>
> Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza nell'accesso AWS verificato

L'infrastruttura globale dei servizi AWS è progettata attorno a regioni Regioni AWS e zone di disponibilità. Le regioni di Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e a velocità effettiva elevata. Con le Zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico 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.

Per ulteriori informazioni sulle Regioni AWS e le zone di disponibilità, consulta Infrastruttura globale di AWS.

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

Sottoreti multiple per un'elevata disponibilità

Quando si crea un endpoint di tipo Verified Access di tipo load balancer, è possibile 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 degli accessi AWS verificati

Il monitoraggio è importante per garantire l'affidabilità, la disponibilità e le prestazioni di AWS Verified Access. AWSfornisce i seguenti strumenti di monitoraggio per controllare l'accesso verificato, segnalare un problema e intervenire automaticamente quando necessario:

- Registri di accesso: acquisisci 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 del tuo Account AWS e fornisce i file di log a un bucket Amazon S3 specificato. Puoi identificare quali utenti e account hanno richiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute. Per ulteriori informazioni, consulta the section called “Log CloudTrail”.

Log di accesso verificati

Dopo che AWS Verified Access ha valutato ogni richiesta di accesso, registra tutti i tentativi di accesso. Ciò fornisce 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 abiliti la registrazione, dovrai configurare una destinazione per l'invio dei log. Il principale IAM utilizzato per configurare la destinazione di registrazione dovrà 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 Verified Access supporta le seguenti destinazioni per la pubblicazione dei log di accesso:

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

Indice

- Incluso il contesto di fiducia
- Esempi di voci di registro per i registri di accesso verificato

Versioni di registrazione

Per impostazione predefinita, il sistema di registrazione Verified Access utilizza Open Cybersecurity Schema Framework (OCSF) versione 0.1. Nella sezione sono disponibili esempi di log che utilizzano la versione 0.1. Esempi della versione 0.1 di OCSF

L'ultima versione di registrazione è compatibile con la versione OCSF 1.0.0-rc.2. Dettagli specifici sullo schema sono disponibili qui Schema OCSF. I log di esempio che utilizzano la versione 1.0.0-rc.2 possono essere visualizzati nella sezione. Esempi della versione OCSF 1.0.0-rc.2

Aggiorna la versione di registrazione

Se desideri aggiornare la versione di registrazione utilizzata, segui la procedura riportata di seguito.

Per aggiornare la versione di registrazione utilizzando la console

1. Apri alla 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

Il principale IAM utilizzato per configurare la destinazione di registrazione dovrà disporre di determinate autorizzazioni affinché la registrazione funzioni correttamente. Di seguito puoi vedere le autorizzazioni richieste per ogni destinazione di registrazione.

Per la consegna a Logs CloudWatch :

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration`sull'istanza Verified Access
- `logs:CreateLogDelivery`,`logs:DeleteLogDelivery`, `logs:GetLogDeliverylogs:ListLogDeliveries`, e `logs:UpdateLogDelivery` su tutte le risorse
- `logs:DescribeLogGroups`e 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:GetBucketPolicy`e `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 log

Quando abiliti la registrazione, dovrai configurare una destinazione per l'invio dei log. Il principale IAM utilizzato per configurare la destinazione di registrazione dovrà 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

Indice

- Disabilitazione dei log di accesso

Abilitare log di accesso

1. Apri alla 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 di queste 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 alla 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.

Incluso il contesto di fiducia

Il contesto di fiducia inviato dal provider di fiducia può essere facoltativamente incluso nei registri di accesso verificato. Questo può essere molto utile quando si definiscono politiche che consentono o negano l'accesso alle applicazioni. Una volta abilitato, il contesto di fiducia verrà trovato nel registro sotto il `data` campo. Se disabilitato, il `data` campo verrà impostato su`null`. Per configurare l'accesso verificato in modo da includere il contesto di fiducia nei log, segui la procedura seguente.

> **Note**
>
> L'inclusione del contesto di attendibilità nei log 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, consulta Abilitare log di accesso la procedura completa.

Indice

Abilita il contesto di fiducia

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

1. Apri alla 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 desideri più includere il contesto di fiducia nei log, puoi rimuoverlo con la procedura seguente.

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

1. Apri alla 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 voci di registro per i registri di accesso verificato

Di seguito sono riportati alcuni esempi di voci di registro.

Indice

Esempi della versione 0.1 di OCSF

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

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 della versione OCSF 1.0.0-rc.2

Indice

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"
            },
            "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
}
```

Registra le chiamate API di accesso AWS verificato utilizzando AWS CloudTrail

AWSVerified Access è integrato conAWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o un utente Servizio AWS in Access. CloudTrailacquisisce tutte le chiamate API per l'accesso verificato come eventi. Le chiamate acquisite includono chiamate dalla console Verified Access e chiamate di codice alle operazioni delle API Verified Access. Se viene creato un trail, è possibile abilitare la distribuzione continua di CloudTrail eventi in un bucket Amazon S3, inclusi gli eventi per l'accesso verificato. Se non configuri un trail, è comunque possibile visualizzare gli eventi più recenti nella console di CloudTrail in Event history (Cronologia eventi). Le informazioni raccolte da permettono CloudTrail di determinare la richiesta effettuata ad Access verificato, l'indirizzo IP da cui è partita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

Per ulteriori informazioni su CloudTrail, consulta la Guida per l'utente di AWS CloudTrail.

Informazioni di accesso verificate in CloudTrail

CloudTrail è abilitato sull'Account AWS al momento della sua creazione. Quando si verifica un'attività in Accesso verificato, questa viene registrata in un CloudTrail evento insieme ad altri Servizio AWS eventi nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nell'Account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia eventi di CloudTrail.

Per una registrazione continua degli eventi nell'account Account AWS che includa eventi per l'accesso verificato, crea un trail. Un trail consente di CloudTrail distribuire i file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri Servizi AWS per analizzare con maggiore dettaglio e usare i dati raccolti nei log CloudTrail. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- Servizi e integrazioni CloudTrail supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di log CloudTrail da più regioni e Ricezione di file di log CloudTrail da più account

Tutte le operazioni di log vengono registrate da CloudTrail e sono documentate nella Documentazione di riferimento delle API Amazon EC2. Ad esempio, le chiamate alle operazioni `CreateVerifiedAccessInstance`, `DeleteVerifiedAccessInstance` e `ModifyVerifiedAccessInstance` generano voci nei file di log CloudTrail.

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 AWS Identity and Access Management (utente 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.

Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail.

Comprendere le voci dei file di log

Un percorso è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato. I file di log di CloudTrail contengono una o più voci di log. Un evento rappresenta una singola richiesta da un'origine. Include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. I file di log di CloudTrail non sono una traccia stack ordinata delle chiamate pubbliche dell'API, quindi non vengono visualizzati in un ordine specifico.

Nell'esempio seguente viene mostrata una voce di log di CloudTrail per l'operazione `CreateVerifiedAccessInstance`.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIKK4OOINJWEXAMPLE:jdoe",
        "arn": "arn:aws:iam::123456789012:user/jdoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "jdoe"
    },
    "eventTime": "2022-11-18T20:44:04Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateVerifiedAccessInstance",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "CreateVerifiedAccessInstanceRequest": {
            "Description": "",
            "ClientToken": "85893b1e-49f6-4d24-97de-280c664edf1b"
        }
    },
    "responseElements": {
        "CreateVerifiedAccessInstanceResponse": {
            "verifiedAccessInstance": {
                "creationTime": "2022-11-18T20:44:04",
                "description": "",
                "verifiedAccessInstanceId": "vai-0d79d91875542c549",
                "verifiedAccessTrustProviderSet": ""
            },
            "requestId": "2eae195d-6bfd-46d7-b46e-a68cb791de09"
        }
    },
    "requestID": "2eae195d-6bfd-46d7-b46e-a68cb791de09",
    "eventID": "297d6529-1144-40f6-abf8-3a76f18d88f0",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
```

```
}
```

Quote per l'accesso AWS verificato

Hai Account AWS delle quote predefinite, precedentemente denominate limiti, per ciascuna di esse. Servizio AWS Salvo dove diversamente specificato, ogni quota si applica a una regione specifica.

Account AWSquote a livello 2

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

Nome	Default	Adattabile	Descrizione
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 riportati i limiti di dimensione per le intestazioni HTTP.

Nome	Default	Adattabile
Riga di richiesta	16 K	No
Intestazione singola	16 K	No
Intestazione di risposta completa	32 K	No
Intestazione completa della richiesta	64 K	No

Dimensione della richiesta OIDC

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

Nome	Default	Adattabile
Dimensione della dichiarazione OIDC	11 KG	No

Cronologia dei documenti per la Verified Access User Guide

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

Modifica	Descrizione	Data
AWSpolitica gestita aggiornata	Aggiornamento apportato alla policy IAM AWS gestita per l'accesso verificato.	17 novembre 2023
Crittografia dei dati a riposo	AWSPer 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
AWSpolitica 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 WAFl'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.