Guida per l'utente

AWS Accesso verificato

AWS Accesso verificato: Guida per l'utente

Table of Contents

Che cos'è Accesso verificato da AWS?

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

Vantaggi dell'accesso verificato

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

Accesso a Verified Access

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

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

- AWS SDKs— Fornisci informazioni specifiche per la linguaAPIs. AWS SDKsSi occupano di molti dettagli di connessione, come il calcolo delle firme e la gestione dei tentativi di richiesta e degli errori. Per ulteriori informazioni, vedere. AWS SDKs
- Interrogazione API: fornisce API azioni di basso livello richiamabili utilizzando HTTPS le richieste. L'utilizzo della Query API è il modo più diretto per accedere all'accesso verificato. Tuttavia, richiede che l'applicazione gestisca dettagli di basso livello, come la generazione dell'hash per firmare la richiesta e la gestione degli errori. Per ulteriori informazioni, consulta le azioni di accesso verificato in Amazon EC2 API Reference.

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

Prezzi

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

Come funziona l'accesso verificato

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

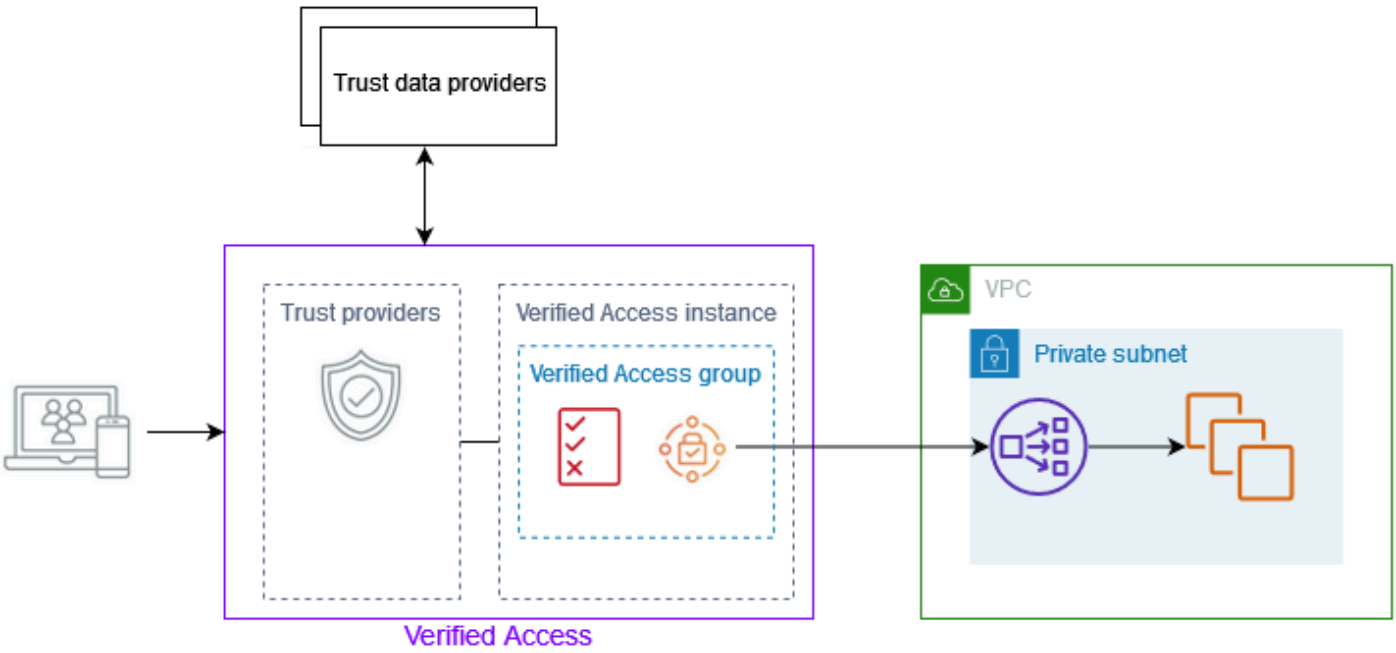
- Dati attendibili inviati dal fornitore fiduciario prescelto (da AWS o da una terza parte).
- Politiche di accesso che crei in Accesso verificato.

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

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

Componenti chiave di Verified Access

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



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

questi dati rispetto alle politiche di accesso dell'utente quando riceve ogni richiesta di accesso a un'applicazione.

Tutorial: Inizia a usare Verified Access

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

Come parte di questo tutorial, aggiungerai un'applicazione a Verified Access. Alla fine del tutorial, utenti specifici potranno accedere a quell'applicazione su Internet, senza utilizzarlaVPN.

> **Note**
>
> Questo tutorial non dimostra l'integrazione con il tuo provider di fiducia basato su dispositivi. Lavoriamo invece solo con un provider fiduciario basato sull'identità.

Attività

Prerequisiti del tutorial Verified Access

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

- La disponibilità di due Account AWS. Un account ospita l'applicazione di destinazione e le risorse di accesso verificato vengono create nell'altro account.
- AWS IAM Identity Center abilitato in Regione AWS in cui lavori. Puoi quindi utilizzare IAM Identity Center come fornitore di fiducia con accesso verificato. Per ulteriori informazioni, consulta Abilita IAM Identity Center nella AWS IAM Identity Center Guida per l'utente.
- Un dominio ospitato pubblicamente e le autorizzazioni necessarie per aggiornare DNS i record del dominio.
- Un'applicazione in esecuzione con 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`.
- Un TLS certificato autofirmato o pubblico. Usa un RSA certificato con una lunghezza di chiave di 1.024 o 2.048.
- Una IAM politica che dispone di tutte le autorizzazioni necessarie per creare un Accesso verificato da AWS istanza annotata qui. Politica per la creazione di istanze di accesso verificato

Passaggio 1: creare 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 la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di VPC navigazione di Amazon, 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. 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 provider fiduciario di accesso verificato

Puoi configurare AWS IAM Identity Center come tuo fornitore di fiducia.

Per creare un provider fiduciario di IAM Identity Center

1. Nel riquadro di VPC navigazione di Amazon, scegli Provider fiduciari di accesso verificato, quindi Crea provider fiduciario di accesso verificato.
2. (Facoltativo) In Tag 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 di policy per il nome di riferimento della politica. Ad esempio, puoi inserire**`idc`**.
4. In Tipo di provider fiduciario, seleziona User trust provider.
5. In Tipo di provider affidabile per utenti, seleziona IAMIdentity 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 di accesso verificato

Ora che hai configurato un provider fiduciario, puoi collegarlo all'istanza di accesso verificato che hai creato in precedenza. Utilizza la procedura seguente per collegare il trust provider alla tua istanza di accesso verificato.

Per collegare un provider fiduciario alla tua istanza

1. Nel riquadro di VPC navigazione di Amazon, scegli Istanze di accesso verificato.
2. Selezionare l'istanza.
3. Scegli Azioni, collega il provider fiduciario Verified Access.
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

In questo passaggio, crei un gruppo che utilizzerai come endpoint nel Passaggio 5.

Per creare un gruppo con accesso verificato

1. Nel riquadro di VPC navigazione di Amazon, scegli Gruppi di accesso verificato, quindi Crea gruppo di accesso verificato.
2. (Facoltativo) In 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, condividi il gruppo che hai appena creato con Account AWS in cui è in esecuzione l'applicazione di destinazione. Per condividere un gruppo ad accesso verificato, è necessario aggiungerlo a una condivisione di risorse. Se non disponi di una condivisione di risorse, devi prima crearne una.

Se fai parte di un'organizzazione in AWS Organizations e la condivisione all'interno dell'organizzazione è abilitata, ai consumatori dell'organizzazione viene automaticamente concesso l'accesso al gruppo condiviso con accesso verificato. 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 Creare una condivisione di risorse nella AWS RAM Guida per l'utente. Per Seleziona il tipo di risorsa, scegli il gruppo di accesso verificato, quindi seleziona la casella di controllo relativa al gruppo con accesso verificato.

Per ulteriori informazioni, consulta Guida introduttiva in AWS RAM Guida per l'utente.

Passaggio 6: aggiungi l'applicazione creando un endpoint di accesso verificato

Utilizza le seguenti procedure per creare un endpoint con accesso verificato. 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 riquadro di VPC navigazione di Amazon, 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 DNS nome per l'applicazione.
    b. In Certificato di dominio ARN, seleziona l'Amazon Resource Name (ARN) del tuo TLS certificato pubblico.
5. Per informazioni dettagliate sull'endpoint, procedi come segue:
    a. Per Tipo di allegato, scegli 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 DNS nome 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 HTTPSo. 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 Sottoreti, seleziona le sottoreti associate al tuo sistema di bilanciamento del carico.
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: configura DNS le impostazioni per l'endpoint di accesso verificato

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

Per ottenere il nome di dominio del tuo endpoint

1. Nel riquadro di VPC navigazione di Amazon, scegli Endpoints di accesso verificato.
2. Seleziona l'endpoint che hai creato in precedenza.
3. Scegli la scheda Dettagli per l'endpoint.
4. In Dominio endpoint, copia il 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 CNAME record con il tuo DNS provider:

Nome record	Tipo	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 della connettività all'applicazione che hai aggiunto a Verified Access

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.

Passaggio 9: Configurazione di una politica di accesso a livello di gruppo con accesso verificato

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

Per modificare un gruppo di accesso verificato

1. Nel riquadro di VPC navigazione di Amazon, 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: Verifica nuovamente la connettività all'applicazione che hai aggiunto a Verified Access

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.

Pulisci le risorse di accesso verificato che hai creato

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 riquadro di VPC navigazione di Amazon, scegli Endpoints di accesso verificato. 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 riquadro di VPC navigazione di Amazon, 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 riquadro di VPC navigazione di Amazon, scegli fornitori di fiducia ad accesso verificato. Seleziona il fornitore di fiducia che hai creato per questo tutorial. Scegli Azioni, Elimina il provider fiduciario di accesso verificato.
5. Nel riquadro di VPC navigazione di Amazon, 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' Accesso verificato da AWS istanza è una AWS risorsa che ti aiuta a organizzare i tuoi fornitori di fiducia e i gruppi di accesso verificato. Un'istanza valuta le richieste delle applicazioni e concede l'accesso solo quando i requisiti di sicurezza sono soddisfatti.

Argomenti

Crea e gestisci un'istanza di accesso verificato

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

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. Apri la VPC console Amazon 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 federali per il processo informativo (FIPS) se desideri che Verified Access sia FIPS conforme.
5. (Facoltativo) Per Trust provider, scegli un provider fiduciario da collegare all'istanza di 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 di accesso verificato

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

Per collegare un provider fiduciario a un'istanza di accesso verificato

1. Apri la VPC console Amazon 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 di accesso verificato

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

Per scollegare un provider fiduciario da un'istanza di accesso verificato

1. Apri la VPC console Amazon 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. Apri la VPC console Amazon 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).

Integra Verified Access con AWS WAF

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

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 Web ACL è una AWS WAF risorsa che ti offre un controllo dettagliato su tutte le HTTP (S) richieste web 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**
>
> È inoltre possibile utilizzare la AWS WAF console o API eseguire questa integrazione. Avrai bisogno dell'Amazon Resource Name (ARN) della tua istanza Verified Access. Puoi

costruirlo ARN utilizzando il seguente formato:`arn:${Partition}:ec2:${Region}:${Account}:verified-access-instance/${VerifiedAccessInstanceId}`.

Argomenti

IAMautorizzazioni necessarie per integrare Verified Access con 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]` Vedi Azioni, risorse e chiavi di condizione per Amazon EC2 nel Service Authorization Reference.

Per lavorare con un WebACL, il AWS Identity and Access Management responsabile deve disporre delle seguenti autorizzazioni.

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

Associa un sito web AWS WAF ACL

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 AWS WAF sito Web esistente ACL per completare la procedura riportata di seguito. Per ulteriori informazioni sul Web, ACLs consulta gli elenchi di controllo degli accessi Web nella Guida per gli AWS WAF sviluppatori.

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

1. Apri la VPC console Amazon 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 Web esistenteACL, quindi scegli Associa Web ACL.

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

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

1. Apri la VPC console Amazon 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 WAF dell'integrazione. Lo stato verrà visualizzato come Associato o Non associato, insieme all'ACLidentificatore web, se si trova nello stato Associato.

Dissocia un Web AWS WAF ACL

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 AWS WAF Web ACL da un'istanza di accesso verificato

1. Apri la VPC console Amazon 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 Disassociate Web. ACL

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

FIPSconformità per Verified Access

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

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

Questa pagina mostra come configurare un ambiente di accesso verificato nuovo o esistente per renderlo FIPS conforme.

Argomenti

- Configura un ambiente di accesso verificato esistente per la conformità FIPS
- Configura un nuovo ambiente di accesso verificato per la conformità FIPS

Configura un ambiente di accesso verificato esistente per la conformità FIPS

Se disponi di un ambiente di accesso verificato esistente e desideri configurarlo per renderlo FIPS conforme, 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 FIPS conforme, 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 Federal Information Process Standards (FIPS) durante la creazione. Inoltre, durante la creazione, allega 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 FIPS conforme, 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 Federal Information Process Standards (FIPS) durante il processo. Inoltre, durante la creazione, collega il provider fiduciario Verified Access che hai creato nel passaggio precedente, selezionandolo dall'elenco a discesa.
3. Crea un gruppo di accesso verificato. Durante la creazione del gruppo, lo associ all'istanza di accesso verificato appena creata.
4. Creane uno o piùEndpoint con accesso verificato. Durante la creazione dei tuoi endpoint, li associ al gruppo creato nel passaggio precedente.

Fornitori di fiducia per l'accesso verificato

Un provider fiduciario è un servizio che invia informazioni su utenti e dispositivi a Accesso verificato da AWS. Queste informazioni sono 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

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

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

Indice

Utilizzo di IAM Identity Center come fornitore di fiducia

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

Prerequisiti e considerazioni

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

- L'istanza di IAM Identity Center deve essere abilitata nella stessa AWS regione in cui desideri creare il provider fiduciario Verified Access.

Per informazioni dettagliate sui diversi tipi di istanze, consulta Gestire le istanze dell'organizzazione e dell'account di IAM Identity Center nella Guida per l'AWS IAM Identity Center utente.

Crea un provider fiduciario di 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 fiduciario di IAM Identity Center (AWS console)

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Provider fiduciari ad 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 Tipo di provider affidabile per utenti, seleziona IAMIdentity 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 fiduciario di IAM Identity Center (AWS CLI)

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

Eliminare un provider fiduciario di IAM Identity Center

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

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

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.

2. Nel riquadro di navigazione, scegli Provider fiduciari ad 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 fiduciario di IAM Identity Center (AWS CLI)

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

Usa un provider di fiducia OpenID Connect

Accesso verificato da AWS supporta provider di identità che utilizzano metodi OpenID Connect (OIDC) standard. Puoi utilizzare provider OIDC compatibili come fornitori di fiducia per l'identità degli utenti con Verified Access. Tuttavia, a causa dell'ampia gamma di potenziali OIDC fornitori, non AWS è in grado di testare ogni OIDC integrazione con Verified Access.

Verified Access ottiene i dati di fiducia che valuta dal OIDC provider. `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 OIDC provider, durante 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

Dovrete raccogliere le seguenti informazioni direttamente dal vostro fornitore di fiducia:

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

Crea un fornitore di OIDC fiducia

Utilizza la procedura seguente per crearne uno OIDC come fornitore di fiducia.

Per creare un provider di OIDC fiducia (AWS console)

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Provider fiduciari ad 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 Tipo di provider di fiducia utente, seleziona OIDC(OpenID Connect).
7. Per Emittente, inserisci l'identificativo dell'emittente. OIDC
8. Per Endpoint di autorizzazione, inserisci l'intero endpoint URL di autorizzazione.
9. Per Token endpoint, inserisci l'intero endpoint URL del token.
10. Per User endpoint, inserisci l'intero endpoint URL dell'utente.
11. Immettere l'identificatore 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 reindirizzamento URI alla lista consentita del tuo OIDC provider. 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 OIDC provider: https:///oauth2/idpresponse `ApplicationDomain`

OIDCPer creare un provider AWS CLI di fiducia ()

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

Modifica un fornitore di OIDC fiducia

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

Per modificare un provider di OIDC fiducia (AWS console)

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Provider fiduciari ad accesso verificato, quindi seleziona il provider fiduciario che desideri modificare in Provider fiduciari ad 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 fornitore di OIDC fiducia (AWS CLI)

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

Eliminare un provider OIDC fiduciario

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 OIDC trust provider (AWS console)

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Provider fiduciari ad 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 OIDC fiduciario (AWS CLI)

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

Provider affidabili basati su dispositivi per l'accesso verificato

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

Indice

Provider affidabili per dispositivi supportati

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

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

Crea un provider di fiducia basato su dispositivi

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

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

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Provider fiduciari ad 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 la chiave di firma pubblica URL, inserisci la chiave univoca URL condivisa 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 reindirizzamento URI alla lista consentita del tuo OIDC provider. 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 OIDC provider: https:///oauth2/idpresponse `DeviceValidationDomain`

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

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

Modifica un provider di fiducia basato su dispositivi

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

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

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Provider fiduciari ad 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 la chiave di firma pubblica URL, modifica la chiave univoca URL condivisa 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 affidabile di dispositivi con accesso verificato (AWS CLI)

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

Elimina un provider di fiducia basato su dispositivi

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

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

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Provider fiduciari ad 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 affidabile di dispositivi con accesso verificato (AWS CLI)

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

Gruppi di accesso verificato

Un record Accesso verificato da AWS group 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 che hanno 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 applicazioni di vendita e impostare una politica di accesso a livello di gruppo. È quindi possibile utilizzare questa politica per definire un set comune di requisiti minimi di sicurezza per tutte le applicazioni di vendita. Questo approccio aiuta a semplificare l'amministrazione delle politiche.

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

Attività

- Crea un gruppo con accesso verificato
- Modifica una politica di gruppo con accesso verificato
- Elimina un gruppo con accesso verificato

Crea un gruppo con accesso verificato

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

Per creare un gruppo con accesso verificato

1. Apri la VPC console Amazon 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 Tag nome e Descrizione, inserisci un nome e una descrizione per il gruppo.
4. Per l'istanza di accesso verificato, seleziona un'istanza di accesso verificato da associare al gruppo.
5. (Facoltativo) Per la definizione della politica, inserisci una politica di accesso verificato da applicare al gruppo.

6. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
7. Scegli Crea gruppo di accesso verificato.

Modifica una politica di gruppo con accesso verificato

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

Per modificare una politica di gruppo con accesso verificato

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

Elimina un gruppo con accesso verificato

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

Per eliminare un gruppo con accesso verificato

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

Endpoint con accesso verificato

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

Indice

Tipi di endpoint Verified Access

I seguenti sono i possibili tipi di endpoint Verified Access:

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

Come funziona Verified Access con reti condivise VPCs e sottoreti

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

- Gli endpoint Verified Access sono supportati dalla condivisione di sottoreti. VPC Un partecipante può creare un endpoint di accesso verificato 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 VPC proprietario non sarà consentito modificare l'endpoint.

- Gli endpoint Verified Access non possono essere creati in un AWS Local Zone e quindi la condivisione tramite Local Zones non è possibile.

Per ulteriori informazioni, consulta Condividi il tuo account VPC con altri account nella Amazon VPC User Guide.

Crea un endpoint di bilanciamento del carico per Verified Access

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

Requisiti

- È supportato solo IPv4 il traffico.
- Sono supportati solo HTTP i HTTPS protocolli and. HTTPSLe connessioni di lunga durata, ad esempio le WebSocket connessioni, non sono supportate.
- Il load balancer deve essere un Application Load Balancer o un Network Load Balancer e deve essere un load balancer interno.
- Il load balancer e le sottoreti devono appartenere allo stesso cloud privato virtuale (). VPC
- HTTPSi sistemi di bilanciamento del carico possono utilizzare certificati autofirmati o pubblici. TLS Utilizza un RSA certificato con una lunghezza di chiave di 1.024 o 2.048.
- È necessario fornire un nome di dominio per l'applicazione. Questo è il DNS nome pubblico che gli utenti utilizzeranno per accedere all'applicazione. Dovrai inoltre fornire un SSL certificato pubblico con un CN che corrisponda a questo nome di dominio. È possibile creare o importare il certificato utilizzando AWS Certificate Manager.

Per creare un endpoint di bilanciamento del carico

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

6. Per i dettagli dell'applicazione, procedi come segue:
   a. Per Dominio dell'applicazione, inserisci un DNS nome per l'applicazione.
   b. In Certificato di dominio ARN, scegli il TLS certificato pubblico.
7. Per i dettagli sull'endpoint, procedi come segue:
   a. Per Tipo di allegato, scegli 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 DNS nome generato da Verified Access per l'endpoint.
   d. Per il tipo di endpoint, scegli Load balancer.
   e. Per Protocollo, scegli HTTPSo. HTTP
   f. In Porta, inserisci il numero di porta.
   g. Per Load balancer ARN, scegli il load balancer.
   h. Per le sottoreti, scegli le sottoreti per il tuo bilanciamento del carico.
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 IPv4 traffico.
- Sono supportati solo HTTP i HTTPS protocolli and.
- 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 DNS nome pubblico che gli utenti utilizzeranno per accedere all'applicazione. Dovrai inoltre fornire un SSL certificato pubblico con un CN che corrisponda a questo nome di dominio. È possibile creare o importare il certificato utilizzando AWS Certificate Manager.

Per creare un endpoint di interfaccia di rete

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Endpoints di accesso verificato.
3. Scegli Crea endpoint di accesso verificato.
4. (Facoltativo) Per Tag nome e Descrizione, inserisci un nome e una descrizione per l'endpoint.
5. Per il gruppo di accesso verificato, scegli un gruppo di accesso verificato per l'endpoint.
6. Per i dettagli dell'applicazione, procedi come segue:
   a. Per Dominio dell'applicazione, inserisci il DNS nome dell'applicazione.
   b. In Certificato di dominio ARN, scegli il TLS certificato pubblico.
7. Per i dettagli sull'endpoint, procedi come segue:
   a. Per Tipo di allegato, scegli 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 DNS nome generato da Verified Access per l'endpoint.
   d. Per il tipo di endpoint, scegli Interfaccia di rete.
   e. Per Protocollo, scegli HTTPSo 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 dall'endpoint di accesso verificato. A tale scopo, aggiungi una regola in entrata che specifica il gruppo di sicurezza per l'endpoint come origine. Ti consigliamo di rimuovere eventuali regole in entrata aggiuntive, in modo che l'applicazione riceva traffico solo dall'endpoint di accesso verificato.

Ti consigliamo di mantenere le regole in uscita esistenti.

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

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Endpoints di accesso verificato.
3. Scegli l'endpoint di accesso verificato, trova il gruppo IDs di sicurezza nella scheda Dettagli e copia l'ID del gruppo di sicurezza per l'endpoint.
4. Fai clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.
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

Utilizzare la procedura seguente per modificare un endpoint Verified Access.

Per modificare un endpoint di accesso verificato

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Endpoints di accesso verificato.
3. Seleziona l'endpoint.
4. Scegli Azioni, Modifica 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

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

Per modificare una policy sugli endpoint di accesso verificato

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

Elimina un endpoint con accesso verificato

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

Per eliminare un endpoint di accesso verificato

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Endpoints di accesso verificato.
3. Seleziona l'endpoint.
4. Scegli Azioni, Elimina endpoint di accesso verificato.

5. Quando viene richiesta la conferma, immettere **`delete`** e quindi scegliere Elimina.

Dati attendibili inviati a Verified Access dai fornitori di servizi fiduciari

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

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

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

Indice

Contesto predefinito per i dati attendibili di Verified Access

Accesso verificato da AWS include alcuni elementi sulla HTTP richiesta corrente per impostazione predefinita in tutte le valutazioni Cedar indipendentemente dai provider di fiducia configurati. Quando viene valutata una politica, Verified Access include i dati sulla HTTP richiesta corrente nel contesto Cedar sotto. `context.http_request key` Se lo desideri, puoi scrivere una politica che valuti in base ai dati. JSONLo schema 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 HTTP richiesta.

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

AWS IAM Identity Center contesto per i dati attendibili di Verified Access

Quando viene valutata una politica, se si definisce AWS IAM Identity Center in qualità di fornitore di fiducia, Accesso verificato da AWS include i dati di fiducia nel contesto Cedar nella chiave specificata

come «Policy Reference Name» nella configurazione del provider di fiducia. Se lo desideri, puoi scrivere una politica che valuti in base ai dati di 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.

JSONLo schema seguente mostra quali dati sono inclusi nella valutazione.

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

```
    },
    "groups": {
      "type": "object",
      "description": "A list of groups the user is a member of",
      "patternProperties": {
        "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{12}$": {
          "type": "object",
          "description": "The Group ID of the group",
          "properties": {
            "group_name": {
              "type": "string",
              "description": "The customer-provided name of the group"
            }
          }
        }
      }
    }
  }
}
```

Di seguito è riportato un esempio di policy che valuta in base ai dati di attendibilità forniti da AWS IAM Identity Center.

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

> **Note**
>
> Poiché i nomi dei gruppi possono essere modificati, IAM Identity Center fa riferimento ai gruppi utilizzando il loro ID di gruppo. Ciò consente di evitare di violare una dichiarazione politica quando si modifica il nome di un gruppo.

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

Questa sezione descrive i dati sulla fiducia forniti a Accesso verificato da AWS da fornitori di servizi fiduciari terzi.

> **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 di uno dei seguenti AWS Estensione del browser Verified Access o 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 policy, i tuoi utenti devono scaricare e installare il Accesso verificato da AWS estensione del browser dal Chrome web store o dal sito aggiuntivo per Firefox sui loro dispositivi.
- Se utilizzi dati CrowdStrikeattendibili nelle tue politiche, per prima cosa gli utenti devono installare Accesso verificato da AWS Host di messaggistica nativo (link per il download diretto). Questo componente è necessario per ottenere i dati attendibili dall' CrowdStrike agente in esecuzione sui

dispositivi degli utenti. Quindi, dopo aver installato questo componente, gli utenti devono installare il Accesso verificato da AWS estensione del browser dal Chrome Web Store o dal sito aggiuntivo di Firefox sui propri dispositivi.

- Se la 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 fiducia terzo. 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. JSONLo schema seguente mostra quali dati sono inclusi nella valutazione.

Per ulteriori informazioni sull'utilizzo di Jamf con accesso verificato, consulta Integrazione dell'accesso AWS verificato con 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 attendibilità 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 terzo. 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. JSONLo schema seguente mostra quali dati sono inclusi nella valutazione.

Per ulteriori informazioni sull'utilizzo CrowdStrike con Verified Access, consulta Proteggere le applicazioni private con CrowdStrike e Accesso verificato da AWSsul 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 politica che valuta i dati sulla fiducia 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. JSONLo schema seguente mostra quali dati sono inclusi nella valutazione.

Per ulteriori informazioni sull'utilizzo JumpCloud con AWS Accesso verificato, vedi Integrazione e JumpCloud AWS Accesso 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 in Verified Access

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

`x-amzn-ava-user-context`

Questa intestazione contiene le affermazioni degli utenti in formato JSON web token (JWT). Il JWT formato include un'intestazione, un payload e una firma codificati in base64. URL Verified Access utilizza ES384 (algoritmo di ECDSA firma 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: reclami utente firmati JWT per IAM Identity Center
- Chiavi pubbliche
- Esempio: recupero e decodifica JWT

Esempio: Firmato JWT per le rivendicazioni OIDC degli utenti

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

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: reclami utente firmati JWT per IAM Identity Center

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

> **Note**
>
> Per IAM Identity Center, nelle rivendicazioni 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 da utilizzare. HTTPS Se configuri l'endpoint Verified Access per l'utilizzoHTTP, assicurati di limitare il traffico verso l'endpoint utilizzando i gruppi di sicurezza.

Per garantire la sicurezza, devi verificare la firma prima di effettuare qualsiasi autorizzazione in base alle affermazioni e verificare che il `signer` campo nell'JWTintestazione contenga l'istanza di accesso verificato prevista. ARN

Per ottenere la chiave pubblica, recupera l'ID della chiave dall'JWTintestazione e usalo per cercare la chiave pubblica dall'endpoint.

L'endpoint per ciascuno Regione AWS è il seguente:

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

Esempio: recupero e decodifica JWT

Il seguente esempio di codice mostra come ottenere l'ID della chiave, la chiave pubblica e il payload in Python 3.9.

```
import jwt
import requests
import base64
import json

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

encoded_jwt = headers.dict['x-amzn-ava-user-context']
jwt_headers = encoded_jwt.split('.')[0]
decoded_jwt_headers = base64.b64decode(jwt_headers)
decoded_jwt_headers = decoded_jwt_headers.decode("utf-8")
decoded_json = json.loads(decoded_jwt_headers)
received_verified_access_instance_arn = decoded_json['signer']

assert expected_verified_access_instance_arn == received_verified_access_instance_arn,
 "Invalid Signer"

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

# Step 3: Get the public key from regional endpoint
url = 'https://public-keys.prod.verified-access.' + region + '.amazonaws.com/' + kid
req = requests.get(url)
pub_key = req.text

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

Politiche di accesso verificato

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

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

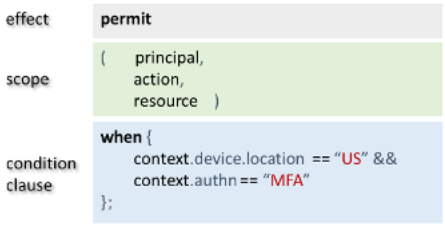
Quando crei un gruppo di accesso verificato o crei un endpoint di accesso verificato, hai la possibilità di definire la politica di accesso verificato. Puoi creare un gruppo o un endpoint senza definire la politica di accesso verificato, ma tutte le richieste di accesso verranno bloccate finché non definirai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

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

Indice

Struttura della dichiarazione sulla politica di accesso verificato

Questa sezione descrive Accesso verificato da AWS dichiarazione politica 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 integralmente facendo riferimento ai dati di attendibilità 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 Esempi di politiche di accesso verificato.

Valutazione della politica di accesso verificato

Un documento politico è un insieme di una o più dichiarazioni politiche (`permito` `forbid` dichiarazioni). La politica si applica se la clausola condizionale (la `when` dichiarazione) è vera. Affinché un documento di policy consenta l'accesso, deve essere applicata almeno una politica di autorizzazione nel documento e non può essere applicata alcuna politica di divieto. Se non si 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**
>
> Accesso verificato da AWS convalida la sintassi quando si crea la policy, ma non convalida i dati inseriti nella clausola condizionale.

Operatori integrati per le politiche di accesso verificato

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

Operatore	Tipi e sovraccarichi	Descrizione
!	Booleano → Booleano	Logico no.
==	qualsiasi → qualsiasi	Uguaglianza. Funziona su argomenti di qualsiasi tipo, anche se i tipi non corrispon dono. I valori di tipi diversi non sono mai uguali tra loro.

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

Operatore	Tipi e sovraccarichi	Descrizione
ha	(entità, attributo) → Booleano	Operatore Infix. `e has f` verifica se il record o l'entità `e` ha un'associazione per l'attributo `f`. `e` Restituisce `false` se non esiste o se `e` esiste ma non ha l'attributo `f`. Gli attributi possono essere espressi come identificatori o stringhe letterali.
like	(stringa, stringa) → Booleano	Operatore Infix. `t like p` controlla se il testo `t` corrisponde allo schema `p`, che può includere caratteri jolly `*` che corrispondono a 0 o più caratteri di qualsiasi carattere. Per far 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).
.containsAll()	(set, set) → Booleano	Verifica se il set A contiene tutti gli elementi del set B.
.containsAny()	(set, set) → Booleano	Verifica se il set A contiene uno qualsiasi degli elementi del set B.

Commenti sulla politica di accesso verificato

Puoi includere dichiarazioni di commento nel tuo Accesso verificato da AWS politiche. 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 della politica di accesso verificato

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

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

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

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

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

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

Esempi di politiche di accesso verificato

Esempio 1: creazione di politiche per IAM Identity Center

> **Note**
>
> Poiché i nomi dei gruppi possono essere modificati, IAM Identity Center fa riferimento ai gruppi che utilizzano il loro ID di gruppo. Questo aiuta a evitare di violare una dichiarazione politica quando si modifica 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 politica di esempio consente l'accesso solo quando un utente appartiene al `finance` gruppo (il cui ID di gruppo è`c242c5b0-6081-1845-6fa8-6e0d9513c107`), ha un indirizzo e-mail verificato e il punteggio di rischio del dispositivo Jamf è. `LOW`

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

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

La seguente politica di esempio consente l'accesso solo quando l'utente appartiene al gruppo «finance», ha un indirizzo email verificato e il punteggio di rischio del dispositivo Jamf èLOW.

```
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

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

Fase 2: Verificare e modificare le politiche

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

- Il contesto di fiducia inviato dal provider di fiducia per l'utente e (facoltativamente) il dispositivo specificato nel passaggio precedente.

- La policy Cedar per l'endpoint Verified Access specificata nel passaggio precedente.
- La policy Cedar per il gruppo Verified Access a cui appartiene l'endpoint.

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

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

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

Fase 3: Rivedere e applicare le modifiche

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

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

Sicurezza nell'accesso verificato

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

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

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

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

Indice

Protezione dei dati in Verified Access

Il AWS modello di responsabilità condivisa modello di di si applica alla protezione dei dati in AWS Accesso verificato. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutte le Cloud AWS. L'utente è responsabile del mantenimento

del controllo sui contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile delle attività di configurazione e gestione della sicurezza per Servizi AWS che usi. Per ulteriori informazioni sulla privacy dei dati, consulta la sezione Privacy dei dati FAQ. Per informazioni sulla protezione dei dati in Europa, consulta la AWS Modello di responsabilità condivisa e post sul GDPR blog sul AWS Blog sulla sicurezza.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS credenziali e configura singoli utenti con AWS IAM Identity Center oppure 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:

- Usa l'autenticazione a più fattori (MFA) con ogni account.
- UsaSSL/TLSper comunicare con AWS risorse. Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Configurazione API e registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per l'acquisizione AWS attività, vedi Lavorare con i CloudTrail sentieri in AWS CloudTrail Guida per l'utente.
- Utilizzo AWS soluzioni di crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se sono necessari FIPS 140-3 moduli crittografici convalidati per l'accesso AWS tramite un'interfaccia a riga di comando o unAPI, utilizza un endpoint. FIPS Per ulteriori informazioni sugli FIPS endpoint disponibili, vedere Federal Information Processing Standard (FIPS) 140-3.

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 consoleAPI, AWS CLI, oppure AWS SDKs. 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. Se fornisci un URL a un server esterno, ti consigliamo vivamente di non includere le informazioni sulle credenziali URL per convalidare la tua richiesta a quel 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 Verified Access per limitare l'accesso a risorse specifiche del tuo. VPC Per l'autenticazione basata sull'utente, puoi anche limitare l'accesso a parti della rete, in base al gruppo di utenti che accede agli endpoint. Per ulteriori informazioni, consulta Politiche di accesso verificato.

Crittografia dei dati a riposo per AWS Accesso verificato

AWS Per impostazione predefinita, Verified Access crittografa i dati inattivi, utilizzando AWS KMSchiavi possedute. 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 seguenti sezioni forniscono i dettagli su come Verified Access utilizza KMS le chiavi per la crittografia dei dati inattivi.

Indice

Accesso e KMS chiavi verificati

AWS chiavi possedute

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

Sebbene non sia possibile disabilitare questo livello di crittografia o selezionare un tipo di crittografia alternativo, è possibile aggiungere un secondo livello di crittografia rispetto a quello esistente AWS

chiavi di crittografia possedute scegliendo una chiave gestita dal cliente al momento della creazione delle risorse di accesso verificato.

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

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

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

Informazioni di identificazione personale

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

Tipo di dati	AWS crittografia a chiave proprietaria	Crittografia con chiavi gestite dal cliente (opzionale)
`Trust provider (user-type)` I provider fiduciari di tipo utente contengono OIDC opzioni come Authoriza tionEndpoint, UserInfoE ndpoint, ClientId ClientSecret, e così via, che vengono prese in considerazionePII.	Abilitato	Abilitato
`Trust provider (device-type)` I provider fiduciari di tipo dispositivo contengono un TenantId, che viene considera to. PII	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 PII nome utente e indirizzo e-mail e così via.	Abilitato	Abilitato
`Endpoint policy` Fornito durante la creazione o la modifica dell'endpoint Verified Access. Contiene le regole per l'autorizzazione	Abilitato	Abilitato

Tipo di dati	AWS crittografia a chiave proprietaria	Crittografia con chiavi gestite dal cliente (opzionale)
delle richieste di accesso. Potrebbe contenere PII nome utente e indirizzo e-mail e così via.		

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

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

Quando crei risorse di accesso verificato crittografate con una chiave gestita dal cliente, Verified Access crea una concessione per tuo conto inviando una CreateGrantrichiesta a AWS KMS. Sovvenzioni in AWS KMS vengono utilizzati 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 le richieste Decrypt a AWS KMS per decrittografare le chiavi di dati crittografate in modo che possano essere utilizzate per decrittografare i dati.
- Invia richieste a RetireGrant AWS KMS per eliminare una sovvenzione.

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

È possibile creare una chiave simmetrica gestita dal cliente utilizzando AWS Management Console, oppure AWS KMS APIs. Segui i passaggi per la creazione di una chiave simmetrica gestita dal cliente nel AWS Key Management Service Guida per gli sviluppatori.

Politiche chiave

Le policy della chiave controllano l'accesso alla chiave gestita dal cliente. Ogni chiave gestita dal cliente deve avere esattamente una policy della chiave, che contiene istruzioni che determinano

chi può usare la chiave e come la possono usare. Quando crei la chiave gestita dal cliente, puoi specificare una policy della chiave. Per ulteriori informazioni, consulta Gestione dell'accesso alle chiavi gestite dal cliente nel AWS Key Management Service Guida per gli sviluppatori.

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

- `kms:CreateGrant`: aggiunge una concessione a una chiave gestita dal cliente. Le concessioni controllano l'accesso a una KMS chiave specificata, che consente l'accesso alle operazioni di concessione richieste da Verified Access. Per ulteriori informazioni sull'utilizzo di Grants, consulta il 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 sulla specificazione delle autorizzazioni in una politica, consulta la AWS Key Management Service Guida per gli sviluppatori.

Per ulteriori informazioni sulla risoluzione dei problemi di accesso tramite chiave, consulta la AWS Key Management Service Guida per gli sviluppatori.

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

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

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

Quando crei una di queste risorse utilizzando il AWS 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 AWS KMS ID chiave che desideri utilizzare. Questo può essere fatto anche quando si modifica una risorsa esistente o utilizzando il AWS CLI.

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

AWS Contesto di crittografia Verified Access

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

AWS contesto di crittografia Verified Access

Verified Access utilizza lo stesso contesto di crittografia in tutti AWS KMS operazioni 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, vedere il contesto di crittografia nella AWS Key Management Service Guida per gli sviluppatori.

Monitoraggio delle chiavi di crittografia per AWS Accesso verificato

Quando utilizzi una KMS chiave gestita dal cliente con AWS Risorse ad accesso verificato, che puoi utilizzare AWS CloudTrailper tenere traccia delle richieste inviate a Verified Access AWS KMS.

I seguenti esempi sono AWS CloudTrail eventi per`CreateGrant`,,`RetireGrant`, e `Decrypt` `DescribeKey``GenerateDataKey`, che monitorano KMS le operazioni richiamate da Verified Access per accedere ai dati crittografati dalla KMS chiave 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 contenuta nel tuo AWS conto. La concessione creata da Verified Access è specifica per la risorsa associata alla chiave gestita dal cliente.

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T16:27:12Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T16:41:42Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "operations": [
            "Decrypt",
            "RetireGrant",
            "GenerateDataKey"
        ],
        "keyId": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae",
        "constraints": {
            "encryptionContextSubset": {
                "aws:verified-access:arn": "arn:aws:ec2:ca-
central-1:111122223333:verified-access-trust-provider/vatp-0e54f581e2e5c97a2"
```

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

RetireGrant

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

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

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

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

```
    "eventCategory": "Management"
}
```

Decrypt

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

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

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

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


DescribeKey

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

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


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

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


GenerateDataKey

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T17:19:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T17:46:49Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:verified-access:arn": "arn:aws:ec2:ca-
central-1:111122223333:verified-access-trust-provider/vatp-00f20a4e455e9340f",
            "aws-crypto-public-key": "A/ATGxaYatPUlOtM+l/mfDndkzHUmX5Hav+29IlIm
+JRBKFuXf24ulztmOIsqFQliw=="
        },
        "numberOfBytes": 32,
        "keyId": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
    },
    "responseElements": null,
    "requestID": "06535808-7cce-4ae1-ab40-e3afbf158a43",
```

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


Gestione delle identità e degli accessi per Verified Access

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

Argomenti

Destinatari

Come si usa AWS Identity and Access Management (IAM) differisce a seconda del lavoro svolto in Verified Access.

Utente del servizio: se utilizzi il servizio di accesso verificato 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 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. È quindi necessario inviare richieste all'IAMamministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base diIAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM Verified Access, consultaCome funziona Verified Access con IAM.

IAMamministratore: se sei un IAM amministratore, potresti voler saperne di più su come scrivere politiche per gestire l'accesso a Verified Access. Per visualizzare esempi di policy basate sull'identità di accesso verificato che puoi utilizzare inIAM, consulta. Esempi di policy basate sull'identità per Verified Access

Autenticazione con identità

L'autenticazione è il modo in cui si accede a AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l'accesso a AWS) come Utente root dell'account AWS, come IAM utente o assumendo un IAM ruolo.

Puoi accedere a AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAMIdentity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali Google o Facebook sono esempi di identità federate. Quando accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente che sei, puoi accedere a AWS Management Console o il AWS portale di accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Accedi ad AWS Guida per l'utente.

Se accedi AWS programmaticamente, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le richieste utilizzando le credenziali

dell'utente. Se non usi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, vedi Firma AWS APIrichieste nella Guida IAM per l'utente.

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

Account AWS utente root

Quando crei un Account AWS, inizi con un'unica identità di accesso con accesso completo a tutti Servizi AWS e le risorse presenti nell'account. Questa identità è denominata Account AWS utente root ed è accessibile effettuando l'accesso 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. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per l'elenco completo delle attività che richiedono l'accesso come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'IAMutente.

Identità federata

Come procedura ottimale, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, un provider di identità Web, il AWS Directory Service, la directory Identity Center o qualsiasi utente che accede Servizi AWS utilizzando le credenziali fornite tramite una fonte di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. È possibile creare utenti e gruppi in IAM Identity Center oppure connettersi e sincronizzarsi con un set di utenti e gruppi nella propria fonte di identità per utilizzarli su tutti i Account AWS e applicazioni. Per informazioni su IAM Identity Center, vedi Cos'è IAM Identity Center? nel AWS IAM Identity Center Guida per l'utente.

IAM users and groups

Un IAMutente è un'identità all'interno del tuo Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente. IAM

Un IAMgruppo 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, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per IAM amministrare le risorse.

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 IAM utente (anziché un ruolo) nella Guida per l'IAMutente.

IAMruoli

Un IAMruolo è un'identità all'interno del tuo Account AWS che dispone di autorizzazioni specifiche. È simile a un IAM utente, ma non è associato a una persona specifica. È possibile assumere temporaneamente un IAM ruolo nel AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un AWS CLI oppure AWS APIoperazione o utilizzando un comando personalizzatoURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere Utilizzo IAM dei ruoli nella Guida per l'IAMutente.

IAMi ruoli 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 informazioni sui ruoli per la federazione, vedere Creazione di un ruolo per un provider di identità di terze parti nella Guida per l'IAMutente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla

il set di autorizzazioni a un ruolo in. IAM Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella AWS IAM Identity Center Guida per l'utente.

- Autorizzazioni IAM utente temporanee: un IAM utente o un ruolo può assumere un IAM ruolo per assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso su più account: puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse su più account IAM nella Guida per l'utente. IAM
- Accesso a più servizi: alcuni Servizi AWS usa le funzionalità in altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è normale che quel 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.
  - Sessioni di accesso diretto (FAS): quando utilizzi un IAM utente o un ruolo per eseguire azioni in AWS, sei considerato un preside. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama un Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi a valle. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse da completare. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, vedere 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 di eseguire un'azione per conto dell'utente. I ruoli collegati ai servizi vengono visualizzati nel Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2istanza e in fase di creazione AWS CLI oppure AWS APIrichieste. Ciò è preferibile alla memorizzazione delle chiavi di accesso all'interno

dell'EC2istanza. Per assegnare un AWS assegnare un ruolo a un'EC2istanza e renderlo disponibile a tutte le relative applicazioni, è necessario creare un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'EC2istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Usare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida per l'IAMutente.

Per sapere se utilizzare IAM ruoli o IAM utenti, consulta Quando creare un IAM ruolo (anziché un utente) nella Guida per l'IAMutente.

Gestione dell'accesso con policy

Puoi controllare l'accesso in AWS creando politiche e allegandole a AWS identità o risorse. Una politica è un oggetto in AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata in AWS come JSON documenti. Per ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere Panoramica delle JSON politiche nella Guida per l'IAMutente.

Gli amministratori possono utilizzare AWS JSONpolitiche per specificare chi ha accesso a cosa. 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 il permesso di eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM politiche. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

IAMle politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, il AWS CLI, o AWS API.

Policy basate su identità

I criteri basati sull'identità sono documenti relativi ai criteri di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per

informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono AWS politiche gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una politica gestita o una politica in linea, consulta Scelta tra politiche gestite e politiche in linea nella Guida per l'IAMutente.

Policy basate su risorse

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata 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 puoi usare AWS politiche gestite da IAM una politica basata sulle risorse.

Liste di controllo degli accessi () ACLs

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

Amazon S3, AWS WAF e Amazon VPC sono esempi di servizi che supportanoACLs. Per ulteriori informazioniACLs, consulta la panoramica di Access control list (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e 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 di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità (utente o ruolo). IAM 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 nella Guida per l'utente. IAM IAM

- Politiche di controllo del servizio (SCPs): SCPs sono JSON politiche che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in AWS Organizations. AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di cui è proprietaria la tua azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. I SCP limiti e le autorizzazioni per le entità presenti negli account dei membri, inclusi tutti Utente root dell'account AWS. Per ulteriori informazioni su Organizations andSCPs, vedere Service control policies nel AWS Organizations Guida per l'utente.
- 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 le politiche di sessione nella Guida IAM per l'utente.

Più tipi di policy

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

Come funziona Verified Access con IAM

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

IAMcaratteristica	Supporto Verified Access
Policy basate su identità	Sì

IAMcaratteristica	Supporto Verified Access
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
ACLs	No
ABAC(tag nelle politiche)	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 altro AWS i servizi funzionano con la maggior parte delle IAM funzionalità, vedi AWS servizi compatibili con IAM la Guida per l'IAMutente.

Politiche basate sull'identità per l'accesso verificato

Supporta le policy basate su identità: sì

Le politiche basate sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM

Con le politiche IAM basate sull'identità, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. 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 ulteriori informazioni su tutti gli elementi che è possibile utilizzare in una JSON politica, vedere il riferimento agli elementi IAM JSON della politica nella Guida per l'IAMutente.

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

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

Politiche basate sulle risorse all'interno di Verified Access

Supporta le policy basate su risorse: no

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata 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 abilitare l'accesso tra più account, puoi specificare un intero account o IAM entità in un altro account come principale in una politica 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 il principale e la risorsa sono diversi Account AWS, un IAM amministratore dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad 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 la sezione Cross Account Resource Access IAM nella Guida IAM per l'utente.

Azioni politiche per l'accesso verificato

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare AWS JSONpolitiche per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'`Action`elemento di una JSON policy descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome di quelle associate AWS APIoperazione. Esistono alcune eccezioni, come le azioni di sola autorizzazione che non hanno un'operazione corrispondente. API 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

Risorse relative alle politiche per l'accesso verificato

Supporta le risorse di policy: sì

Gli amministratori possono utilizzare AWS JSONpolitiche per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Resource` JSON policy specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il relativo Amazon Resource Name (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 relativiARNs, consulta Resources Defined by Amazon EC2 nel Service Authorization Reference. Per sapere con quali azioni puoi specificare le caratteristiche ARN di ogni risorsa, consulta Azioni definite da Amazon EC2.

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

Chiavi relative alle condizioni delle policy per Verified Access

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

Gli amministratori possono utilizzare AWS JSONpolitiche per specificare chi ha accesso a cosa. 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 specificate più `Condition` elementi in un'istruzione o più chiavi in un singolo `Condition` elemento, AWS li valuta utilizzando un'`AND`operazione logica. Se specificate più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'`OR`operazione 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, è possibile concedere a un IAM utente l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il relativo nome IAM utente. Per ulteriori informazioni, consulta gli elementi IAM della politica: variabili e tag nella Guida IAM per l'utente.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per vedere tutto AWS chiavi di condizione globali, vedi AWS chiavi di contesto della condizione globale nella Guida IAM per l'utente.

Per visualizzare un elenco di chiavi di accesso verificato, consulta Condition Keys for Amazon EC2 nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, 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

ACLsin Accesso verificato

SupportiACLs: no

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

ABACcon accesso verificato

Supporti ABAC (tag nelle politiche): Parziale

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. È possibile allegare tag a IAM entità (utenti o ruoli) e a molte AWS risorse. L'etichettatura di entità e risorse è il primo passo diABAC. Quindi si progettano ABAC politiche per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa a cui sta tentando di accedere.

ABACè utile in ambienti in rapida crescita e aiuta in situazioni in cui la gestione delle politiche diventa complicata.

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 suABAC, vedere Cos'è? ABAC nella Guida IAM per l'utente. Per visualizzare un tutorial con i passaggi per la configurazioneABAC, consulta Utilizzare il controllo di accesso basato sugli attributi (ABAC) nella Guida per l'IAMutente.

Utilizzo di credenziali temporanee con accesso verificato

Supporta le credenziali temporanee: sì

Medio Servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, tra cui Servizi AWS lavorare con credenziali temporanee, vedere Servizi AWS che funzionano con IAM la Guida per l'IAMutente.

Stai utilizzando credenziali temporanee se accedi a AWS Management Console utilizzando qualsiasi metodo tranne il nome utente e la password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sul cambio di ruolo, consulta Passare a un ruolo (console) nella Guida per l'IAMutente.

È possibile creare manualmente credenziali temporanee utilizzando AWS CLI oppure AWS API. È quindi possibile utilizzare tali credenziali temporanee per accedere AWS. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, vedere Credenziali di sicurezza temporanee in. IAM

Autorizzazioni principali per più servizi per l'accesso verificato

Supporta sessioni di accesso diretto (FAS): Sì

Quando si utilizza un IAM utente o un ruolo per eseguire azioni in AWS, sei considerato un preside. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama un Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi a valle. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse da completare. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.

Ruoli di servizio per Verified Access

Supporta i ruoli di servizio: No

Un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, vedere 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 ruoli collegati ai servizi: Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo di eseguire un'azione per conto dell'utente. I ruoli collegati ai servizi

vengono visualizzati nel Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

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

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

Per informazioni su come creare una politica IAM basata sull'identità utilizzando questi documenti di esempioJSON, consulta Creazione di IAM politiche nella Guida per l'IAMutente.

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

Argomenti

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

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse di accesso verificato nel tuo account. Queste azioni possono comportare costi per Account AWS. Quando crei o modifichi politiche basate sull'identità, segui queste linee guida e consigli:

- Inizia con AWS politiche gestite e passaggio alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza il AWS politiche gestite che concedono autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Si consiglia di ridurre ulteriormente le autorizzazioni definendo AWS politiche gestite dai clienti

specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta AWS politiche gestite o AWS politiche gestite per le funzioni lavorative nella Guida per IAM l'utente.

- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM politiche, concedi solo le autorizzazioni necessarie 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 per applicare le autorizzazioni, consulta Politiche e autorizzazioni nella Guida IAM per l'utente. IAM IAM
- Utilizza le condizioni nelle IAM politiche per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue politiche per limitare l'accesso ad azioni e risorse. Ad esempio, puoi scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzandoSSL. È inoltre possibile utilizzare le condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta Elementi IAM JSON della politica: Condizione nella Guida IAM per l'utente.
- Usa IAM Access Analyzer per convalidare IAM le tue policy e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy () e alle best practice. JSON IAM IAMAccess Analyzer fornisce più di 100 controlli delle politiche e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, vedere Convalida delle policy di IAM Access Analyzer nella Guida per l'utente. IAM
- Richiedi l'autenticazione a più fattori (MFA): se disponi di uno scenario che richiede l'utilizzo di IAM utenti o di un utente root Account AWS, attivala MFA per una maggiore sicurezza. Per richiedere MFA quando vengono richiamate API le operazioni, aggiungi MFA delle condizioni alle tue politiche. Per ulteriori informazioni, vedere Configurazione dell'APIaccesso MFA protetto nella Guida per l'IAMutente.

Per ulteriori informazioni sulle procedure consigliate inIAM, consulta la sezione Procedure consigliate in materia di sicurezza IAM nella Guida per l'IAMutente.

Politica per la creazione di istanze di accesso verificato

Per creare un'istanza di accesso verificatoIAM, i responsabili devono aggiungere questa dichiarazione aggiuntiva alla loro IAM politica.

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

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

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

Esempio di politica per la creazione di un'istanza di accesso verificato. In questo esempio, `123456789012` è AWS numero di conto ed `us-east-1` è 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 come è possibile creare una politica che consenta IAM agli utenti di visualizzare le politiche in linea e gestite allegate alla loro identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando a livello di codice il AWS CLI oppure AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

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

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

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

Problemi

- Non sono autorizzato a eseguire un'azione in Verified Access
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire l'accesso a persone esterne al mio Account AWS per accedere alle mie risorse di accesso verificato

Non sono autorizzato a eseguire un'azione in Verified Access

Se ricevi un errore che indica che non disponi dell'autorizzazione per eseguire un'operazione, le tue policy devono essere aggiornate in modo che ti sei consentito eseguire tale operazione.

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

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

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

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

Non sono autorizzato a eseguire iam: PassRole

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

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

L'errore di esempio seguente si verifica quando un IAM utente 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`.

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

Voglio consentire l'accesso a persone esterne al mio Account AWS per accedere alle mie risorse di accesso verificato

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

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Verified Access supporta queste funzionalità, consulta. Come funziona Verified Access con IAM
- Per scoprire come fornire l'accesso alle tue risorse in tutto il mondo Account AWS di cui sei proprietario, vedi Fornire l'accesso a un IAM utente in un altro Account AWS che possiedi nella Guida per l'IAMutente.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, vedi Fornire l'accesso a Account AWS di proprietà di terzi nella Guida per l'IAMutente.
- 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'IAMutente.
- Per conoscere la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse tra account nella Guida per l'utente. IAM IAM

Usa ruoli collegati ai servizi per l'accesso verificato

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

Un ruolo collegato al servizio semplifica la configurazione di Verified Access perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Verified Access definisce le autorizzazioni dei suoi ruoli collegati al servizio e, se non diversamente definito, solo Verified Access può assumerne i

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

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta i AWS servizi che funzionano con IAM e cerca i servizi con Sì nella colonna Ruoli collegati ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni relative ai ruoli collegati ai servizi per Verified Access

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

Il ruolo AWSServiceRoleForVPCVerifiedAccesscollegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `verified-access.amazonaws.com`

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

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

È inoltre possibile visualizzare le autorizzazioni per questa politica nella oppure è possibile visualizzare la AWS Management Console AWSVPCVerifiedAccessServiceRolePolicyAWSVPCVerifiedAccessServiceRolePolicypolitica nella AWS Managed Policy Reference Guide.

È necessario configurare le autorizzazioni per consentire a un'IAMentità (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio. Per ulteriori informazioni, consulta Autorizzazioni dei ruoli collegati ai servizi nella Guida per l'utente. IAM

Crea un ruolo collegato al servizio per Verified Access

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando CreateVerifiedAccessEndpointrichiami il AWS Management Console, il o il AWS CLI AWS API, 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 ancora CreateVerifiedAccessEndpointuna volta, Verified Access crea nuovamente il ruolo collegato al servizio per te.

Modifica un ruolo collegato al servizio per Verified Access

L'accesso verificato non consente di modificare il ruolo collegato al AWSServiceRoleForVPCVerifiedAccessservizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. Tuttavia, puoi modificare la descrizione del ruolo utilizzando. IAM Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'IAMutente.

Eliminare un ruolo collegato al servizio per Verified Access

Non è necessario eliminare manualmente il AWSServiceRoleForVPCVerifiedAccessruolo. Quando DeleteVerifiedAccessEndpointrichiami il AWS Management Console, il o il AWS CLI AWS API, Verified Access pulisce le risorse ed elimina automaticamente il ruolo collegato al servizio.

Per eliminare manualmente il ruolo collegato al servizio utilizzando IAM

Usa la IAM console AWS CLI, o il AWS API per eliminare il ruolo collegato al AWSServiceRoleForVPCVerifiedAccessservizio. Per ulteriori informazioni, vedere Eliminazione di un ruolo collegato al servizio nella Guida per l'utente. IAM

Regioni supportate per i ruoli collegati al servizio Verified Access

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

AWS politiche gestite per l'accesso verificato

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

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti 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 politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove API operazioni per i servizi esistenti.

Per ulteriori informazioni, consulta le politiche AWS gestite nella Guida IAM per l'utente.

AWS politica gestita: AWSVPCVerifiedAccessServiceRolePolicy

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

Verified Access: aggiornamenti alle politiche AWS gestite

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

Modifica	Descrizione	Data
AWSVPCVerifiedAccessServiceRolePolicy- Politica aggiornata	Verified Access ha aggiornato la sua politica di gestione per 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	31 maggio 2023

Modifica	Descrizione	Data
	del gruppo di sicurezza all'`ec2:CreateNetworkInterface` autorizzazione.	
AWSVPCVerifiedAccessServiceRolePolicy: nuova policy	Verified Access ha aggiunto una nuova politica per consentirgli di fornire le risorse necessarie per utilizzare il servizio nell'account.	29 novembre 2022
Verified Access ha iniziato a tenere traccia delle modifiche	Verified Access ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	29 novembre 2022

Convalida della conformità per Verified Access

Accesso verificato da AWS può essere configurato per supportare la conformità agli standard federali di elaborazione delle informazioni (FIPS). Per maggiori informazioni e dettagli sulla configurazione della FIPS conformità per Verified Access, vai aFIPSconformità per Verified Access.

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 i passaggi per l'implementazione di ambienti di base incentrati sulla AWS sicurezza e la conformità.

- Architettura per la HIPAA sicurezza e la conformità su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee. HIPAA

  > **Note**
  >
  > Non tutte sono idonee. Servizi AWS HIPAA Per ulteriori informazioni, consulta la Guida ai servizi HIPAA idonei.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe riguardare il settore e la località in cui operi.
- 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
- Evaluating Resources with Rules nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- 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, ad esempio 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 AWS l'utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza nell'accesso verificato

L'infrastruttura AWS globale è costruita attorno a zone Regioni AWS di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza

interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

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

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

Più sottoreti per un'elevata disponibilità

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

Monitoraggio Accesso verificato da AWS

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

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

Log di accesso verificati

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

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

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

Indice

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

Versioni di registrazione degli accessi verificate

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

L'ultima versione di registrazione è compatibile con OCSF la versione 1.0.0-rc.2. I dettagli specifici sullo schema sono disponibili qui Schema. OCSF Nella sezione sono disponibili esempi di log che utilizzano la versione 1.0.0-rc.2. OCSFesempi di log della versione 1.0.0-rc.2 per Verified Access

Se si desidera aggiornare la versione di registrazione utilizzata, utilizzare la procedura seguente.

Per aggiornare la versione di registrazione utilizzando la console

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

Per aggiornare la versione di registrazione utilizzando il AWS CLI

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

Autorizzazioni di registrazione degli accessi verificate

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

Per la consegna ai registri CloudWatch :

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

Per la consegna ad Amazon S3:

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

Per la consegna a Firehose:

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

Abilita o disabilita i registri di accesso verificato

È possibile utilizzare le procedure descritte in questa sezione per abilitare o disabilitare la registrazione. Quando si abilita la registrazione, è necessario configurare una destinazione per l'invio dei log. Il IAM principale utilizzato per configurare la destinazione di registrazione deve disporre di determinate autorizzazioni affinché la registrazione funzioni correttamente. Le IAM autorizzazioni richieste per ciascuna destinazione di registrazione sono visualizzate nella sezione. Autorizzazioni di registrazione degli accessi verificate

Indice

Abilitare log di accesso

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

Per disabilitare i registri di accesso verificato utilizzando il AWS CLI

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

Abilita o disabilita il contesto di fiducia di accesso verificato

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

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

Indice

Abilita il contesto di fiducia

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

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

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

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

Disabilita il contesto di fiducia

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

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

1. Apri la VPC console Amazon 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.

OCSFesempi di log della versione 0.1 per Verified Access

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

Esempi

Accesso concesso con OIDC

In questa voce di registro di esempio, Verified Access consente l'accesso a un endpoint con un provider di fiducia per gli OIDC utenti.


```
{
    "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 e OIDC JAMF

In questo esempio di voce di registro, Verified Access consente l'accesso a un endpoint sia con provider affidabili che con OIDC i JAMF device trust.


```
{
    "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 e OIDC CrowdStrike

In questo esempio di voce di registro, Verified Access consente l'accesso a un endpoint sia con provider affidabili che con OIDC i CrowdStrike device trust.


```
{
    "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
}
```

OCSFesempi di log della versione 1.0.0-rc.2 per Verified Access

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

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 API chiamate con accesso verificato utilizzando AWS CloudTrail

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

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

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

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

Per una registrazione continua degli eventi nel tuo Account AWS negli ultimi 90 giorni, crea un trail o un archivio dati di eventi CloudTrailLake.

CloudTrail sentieri

Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Tutti i percorsi creati utilizzando il AWS Management Console sono multiregionali. È possibile creare un percorso a regione singola o multiregione utilizzando il AWS CLI. La creazione di un percorso multiregionale è consigliata perché consente di registrare tutte le attività Regioni AWS nel tuo account. Se crei un percorso a regione singola, puoi visualizzare solo gli eventi registrati nel percorso Regione AWS. Per ulteriori informazioni sui sentieri, vedi Creazione di un percorso per il tuo Account AWSe Creazione di un percorso per un'organizzazione in AWS CloudTrail Guida per l'utente.

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

CloudTrail Archivi di dati sugli eventi sul lago

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

CloudTrail Gli archivi di dati e le richieste di Lake Event comportano dei costi. Quando crei un datastore di eventi, scegli l'opzione di prezzo da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di

conservazione predefinito e quello massimo per il datastore di eventi. Per ulteriori informazioni sui CloudTrail prezzi, consulta AWS CloudTrail Prezzi.

Eventi di gestione degli accessi verificati

Gli eventi di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse del Account AWS. Queste operazioni sono note anche come operazioni sul piano di controllo. Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

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

Esempi di eventi Verified Access

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


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

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


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

Quote per Accesso verificato da AWS

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

Account AWS quote a livello 2

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

Nome	Predefinita	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.

HTTPintestazioni

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

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

OIDCdimensione del reclamo

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

Nome	Predefinita	Adattabile
OIDCdimensione della richiesta	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
AWS politica gestita aggiornata	Aggiornamento apportato alla IAM politica AWS gestita per l'accesso verificato.	17 novembre 2023
Crittografia dei dati a riposo	AWS Per impostazione predefinita, Verified Access crittografa i dati inattivi, utilizzando KMS chiavi AWS proprietarie.	28 settembre 2023
Support per la FIPS conformità	Configura l'accesso verificato per la FIPS conformità.	26 settembre 2023
Registrazione avanzata	Aggiunta della funzionalità di registrazione che aggiunge contesti di fiducia ai log.	19 giugno 2023
AWS politica gestita aggiornata	Aggiornamento apportato alla IAM politica AWS gestita per l'accesso verificato.	31 maggio 2023
Versione GA	Versione GA della Verified Access User Guide. Include AWS WAF l'integrazione.	27 aprile 2023
Versione di anteprima	Versione di anteprima della Verified Access User Guide	29 novembre 2022

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