Guida per gli sviluppatori

AWS Responsabile della sicurezza di rete



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Responsabile della sicurezza di rete: Guida per gli sviluppatori

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Che cos'è AWS Network Security Manager? 1
In che modo AWS Network Security Manager funziona a colpo d'occhio 1
Caratteristiche di AWS Responsabile della sicurezza di rete 1
Casi d’uso 2
Servizi correlati 3
Accesso AWS Responsabile della sicurezza di rete 3
Prezzi 4
È la prima volta che utilizzi ? 4
Come funziona AWS Network Security Manager 5
AWS Modello di risorse di Network Security Manager 5
AWS Ciclo di vita delle risorse, unione e sincronizzazione di Network Security Manager 6
Bozza e ciclo di vita attivo 6
Controllo delle versioni 7
Priority-based fusione delle politiche 8
Scoperta delle risorse con AWS Config 9
Sincronizzazione e correzione 10
Account per amministratori e membri 11
Service-linked ruolo 12
Configurazione di AWS Network Security Manager 13
Scegli il tuo modello organizzativo 13
Configurazione per l'uso con un solo account 13
Configurazione per l'uso su più account con AWS Organizations 14
Creare un AWS Account amministratore di Network Security Manager 15
Crea un'identità IAM con AWS Autorizzazioni di Network Security Manager 17
Registrati per un Account AWS 18
Utilizzo AWS Network Security Manager nelle regioni disattivate per impostazione predefinita ... 18
Tutorial: implementa la tua prima protezione di sicurezza di rete 19
Prerequisiti 19
Fase 1: Creare una regola 20
Fase 2: Creare un modello 21
Fase 3: Creare una politica 22
Fase 4: Creare un ambito 23
Fase 5: Creare e pubblicare una distribuzione 23
Fase 6: Monitoraggio dello stato di sincronizzazione 24

Fase 7: pulire 25
Fasi successive 26
Gestione di firewall e servizi di sicurezza 27
Gestione degli ACL Web per WAF AWS 27
AWS Concetti WAF 27
Creazione rapida per AWS WAF 31
Processo di creazione standard per AWS WAF 35
Gestione delle protezioni DDoS per Shield Advanced AWS 41
Creazione rapida per AWS Shield Advanced 42
Processo di creazione standard per AWS Shield Advanced 46
AWS Responsabile della sicurezza di rete e Firewall Manager 50
Coesistenza con AWS Firewall Manager 50
Precedenza durante la riparazione 50
Migrazione pianificata da AWS Firewall Manager 50
Sicurezza 52
Protezione dei dati 53
Crittografia dei dati a riposo 54
Crittografia dei dati in transito 54
Gestione delle chiavi 54
Gestione dell'identità e degli accessi 54
Destinatari 55
Autenticazione con identità 55
Gestione dell'accesso tramite policy 56
In che modo AWS Network Security Manager funziona con IAM 58
Identity-based esempi di politiche 64
Risoluzione dei problemi 69
Service-linked ruoli 71
Service-linked autorizzazioni di ruolo 71
Creazione di un ruolo collegato ai servizi 82
Modificare un ruolo collegato ai servizi 82
Eliminazione del ruolo collegato ai servizi 83
Regioni supportate 83
Convalida della conformità 84
Resilienza 84
Sicurezza dell'infrastruttura 85
Best practice di sicurezza 85

Controlli preventivi 85
Controlli di rilevamento 86
Monitoraggio AWS Responsabile della sicurezza di rete 87
Monitoraggio dello stato di sincronizzazione 87
Operazioni sullo stato della sincronizzazione 87
Comprensione dei valori dello stato di sincronizzazione 88
Comprensione dei timestamp di valutazione 88
Cross-account visibilità 88
Diagnosi delle risorse non sincronizzate 89
CloudTrail registri 89
AWS Informazioni su Network Security Manager in CloudTrail 90
Esempio: evento CreatePolicy 91
Quote 94
Quote delle risorse 94
Quote di composizione delle risorse 94
Quote di configurazione dell'ambito 95
Quote degli account di amministratore 95
Quote di impaginazione delle API 95
Regolabilità delle quote 96
Cronologia dei documenti 97
..... xcviii

Che cos'è AWS Responsabile della sicurezza di rete?

Con AWS Network Security Manager, puoi definire e implementare centralmente le protezioni di sicurezza della rete, come le regole WAF AWS e AWS Shield Advanced, su uno o più account e risorse dell'organizzazione. Invece di lavorare con ogni risorsa singolarmente, è possibile definire oggetti di policy riutilizzabili (regole, modelli e policy) una sola volta e distribuirli su larga scala, con un monitoraggio continuo per rilevare e correggere eventuali variazioni nelle politiche.

In che modo AWS Network Security Manager funziona a colpo d'occhio

È possibile definire una serie di oggetti di policy gerarchici e applicarli a ambiti mirati. Il livello più basso di oggetti politici sono le regole. È possibile raggruppare le regole in modelli, che è possibile combinare in politiche con risoluzione dei conflitti basata sulle priorità. Quindi seleziona gli account e le risorse da proteggere con un ambito e applica le tue politiche pubblicando una distribuzione.

Dopo l'implementazione, AWS Network Security Manager monitora continuamente l'ambiente interessato e le politiche implementate per verificare se corrispondono alle definizioni previste. In caso contrario, AWS Network Security Manager può facoltativamente correggere le risorse che si discostano dalla configurazione prevista. Per informazioni complete sul modello di risorse, sul ciclo di vita e sull'architettura, vedere. Come funziona AWS Network Security Manager

Caratteristiche di AWS Responsabile della sicurezza di rete

- Supporto per diversi tipi di firewall: AWS Network Security Manager supporta configurazioni e gruppi di regole AWS WAF per Web ACL. I tipi di risorse protette includono CloudFront distribuzioni Amazon, Application Load Balancers e fasi Amazon API Gateway. AWS Network Security Manager supporta anche AWS Shield Advanced per la protezione DDoS di CloudFront distribuzioni Amazon, Application Load Balancer, Classic Load Balancer e indirizzi IP elastici.
- Configurazioni di sicurezza riutilizzabili: definisci gli oggetti delle policy una sola volta come regole, raggruppali in modelli e crea ambiti per indirizzare le risorse. Riutilizza regole, modelli e ambiti in più politiche e implementazioni.
- Priority-based unione delle policy: quando più policy proteggono la stessa risorsa, AWS Network Security Manager unisce le relative configurazioni in base alla priorità delle policy, garantendo una risoluzione prevedibile dei conflitti.

- Single-account e supporto per più amministratori: utilizza AWS Network Security Manager in un unico account o designa più account di amministratore, ciascuno con un livello di priorità. Quando le politiche degli amministratori si sovrappongono, AWS Network Security Manager risolve i conflitti prima in base alla priorità dell'amministratore, poi in base alla priorità delle politiche all'interno di ciascun account.
- Bozza e stati attivi: ogni risorsa di AWS Network Security Manager, incluse regole, modelli, politiche, ambiti e distribuzioni, supporta gli stati Bozza e Attivo. Salva le risorse come bozza senza influire sulle protezioni in tempo reale, quindi pubblicale quando sei pronto per applicarle.
- Istantanee con versione: ogni risorsa di AWS Network Security Manager, incluse regole, modelli, policy, ambiti e distribuzioni, supporta istantanee immutabili con numero di versione. Utilizza il controllo delle versioni per preservare le configurazioni delle risorse di Network Security Manager note e valide. AWS
- Protected-resource diagnostica di sincronizzazione: per ogni risorsa pertinente, visualizza esattamente quali impostazioni non sono sincronizzate e perché, confrontando le impostazioni previste con i valori effettivi per ogni campo di configurazione.
- Riparazione automatica: facoltativamente, abilita AWS Network Security Manager a correggere automaticamente le risorse non sincronizzate e ad allinearle alla configurazione prevista senza intervento manuale.
- Natural-language generazione di regole: usa l'`GenerateRuleConfiguration`operazione per descrivere una regola in un linguaggio semplice e ricevi la configurazione JSON corrispondente, fornita da Amazon Bedrock.

Casi d’uso

I seguenti sono casi d'uso comuni per AWS Network Security Manager:

- Applica le regole AWS WAF di base a tutti gli account: definisci un set di gruppi di regole AWS WAF che ogni applicazione connessa a Internet deve utilizzare, quindi distribuiscili nell'intera organizzazione. AWS Network Security Manager applica automaticamente le regole alle nuove risorse pertinenti man mano che entrano nell'ambito.
- Crea regole AWS WAF specifiche o personalizzate su risorse specifiche: definisci un set di regole AWS WAF che si applicano solo a un set specifico di risorse. Questo set può essere un'unità aziendale o un'applicazione specifica identificata tramite ID AWS account, unità organizzativa, tag o Amazon Resource Names (ARN).

- Verifica la protezione DDoS sulle risorse connesse a Internet: crea una policy AWS Shield Advanced applicabile ai tipi di risorse pubbliche e distribuiscila a livello dell'organizzazione in modo che le risorse critiche abbiano la protezione DDoS abilitata.
- Rileva e correggi le deviazioni di configurazione: utilizza il monitoraggio dello stato della sincronizzazione per identificare le risorse le cui configurazioni del firewall si sono discostate dallo stato previsto e, facoltativamente, abilita la correzione automatica per riportarle alla conformità.
- Delega la gestione della sicurezza a più team: designa più account di amministratore con diversi livelli di priorità e accesso mirato a account, unità organizzative o tipi di firewall specifici, permettendo ai team di gestire le proprie politiche di sicurezza entro limiti definiti.

Servizi correlati

- AWS WAF: usa AWS WAF per proteggere le tue applicazioni web e le tue API da exploit e bot web comuni che potrebbero influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive. AWS Network Security Manager utilizza AWS WAF per creare e gestire ACL Web e gruppi di regole per le risorse in un singolo account o tra più account dell'organizzazione.
- AWS Shield Advanced: un servizio di protezione DDoS gestito che fornisce protezioni estese per le applicazioni in esecuzione. AWS AWS Network Security Manager utilizza Shield Advanced per fornire protezioni DDoS per le risorse in un singolo account o tra più account dell'organizzazione.
- AWS Organizzazioni: consente di gestire e governare centralmente l'ambiente man mano che crescono e scalano le AWS risorse. AWS Network Security Manager richiede AWS alle Organizzazioni di gestire le protezioni tra gli account dei membri.
- AWS Config: un servizio che consente di valutare, controllare e valutare le configurazioni delle risorse. AWS AWS Network Security Manager utilizza un registratore AWS Config collegato al servizio per scoprire le risorse negli account dei membri.

Accesso AWS Responsabile della sicurezza di rete

È possibile accedere a AWS Network Security Manager tramite le seguenti interfacce:

AWS Console di gestione

Un'interfaccia basata sul Web per la gestione delle risorse AWS di Network Security Manager.

Aprire la console AWS di Network Security Manager all'indirizzo https://console.aws.amazon.com/network-security-manager/.

AWS Interfaccia a riga di comando (AWS CLI)

Fornisce comandi per le operazioni AWS di Network Security Manager. Per ulteriori informazioni, consulta la pagina di Riferimento ai comandi CLI AWS.

AWS SDK

AWS fornisce SDK costituiti da librerie e codice di esempio per vari linguaggi e piattaforme di programmazione. Gli SDK offrono un modo pratico per creare l'accesso programmatico a AWS Network Security Manager. Per ulteriori informazioni, consulta Strumenti per Amazon Web Services.

AWS API Network Security Manager

Un'API REST che utilizza JSON su HTTPS. Il formato dell'endpoint dell'API è. `network-security-manager.{region}.api.aws` Per ulteriori informazioni, consulta il riferimento alle API di AWS Network Security Manager.

Per iniziare a usare AWS Network Security Manager, consulta Configurazione di AWS Network Security Manager eTutorial: implementa la tua prima protezione di sicurezza di rete.

Prezzi

Paghi per ogni risorsa che AWS Network Security Manager monitora e protegge. Si applicano costi aggiuntivi per i servizi di sicurezza sottostanti distribuiti, come AWS WAF e AWS Shield Advanced. Per informazioni dettagliate sui prezzi, consulta i prezzi AWS di Network Security Manager sul AWS sito Web.

È la prima volta che utilizzi ?

Se utilizzi AWS Network Security Manager per la prima volta, ti consigliamo di leggere i seguenti argomenti nell'ordine:

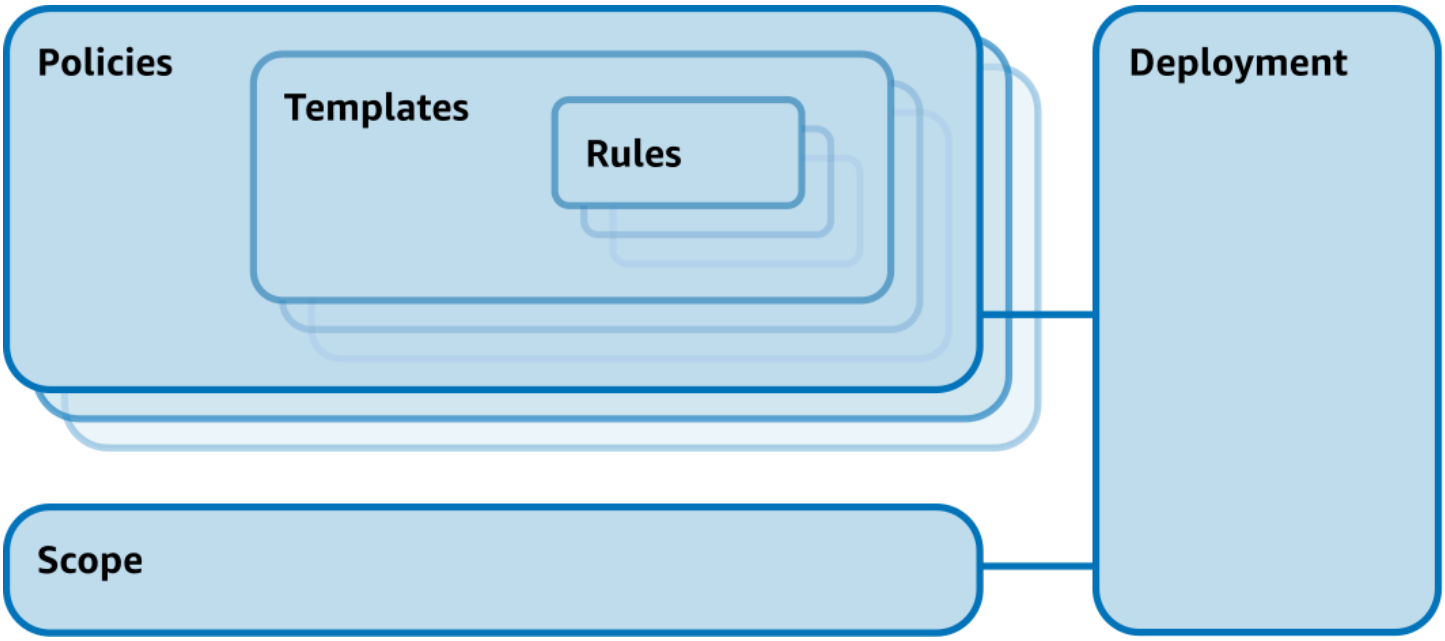
1. Come funziona AWS Network Security Manager— Scopri il modello di risorse, gli stati del ciclo di vita, l'unione delle politiche e la sincronizzazione.
2. Configurazione di AWS Network Security Manager— Completa i prerequisiti per l'utilizzo di Network Security Manager. AWS
3. Tutorial: implementa la tua prima protezione di sicurezza di rete— Segui un tutorial completo che crea la tua prima implementazione.

In che modo AWS Network Security Manager funziona

Utilizza il modello di risorse di AWS Network Security Manager per progettare e gestire le protezioni di sicurezza di rete per le risorse di un singolo account o tra più account della tua organizzazione. Questo capitolo spiega i cinque tipi di risorse, come formano una gerarchia e i concetti chiave che ne regolano il comportamento.

AWS Modello di risorse di Network Security Manager

AWS Network Security Manager utilizza cinque tipi di risorse disposti in una gerarchia di composizione:



Le risorse fanno riferimento l'una all'altra verso l'alto nella gerarchia. Le regole vengono utilizzate all'interno di modelli e policy. I modelli, le regole o entrambi vengono utilizzati all'interno delle politiche. Un ambito fa riferimento alle risorse che le policy proteggono all'interno di una distribuzione.

Le sezioni seguenti descrivono ogni tipo di risorsa nella gerarchia.

Regola: l'unità atomica della configurazione della sicurezza di rete. Esistono due tipi di regole: le regole di ispezione del traffico e le regole di configurazione del firewall. L'ispezione del traffico si concentra sul modo in cui il servizio di sicurezza affronta il traffico. Una regola di configurazione specifica le operazioni del sistema al di fuori dell'ispezione del traffico. La struttura di una regola varia in base al tipo di firewall.

Modello: un gruppo di regole ordinato e riutilizzabile per un singolo tipo di firewall. Utilizza i modelli per raggruppare le regole correlate e condividerle tra più policy. I modelli sono opzionali.

Policy: combina un insieme ordinato di modelli e regole con impostazioni di applicazione per un tipo di firewall. Ogni policy ha una priorità (un numero più basso indica una priorità più alta). Quando più politiche proteggono la stessa risorsa, la priorità determina la modalità di risoluzione dei conflitti. Per le regole di ispezione del traffico, la priorità determina l'ordine in cui le regole vengono aggregate. Per quanto riguarda le regole di configurazione del firewall, la priorità determina quale configurazione si applica a ciascuna risorsa e alle relative politiche.

Ambito: una selezione dichiarativa dei settori in cui applicare le protezioni. Un ambito specifica i tipi di risorse da proteggere ed è possibile facoltativamente filtrare le risorse per tag o attributo di configurazione. In modalità multi-account, un ambito specifica anche quali account o unità organizzative includere o escludere. In modalità account singolo, l'ambito si applica all'account stesso. La modalità di un ambito viene fissata al momento della creazione. Non è possibile cambiare un ambito tra la modalità multi-account e quella con account singolo in nessuna delle due direzioni, quindi un ambito con più account non può mai diventare un ambito a account singolo o viceversa.

Distribuzione : associa una o più politiche a un ambito. La pubblicazione di una distribuzione attiva l'applicazione. AWS Network Security Manager rileva le risorse incluse nell'ambito, calcola la configurazione prevista e, facoltativamente, corregge le risorse non sincronizzate.

Per i limiti di composizione delle risorse, vedere. Quote

AWS Ciclo di vita delle risorse, unione e sincronizzazione di Network Security Manager

Nelle sezioni seguenti vengono illustrati i comportamenti e i meccanismi che regolano il funzionamento delle risorse di AWS Network Security Manager dopo la loro creazione.

Bozza e ciclo di vita attivo

Ogni risorsa di AWS Network Security Manager, incluse regole, modelli, policy, ambiti e distribuzioni, ha lo stato Bozza o Attiva:

- Attivo: lo stato predefinito. La risorsa è pubblicata e disponibile per l'uso. Altre risorse possono farvi riferimento e le implementazioni che la includono ne impongono la configurazione.

- Bozza: la risorsa è stata salvata ma non è ancora attiva. Le bozze di risorse non vengono applicate e non possono essere referenziate da altre risorse. Quando crei o aggiorni una risorsa, scegli Salva bozza per mantenerla nello stato di bozza.

Per impostazione predefinita, AWS Network Security Manager crea le risorse come Attive. Per creare una risorsa come bozza utilizzando l'API, imposta il `isPublished` parametro su `false` nell'operazione di creazione o aggiornamento.

Quando aggiorni una risorsa, si applicano i seguenti scenari:

Stato attuale	Azione	Risultato
Draft	Scegli Salva bozza	Aggiorna la bozza (rimane bozza)
Draft	Scegli Pubblica	Pubblica la bozza (diventa attiva)
Attivo	Scegli Pubblica	Aggiorna e rimani attivo (attivo)
Attivo	Scegli Salva bozza	Crea una bozza di sovrapposizione (diventa Bozza con una risorsa attiva al di sotto)

Il `hasPublishedVersion` campo appare nell'elenco e ottieni risposte. Questo campo indica se esiste una risorsa attiva pubblicata sotto una bozza. Quando una risorsa ha lo stato Bozza e `hasPublishedVersion: true` una bozza in sospeso si trova sopra una risorsa attiva e pubblicata.

Non è possibile eliminare una risorsa attiva a cui fa riferimento un'altra risorsa attiva.

Controllo delle versioni

Ogni risorsa di AWS Network Security Manager, incluse regole, modelli, politiche, ambiti e distribuzioni, può essere versionata. Per creare una versione di una risorsa attiva, seleziona la risorsa, scegli Azione, quindi scegli Crea istantanea con versione. Le versioni non vengono create automaticamente a ogni aggiornamento.

> **AWS Alternativa CLI**
>
> Puoi anche creare una versione utilizzando l'operazione `Create{Resource}Snapshot` API su una risorsa attiva.

Proprietà chiave della versione:

- Ogni versione ha un numero univoco (un numero intero sequenziale) e un ARN qualificato per la versione (ad esempio,). `arn:aws:network-security-manager:us-east-1:123456789012:rule:abc123:3`
- Le versioni sono immutabili. Non possono essere aggiornate.
- Puoi creare fino a 10 versioni per risorsa.
- Le versioni sono etichettabili.

Usa le versioni per conservare le varianti di configurazione desiderate. Per ripristinare una risorsa, leggi una versione, quindi aggiorna la risorsa attiva con la configurazione desiderata della versione.

Priority-based fusione delle politiche

Quando più policy proteggono la stessa risorsa, AWS Network Security Manager unisce le relative configurazioni in un unico risultato. Un numero di priorità più basso indica una priorità più alta (la priorità 1 ha la precedenza sulla priorità 2). Quando AWS Network Security Manager unisce le policy che contengono regole di ispezione del traffico, la priorità determina l'ordine in cui le regole vengono aggregate. Per le regole di configurazione del firewall, la politica di priorità più elevata determina la configurazione da applicare.

AWS Network Security Manager valuta la priorità a due livelli, in questo ordine:

1. Priorità dell'amministratore: AWS Network Security Manager valuta innanzitutto la priorità dell'amministratore. A ogni amministratore dell'organizzazione viene assegnata una priorità, come descritto inthe section called “Account per amministratori e membri”. Quando AWS Network Security Manager unisce i criteri, assegna un criterio di amministratore a un livello superiore rispetto ai criteri relativi all'account singolo di un account membro. Se i criteri di amministratore e i criteri relativi all'account singolo di un account membro si applicano entrambi a una risorsa e sono in conflitto, la configurazione della politica di amministratore vince. Un account membro non può disattivare, sostituire o esonerarsi da una politica di amministratore.

2. Priorità delle politiche: all'interno di ciascun account, AWS Network Security Manager utilizza quindi la priorità delle politiche per risolvere i conflitti rimanenti. I valori di priorità delle policy sono numeri interi che iniziano da 1 e devono essere univoci per account.

La priorità dell'amministratore viene impostata con il `priority` campo richiesto dell'`PutAdminAccount`operazione, un numero intero compreso tra 1 e 10. I valori di priorità sono univoci, quindi due amministratori non condividono mai una priorità e non è richiesta alcuna interruzione dei pareggi. Per ulteriori informazioni, consulta il riferimento alle API AWS di Network Security Manager.

Il risultato combinato di tutte le politiche applicabili a una risorsa è la configurazione effettiva del firewall. AWS Network Security Manager calcola questa configurazione, la confronta con la configurazione effettiva della risorsa e riporta eventuali differenze come stato di sincronizzazione.

Quando le politiche sono in conflitto, AWS Network Security Manager confronta ogni attributo e applica il valore della politica con priorità più alta. Se la politica con priorità più alta non definisce un attributo, si applica il valore della politica con priorità più bassa. Una risorsa che corrisponde alla configurazione effettiva è IN_SYNC. Una risorsa protetta da una politica a priorità inferiore le cui impostazioni sono state sostituite da una politica a priorità più alta riporta come OUT_OF_SYNC per la distribuzione con priorità inferiore. Si tratta di un comportamento previsto, non di un errore.

Scoperta delle risorse con AWS Config

AWS Network Security Manager rileva le risorse protette negli account utilizzando un registratore di AWS configurazione Config collegato al servizio. Questo registratore viene creato automaticamente in ogni account quando quell'account entra nell'ambito di una distribuzione. A differenza di AWS Firewall Manager, non è necessario eseguire alcuna configurazione aggiuntiva. AWS L'utilizzo della configurazione da parte di AWS Network Security Manager non viene addebitato al cliente di AWS Network Security Manager.

Caratteristiche principali del registratore collegato al servizio:

- È denominato `AWSConfigurationRecorderForNetworkSecurityManager`.
- È separato da qualsiasi registratore di configurazione gestito dal cliente presente nell'account.
- Registra solo i tipi di risorse pertinenti agli ambiti e alle distribuzioni attivi.
- Non è necessario configurare AWS Config o creare un registratore di configurazione. AWS Network Security Manager lo gestisce automaticamente. AWS L'utilizzo di Config da parte di AWS Network Security Manager non è a carico del cliente.

- Non è possibile modificare o eliminare il registratore mentre è in uso. AWS Network Security Manager ne gestisce automaticamente il ciclo di vita.

Non è necessario abilitare o configurare AWS Config manualmente per il funzionamento di AWS Network Security Manager. Il servizio gestisce automaticamente l'individuazione delle risorse dopo la pubblicazione di una distribuzione.

Sincronizzazione e correzione

L'applicazione in AWS Network Security Manager è asincrona e alla fine coerente. Dopo la pubblicazione di una distribuzione o quando una risorsa cambia, si verificano le seguenti fasi:

1. Individuazione delle risorse: AWS Network Security Manager rileva le risorse nell'ambito utilizzando un registratore AWS Config collegato al servizio.
2. Calcolo della configurazione: per ogni risorsa rilevata, AWS Network Security Manager calcola la configurazione effettiva del firewall unendo tutte le politiche applicabili per priorità.
3. Valutazione della sincronizzazione: AWS Network Security Manager confronta la configurazione effettiva con la configurazione effettiva della risorsa e registra lo stato della sincronizzazione.
4. Correzione (opzionale): se si imposta `remediationEnabled` la policy, AWS Network Security Manager corregge le risorse non sincronizzate in modo che corrispondano alla configurazione effettiva.

Ogni fase è asincrona. Conseguenze per il flusso di lavoro:

- C'è un ritardo tra la pubblicazione di una distribuzione e la protezione delle risorse.
- Esiste un ritardo tra la creazione di una nuova risorsa nell'ambito e la sua protezione.
- Il `Last Checked` timestamp sulle voci relative allo stato della sincronizzazione indica l'ultima volta che AWS Network Security Manager ha valutato una risorsa.

La riparazione e la pulizia delle risorse sono impostazioni a livello di policy. Ciascuna di esse viene configurata in base alla politica dell'oggetto. `policyConfiguration`

`remediationEnabled`

Speciifica se AWS Network Security Manager corregge automaticamente le risorse non conformi. Quando si abilita questa impostazione, AWS Network Security Manager corregge le risorse non sincronizzate in modo che corrispondano alla configurazione effettiva.

`resourcesCleanUp`

Speciifica se AWS Network Security Manager rimuove automaticamente le risorse create quando non sono più necessarie. AWS Network Security Manager elimina un firewall creato quando si rimuove la distribuzione o quando l'account o la risorsa non rientrano nell'ambito di applicazione.

Le `resourcesCleanUp` impostazioni `remediationEnabled` e sono entrambe predefinite su. `false` AWS Network Security Manager non ripristina né ripulisce le risorse finché non si abilitano queste impostazioni. L'`policyConfiguration`oggetto è inoltre valido`wafConfig`, il che si applica alle politiche AWS WAF. Per ulteriori informazioni, vedere il riferimento alle API di AWS Network Security Manager.

Quando una risorsa non è sincronizzata, lo stato di sincronizzazione include motivi di non sincronizzazione con dettagli per impostazione che mostrano i valori previsti rispetto ai valori effettivi. I motivi sono organizzati nelle seguenti categorie:

- `missingFirewall`— Nessuna protezione firewall è associata alla risorsa.
- `invalidFirewall`— Esiste un firewall ma la sua configurazione è diversa dalla configurazione effettiva. Ciò include sei gruppi di dettagli:`incorrectSingleValueConfigurations`,,`missingAppendableConfigurationValues`, `unexpectedAppendableConfigurationValues` `incorrectAppendableConfigurationOrdermissingMergeableConfigurationValues`, e. `unexpectedMergeableConfigurationValues`

Se la correzione è abilitata ma AWS Network Security Manager non è in grado di correggere una risorsa`issueType`, il `remediationIssues` campo fornisce una `message` descrizione del problema e un `correctiveAction` suggerimento su come risolverlo.

AWS Network Security Manager non valuta le impostazioni che non gestisce. Se un campo non compare in nessuna regola di contribuzione, AWS Network Security Manager lo ignora durante la valutazione della sincronizzazione.

Account per amministratori e membri

AWS Network Security Manager utilizza un modello di gestione tra account basato su AWS Organizations:

- Account amministratore: l'account in cui si creano e gestiscono le risorse di AWS Network Security Manager (regole, modelli, politiche, ambiti e distribuzioni). Si designano uno o più account amministratore, ciascuno con una priorità da 1 a 10.
- Account membri: gli account in cui AWS Network Security Manager rileva le risorse, valuta lo stato della sincronizzazione e, facoltativamente, corregge le configurazioni non sincronizzate. AWS Network Security Manager agisce sugli account dei membri tramite un ruolo collegato al servizio. Per ulteriori informazioni, consulta the section called “Service-linked ruolo”.

Facoltativamente, è possibile assegnare a ciascun amministratore un sottoinsieme di account, unità organizzative e tipi di firewall. Utilizza questa funzionalità per delegare la gestione di aree specifiche a team diversi.

AWS Network Security Manager è un servizio regionale. Crei risorse e distribuzioni per regione senza dipendenze tra regioni.

Service-linked ruolo

AWS Network Security Manager utilizza un ruolo collegato ai servizi IAM denominato `AWSServiceRoleForNetworkSecurityManager` per agire per conto dell'utente negli account dei membri dell'organizzazione. Questo ruolo si affida al responsabile del `network-security-manager.amazonaws.com` servizio. Utilizza la politica `NetworkSecurityManagerServiceRolePolicy` AWS gestita.

AWS Network Security Manager crea questo ruolo automaticamente quando si attiva il servizio, quindi non è necessaria alcuna configurazione manuale. Il ruolo consente a AWS Network Security Manager di gestire le protezioni AWS WAF e AWS Shield Advanced, scoprire risorse protette tramite AWS Config ed eseguire operazioni su più account. Per ulteriori informazioni, consulta the section called “Service-linked ruoli”.

Configurazione AWS Responsabile della sicurezza di rete

Con AWS Network Security Manager, puoi lavorare in due modelli organizzativi. Usalo direttamente in un singolo account o usalo con AWS Organizations per gestire le protezioni su più account. I passaggi di configurazione dipendono dal modello scelto.

Argomenti

- Scegli il tuo modello organizzativo
- Configurazione per l'uso con un solo account
- Configurazione per l'uso su più account con AWS Organizations
- Creare un AWS Account amministratore di Network Security Manager
- Crea un'identità IAM con AWS Autorizzazioni di Network Security Manager
- Utilizzo AWS Network Security Manager nelle regioni disattivate per impostazione predefinita

Scegli il tuo modello organizzativo

Scegli tra i seguenti modelli organizzativi:

- Single-account— Usa AWS Network Security Manager per proteggere le risorse in un unico account. Non hai bisogno di AWS Organizations o di un account amministratore. Crea un'identità IAM con le autorizzazioni di AWS Network Security Manager e inizia a utilizzare direttamente il servizio. AWS Network Security Manager crea automaticamente un ruolo collegato al servizio nel tuo account.
- Multi-account— Utilizza AWS Network Security Manager with AWS Organizations per proteggere le risorse su più account. Questa modalità richiede la configurazione di AWS Organizations, l'abilitazione dell'accesso affidabile e la creazione di un account amministratore.

Configurazione per l'uso con un solo account

Per utilizzare AWS Network Security Manager in un singolo account, crea un'identità IAM con le autorizzazioni appropriate e inizia a utilizzare direttamente il servizio. Non è necessario creare un account amministratore. AWS Network Security Manager crea automaticamente un ruolo collegato al servizio nell'account in background. Passa a the section called “Crea un'identità IAM con AWS Autorizzazioni di Network Security Manager”.

Configurazione per l'uso su più account con AWS Organizations

Per gestire le protezioni su più account, stabilisci l'appartenenza e la configurazione richieste di AWS Organizations.

1. Scegli un account da utilizzare come amministratore di AWS Network Security Manager per l'organizzazione: si tratta dell'account da cui creare e gestire le risorse di AWS Network Security Manager.
2. Verifica l'appartenenza all'organizzazione: se l'account scelto non è già membro dell'organizzazione, fallo iscrivere. Segui le indicazioni riportate nella sezione Invitare un AWS account a entrare a far parte della tua organizzazione nella AWS Organizations User Guide.
3. Abilita tutte le funzionalità della tua organizzazione — AWS Organizations ha due set di funzionalità disponibili: funzionalità di fatturazione consolidata e tutte le funzionalità. Per utilizzare AWS Network Security Manager, l'organizzazione deve essere abilitata a tutte le funzionalità. Se la tua organizzazione è configurata solo per la fatturazione consolidata, segui le indicazioni riportate nella sezione Abilitazione di tutte le funzionalità dell'organizzazione nella AWS Organizations User Guide.
4. Abilita l'accesso affidabile per AWS Network Security Manager: abilita l'accesso affidabile per AWS Network Security Manager nelle AWS organizzazioni. Con l'accesso affidabile abilitato, AWS Network Security Manager può creare un ruolo collegato al servizio negli account dei membri e gestire le risorse per loro conto.
5. Registra un account amministratore delegato: registra l'account prescelto come amministratore delegato per AWS Network Security Manager in Organizations AWS . Utilizza l'account di gestione Organizations per completare questo passaggio.

> ⚠ Multi-account le protezioni sono disattivate quando si disattiva l'accesso affidabile
>
> Se si disattiva l'accesso affidabile per AWS Network Security Manager in AWS Organizations o si annulla la registrazione di un account amministratore delegato, AWS Network Security Manager imposta l'ambito e la distribuzione di più account su uno `DISABLED` stato e ripulisce le protezioni gestite.

Creare un AWS Account amministratore di Network Security Manager

Questo passaggio si applica solo alla modalità multi-account. Solo l'account di gestione dell'organizzazione può creare account amministratore di AWS Network Security Manager.

Dopo aver completato la configurazione di Organizations, registra il tuo account come amministratore di AWS Network Security Manager. È possibile eseguire questa operazione dalla console o dall'interfaccia a riga di AWS comando (AWS CLI).

Quando si crea un account amministratore, AWS Network Security Manager crea automaticamente un ruolo collegato ai servizi in tutti gli account dell'organizzazione. Con questo ruolo, AWS Network Security Manager scopre le risorse e gestisce le protezioni negli account dei membri.

Con AWS Network Security Manager, puoi avere più amministratori che gestiscono le risorse firewall della tua organizzazione. Se si desidera utilizzare più amministratori nell'organizzazione, è possibile applicare condizioni di ambito amministrativo a ciascun amministratore per definire le risorse che può gestire. Ciò offre la flessibilità necessaria per avere diversi ruoli di amministratore all'interno dell'organizzazione e aiuta a mantenere il principio dell'accesso con privilegi minimi. Ad esempio, un amministratore può gestire un insieme di unità organizzative (OU). Un altro amministratore può gestire solo tipi di policy specifici.

Per il numero massimo di amministratori che puoi avere per organizzazione, vediQuote.

> **Registrazione regionale**
>
> Si registra un account amministratore di AWS Network Security Manager in un'unica AWS regione. Per utilizzare AWS Network Security Manager in altre regioni, ripeti questo passaggio in ogni regione.

Per creare un account amministratore utilizzando la console

1. Aprire la console di AWS Network Security Manager all'indirizzo https://console.aws.amazon.com/network-security-manager/.
2. Nel pannello di navigazione scegli Impostazioni.
3. Scegli Aggiungi amministratore.

4. Seleziona l'account e inserisci un valore di priorità (da 1 a 10).
5. Scegli Aggiungi amministratore per confermare.

Per creare un account amministratore utilizzando il AWS CLI

Chiama `PutAdminAccount`l'operazione. È necessario fornire un valore di priorità (da 1 a 10).

L'esempio AWS CLI seguente registra un account come amministratore di AWS Network Security Manager con priorità 1:

```
aws network-security-manager put-admin-account \
    --account-id 123456789012 \
    --priority 1
```

È possibile designare più account di amministratore, ciascuno con una priorità diversa. Facoltativamente, è possibile limitare ogni amministratore a account, unità organizzative o tipi di firewall specifici fornendo un `adminScope` parametro.

Per rimuovere un account amministratore utilizzando la console

> **Multi-account protezioni disabilitate quando si rimuove un amministratore**
>
> Quando si rimuove un account amministratore, AWS Network Security Manager imposta l'ambito e la distribuzione di più account su uno `DISABLED` stato e ripulisce le protezioni gestite.

1. Apri la console di AWS Network Security Manager all'indirizzo. https://console.aws.amazon.com/network-security-manager/
2. Nel pannello di navigazione scegli Impostazioni.
3. Seleziona l'account amministratore che desideri rimuovere.
4. Scegli Remove administrator (Rimuovi amministratore).
5. Per confermare, scegli Conferma l'eliminazione dell'amministratore.

Crea un'identità IAM con AWS Autorizzazioni di Network Security Manager

Per utilizzare AWS Network Security Manager, è necessaria un'identità IAM (utente o ruolo) con le autorizzazioni per chiamare le operazioni di AWS Network Security Manager. Le azioni IAM utilizzano il prefissonetwork-security-manager.

L'esempio seguente di politica IAM contiene tre istruzioni. La prima istruzione garantisce l'accesso completo a tutte le operazioni AWS di Network Security Manager. La seconda istruzione concede le AWS autorizzazioni aggiuntive di Organizations e AWS WAF di cui AWS Network Security Manager ha bisogno. AWS Network Security Manager utilizza queste autorizzazioni per identificare gli account e le unità organizzative (OU) dell'organizzazione e per elencare i gruppi di regole WAF e i prodotti gestiti disponibili. Queste autorizzazioni consentono inoltre a AWS Network Security Manager di abilitare l'accesso affidabile e registrare un amministratore delegato in Organizations AWS . La terza istruzione concede l'iam:CreateServiceLinkedRoleautorizzazione necessaria a AWS Network Security Manager per creare il proprio ruolo collegato ai servizi, necessario sia per l'utilizzo con account singolo che con più account.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "network-security-manager:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAccountsForParent",
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "wafv2:ListRuleGroups",
                "wafv2:ListAvailableManagedRuleGroups",
                "wafv2:DescribeAllManagedProducts"
            ],
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*"
        }
    ]
}
```

Per l'uso in produzione, si consiglia di concedere solo le autorizzazioni minime richieste. Per ulteriori informazioni, consulta the section called “Gestione dell’identità e degli accessi”.

Registrati per un Account AWS

Per iniziare AWS, hai bisogno di un Account AWS. Per informazioni sulla creazione di un Account AWS, vedi Guida introduttiva a un Account AWS nella Guida Gestione dell’account AWS di riferimento.

Utilizzo AWS Network Security Manager nelle regioni disattivate per impostazione predefinita

Per utilizzare AWS Network Security Manager in un'area che è disabilitata per impostazione predefinita, è necessario abilitare la regione sia per l'account di gestione dell'organizzazione che per l'account amministratore di AWS Network Security Manager. Per informazioni sulle regioni disattivate per impostazione predefinita e su come abilitarle, vedere Gestione AWS delle regioni nella AWS Guida generale.

Per abilitare una regione disattivata

Sia per l'account di gestione Organizations che per l'account amministratore di AWS Network Security Manager, segui le indicazioni in Enabling a Region nella Guida AWS generale.

Implementa la tua prima protezione di sicurezza di rete

Questo tutorial illustra la distribuzione di un ACL Web AWS WAF utilizzando la console Network Security Manager. AWS Completate i seguenti passaggi:

1. Creazione di una regola
2. Crea un modello
3. Creazione di una policy
4. Creazione di un ambito
5. Crea e pubblica una distribuzione
6. Monitora lo stato della sincronizzazione

In questo tutorial, creerai un ACL web AWS WAF che protegge gli Application Load Balancer negli account selezionati. Questo processo è in gran parte identico per tutti i servizi di sicurezza e i firewall supportati da Network Security Manager. AWS

Tempo di completamento: circa 10 minuti

Costo: questo tutorial utilizza AWS servizi che potrebbero comportare costi. Per i prezzi correnti, consulta i prezzi AWS di Network Security Manager sul AWS sito Web.

Prerequisiti

Prima di iniziare, verifica di soddisfare i seguenti requisiti:

- Fasi di configurazione completate come descritto inConfigurazione di AWS Network Security Manager.
- Un' AWS identità di Identity and Access Management (IAM) AWS con autorizzazioni di Network Security Manager.
- Un'organizzazione AWS Organizations con tutte le funzionalità abilitate e un account amministratore designato di AWS Network Security Manager (richiesto per le distribuzioni con più account).
- Accesso alla console di AWS Network Security Manager.

Fase 1: Creare una regola

Una regola è l'elemento costitutivo della configurazione di sicurezza. In questo passaggio, crei due regole AWS WAF: una che imposta l'azione predefinita e una che imposta la configurazione di visibilità. Azione predefinita e VisibilityConfig sono campi obbligatori per un ACL Web AWS WAF.

Per creare la regola di azione predefinita, segui questi passaggi:

1. Apri la console AWS di Network Security Manager all'indirizzo https://console.aws.amazon.com/network-security-manager/.
2. Nel riquadro di navigazione seleziona Overview (Panoramica).
3. Nella pagina Panoramica, scegli Crea regola.
4. Per Nome regola, inserisci un nome descrittivo, ad esempio`my-default-action-rule`.
5. Nella sezione Definizione della regola, per Tipo di firewall, scegli AWS WAF.
6. Per Seleziona il tipo di regola, scegli Configurazione.
7. Scegli Inserisci tipi di configurazione, quindi seleziona Azione predefinita. Viene visualizzato un editor JSON con una configurazione predefinita.
8. Nell'editor JSON, rimuovi la `Block` sezione e mantieni solo la `Allow` sezione.
9. Scegli Crea regola.

Per creare la VisibilityConfig regola, segui questi passaggi:

1. Nel riquadro di navigazione seleziona Overview (Panoramica).
2. Nella pagina Panoramica, scegli Crea regola.
3. Per Nome regola, inserisci un nome descrittivo, ad esempio`my-visibility-config-rule`.
4. Nella sezione Definizione della regola, per Tipo di firewall, scegli AWS WAF.
5. Per Seleziona il tipo di regola, scegli Configurazione.
6. Scegli Inserisci tipi di configurazione, quindi seleziona VisibilityConfig. Viene visualizzato un editor JSON con una configurazione predefinita.
7. Scegli Crea regola.

> **AWS Alternativa CLI**
>
> Puoi anche creare regole con la AWS CLI:

```
aws network-security-manager create-rule \
    --rule-name "my-default-action-rule" \
    --firewall-type WAF \
    --rule-type CONFIGURATION \
    --configuration '{"DefaultAction": {"Allow": {}}}' \
    --is-published true

aws network-security-manager create-rule \
    --rule-name "my-visibility-config-rule" \
    --firewall-type WAF \
    --rule-type CONFIGURATION \
    --configuration '{"VisibilityConfig": {"SampledRequestsEnabled": true,
 "CloudWatchMetricsEnabled": true, "MetricName": "my-web-acl-metric"}}' \
    --is-published true
```

Fase 2: Creare un modello

Un modello raggruppa una o più regole da riutilizzare tra le politiche. In questo passaggio, crei un modello che include la regola del passaggio 1:

1. Nel riquadro di navigazione seleziona Overview (Panoramica).
2. Nella pagina Panoramica, scegli Crea modello.
3. Per Nome modello, inserisci un nome descrittivo, ad esempio`my-waf-template`.
4. Per il tipo di firewall, scegli AWS WAF.
5. Nella sezione Regole, scegli Aggiungi regola e seleziona le regole che hai creato nel passaggio 1.
6. Scegli Crea modello.

AWS Alternativa CLI

Puoi anche creare un modello con la AWS CLI:

```
aws network-security-manager create-template \
    --template-name "my-waf-template" \
    --firewall-type WAF \
    --associated-rule-list '[{"ruleIdentifier": "rule-arn-from-step-1"}]' \
```

```
    --is-published true
```

Fase 3: Creare una politica

Una policy combina modelli e impostazioni di applicazione. In questo passaggio, si crea una politica che fa riferimento al modello e consente la correzione automatica:

1. Nel riquadro di navigazione seleziona Overview (Panoramica).
2. Nella pagina Panoramica, scegli Crea politica.
3. Per Nome della politica, inserisci un nome descrittivo, ad esempio`my-waf-policy`.
4. Per il tipo di firewall, scegli AWS WAF.
5. Nella sezione Priorità delle politiche, vengono visualizzate le politiche esistenti e le relative priorità. Esamina la priorità della nuova politica. Se hai bisogno di modificarla, scegli il campo di priorità e modifica il valore in 1 un numero di priorità non utilizzato.
6. Nella sezione Modelli e regole, scegli Aggiungi modello e seleziona il modello creato nel passaggio 2.
7. Per Riparazione, seleziona Abilitato.
8. Per Risoluzione ACL web del cliente esistente, scegli Nessuna riparazione.
9. Scegli Crea policy.

AWS Alternativa CLI

Puoi anche creare una policy con la AWS CLI:

```
aws network-security-manager create-policy \
    --policy-name "my-waf-policy" \
    --firewall-type WAF \
    --priority 1 \
    --associated-template-and-rule-list '[{"templateIdentifier": "template-arn-
from-step-2"}]' \
    --policy-configuration '{"remediationEnabled": true, "resourcesCleanUp":
 false, "wafConfig": {"existingCustomerWebACLResolution": "NO_REMEDIATION"}}' \
    --is-published true
```

Fase 4: Creare un ambito

Un ambito definisce dove si applicano le protezioni. In questo passaggio, crei un ambito destinato agli Application Load Balancer nei tuoi account:

1. Nel riquadro di navigazione seleziona Overview (Panoramica).
2. Nella pagina Panoramica, scegli Crea ambito.
3. Per Nome dell'ambito, inserisci un nome descrittivo, ad esempio`my-alb-scope`.
4. (Facoltativo) Nella sezione Selezione dell'account e dell'unità organizzativa, per Seleziona il metodo di controllo dell'ambito amministrativo, seleziona Ambito per l'intera AWS organizzazione (tutte le unità organizzative e gli account). Salta questo passaggio per le implementazioni con account singolo.
5. Nella sezione Risorse, per Tipi di risorse, seleziona Application Load Balancer.
6. Scegli Crea ambito.

AWS Alternativa CLI

Puoi anche creare un ambito con la AWS CLI:

```
aws network-security-manager create-scope \
    --scope-name "my-alb-scope" \
    --scope-configuration '{
        "accountFilter": {"includeAll": {}},
        "resourceScopes": {
            "AWS::ElasticLoadBalancingV2::LoadBalancer::application": {
                "includeAll": true
            }
        }
    }' \
    --is-published true
```

Fase 5: Creare e pubblicare una distribuzione

Una distribuzione vincola le politiche a un ambito e ne attiva l'applicazione. Per creare e pubblicare una distribuzione:

1. Nel riquadro di navigazione seleziona Overview (Panoramica).
2. Nella pagina Panoramica, scegli Crea distribuzione.
3. Per Nome di distribuzione, inserisci un nome descrittivo, ad esempio`my-first-deployment`.
4. Nella sezione Politiche, scegli Aggiungi politica e seleziona la politica che hai creato nel passaggio 3.
5. Nella sezione Ambiti, scegli Aggiungi ambito e seleziona l'ambito creato nel Passaggio 4.
6. Scegli Create deployment (Crea distribuzione).

AWS Network Security Manager inizia a scoprire le risorse e ad applicare le protezioni. Questo processo è asincrono e il completamento potrebbe richiedere alcuni minuti.

AWS Alternativa CLI

Puoi anche creare e pubblicare una distribuzione con la AWS CLI:

```
aws network-security-manager create-deployment \
    --deployment-name "my-first-deployment" \
    --associated-policy-list '[{"policyIdentifier": "policy-arn-from-step-3"}]'
 \
    --associated-scope-list '[{"scopeIdentifier": "scope-arn-from-step-4"}]' \
    --deployment-configuration '{"enableCrossAccountVisibility": true}' \
    --is-published true
```

Fase 6: Monitoraggio dello stato di sincronizzazione

Dopo la pubblicazione di una distribuzione, AWS Network Security Manager rileva le risorse e ne sincronizza le configurazioni. Per monitorare lo stato di ogni risorsa:

1. Nel riquadro di navigazione seleziona Overview (Panoramica).
2. Seleziona la scheda Distribuzioni.
3. Scegli la distribuzione che hai creato nel passaggio 5.
4. Scegli la scheda Sincronizzazione.
5. Verifica lo stato di sincronizzazione per ogni risorsa:
   - IN_SYNC: la configurazione delle risorse corrisponde alle impostazioni di protezione desiderate.

- OUT_OF_SYNC — La configurazione delle risorse non corrisponde. AWS Network Security Manager risolve questo problema automaticamente quando la riparazione è abilitata.
- NOT_APPLICABLE — La risorsa rientra nell'ambito ma non può essere valutata da questa distribuzione.

AWS Alternativa CLI

Puoi anche controllare lo stato della sincronizzazione con la AWS CLI:

```
aws network-security-manager list-resource-synchronization-statuses \
    --deployment-identifier "deployment-arn-from-step-5"
```

Fase 7: pulire

Se non ti servono più le risorse che hai creato, eliminale al contrario per impedirne l'applicazione e rimuovere le protezioni dalle risorse pertinenti:

L'ordine inverso è importante perché queste risorse fanno riferimento l'una all'altra. Per vedere cosa è associato a una risorsa prima di eliminarla, chiama `ListResourceAssociations` l'ARN di quella risorsa. Restituisce l'ARN e il tipo di risorsa di ogni risorsa associata. Per ulteriori informazioni, consulta il riferimento alle API di AWS Network Security Manager.

1. Nel riquadro di navigazione seleziona Overview (Panoramica). Seleziona la scheda Distribuzioni. Seleziona la tua distribuzione, scegli Azione, quindi scegli Elimina.
2. Scegli la scheda Ambiti. Seleziona il tuo ambito, scegli Azione, quindi scegli Elimina.
3. Scegliere la scheda Policy. Seleziona la tua politica, scegli Azione, quindi scegli Elimina.
4. Scegliere la scheda Templates (Modelli). Seleziona il modello, scegli Azione, quindi scegli Elimina.
5. Scegliere la scheda Rules (Regole). Seleziona la regola, scegli Azione, quindi scegli Elimina.

AWS Alternativa CLI

Prima di eliminare una risorsa, controllane le associazioni per pianificare l'ordine di eliminazione:

```
aws network-security-manager list-resource-associations \
```

```
    --resource-arn "resource-arn"
```

Se una risorsa presenta ancora associazioni, rimuovi o elimina prima le risorse associate. Puoi eliminare le risorse con la AWS CLI in ordine inverso:

```
aws network-security-manager delete-deployment \
    --deployment-identifier "deployment-arn"

aws network-security-manager delete-scope \
    --scope-identifier "scope-arn"

aws network-security-manager delete-policy \
    --policy-identifier "policy-arn"

aws network-security-manager delete-template \
    --template-identifier "template-arn"

aws network-security-manager delete-rule \
    --rule-identifier "rule-arn"
```

Fasi successive

Ora che hai una distribuzione funzionante, esplora i seguenti modi per espandere la protezione della sicurezza della rete:

- Scopri il modello e il ciclo di vita delle risorse in. Come funziona AWS Network Security Manager
- Usa il draft/publish flusso di lavoro per organizzare le modifiche prima che abbiano effetto. Per ulteriori informazioni, consulta the section called “Bozza e ciclo di vita attivo”.
- Crea istantanee per conservare configurazioni già valide. Per ulteriori informazioni, consulta the section called “Controllo delle versioni”.
- Utilizzatelo `GenerateRuleConfiguration` per creare regole a partire da descrizioni in linguaggio naturale. Per ulteriori informazioni, consulta il riferimento alle API AWS di Network Security Manager.
- Esplora la gestione delle protezioni AWS WAF e AWS Shield Advanced nella tua organizzazione. Per ulteriori informazioni, consulta Gestione di firewall e servizi di sicurezza.

Gestione di firewall e servizi di sicurezza

Con AWS Network Security Manager, puoi definire e implementare policy di sicurezza per più firewall e servizi di sicurezza. Sebbene gli elementi comuni coprano il portafoglio di sicurezza di AWS rete, esistono importanti variazioni che è necessario affrontare all'interno di AWS Network Security Manager.

Per ogni servizio di sicurezza di rete supportato, le seguenti sottosezioni descrivono gli elementi e i passaggi unici per una creazione rapida e un processo di creazione dettagliato standard.

Gestione degli ACL Web per AWS WAF

Con AWS Network Security Manager, configuri e distribuisci centralmente gli elenchi di controllo degli accessi Web AWS WAF (ACL Web) tra gli account e le risorse della tua organizzazione. È possibile definire le regole di AWS Network Security Manager per AWS WAF, raggrupparle in modelli di protezione e applicarle su larga scala tramite le politiche e le implementazioni di AWS Network Security Manager.

AWS Concetti WAF

I seguenti concetti sono specifici per l'utilizzo di AWS Network Security Manager con AWS WAF. Per ulteriori informazioni sul funzionamento di AWS Network Security Manager, vedereCome funziona AWS Network Security Manager.

AWS Tipi di regole WAF

Per AWS WAF, una regola è di due tipi:

- ISPEZIONE: contiene una definizione di gruppo di regole che utilizza `PreProcessFirewallManagerRuleGroups` (regole eseguite prima delle regole definite dal cliente) o `PostProcessFirewallManagerRuleGroups` (regole che vengono eseguite dopo).
- CONFIGURAZIONE: contiene una singola impostazione di configurazione ACL Web. La configurazione JSON deve contenere esattamente una chiave di primo livello corrispondente a un'impostazione supportata (ad esempio,`Description`,`DefaultAction`,`VisibilityConfig`,`LoggingConfiguration`,`CaptchaCon` `DataProtectionConfig` `AssociationConfig` `OnSourceDDoSProtectionConfigTokenDomains`, o). `MonetizationConfig`

La maggior parte delle impostazioni di configurazione Web ACL corrisponde ai parametri dell'operazione WAF. AWS `CreateWebACL` Per ulteriori informazioni su queste impostazioni e le relative definizioni, consulta CreateWebACL nel AWS WAF API Reference.

L'eccezione è quella che `LoggingConfiguration` si configura separatamente. Per ulteriori informazioni, consulta the section called “Registrazione dei log”.

AWS Fusione delle politiche WAF

Per AWS WAF, ogni impostazione di configurazione utilizza una delle seguenti strategie di unione:

SingleValue

Impostazioni che possono avere un solo valore. La politica con la priorità più alta vince. I valori di priorità sono univoci, quindi due policy non possono definire valori diversi con la stessa priorità. Per ulteriori informazioni su come AWS Network Security Manager risolve la priorità, vedere. the section called “Priority-based fusione delle politiche” Le seguenti impostazioni utilizzano SingleValue:`DefaultAction`,,`VisibilityConfig`,`CaptchaConfig`,`ChallengeConfig`, `OnSourceDDoSProtectionConfig` `LoggingConfigurationMonetizationConfig`, e. `Description`

Aggiungi (e AppendAndSort)

Le voci di tutte le politiche vengono aggiunte all'elenco in ordine di priorità. `TokenDomainse` `DataProtectionConfig.DataProtections` usa Append. `PreProcessFirewallManagerRuleGroups`and `PostProcessFirewallManagerRuleGroups` use AppendAndSort, che aggiunge i gruppi di regole da tutte le politiche e li ordina per priorità. L'ordine è importante perché AWS WAF valuta i gruppi di regole in sequenza.

Unione

Le voci di tutte le politiche si fondono in un unico set, indipendentemente dalla priorità. `CustomResponseBodiese` `AssociationConfig.RequestBody` usa Merge.

Le strategie Append e Merge rimuovono le voci duplicate. AppendAndSort Quando due policy contribuiscono a una configurazione identica, AWS Network Security Manager esclude la voce dalla policy con priorità più alta. La configurazione effettiva contiene quindi una copia di tale voce, non una copia per ogni policy che contribuisce.

Risoluzione ACL web esistente

Utilizza l'`existingCustomerWebACLResolution`impostazione di una policy AWS WAF per specificare in che modo AWS Network Security Manager gestisce le risorse che dispongono già di un ACL Web gestito dal cliente:

- `RETROFIT`— Aggiorna l'ACL web esistente per allinearlo alla configurazione effettiva.
- `OVERRIDE_ASSOCIATION`— Associate invece alla risorsa un ACL web gestito da AWS Network Security Manager.
- `NO_REMEDIATION`— Non rimediare se il tuo ACL web esiste.

Registrazione del traffico ACL web

È possibile controllare la registrazione ACL Web con l'`LoggingConfiguration`impostazione di un criterio. AWS Network Security Manager applica questa impostazione utilizzando l'operazione AWS `PutLoggingConfiguration` WAF. È possibile definire una sola destinazione di registrazione per ogni ACL Web. Per ulteriori informazioni, vedere PutLoggingConfigurationnel AWS WAF API Reference.

Ogni ACL Web pertinente all'ambito gestito dalla policy invia i propri log alla destinazione specificata dalla policy. In questo modo è possibile centralizzare la registrazione di tutti gli account dell'organizzazione. Usalo per ottenere informazioni dettagliate sul traffico che i tuoi ACL web analizzano a livello di organizzazione.

Per la registrazione centralizzata su più account, puoi inviare i log a un bucket Amazon S3 o a un flusso di distribuzione Amazon Data Firehose. Ogni tipo di destinazione richiede una configurazione aggiuntiva, che devi completare prima che AWS Network Security Manager possa gestire la registrazione AWS WAF tra le risorse e gli account pertinenti. Il nome della destinazione deve iniziare con. `aws-waf-logs-`

Amazon Data Firehose

Crea il flusso di consegna con le seguenti caratteristiche:

- Creato utilizzando l'account amministratore di AWS Network Security Manager
- Un nome che inizia con`aws-waf-logs-`, ad esempio `aws-waf-logs-network-security-manager-central`
- Una PUT fonte

- Creato nella regione in cui operi o nella regione Stati Uniti orientali (Virginia settentrionale) se acquisisci log per Amazon CloudFront

Prima di utilizzare il flusso di distribuzione, testalo per confermare che abbia una velocità di trasmissione sufficiente per i log della tua organizzazione. Per ulteriori informazioni, consulta Creazione di un flusso di distribuzione di Amazon Data Firehose nella Amazon Data Firehose Developer Guide.

Simple Storage Service (Amazon S3)

Crea il bucket seguendo le indicazioni di Amazon S3 nella WAF Developer AWS Guide. È inoltre necessario configurare il bucket con le autorizzazioni che consentono la consegna dei log per scrivere al suo interno. La seguente politica del bucket concede tali autorizzazioni.

```
{
    "Version":"2012-10-17",
    "Id": "AWSLogDeliveryForNetworkSecurityManager",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheckNetworkSecurityManager",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::aws-waf-logs-bucket-suffix"
        },
        {
            "Sid": "AWSLogDeliveryWriteNetworkSecurityManager",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::aws-waf-logs-bucket-suffix/policy-id/AWSLogs/
*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
```

```
}
```

*bucket-suffix*Sostituiscilo con il tuo suffisso del nome del bucket e sostituiscilo *policy-id* con l'ID della tua policy.

> **CloudWatch Logs supporta solo l'uso di un solo account**
>
> Se utilizzi AWS Network Security Manager su più account, non puoi utilizzare un gruppo di log di Amazon CloudWatch Logs come destinazione di registrazione. Il gruppo di log deve trovarsi nello stesso AWS account e nella stessa regione dell'ACL web. Per le distribuzioni con più account, utilizza invece un bucket Amazon S3 o un flusso di distribuzione Amazon Data Firehose.

Creazione rapida per AWS WAF

Con Quick Create, definisci e distribuisci le protezioni AWS WAF in un unico flusso di lavoro guidato. Usa Quick Create quando desideri configurare una protezione ACL web completa dalle regole fino alla distribuzione in un'unica sessione.

Per definire e implementare una protezione AWS WAF con Quick Create, completa le seguenti procedure nell'ordine.

Per creare la policy e aggiungere protezioni

1. Apri la console AWS di Network Security Manager all'indirizzo https://console.aws.amazon.com/network-security-manager/.
2. Nel riquadro di navigazione seleziona Overview (Panoramica).
3. In alto a destra della pagina Panoramica, scegli Creazione e distribuzione rapide. La pagina di creazione e distribuzione rapida viene visualizzata con più riquadri.
4. Nel riquadro dei dettagli della politica, in Nome, inserisci il nome di una politica. (Facoltativo) In Descrizione, immetti una descrizione.
5. Nel riquadro Definisci le protezioni, scegli il tipo di firewall con cui desideri lavorare. Seleziona AWS WAF. Viene visualizzato un riquadro secondario Modelli e regole, in cui è possibile aggiungere regole o modelli.

6. Per aggiungere regole, scegli Aggiungi o gestisci regole. Nella finestra visualizzata, per Seleziona il tipo di regola, scegli una delle seguenti opzioni:
   - AWS Regole gestite: la tabella mostra tutte le regole AWS gestite supportate da AWS WAF.
   - Regole: la tabella mostra i gruppi di regole AWS WAF di cui sei proprietario, oltre alle AWS Managed Rules.

   Seleziona le caselle di controllo relative alle regole che desideri aggiungere alla tua politica. Quindi scegli Aggiungi regole.
7. Per aggiungere modelli, scegli Aggiungi modelli. Nella finestra Aggiungi modelli che appare, la tabella mostra tutti i modelli disponibili. Seleziona i modelli che desideri, insieme alla versione da includere nella politica. Quindi scegli Aggiungi modelli.

Per configurare la politica

1. Controlla le tue selezioni nella tabella Modelli e regole. Il numero intero nella colonna Posizione determina l'ordine di valutazione delle regole e dei modelli. Per modificare l'ordine di valutazione, scegliete il valore della posizione nella colonna Posizione. Utilizzate le frecce per modificare il valore. Per accettare la modifica, scegli Conferma. Per annullare la modifica, scegli Annulla.
2. In Configurazione delle politiche nel riquadro Definisci le protezioni, decidi le azioni automatizzate che AWS Network Security Manager intraprende nell'ambito di destinazione:
   - La riparazione applica la politica definita a tutte le risorse il cui stato di sicurezza non è sincronizzato con lo stato desiderato descritto in AWS Network Security Manager.
   - La pulizia delle risorse elimina il firewall creato da AWS Network Security Manager per una risorsa quando la distribuzione viene rimossa o quando l'account o la risorsa non rientrano nell'ambito.
   - La risoluzione WebACL esistente del cliente determina come risolvere i conflitti tra la politica che state definendo e quella che potrebbe essere già implementata. Dal menu, scegliete una delle seguenti opzioni:
     - Nessuna riparazione salta la riparazione su tutte le risorse che dispongono già di un ACL Web.
     - L'associazione Override sostituisce l'ACL web esistente con l'ACL web creato da Network Security Manager AWS .
     - Retrofit aggiorna le sue regole su ogni ACL web esistente e mantiene l'ACL web associato alla risorsa.

3. Nel riquadro di priorità delle politiche, imposta la priorità. AWS Network Security Manager valuta le politiche in base alla loro priorità per risolvere i conflitti. Le posizioni più basse (numeri interi inferiori) hanno una priorità più alta. Per modificare la priorità, scegliete il valore Posizione. Quindi incrementalo con le frecce o inserisci direttamente un valore. Per confermare la selezione, scegliete Conferma. Per annullare la modifica, scegliete Annulla.

Per impostare l'ambito

1. Nel riquadro Imposta l'ambito, definite il set di risorse a cui si applicano le politiche. Per Nome ambito, inserisci un nome. (Facoltativo) In Descrizione, immetti una descrizione.
2.
> Multi-account solo modalità
>
> Questo passaggio si applica solo alla modalità multi-account. In modalità multi-account, utilizza il riquadro secondario di selezione dell'account e dell'unità organizzativa per scegliere quali account o unità organizzative includere o escludere. In modalità account singolo, questo riquadro secondario non viene visualizzato nella console, quindi salta questo passaggio.

   Nel riquadro secondario di selezione dell'account e dell'unità organizzativa, seleziona una delle seguenti opzioni:
   - Ambito dell'intera AWS organizzazione. Non è richiesta alcuna ulteriore definizione.
   - Riguarda l'intera AWS organizzazione, ma esclude unità organizzative e account specifici. Vengono visualizzati un riquadro secondario Unità organizzative e un riquadro secondario Account. Per escludere le unità organizzative, scegli Aggiungi unità organizzative. Seleziona le unità organizzative nell'albero dell'organizzazione, quindi scegli Aggiungi unità organizzative. Per escludere singoli account, scegli Aggiungi account. Seleziona gli account nell'albero dell'organizzazione, quindi scegli Aggiungi account.
   - Non limitatevi all'intera AWS organizzazione e includete solo unità organizzative e account specifici. Utilizza lo stesso meccanismo Aggiungi unità organizzative e Aggiungi account per includere le unità organizzative e gli account desiderati.
3. Nel riquadro secondario Risorse, per Tipi di risorse, seleziona tutti i tipi di risorse AWS WAF o specifici. Le opzioni sono una o più delle seguenti:
   - Application Load Balancer
   - API REST di Amazon API Gateway

- CloudFront Distribution (Distribuzione)

> **CloudFront Requisiti regionali**
>
> Per proteggere le risorse di CloudFront distribuzione, utilizzate la regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`).

> **Tipi di risorse globali e regionali**
>
> Puoi selezionare il tipo di risorsa globale (CloudFront Distribution) o i tipi di risorse regionali (Application Load Balancer e Amazon API Gateway REST API), ma non entrambi.
> Dopo aver selezionato un tipo di risorsa, non puoi passare dal tipo di risorsa CloudFront Distribution a quello regionale quando aggiorni la configurazione.

> **Risorse non gestite CloudFront**
>
> AWS Network Security Manager non gestisce le CloudFront distribuzioni che utilizzano il piano CloudFront tariffario forfettario o CloudFront le distribuzioni temporanee. Queste risorse sembrano non sincronizzate.

4. Per ogni tipo di risorsa selezionato, scegliete una delle seguenti opzioni che si escludono a vicenda:
   - Includi tutte le risorse
   - Includi risorse specifiche
   - Escludi risorse specifiche
5. Se scegli Includi risorse specifiche, scegli uno dei seguenti tipi di espressione, quindi crea le combinazioni appropriate di tag o ARN:
   - Criteri singoli
   - Soddisfa tutti i criteri (AND)
   - Corrisponde a qualsiasi criterio (OR)
   - NON

Tutti i tipi di risorse hanno i criteri di inclusione Tag e ARN. Se scegli Tag, inserisci una chiave e un valore opzionale. Puoi identificare più tag. Se il tipo di risorsa è Application Load Balancer, viene visualizzato un criterio di configurazione aggiuntivo. In Configurazione, scegliete uno schema, che include le opzioni Internet-facingo Interno.

Per rivedere e implementare la politica

1. Nel riquadro Revisione e distribuzione, per Nome distribuzione, inserisci un nome. (Facoltativo) In Descrizione, immetti una descrizione. Per determinare se il contenuto della distribuzione è visibile agli altri account dell'organizzazione, seleziona Abilita la visibilità tra account per questa distribuzione.
2. (Facoltativo) Per aggiungere tag alla risorsa, scegli Aggiungi nuovo tag, quindi inserisci le combinazioni Chiave e Valore facoltative.
3. Per eseguire ciò che hai definito, scegli Crea e distribuisci. Una volta completato il processo, viene visualizzata la pagina Distribuzioni, in cui è possibile visualizzare i dettagli di ciò che è stato creato.

⚠ Le distribuzioni potrebbero comportare costi

Una distribuzione crea servizi di sicurezza di rete e li collega a una risorsa protetta. AWS Network Security Manager addebita i costi per le risorse protette. I servizi di sicurezza stessi proteggono la risorsa, il che comporta costi aggiuntivi. Prima della distribuzione, consulta la pagina dei prezzi AWS di Network Security Manager e la pagina dei prezzi AWS WAF.

Processo di creazione standard per AWS WAF

Con il processo di creazione standard, puoi creare ogni componente AWS WAF (regole, modelli, politiche, ambiti e implementazioni) individualmente per un controllo completo. Utilizza questo approccio quando desideri creare componenti riutilizzabili e combinarli secondo necessità.

Una policy AWS WAF di AWS Network Security Manager può contenere regole e modelli. Quando si applica la policy, AWS Network Security Manager crea un ACL web in ogni account pertinente.

Per creare una regola (console)

1. Accedi alla Console di AWS gestione utilizzando il tuo account amministratore di AWS Network Security Manager, quindi apri la console AWS Network Security Manager all'indirizzo. https://console.aws.amazon.com/network-security-manager/

   > Configurazione dell'account amministratore
   >
   > Per informazioni sulla configurazione di un account amministratore di AWS Network Security Manager, vedereConfigurazione di AWS Network Security Manager.

2. Nel pannello di navigazione, scegli AWS Network Security Manager, quindi Panoramica.
3. Nel riquadro Panoramica, scegli Crea regola. Inserisci un nome descrittivo, quindi inserisci una descrizione facoltativa.
4. Nel riquadro di definizione delle regole, per Tipo di firewall, scegli AWS WAF.
5. Per Tipo di regola, scegli Ispezione o Configurazione.

   Se scegli Inspection, viene visualizzato un riquadro dell'editor JSON denominato Define rule group reference con le seguenti opzioni:

   - Inserisci modello: seleziona un modello JSON per le regole First (pre-elaborazione) o Last (post-elaborazione). Quando effettui una selezione, AWS Network Security Manager inserisce il JSON corrispondente nell'editor, insieme alle icone di avviso se sono necessari input per completare il modello.
   - Inserisci gruppo di regole: presenta un elenco di selezione basato su tre opzioni:
     - Un gruppo di regole AWS Managed Rules (AMR)
     - Un gruppo di regole personalizzato esistente
     - Un gruppo di regole AWS del Marketplace

     AWS Network Security Manager presenta i gruppi di regole associati alla tua scelta e puoi selezionare una singola istanza da includere. Dopo aver effettuato la selezione, scegli Seleziona gruppo di regole. AWS Network Security Manager inserisce i riferimenti alla regola di ispezione con la sintassi corretta nell'editor JSON.
   - Inserisci con AI: apre una finestra di sovrapposizione denominata generatore di configurazione AI. Usa questo strumento per descrivere la tua regola in un linguaggio semplice e AWS Network Security Manager genera il JSON associato nell'editor. È quindi possibile rivedere il codice generato e scegliere di accettare, modificare o eliminare l'output.

6. (Facoltativo) Una volta completata la definizione della regola JSON, puoi associare un tag alla regola. Scegli Add new tag (Aggiungi nuovo tag) e completa i campi Key (Chiave) e facoltativamente Value (Valore).
7. Al termine delle definizioni, scegli Salva bozza per salvare un oggetto inattivo, potenzialmente incompleto, oppure Crea regola.

> ⚠ I nomi Web ACL sono permanenti
>
> Non è possibile modificare un nome ACL Web dopo averlo creato. Se si aggiorna il nome della politica, AWS Network Security Manager non aggiorna il nome ACL Web associato. Per fare in modo che AWS Network Security Manager crei un ACL Web con un nome diverso, è necessario creare una nuova politica.

Per creare un modello (console)

Un modello riunisce le regole in ordine di priorità per la valutazione all'interno di una politica. Puoi organizzare i tipi di regole in raggruppamenti in linea con i tuoi obiettivi di sicurezza. Puoi anche consentire a diversi team di creare dichiarazioni di controllo di sicurezza in linea con le loro responsabilità e competenze.

1. Nella pagina Panoramica, nel riquadro Panoramica, scegli Crea modello. Nella pagina Crea modello, inserisci un nome per il modello, inserisci una descrizione opzionale e scegli un tipo di firewall (in questo caso, AWS WAF).
2. Quando scegli un tipo di firewall, viene visualizzato il riquadro Regole. Scegli uno dei due pulsanti Aggiungi regole per aprire un elenco di regole disponibili. Seleziona la casella di controllo a sinistra del nome di una regola per aggiungerla al modello. Per scegliere una versione specifica di una regola, seleziona il campo Versione della regola. Se sono disponibili più versioni, seleziona la versione desiderata, quindi scegli Conferma.
3. (Facoltativo) Crea un tag per il modello. Al termine, scegli Salva bozza o Crea modello. Per continuare a creare una politica, scegli Crea modello.

Per creare una policy - (console)

Questa è la fase finale della definizione delle politiche e della preparazione per l'implementazione.

1. Nella pagina Panoramica, nel riquadro Panoramica, scegli Crea politica. Nella pagina Crea policy, inserisci un nome e una descrizione facoltativa, quindi scegli un tipo di firewall (in questo caso, AWS WAF).
2. Nel riquadro di priorità delle politiche, imposta la priorità. AWS Network Security Manager valuta le politiche in base alla loro priorità per risolvere i conflitti. Le posizioni più basse (numeri interi inferiori) hanno una priorità più alta. Per modificare la priorità, scegliete il valore Posizione. Quindi incrementalo con le frecce o inserisci direttamente un valore. Per confermare la selezione, scegliete Conferma. Per annullare la modifica, scegliete Annulla.
3. Nel riquadro di configurazione della politica, decidi le azioni automatiche che AWS Network Security Manager intraprende nell'ambito di destinazione:
   - La riparazione applica la politica definita a tutte le risorse il cui stato di sicurezza non è sincronizzato con lo stato desiderato descritto in AWS Network Security Manager.
   - La pulizia delle risorse elimina il firewall creato da AWS Network Security Manager per una risorsa quando la distribuzione viene rimossa o quando l'account o la risorsa non rientrano nell'ambito.
   - La risoluzione WebACL esistente del cliente determina come risolvere i conflitti tra la politica che state definendo e quella che potrebbe essere già implementata. Dal menu, scegliete una delle seguenti opzioni:
     - Nessuna riparazione salta la riparazione su tutte le risorse che dispongono già di un ACL Web.
     - L'associazione Override sostituisce l'ACL web esistente con l'ACL web creato da Network Security Manager AWS .
     - Retrofit aggiorna le sue regole su ogni ACL web esistente e mantiene l'ACL web associato alla risorsa.
4. Una volta completate queste impostazioni di configurazione, selezionate le regole e i modelli che desiderate aggiungere alla policy. Nel riquadro Modelli e regole, scegli Aggiungi regole o Aggiungi modelli per compilare la politica. Entrambi i processi aprono una finestra che funziona allo stesso modo del processo di selezione delle regole descritto in precedenza in questa sezione.

Per creare un ambito (console)

1. È possibile iniziare questo passaggio dalla pagina Panoramica o da altre aree all'interno dello strumento. Nel riquadro dei dettagli dell'ambito, inserisci un nome dell'ambito e una descrizione opzionale.

2. **Multi-account solo modalità**

   Questo passaggio si applica solo alla modalità multi-account. In modalità multi-account, utilizza il riquadro secondario di selezione dell'account e dell'unità organizzativa per scegliere quali account o unità organizzative includere o escludere. In modalità account singolo, questo riquadro secondario non viene visualizzato nella console, quindi salta questo passaggio.

   Nel riquadro di selezione Account e unità organizzativa, scegli uno dei tre metodi per controllare l'ambito amministrativo:

   - Ambito AWS dell'intera organizzazione (tutte le unità organizzative e gli account): non è richiesta alcuna ulteriore definizione.
   - Riguarda l'intera AWS organizzazione ma esclude unità organizzative e account specifici: vengono visualizzati due riquadri secondari, uno per le unità organizzative e uno per gli account. Scegli Aggiungi unità organizzative per aprire la finestra Aggiungi unità organizzative, seleziona le unità organizzative necessarie dall'albero dell'organizzazione, quindi scegli Aggiungi unità organizzative. Per aggiungere singoli account, nel riquadro secondario Account, scegli Aggiungi account, seleziona gli account dall'albero dell'organizzazione e quindi scegli Aggiungi account.
   - Non limitarti all'intera AWS organizzazione, ma includi solo unità organizzative e account specifici: utilizza gli stessi pannelli secondari per aggiungere unità organizzative o account con lo stesso meccanismo descritto per l'opzione precedente.

3. Quindi, seleziona le risorse nel riquadro secondario Risorse. Nella casella di selezione Tipi di risorse, selezionate tutti i tipi di risorse AWS WAF o specifici. Per AWS WAF, le opzioni sono una o tutte le seguenti:

   - Application Load Balancer
   - API REST di Amazon API Gateway
   - CloudFront Distribution (Distribuzione)

   CloudFront Requisiti regionali

   Per proteggere le risorse di CloudFront distribuzione, utilizzate la regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`).

> **Tipi di risorse globali e regionali**
>
> Puoi selezionare il tipo di risorsa globale (CloudFront Distribution) o i tipi di risorse regionali (Application Load Balancer e Amazon API Gateway REST API), ma non entrambi.
> Dopo aver selezionato un tipo di risorsa, non puoi passare dal tipo di risorsa CloudFront Distribution a quello regionale quando aggiorni la configurazione.

> **Risorse non gestite CloudFront**
>
> AWS Network Security Manager non gestisce le CloudFront distribuzioni che utilizzano il piano CloudFront tariffario forfettario o CloudFront le distribuzioni temporanee. Queste risorse sembrano non sincronizzate.

4. Per ogni tipo di risorsa selezionato, scegliete una delle seguenti opzioni che si escludono a vicenda:
   - Includi tutte le risorse
   - Includi risorse specifiche
   - Escludi risorse specifiche
5. Se scegli Includi risorse specifiche, seleziona uno dei seguenti tipi di espressione:
   - Criteri singoli
   - Soddisfa tutti i criteri (AND)
   - Corrisponde a qualsiasi criterio (OR)
   - NON
6. Ogni tipo di espressione supporta criteri di inclusione e ARN singoli o multipli, quindi puoi creare combinazioni di tag o ARN. Tutti i tipi di risorse supportano i criteri di inclusione Tag e ARN. Se scegli Tag, identifica una chiave e un valore opzionale. Puoi identificare più tag.
7. Per un Application Load Balancer, viene visualizzato un criterio di configurazione aggiuntivo. All'interno di Configuration, è possibile impostare uno schema con le opzioni Internet-facingInternal.

Per creare una distribuzione (console)

Una distribuzione vincola le politiche a un ambito e ne attiva l'applicazione, il che fa sì che AWS Network Security Manager applichi le regole AWS WAF alle risorse pertinenti.

1. Nella pagina Panoramica, nel riquadro Panoramica, scegli Crea distribuzione. Puoi iniziare questo passaggio anche da altre aree dello strumento.
2. Scegli la politica che desideri implementare.
3. Scegli l'ambito che definisce gli account e le risorse in cui AWS Network Security Manager applica la politica.
4. Per Nome della distribuzione, inserisci un nome. (Facoltativo) In Descrizione, immetti una descrizione.
5. (Facoltativo) Per rendere la distribuzione visibile agli altri account dell'organizzazione, seleziona Abilita la visibilità tra account per questa distribuzione.
6. (Facoltativo) Per aggiungere tag, scegli Aggiungi nuovo tag, quindi inserisci le combinazioni di chiavi e valori opzionali.
7. Scegliere Create and deploy (Crea e implementa). Viene visualizzata la pagina Distribuzioni, in cui è possibile visualizzare i dettagli di ciò che AWS Network Security Manager ha creato.

⚠ Le distribuzioni potrebbero comportare costi

Una distribuzione crea servizi di sicurezza di rete e li collega a una risorsa protetta. AWS Network Security Manager addebita i costi per le risorse protette. I servizi di sicurezza stessi proteggono la risorsa, il che comporta costi aggiuntivi. Prima della distribuzione, consulta la pagina dei prezzi AWS di Network Security Manager e la pagina dei prezzi AWS WAF.

Gestione delle protezioni DDoS per AWS Shield Advanced

Con AWS Network Security Manager, configuri e distribuisci centralmente le protezioni AWS Shield Advanced tra account e risorse della tua organizzazione. È possibile definire politiche di protezione DDoS e applicarle su larga scala tramite le politiche e le implementazioni di AWS Network Security Manager.

AWS Network Security Manager viene fatturato separatamente

AWS Network Security Manager non fa parte dell'offerta AWS Shield Advanced. Per ulteriori informazioni sui prezzi, consulta i prezzi di AWS Network Security Manager e i prezzi di AWS Shield Advanced.

AWS Abbonamento Shield Advanced

Quando una distribuzione attiva include un account nel suo ambito, AWS Network Security Manager sottoscrive tale account a AWS Shield Advanced. AWS Network Security Manager non annulla l'abbonamento quando l'account esce dall'ambito o quando si rimuove la distribuzione. Per annullare un abbonamento a AWS Shield Advanced, consulta la sezione Abbonamento a AWS Shield Advanced nella AWS WAF Developer Guide.

Creazione rapida per AWS Shield Advanced

Con Quick Create, definisci e distribuisci le protezioni AWS Shield Advanced in un unico flusso di lavoro guidato. Usa Quick Create quando desideri configurare la protezione DDoS dalle policy fino alla distribuzione in un'unica sessione.

Per definire e implementare una protezione AWS Shield Advanced con Quick Create, completa le seguenti procedure nell'ordine.

Per creare la policy e configurare le protezioni

Completa questa procedura:

1. Apri la console AWS di Network Security Manager all'indirizzo https://console.aws.amazon.com/network-security-manager/.
2. Nel riquadro di navigazione seleziona Overview (Panoramica).
3. Nella pagina Panoramica, scegli Creazione e distribuzione rapide. La pagina di creazione e distribuzione rapida viene visualizzata con più riquadri.
4. Nel riquadro dei dettagli della politica, in Nome, inserisci il nome di una politica. (Facoltativo) In Descrizione, immetti una descrizione.

5. Nel riquadro Definisci le protezioni, scegli il tipo di firewall con cui desideri lavorare. Seleziona AWS Shield Advanced.
6. In Configurazione delle politiche nel riquadro Definisci le protezioni, decidi le azioni automatizzate che AWS Network Security Manager intraprende nell'ambito mirato:
   - Remediation applica la policy definita a tutte le risorse il cui stato di sicurezza non corrisponde allo stato desiderato descritto da AWS Network Security Manager.
   - La pulizia delle risorse elimina la protezione DDoS creata da AWS Network Security Manager per una risorsa quando la distribuzione viene rimossa o quando l'account o la risorsa non rientrano nell'ambito.
   - La risoluzione degli attacchi DDoS dei clienti esistenti determina come risolvere i conflitti tra la politica che si sta definendo e quella che potrebbe essere già implementata. Dal menu, scegli una delle seguenti opzioni:
     - Nessuna riparazione salta la correzione su tutte le risorse che dispongono già di una protezione DDoS.
     - L'associazione Override sostituisce la protezione DDoS esistente con la protezione DDoS creata da Network Security Manager AWS .
     - Retrofit aggiorna le proprie regole su ogni protezione DDoS esistente e mantiene la protezione DDoS associata alla risorsa.
7. Nel riquadro Priorità delle politiche, imposta la priorità. AWS Network Security Manager valuta le politiche in base alla loro priorità per risolvere i conflitti. Le posizioni più basse (numeri interi inferiori) hanno una priorità più alta.

   Per modificare la priorità, scegliete il valore Posizione. Quindi incrementalo con le frecce o inserisci direttamente un valore. Per confermare la selezione, scegliete Conferma. Per annullare la modifica, scegliete Annulla.

Per impostare l'ambito

Completa questa procedura:

1. Nel riquadro Imposta l'ambito, definite il set di risorse a cui si applicano le politiche. Per Nome dell'ambito, inserisci un nome. (Facoltativo) In Descrizione, immetti una descrizione.

2.

> **Multi-account solo modalità**
>
> Questo passaggio si applica solo alla modalità multi-account. In modalità multi-account, utilizza il riquadro secondario di selezione dell'account e dell'unità organizzativa per scegliere quali account o unità organizzative includere o escludere. In modalità account singolo, questo riquadro secondario non viene visualizzato nella console, quindi salta questo passaggio.

Nel riquadro secondario di selezione dell'account e dell'unità organizzativa, seleziona una delle seguenti opzioni:

- Ambito dell'intera AWS organizzazione. Non è richiesta alcuna ulteriore definizione.
- Riguarda l'intera AWS organizzazione, ma esclude unità organizzative e account specifici. Vengono visualizzati un riquadro secondario Unità organizzative e un riquadro secondario Account. Per escludere le unità organizzative, scegli Aggiungi unità organizzative. Seleziona le unità organizzative nell'albero dell'organizzazione, quindi scegli Aggiungi unità organizzative. Per escludere singoli account, scegli Aggiungi account. Seleziona gli account nell'albero dell'organizzazione, quindi scegli Aggiungi account.
- Non limitatevi all'intera AWS organizzazione e includete solo unità organizzative e account specifici. Utilizza lo stesso meccanismo Aggiungi unità organizzative e Aggiungi account per includere le unità organizzative e gli account desiderati.

3. Nel riquadro secondario Risorse, per Tipi di risorse, seleziona tutti o alcuni tipi di risorse AWS Shield Advanced. Le opzioni sono una o più delle seguenti:
   - Application Load Balancer
   - CloudFront Distribution (Distribuzione)
   - Classic Load Balancer
   - indirizzo IP elastico
4. Per ogni tipo di risorsa selezionato, scegliete una delle seguenti opzioni che si escludono a vicenda:
   - Includi tutte le risorse
   - Includi risorse specifiche
   - Escludi risorse specifiche
5. Se scegli Includi risorse specifiche, scegli uno dei seguenti tipi di espressione, quindi crea le combinazioni appropriate di tag o ARN:

- Criteri singoli
- Soddisfa tutti i criteri (AND)
- Corrisponde a qualsiasi criterio (OR)
- NON

Tutti i tipi di risorse hanno i criteri di inclusione Tag e ARN. Se scegliete Tag, inserite una chiave e un valore opzionale. Puoi identificare più tag.

> **CloudFront Requisito regionale**
>
> Per proteggere le risorse di CloudFront distribuzione, utilizzate la regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`).

Per rivedere e implementare la politica

Completa questa procedura:

1. Nel riquadro Revisione e distribuzione, per Nome distribuzione, inserisci un nome. (Facoltativo) In Descrizione, immetti una descrizione. Per determinare se il contenuto della distribuzione è visibile agli altri account dell'organizzazione, seleziona Abilita la visibilità tra account per questa distribuzione.
2. (Facoltativo) Per aggiungere tag alla risorsa, scegli Aggiungi nuovo tag, quindi inserisci le combinazioni Chiave e Valore facoltative.
3. Per creare e implementare la politica e l'ambito, scegli Crea e distribuisci. Al termine del processo, viene visualizzata la pagina Distribuzioni, in cui è possibile visualizzare i dettagli di ciò che AWS Network Security Manager ha creato.

> **Le distribuzioni potrebbero comportare costi**
>
> Una distribuzione crea servizi di sicurezza di rete e li collega a una risorsa protetta. AWS Network Security Manager addebita i costi per le risorse protette. I servizi di sicurezza stessi proteggono la risorsa, il che comporta costi aggiuntivi. Prima della distribuzione, consulta la pagina dei prezzi di AWS Network Security Manager e la pagina dei prezzi di AWS Shield Advanced.

Processo di creazione standard per AWS Shield Advanced

Con il processo di creazione standard, puoi configurare ogni componente di AWS Shield Advanced (politiche, ambiti e implementazioni) individualmente per il controllo completo. Utilizza questo approccio quando desideri creare componenti riutilizzabili e combinarli secondo necessità.

Una policy AWS Shield Advanced è semplice e non contiene regole, gruppi di regole o modelli. Quando si applica la policy, AWS Network Security Manager crea una protezione DDoS AWS Shield Advanced in ogni account interessato. Per informazioni sul funzionamento di AWS Network Security Manager, consulta. Come funziona AWS Network Security Manager

Per creare una policy - (console)

Completa questa procedura:

1. Accedere alla Console di AWS gestione utilizzando l'account amministratore di AWS Network Security Manager, quindi aprire la console di AWS Network Security Manager all'indirizzo https://console.aws.amazon.com/network-security-manager/.

   > Configurazione dell'account amministratore
   >
   > Per informazioni sulla configurazione di un account amministratore di AWS Network Security Manager, vedereConfigurazione di AWS Network Security Manager.

2. Nel pannello di navigazione, scegli AWS Network Security Manager, quindi Panoramica.
3. Nel riquadro Panoramica, scegli Crea politica. Immettete un nome e una descrizione facoltativa, quindi scegliete un tipo di firewall (in questo caso, AWS Shield Advanced).
4. Nel riquadro di priorità delle politiche, imposta la priorità. AWS Network Security Manager valuta le politiche in base alla loro priorità per risolvere i conflitti. Le posizioni più basse (numeri interi inferiori) hanno una priorità più alta.

   Per modificare la priorità, scegliete il valore Posizione. Quindi incrementalo con le frecce o inserisci direttamente un valore. Per confermare la selezione, scegliete Conferma. Per annullare la modifica, scegliete Annulla.
5. Nel riquadro di configurazione della politica, decidi le azioni automatiche che AWS Network Security Manager intraprende nell'ambito di destinazione:
   - La riparazione applica la politica definita a tutte le risorse il cui stato di sicurezza non corrisponde allo stato desiderato descritto da AWS Network Security Manager.

- La pulizia delle risorse elimina la protezione DDoS creata da AWS Network Security Manager per una risorsa quando la distribuzione viene rimossa o quando l'account o la risorsa non rientrano nell'ambito.
- La risoluzione degli attacchi DDoS dei clienti esistenti determina come risolvere i conflitti tra la politica che si sta definendo e quella che potrebbe essere già implementata. Dal menu, scegli una delle seguenti opzioni:
  - Nessuna riparazione salta la correzione su tutte le risorse che dispongono già di una protezione DDoS.
  - L'associazione Override sostituisce la protezione DDoS esistente con la protezione DDoS creata da Network Security Manager AWS .
  - Retrofit aggiorna le proprie regole su ogni protezione DDoS esistente e mantiene la protezione DDoS associata alla risorsa.

Per creare un ambito (console)

Completa questa procedura:

1. Nel riquadro dei dettagli dell'ambito, inserisci un nome dell'ambito e una descrizione opzionale.
2.
   > **Multi-account solo modalità**
   >
   > Questo passaggio si applica solo alla modalità multi-account. In modalità multi-account, utilizza il riquadro secondario di selezione dell'account e dell'unità organizzativa per scegliere quali account o unità organizzative includere o escludere. In modalità account singolo, questo riquadro secondario non viene visualizzato nella console, quindi salta questo passaggio.

   Nel riquadro di selezione Account e unità organizzativa, scegli uno dei tre metodi per controllare l'ambito amministrativo:
   - Ambito AWS dell'intera organizzazione (tutte le unità organizzative e gli account): non è richiesta alcuna ulteriore definizione.
   - Riguarda l'intera AWS organizzazione ma esclude unità organizzative e account specifici: vengono visualizzati due riquadri secondari, uno per le unità organizzative e uno per gli account. Scegli Aggiungi unità organizzative per aprire la finestra Aggiungi unità organizzative, seleziona le unità organizzative necessarie, quindi scegli Aggiungi unità organizzative. Per aggiungere

singoli account, nel riquadro secondario Account, scegli Aggiungi account, seleziona gli account e quindi scegli Aggiungi account.

- Non limitarti all'intera AWS organizzazione, ma includi solo unità organizzative e account specifici: utilizza gli stessi pannelli secondari per aggiungere unità organizzative o account.

3. Quindi, seleziona le risorse nel riquadro secondario Risorse. Nella casella di selezione Tipi di risorse, selezionate tutti o alcuni tipi di risorse AWS Shield Advanced. Per AWS Shield Advanced, le opzioni sono una o tutte le seguenti:
   - Application Load Balancer
   - CloudFront Distribution (Distribuzione)
   - Classic Load Balancer
   - indirizzo IP elastico
4. Per ogni tipo di risorsa selezionato, scegliete una delle seguenti opzioni che si escludono a vicenda:
   - Includi tutte le risorse
   - Includi risorse specifiche
   - Escludi risorse specifiche
5. Se scegli Includi risorse specifiche, seleziona uno dei seguenti tipi di espressione:
   - Criteri singoli
   - Soddisfa tutti i criteri (AND)
   - Corrisponde a qualsiasi criterio (OR)
   - NON
6. Ogni tipo di espressione supporta criteri di inclusione e ARN singoli o multipli, quindi puoi creare combinazioni di tag o ARN. Tutti i tipi di risorse supportano i criteri di inclusione Tag e ARN. Se scegli Tag, identifica una chiave e un valore opzionale. Puoi identificare più tag.

> **CloudFront Requisito regionale**
>
> Per proteggere le risorse di CloudFront distribuzione, utilizzate la regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`).

Per creare una distribuzione (console)

Una distribuzione vincola le politiche a un ambito e ne attiva l'applicazione. AWS Network Security Manager applica quindi le protezioni DDoS AWS Shield Advanced alle risorse pertinenti.

Completa questa procedura:

1. Nella pagina Panoramica, nel riquadro Panoramica, scegli Crea distribuzione.
2. Scegli la politica che desideri implementare.
3. Scegli l'ambito che definisce gli account e le risorse in cui AWS Network Security Manager applica la politica.
4. Per Nome della distribuzione, inserisci un nome. (Facoltativo) In Descrizione, immetti una descrizione.
5. (Facoltativo) Per rendere la distribuzione visibile agli altri account dell'organizzazione, seleziona Abilita la visibilità tra account per questa distribuzione.
6. (Facoltativo) Per aggiungere tag, scegli Aggiungi nuovo tag, quindi inserisci le combinazioni di chiavi e valori opzionali.
7. Scegliere Create and deploy (Crea e implementa). Viene visualizzata la pagina Distribuzioni, in cui è possibile visualizzare i dettagli di ciò che AWS Network Security Manager ha creato.

⚠ Le distribuzioni potrebbero comportare costi

Una distribuzione crea servizi di sicurezza di rete e li collega a una risorsa protetta. AWS Network Security Manager addebita i costi per le risorse protette. I servizi di sicurezza stessi proteggono la risorsa, il che comporta costi aggiuntivi. Prima della distribuzione, consulta la pagina dei prezzi di AWS Network Security Manager e la pagina dei prezzi di AWS Shield Advanced.

AWS Network Security Manager e AWS Firewall Manager

AWS Network Security Manager è il servizio che sostituisce AWS Firewall Manager. I due sono servizi completamente separati, ciascuno con funzionalità uniche e un modello di prezzo diverso. Se attualmente utilizzi AWS Firewall Manager, non devi intraprendere alcuna azione: i firewall e le policy esistenti continuano a funzionare. Questo capitolo descrive come coesistono i due servizi, come funziona la precedenza quando si utilizzano entrambi e come funzionerà la migrazione quando sarà disponibile.

AWS Network Security Manager e AWS Firewall Manager operano fianco a fianco e indipendentemente l'uno dall'altro. A un certo punto, AWS Firewall Manager smetterà di essere venduto e quindi smetterà di funzionare.

Coesistenza con AWS Firewall Manager

AWS Network Security Manager non influisce sui firewall creati con AWS Firewall Manager a meno che non si avvii un'azione per modificarli. I firewall e le policy creati con AWS Firewall Manager continuano a funzionare a meno che non vengano terminati. Ciò è vero anche dopo il ritiro di AWS Firewall Manager.

Precedenza durante la riparazione

Mentre entrambi i servizi sono operativi, è possibile intraprendere azioni che influiscono sui firewall creati con AWS Firewall Manager. Quando si creano le policy di AWS Network Security Manager, le si applica a un ambito, che è un insieme di risorse di destinazione. Se tale ambito include risorse già affrontate da una policy di AWS Firewall Manager, AWS Network Security Manager ha la precedenza durante la riparazione. In tal caso, la politica e l'ambito di AWS Network Security Manager sostituiscono il AWS firewall e la politica esistenti di Firewall Manager. Il comportamento specifico dipende dalle opzioni di risoluzione selezionate.

Migrazione pianificata da AWS Firewall Manager

La migrazione da AWS Firewall Manager a AWS Network Security Manager consolida la gestione del firewall in un unico servizio e consente di utilizzarne le funzionalità. La migrazione è pianificata ma non è ancora disponibile. Quando la migrazione sarà disponibile, sarà possibile spostare le policy di

AWS Firewall Manager in AWS Network Security Manager. La migrazione richiederà nuove azioni in entrambi i servizi che non sono ancora state implementate.

Il processo pianificato copierà una policy selezionata da AWS Firewall Manager, la trasferirà a AWS Network Security Manager e la tradurrà nella nuova struttura di policy. Questo processo non influisce sulla policy originale o sui firewall associati in AWS Firewall Manager.

Sicurezza in AWS Responsabile della sicurezza di rete

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. Third-party i revisori 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 a AWS Network Security Manager, vedere AWS Servizi nell'ambito del programma di conformitàAWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Inoltre, sei responsabile anche di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza AWS Network Security Manager. I seguenti argomenti mostrano come configurare AWS Network Security Manager 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 AWS Network Security Manager.

Argomenti

- Protezione dei dati in AWS Responsabile della sicurezza di rete
- Gestione delle identità e degli accessi per AWS Responsabile della sicurezza di rete
- Utilizzo di ruoli collegati ai servizi per AWS Responsabile della sicurezza di rete
- Convalida della conformità per AWS Responsabile della sicurezza di rete
- Resilienza in AWS Responsabile della sicurezza di rete
- Sicurezza dell'infrastruttura in AWS Responsabile della sicurezza di rete
- Le migliori pratiche di sicurezza per AWS Responsabile della sicurezza di rete

Protezione dei dati in AWS Responsabile della sicurezza di rete

Il modello di responsabilità AWS condivisa (modello di) si applica alla protezione dei dati in AWS Network Security Manager. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, consulta Domande frequenti sulla privacy dei dati . Per ulteriori informazioni sulla protezione dei dati in Europa, consulta il Centro generale sulla protezione dei dati (GDPR).

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

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

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

Crittografia dei dati a riposo

AWS Network Security Manager crittografa tutti i dati inattivi utilizzando le AWS chiavi Key Management Service (AWS KMS). Service-managed Le chiavi KMS proteggono le configurazioni delle risorse, lo stato di distribuzione e i dati di sincronizzazione. Non è necessario configurare o gestire queste chiavi.

Crittografia dei dati in transito

AWS Network Security Manager crittografa tutti i dati in transito utilizzando Transport Layer Security (TLS). Tutte le richieste API richiedono TLS 1.2 o versione successiva. Le connessioni agli endpoint dell'API AWS Network Security Manager utilizzano esclusivamente HTTPS.

Gestione delle chiavi

AWS Network Security Manager utilizza chiavi AWS KMS gestite dal servizio per la crittografia a riposo. Al momento non è possibile fornire le proprie chiavi KMS.

Gestione delle identità e degli accessi per AWS Responsabile della sicurezza di rete

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

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell’accesso tramite policy
- In che modo AWS Network Security Manager funziona con IAM
- Identity-based esempi di policy per AWS Responsabile della sicurezza di rete
- Risoluzione dei problemi AWS Identità e accesso di Network Security Manager

Destinatari

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

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta Risoluzione dei problemi AWS Identità e accesso di Network Security Manager)
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta In che modo AWS Network Security Manager funziona con IAM)
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta Identity-based esempi di policy per AWS Responsabile della sicurezza di rete)

Autenticazione con identità

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

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

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

Account AWS utente root

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

Identità federata

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

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

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

Utenti e gruppi IAM

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

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

Ruoli IAM

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

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

Gestione dell'accesso tramite policy

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

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

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

Identity-based politiche

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

Identity-based le politiche possono essere politiche in linea (incorporate direttamente in una singola identità) o politiche gestite (politiche autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scegliere tra policy gestite e policy in linea nella Guida per l'utente di IAM.

Resource-based politiche

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

Resource-based le politiche sono politiche in linea che si trovano in quel servizio. Non è possibile utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Altri tipi di policy

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

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.

- Policy di controllo dei servizi (SCP): specifica il numero massimo di autorizzazioni per un'organizzazione o un'unità organizzativa (OU) in AWS Organizations. Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di controllo delle risorse (RCP): imposta le autorizzazioni massime disponibili per le risorse degli account. Per ulteriori informazioni, consulta Policy di controllo delle risorse (RCP) nella Guida per l'utente di AWS Organizations .
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

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

In che modo AWS Network Security Manager funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS Network Security Manager, scopri quali funzionalità IAM sono disponibili per l'uso con AWS Network Security Manager.

Funzionalità IAM	AWS Supporto per Network Security Manager
Identity-based politiche	Sì
Resource-based politiche	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì

Funzionalità IAM	AWS Supporto per Network Security Manager
Autorizzazioni del principale	Sì
Ruoli di servizio	Sì
Service-linked ruoli	Sì

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

Identity-based politiche per AWS Responsabile della sicurezza di rete

Supporta le policy basate sull'identità: sì

Identity-based le policy sono documenti di policy sulle autorizzazioni JSON che puoi allegare a un'identità, ad esempio un utente IAM, un gruppo di utenti o un ruolo. Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente di IAM.

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

Resource-based politiche interne AWS Responsabile della sicurezza di rete

Supporta le policy basate su risorse: no

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

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

AWS Network Security Manager non supporta politiche basate sulle risorse.

Azioni politiche per AWS Responsabile della sicurezza di rete

Supporta le operazioni di policy: si

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

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

Per visualizzare un elenco delle azioni di AWS Network Security Manager, vedere Azioni definite da AWS Network Security Manager nel Service Authorization Reference.

Le azioni politiche in AWS Network Security Manager utilizzano il seguente prefisso prima dell'azione:

```
network-security-manager
```

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

```
"Action": [
      "network-security-manager:action1",
      "network-security-manager:action2"
         ]
```

AWS Network Security Manager definisce le azioni IAM tra i suoi tipi di risorse. Queste includono le operazioni di creazione, lettura, aggiornamento ed eliminazione (CRUD) per regole, modelli, politiche, ambiti e implementazioni, oltre alle operazioni di snapshot, tagging, amministrative, sullo stato di sincronizzazione e sull'associazione delle risorse.

Risorse politiche per AWS Responsabile della sicurezza di rete

Supporta le risorse relative alle policy: sì

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

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di risorse di AWS Network Security Manager e dei relativi ARN, vedere Resources Defined by AWS Network Security Manager nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare l'ARN di ogni risorsa, vedere Azioni definite da AWS Network Security Manager.

AWS Network Security Manager definisce un tipo di risorsa IAM per ciascuna delle relative risorse (regola, modello, policy, ambito e distribuzione), oltre a un tipo di snapshot per ciascuna di esse (ad esempio,`rule-snapshot`). Il formato ARN è:

```
arn:aws:network-security-manager:{region}:{account}:{resource-type}:{resource-id}
```

Gli ARN di bozza aggiungono `:DRAFT` e gli ARN di snapshot aggiungono il numero di versione (ad esempio,). `:3`

Le bozze non sono tipi di risorse IAM separati. Ai fini dell'autorizzazione, una bozza viene considerata come un elemento secondario della relativa risorsa attiva, che è la fonte principale. Un ARN `:DRAFT` qualificato autorizza la risorsa attiva, quindi l'autorizzazione ad agire su una bozza deriva dall'autorizzazione ad agire su quella risorsa attiva.

Le istantanee differiscono dalle bozze. Ogni snapshot è un tipo di risorsa IAM a sé stante, quindi un ARN con certificazione di versione effettua l'autorizzazione direttamente su quel tipo di risorsa snapshot, non sulla risorsa attiva principale.

Chiavi relative alle condizioni delle policy per AWS Responsabile della sicurezza di rete

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

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

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

Per visualizzare un elenco delle chiavi di condizione di AWS Network Security Manager, consulta Condition Keys for AWS Network Security Manager nel Service Authorization Reference. Per sapere con quali azioni e risorse è possibile utilizzare una chiave di condizione, vedere Azioni definite da AWS Network Security Manager.

AWS Network Security Manager supporta le seguenti chiavi AWS globali di condizione dei tag per il controllo degli accessi basato sugli attributi (ABAC):

- `aws:ResourceTag/${TagKey}`
- `aws:RequestTag/${TagKey}`
- `aws:TagKeys`

Tag-based le chiavi di condizione si applicano alle risorse e alle istantanee attive. Le bozze di risorse non sono etichettabili e non supportano condizioni. `aws:ResourceTag`

ACL in AWS Responsabile della sicurezza di rete

Supporta le ACL: no

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

AWS Network Security Manager non supporta gli elenchi di controllo degli accessi (ACL).

ABAC con AWS Responsabile della sicurezza di rete

Supporta ABAC (tag nelle policy): sì

Attribute-based il controllo degli accessi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base ad attributi chiamati tag. È possibile allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa.

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

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

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

AWS Network Security Manager supporta il controllo degli accessi basato sugli attributi utilizzando tutte e tre le chiavi AWS globali di condizione dei tag. È possibile limitare l'accesso alle risorse AWS di Network Security Manager in base ai tag associati a tali risorse.

Utilizzo di credenziali temporanee con AWS Responsabile della sicurezza di rete

Supporta le credenziali temporanee: sì

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

Cross-service autorizzazioni principali per AWS Responsabile della sicurezza di rete

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

Le sessioni di accesso inoltrato (FAS) utilizzano le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per AWS Responsabile della sicurezza di rete

Supporta i ruoli di servizio: sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per

ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità AWS di Network Security Manager. Modifica i ruoli di servizio solo quando AWS Network Security Manager fornisce indicazioni in tal senso.

Service-linked ruoli per AWS Responsabile della sicurezza di rete

Supporta i ruoli collegati ai servizi: Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo di eseguire un'azione per conto dell'utente. Service-linked i ruoli appaiono nel tuo Account AWS account e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

AWS Network Security Manager utilizza un ruolo collegato al servizio per operare negli account dei membri dell'organizzazione. AWS Network Security Manager crea automaticamente il ruolo collegato al servizio quando si abilita il servizio. Il ruolo concede a AWS Network Security Manager l'autorizzazione a gestire le risorse AWS WAF e AWS Shield Advanced. Il ruolo concede inoltre l'accesso a AWS Config per l'individuazione delle risorse e l'autorizzazione a eseguire operazioni su più account.

Per informazioni dettagliate sulla creazione e la gestione dei ruoli collegati ai servizi di AWS Network Security Manager, vedere. the section called "Service-linked ruoli"

Identity-based esempi di policy per AWS Responsabile della sicurezza di rete

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

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

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da AWS Network Security Manager, incluso il formato degli ARN per ciascun tipo di risorsa, vedere Azioni, risorse e chiavi di condizione per AWS Network Security Manager nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo di AWS Console di Network Security Manager
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Read-only accesso a AWS Responsabile della sicurezza di rete
- Gestisci solo regole e modelli

Best practice per le policy

Identity-based le politiche determinano se qualcuno può creare, accedere o eliminare le risorse di AWS Network Security Manager nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy AWS gestite che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.
- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per

maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.

- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare Protezione dell'accesso API con MFA nella Guida per l'utente di IAM.

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

Utilizzo di AWS Console di Network Security Manager

Per accedere alla console di AWS Network Security Manager, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentire di elencare e visualizzare i dettagli sulle risorse di AWS Network Security Manager presenti in. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per accedere alla console di AWS Network Security Manager, un principale deve disporre di autorizzazioni minime per le azioni `network-security-manager:List*` e`network-security-manager:Get*`.

Consentire agli utenti di visualizzare le loro autorizzazioni

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Read-only accesso a AWS Responsabile della sicurezza di rete

La seguente politica garantisce un accesso principale in sola lettura a tutte le risorse di AWS Network Security Manager. Ciò è utile per i revisori o i ruoli di monitoraggio che devono visualizzare le configurazioni e lo stato della sincronizzazione senza apportare modifiche.

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

```
        {
            "Effect": "Allow",
            "Action": [
                "network-security-manager:Get*",
                "network-security-manager:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Gestisci solo regole e modelli

La seguente politica consente a un responsabile di creare, aggiornare ed eliminare regole e modelli, senza concedere l'accesso a politiche, ambiti o distribuzioni. Ciò è utile per i team che creano configurazioni di sicurezza ma non ne controllano l'applicazione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "network-security-manager:CreateRule",
                "network-security-manager:GetRule",
                "network-security-manager:UpdateRule",
                "network-security-manager:DeleteRule",
                "network-security-manager:ListRules",
                "network-security-manager:CreateRuleSnapshot",
                "network-security-manager:ListRuleSnapshots",
                "network-security-manager:CreateTemplate",
                "network-security-manager:GetTemplate",
                "network-security-manager:UpdateTemplate",
                "network-security-manager:DeleteTemplate",
                "network-security-manager:ListTemplates",
                "network-security-manager:CreateTemplateSnapshot",
                "network-security-manager:ListTemplateSnapshots",
                "network-security-manager:TagResource",
                "network-security-manager:UntagResource",
                "network-security-manager:ListTagsForResource"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Risoluzione dei problemi AWS Identità e accesso di Network Security Manager

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con AWS Network Security Manager e IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in AWS Responsabile della sicurezza di rete
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire l'accesso a persone esterne al mio Account AWS per accedere al mio AWS risorse di Network Security Manager

Non sono autorizzato a eseguire un'azione in AWS Responsabile della sicurezza di rete

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

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

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 network-security-manager: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 `network-security-manager:`*`GetWidget`*.

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

Non sono autorizzato a eseguire iam: PassRole

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

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

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

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

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

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

Voglio consentire l'accesso a persone esterne al mio Account AWS per accedere al mio AWS risorse di Network Security Manager

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

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS Network Security Manager supporta queste funzionalità, vedereIn che modo AWS Network Security Manager funziona con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM di un altro Account AWS utente di tua proprietà nella IAM User Guide.

- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente di IAM.

Utilizzo di ruoli collegati ai servizi per AWS Responsabile della sicurezza di rete

AWS Network Security Manager utilizza ruoli collegati ai servizi IAM. Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a AWS Network Security Manager. Service-linked i ruoli sono predefiniti da AWS Network Security Manager e includono tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per conto dell'utente.

Un ruolo collegato al servizio semplifica la configurazione di AWS Network Security Manager perché non è necessario aggiungere manualmente le autorizzazioni necessarie. AWS Network Security Manager definisce le autorizzazioni dei ruoli collegati ai servizi. Salvo diversa definizione, solo AWS Network Security Manager può assumerne i ruoli. Le autorizzazioni definite includono policy di attendibilità e di autorizzazioni. Non puoi collegare tale politica di autorizzazioni a nessun'altra entità IAM.

Puoi eliminare un ruolo collegato al servizio solo dopo aver eliminato per la prima volta le risorse correlate. Ciò protegge le risorse di AWS Network Security Manager perché non è possibile rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta AWS i servizi che funzionano con IAM e cerca i servizi che includono Sì nella colonna dei ruoli. Service-linked Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Service-linked autorizzazioni di ruolo per AWS Responsabile della sicurezza di rete

AWS Network Security Manager utilizza il ruolo collegato al servizio denominato. `AWSServiceRoleForNetworkSecurityManager` Questo ruolo collegato al servizio prevede che il responsabile del `network-security-manager.amazonaws.com` servizio assuma il ruolo.

La politica di autorizzazione dei ruoli denominata `NetworkSecurityManagerServiceRolePolicy` è una politica AWS gestita che consente a AWS Network Security Manager di completare azioni sulle risorse specificate.

La seguente politica di attendibilità consente al responsabile del `network-security-manager.amazonaws.com` servizio di assumere il ruolo.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "network-security-manager.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

> **Note**
>
> Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio è necessario configurare le relative autorizzazioni. Per ulteriori informazioni, consulta le autorizzazioni dei Service-linked ruoli nella Guida per l'utente IAM.

Dettagli delle autorizzazioni

AWS Network Security Manager richiede ogni gruppo di autorizzazioni per proteggere e scoprire le risorse dell'account e dell'organizzazione. La policy `NetworkSecurityManagerServiceRolePolicy` gestita concede le seguenti autorizzazioni, raggruppate per servizio:

- `wafv2`— Creazione, lettura, aggiornamento ed eliminazione degli ACL Web e dei gruppi di regole di Firewall Manager. Associa e dissocia gli ACL Web con risorse protette. Gestisci le configurazioni di registrazione Web ACL e le politiche di autorizzazione dei gruppi di regole. Etichetta e rimuovi i tag dalle risorse. Convalida l'ACL web e le configurazioni delle regole di AWS Network Security Manager.

- `shield`— Crea, descrivi, elenca ed elimina le protezioni AWS Shield Advanced. Crea e descrivi l'abbonamento AWS Shield Advanced.
- `elasticloadbalancing`— Descrivi gli Application Load Balancer e i tag. Crea, elimina e imposta associazioni ACL Web su Application Load Balancers.
- `cloudfront`— Ottieni ed elenca CloudFront le distribuzioni, le configurazioni e i tag di Amazon. Associa e dissocia gli ACL web di distribuzione. Leggi le origini del VPC.
- `apigateway`— Leggi le API REST, le fasi e i tag di Amazon API Gateway. Imposta l'ACL Web su una fase API.
- `ec2`— Leggi gli ACL Web e le associazioni delle istanze di Amazon EC2 Verified Access. Descrivi gli indirizzi IP elastici per la protezione AWS Shield Advanced.
- `cognito-idp`,, `apprunner` `appsyncamplify`, e `bedrock-agentcore` — Leggi le associazioni ACL Web per pool di utenti, servizi, API AWS AppSync GraphQL AWS App Runner , AWS Amplify app e gateway Amazon AgentCore Bedrock di Amazon Cognito in AWS modo che Network Security Manager possa scoprire le risorse protette.
- `config`— Seleziona le configurazioni delle risorse e gestisci il registratore di AWS Config configurazione collegato ai servizi che Network Security Manager utilizza per individuare le risorse pertinenti. AWS
- `organizations`— Leggi la tua organizzazione, gli account, le radici, le unità organizzative e gli amministratori delegati in modo che AWS Network Security Manager possa operare in tutta l'organizzazione.
- `logs`— Crea, leggi, aggiorna, elimina ed elenca le consegne di log per la registrazione ACL web.
- `s3`— Ottieni e installa policy bucket sui bucket Amazon S3 i cui nomi iniziano `aws-waf-logs-` con in modo da poter distribuire i log ACL Web.
- `iam`— Creare i ruoli collegati ai servizi richiesti da AWS Shield Advanced e AWS WAF, nell'ambito della chiave di condizione. AWS Config`iam:AWSServiceName`

Il seguente codice JSON mostra la politica completa delle autorizzazioni. `NetworkSecurityManagerServiceRolePolicy`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LogsGeneral",
      "Effect": "Allow",
```

```
      "Action": [
        "logs:ListLogDeliveries",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3LogBucketGeneral",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource": "arn:aws:s3:::aws-waf-logs-*"
    },
    {
      "Sid": "CloudfrontVpcOriginAccess",
      "Effect": "Allow",
      "Action": [
        "cloudfront:GetVpcOrigin"
      ],
      "Resource": "arn:aws:cloudfront::*:vpcorigin/*"
    },
    {
      "Sid": "ConfigUnscoped",
      "Effect": "Allow",
      "Action": [
        "config:SelectResourceConfig"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DescribeOrganizationUnScoped",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
```

```
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DescribeAccountScoped",
      "Effect": "Allow",
      "Action": "organizations:DescribeAccount",
      "Resource": "arn:aws:organizations::*:account/o-*/*"
    },
    {
      "Sid": "DescribeOrganizationUnitScoped",
      "Effect": "Allow",
      "Action": "organizations:DescribeOrganizationalUnit",
      "Resource": "arn:aws:organizations::*:ou/o-*/ou-*"
    },
    {
      "Sid": "ListDelegatedAdministratorsScoped",
      "Effect": "Allow",
      "Action": "organizations:ListDelegatedAdministrators",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "network-security-manager.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "LoadBalancerNonMutationApiAccess",
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeWebACLAssociation"
      ],
      "Resource": "*"
    },
    {
      "Sid": "LoadBalancerGetWebACLScoped",
      "Effect": "Allow",
      "Action": "elasticloadbalancing:GetLoadBalancerWebACL",
      "Resource": "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
```

```
    },
    {
      "Sid": "CloudFrontDistributionNonMutationApiAccess",
      "Effect": "Allow",
      "Action": [
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListTagsForResource"
      ],
      "Resource": "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid": "ApiGatewayStageNonMutationApiAccess",
      "Effect": "Allow",
      "Action": "apigateway:GET",
      "Resource": [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*"
      ]
    },
    {
      "Sid": "Wafv2General",
      "Effect": "Allow",
      "Action": [
        "wafv2:TagResource",
        "wafv2:ListResourcesForWebACL",
        "wafv2:AssociateWebACL",
        "wafv2:ListTagsForResource",
        "wafv2:UntagResource",
        "wafv2:GetWebACL",
        "wafv2:DisassociateFirewallManager",
        "wafv2:DeleteWebACL",
        "wafv2:DisassociateWebACL",
        "wafv2:ValidateNetworkSecurityManagerWebACLConfiguration",
        "wafv2:ValidateNetworkSecurityManagerRuleConfiguration"
      ],
      "Resource": "arn:aws:wafv2:*:*:*/webacl/*"
    },
    {
      "Sid": "Wafv2WebAclAndRuleGroupMutation",
      "Effect": "Allow",
      "Action": [
```

```
        "wafv2:UpdateWebACL",
        "wafv2:CreateWebACL",
        "wafv2:DeleteFirewallManagerRuleGroups",
        "wafv2:PutFirewallManagerRuleGroups"
      ],
      "Resource": [
        "arn:aws:wafv2:*:*:*/webacl/*",
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/ipset/*",
        "arn:aws:wafv2:*:*:regional/ipset/*",
        "arn:aws:wafv2:*:*:global/regexpatternset/*",
        "arn:aws:wafv2:*:*:regional/regexpatternset/*"
      ]
    },
    {
      "Sid": "Wafv2Logging",
      "Effect": "Allow",
      "Action": [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource": "arn:aws:wafv2:*:*:*/webacl/*"
    },
    {
      "Sid": "Wafv2ListLogging",
      "Effect": "Allow",
      "Action": "wafv2:ListLoggingConfigurations",
      "Resource": "*"
    },
    {
      "Sid": "Wafv2ListWebACLs",
      "Effect": "Allow",
      "Action": "wafv2:ListWebACLs",
      "Resource": "*"
    },
    {
      "Sid": "Wafv2PermissionPolicy",
      "Effect": "Allow",
      "Action": [
        "wafv2:PutPermissionPolicy",
```

```
        "wafv2:GetPermissionPolicy",
        "wafv2:DeletePermissionPolicy"
      ],
      "Resource": [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*"
      ]
    },
    {
      "Sid": "Wafv2WebaclDescribe",
      "Effect": "Allow",
      "Action": "wafv2:GetWebACLForResource",
      "Resource": "arn:aws:wafv2:*:*:*/webacl/*"
    },
    {
      "Sid": "CloudFrontListDistributions",
      "Effect": "Allow",
      "Action": [
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListDistributions"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudFrontDistributionMutation",
      "Effect": "Allow",
      "Action": [
        "cloudfront:AssociateDistributionWebACL",
        "cloudfront:DisassociateDistributionWebACL"
      ],
      "Resource": "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid": "ElbWebAclRemediationScoped",
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:CreateWebACLAssociation",
        "elasticloadbalancing:DeleteWebACLAssociation"
      ],
      "Resource": "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid": "ElbSetWebAcl",
      "Effect": "Allow",
```

```
      "Action": "elasticloadbalancing:SetWebACL",
      "Resource": "*"
    },
    {
      "Sid": "ApiGatewayWebAclRemediation",
      "Effect": "Allow",
      "Action": "apigateway:SetWebACL",
      "Resource": "arn:aws:apigateway:*::/restapis/*/stages/*"
    },
    {
      "Sid": "CognitoWebAclIntegration",
      "Effect": "Allow",
      "Action": [
        "cognito-idp:GetWebACLForResource",
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AppRunnerWebAclIntegration",
      "Effect": "Allow",
      "Action": [
        "apprunner:DescribeWebAclForService",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource": "*"
    },
    {
      "Sid": "VerifiedAccessWebAclIntegration",
      "Effect": "Allow",
      "Action": [
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AppSyncWebAclIntegration",
      "Effect": "Allow",
      "Action": [
        "appsync:GetWebACLForResource",
        "appsync:ListResourcesForWebACL"
      ],
      "Resource": "*"
```

```
    },
    {
      "Sid": "AmplifyWebAclIntegration",
      "Effect": "Allow",
      "Action": [
        "amplify:GetWebACLForResource",
        "amplify:ListResourcesForWebACL"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ShieldGeneral",
      "Effect": "Allow",
      "Action": [
        "shield:CreateProtection",
        "shield:DeleteProtection",
        "shield:DescribeProtection",
        "shield:ListProtections",
        "shield:CreateSubscription",
        "shield:DescribeSubscription",
        "shield:GetSubscriptionState",
        "ec2:DescribeAddresses",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ShieldSlrCreation",
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/shield.amazonaws.com/*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "shield.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowConfigRecorderList",
      "Effect": "Allow",
      "Action": "config:ListConfigurationRecorders",
      "Resource": "*"
    },
```

```
    {
      "Sid": "AllowPutServiceLinkedConfigRecorder",
      "Effect": "Allow",
      "Action": "config:PutServiceLinkedConfigurationRecorder",
      "Resource": "*"
    },
    {
      "Sid": "AllowConfigRecorderScopedAccess",
      "Effect": "Allow",
      "Action": [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:AssociateResourceTypes",
        "config:DisassociateResourceTypes"
      ],
      "Resource": "arn:aws:config:*:*:configuration-recorder/*"
    },
    {
      "Sid": "AllowCreateConfigServiceLinkedRole",
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "config.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowListActionsForAgentCoreGateway",
      "Effect": "Allow",
      "Action": [
        "bedrock-agentcore:GatewayListResourcesForWebACL"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowGetActionForAgentCoreGateway",
      "Effect": "Allow",
      "Action": [
        "bedrock-agentcore:GatewayGetWebACLForResource"
      ],
      "Resource": "arn:aws:bedrock-agentcore:*:*:gateway/*"
```

```
    },
    {
      "Sid": "WafV2LoggingSlrCreation",
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/wafv2.amazonaws.com/*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "wafv2.amazonaws.com"
        }
      }
    }
  ]
}
```

Creazione di un ruolo collegato ai servizi per AWS Responsabile della sicurezza di rete

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando abiliti AWS Network Security Manager, AWS Network Security Manager crea automaticamente il ruolo collegato al servizio. Non è necessario eseguire alcuna operazione manuale.

Se si elimina questo ruolo collegato al servizio e quindi è necessario crearlo nuovamente, AWS Network Security Manager ricrea il ruolo al successivo utilizzo del servizio. Non è necessario intraprendere alcuna azione.

Per ulteriori informazioni, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente IAM.

Modifica di un ruolo collegato ai servizi per AWS Responsabile della sicurezza di rete

Non è possibile modificare le autorizzazioni del ruolo collegato al `AWSServiceRoleForNetworkSecurityManager` servizio. Dopo aver creato un ruolo collegato al servizio, non è possibile modificarne il nome, perché potrebbero farvi riferimento diverse entità. È possibile tuttavia modificarne la descrizione utilizzando IAM.

Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per AWS Responsabile della sicurezza di rete

Se non è più necessario utilizzare AWS Network Security Manager, si consiglia di eliminare il ruolo `AWSServiceRoleForNetworkSecurityManager` collegato al servizio.

Prima di eliminare il ruolo collegato al servizio, pulisci le risorse gestite da AWS Network Security Manager. Disattiva AWS Network Security Manager e rimuovi le politiche e gli ambiti in modo che nessuna risorsa gestita da AWS Network Security Manager rimanga nel tuo account. È quindi possibile eliminare il ruolo manualmente.

> **Note**
>
> Se AWS Network Security Manager utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, seleziona Ruoli.
3. Nella casella di ricercaAWSServiceRoleForNetworkSecurityManager, immettere e quindi selezionare il ruolo.
4. Scegliere Elimina.
5. Per confermare l'eliminazione, inserite il nome del ruolo, quindi scegliete Elimina.

Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente IAM.

Regioni supportate per AWS Ruoli collegati ai servizi di Network Security Manager

AWS Network Security Manager supporta l'utilizzo di ruoli collegati ai servizi in tutte le AWS regioni in cui è disponibile AWS Network Security Manager.

Convalida della conformità per AWS Responsabile della sicurezza di rete

La nostra nuova esperienza AWS di registrazione non è progettata per carichi di lavoro regolamentati. Se utilizzi la nostra nuova esperienza di AWS registrazione, ma desideri utilizzarla AWS per carichi di lavoro regolamentati, puoi iscriverti a AWS (avanzata) o attivare funzionalità avanzate per il tuo ambiente. AWS

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

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

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

Resilienza in AWS Responsabile della sicurezza di rete

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone 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 è possibile 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, AWS Network Security Manager offre diverse funzionalità per supportare le esigenze di resilienza e backup dei dati.

Sicurezza dell'infrastruttura in AWS Responsabile della sicurezza di rete

In quanto servizio gestito, AWS Network Security Manager è protetto dalle procedure di sicurezza di rete AWS globali descritte nel white paper Amazon Web Services: Overview of Security Processes.

Utilizzi chiamate API AWS pubblicate per accedere a AWS Network Security Manager attraverso la rete. I client devono supportare Transport Layer Security (TLS) 1.0 o versioni successive. È consigliabile TLS 1.2 o versioni successive. I client devono inoltre supportare suite di crittografia con Perfect Forward Secrecy (PFS) come DHE (Ephemeral) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa è possibile utilizzare Servizio di token di sicurezza AWS (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Le migliori pratiche di sicurezza per AWS Responsabile della sicurezza di rete

Le seguenti procedure consigliate consentono di mantenere una configurazione sicura AWS di Network Security Manager.

Controlli preventivi

- Usa il privilegio minimo di IAM: concedi solo le autorizzazioni necessarie a ciascun utente o ruolo per eseguire le attività di AWS Network Security Manager. Utilizza le chiavi di condizione IAM per limitare l'accesso a risorse specifiche quando possibile.
- Usa ruoli collegati ai servizi: AWS Network Security Manager utilizza ruoli collegati ai servizi per eseguire azioni per tuo conto. Questi ruoli dispongono di autorizzazioni predefinite limitate all'accesso minimo richiesto.
- Configura gli ambiti con attenzione: definisci le configurazioni degli ambiti che riguardano solo gli account e i tipi di risorse che richiedono protezione. Ambiti troppo ampi possono portare a un'applicazione involontaria.

Controlli di rilevamento

- Abilita AWS CloudTrail la registrazione: CloudTrail registra tutte le chiamate API di AWS Network Security Manager. Esamina questi registri per verificare chi ha apportato modifiche alle configurazioni di sicurezza e quando.
- Monitora lo stato di sincronizzazione: controlla regolarmente lo stato di sincronizzazione delle distribuzioni per identificare le risorse che non sono sincronizzate con il livello di sicurezza previsto.

Monitoraggio AWS Responsabile della sicurezza di rete

Monitoring AWS Network Security Manager ti aiuta a capire se le tue risorse sono protette come previsto. AWS Network Security Manager offre le seguenti funzionalità di monitoraggio:

- API sullo stato della sincronizzazione: interroga lo stato di protezione delle singole risorse nelle distribuzioni.
- AWS CloudTrail-- Registra tutte le chiamate API AWS di Network Security Manager per il controllo, la conformità e la risoluzione dei problemi operativi.

Monitoraggio dello stato di sincronizzazione

Il modo principale per controllare se le risorse sono protette è tramite le API di stato della sincronizzazione. AWS Network Security Manager valuta ogni risorsa pertinente e registra se la configurazione effettiva del firewall corrisponde alla configurazione prevista.

Operazioni sullo stato della sincronizzazione

AWS Network Security Manager fornisce due operazioni per interrogare lo stato della sincronizzazione:

ListResourceSynchronizationStatuses

Restituisce lo stato di ogni risorsa per una distribuzione specifica. Richiede un parametro`deploymentIdentifier`. Facoltativamente, filtra per `synchronizationStatus` (IN_SYNC, OUT_OF_SYNC o NOT_APPLICABLE).

ListAggregateResourceSynchronizationStatuses

Restituisce lo stato aggregato per risorsa in tutte le distribuzioni. Facoltativamente`synchronizationStatus`, filtra per. Questa operazione mostra il risultato combinato di tutte le politiche che si applicano a ciascuna risorsa.

Entrambe le operazioni supportano l'impaginazione con `maxResults` (da 1 a 100) e`nextToken`.

Comprensione dei valori dello stato di sincronizzazione

IN_SYNC

La configurazione effettiva del firewall della risorsa corrisponde alla configurazione effettiva calcolata in base a tutte le politiche applicabili.

OUT_OF_SYNC

La configurazione effettiva della risorsa è diversa dalla configurazione effettiva. Il `outOfSyncReasons` campo fornisce dettagli per impostazione che mostrano i valori previsti rispetto a quelli effettivi.

NOT_APPLICABLE

L'account e il tipo di risorsa rientrano nell'ambito, ma la risorsa stessa non corrisponde ai filtri dell'ambito (ad esempio, un filtro tag la esclude). Non è richiesta alcuna azione.

Se una risorsa non compare affatto nei risultati, l'account o il tipo di risorsa non rientra nell'ambito della distribuzione. Controlla la configurazione del tuo ambito.

Comprensione dei timestamp di valutazione

Ogni voce relativa allo stato della sincronizzazione include due timestamp:

- `evaluatedAt`-- Quando AWS Network Security Manager ha valutato l'ultima volta la configurazione della risorsa. Un `evaluatedAt` valore non aggiornato indica che la valutazione non è ancora stata eseguita per le modifiche recenti.
- `updatedAt`-- Data dell'ultima modifica dello stesso record dello stato di sincronizzazione. Se `updatedAt` è più vecchio di`evaluatedAt`, lo stato è stabile dall'ultima valutazione.

Cross-account visibilità

Quando più amministratori proteggono la stessa risorsa, la visibilità dello stato di sincronizzazione aggregata dipende dall'`enableCrossAccountVisibility`impostazione di ciascuna distribuzione.

- Se per tutte le distribuzioni relative a una risorsa è abilitata la visibilità su più account, qualsiasi amministratore può visualizzare lo stato aggregato completo e i motivi della mancata sincronizzazione.

- Se in una distribuzione è disattivata la visibilità tra account, gli altri amministratori visualizzano un indicatore anziché i motivi dettagliati. `NOT_VISIBLE` Ciò indica che anche un altro amministratore protegge la risorsa ma non ha una visibilità condivisa.

Diagnosi delle risorse non sincronizzate

Quando una risorsa riporta OUT_OF_SYNC, il campo identifica le differenze di configurazione specifiche. `outOfSyncReasons` Il motivo principale è uno dei seguenti:

- `missingFirewall`-- Nessuna protezione firewall è associata alla risorsa.
- `invalidFirewall`-- Esiste un firewall ma la sua configurazione non corrisponde alle aspettative. Le differenze specifiche sono elencate in bucket classificati.

Se la riparazione è abilitata ma non è possibile correggere la risorsa, il `remediationIssues` campo `correctiveAction` fornisce una guida su come risolvere il problema manualmente. La riparazione è un'impostazione a livello di policy che è disattivata per impostazione predefinita. Per ulteriori informazioni, consulta the section called “Sincronizzazione e correzione”.

Distribuzioni multiple con configurazioni diverse possono indirizzare la stessa risorsa. In questo caso, lo stato di sincronizzazione per distribuzione può essere OUT_OF_SYNC mentre lo stato di sincronizzazione aggregata è IN_SYNC. Si tratta di un comportamento previsto, non di un errore. Le impostazioni di un criterio con priorità più alta hanno avuto la precedenza durante l'unione. Di conseguenza, la risorsa corrisponde alla configurazione effettiva, anche se non corrisponde alla configurazione della distribuzione con priorità più bassa.

Registrazione dei log AWS Chiamate API Network Security Manager con AWS CloudTrail

AWS Network Security Manager è integrato con AWS CloudTrail un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio. CloudTrail acquisisce tutte le chiamate API per AWS Network Security Manager come eventi di gestione. Le chiamate acquisite includono chiamate dalla console di AWS Network Security Manager e chiamate programmatiche alle operazioni dell'API AWS Network Security Manager.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per AWS Network Security Manager. Se non configuri un percorso, puoi comunque

visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Per ulteriori informazioni, consulta la Guida per l'utente di AWS CloudTrail.

AWS Informazioni su Network Security Manager in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività in AWS Network Security Manager, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti in Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi del tuo Account AWS, inclusi gli eventi per AWS Network Security Manager, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il percorso registra gli eventi di tutte le regioni della partizione. AWS Fornisce i file di log al bucket Amazon S3 specificato. Puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail

Tutte le operazioni AWS di Network Security Manager vengono registrate da. CloudTrail Le operazioni pubbliche includono quanto segue:

- Operazioni di creazione, lettura, aggiornamento ed eliminazione (CRUD) per regole, modelli, politiche, ambiti e distribuzioni
- Operazioni di istantanea
- Operazioni di etichettatura
- Operazioni relative all'account dell'amministratore
- Operazioni sullo stato della sincronizzazione
- Operazioni di associazione delle risorse
- Operazioni di generazione di regole

Ogni voce di evento include le seguenti informazioni:

- L'origine dell'evento: `network-security-manager.amazonaws.com`
- Il nome dell'evento, che è il nome dell'operazione API (ad esempio, `CreatePolicy` o`ListDeployments`)
- Le risorse interessate, identificate per ARN e tipo di risorsa

Read-only le operazioni (come `GetPolicyListRules`, `eListResourceSynchronizationStatuses`) vengono registrate `readOnly: true` e non includono elementi di risposta. Le operazioni di modifica includono i parametri di richiesta e gli elementi di risposta.

> **Note**
>
> CloudTrail rimuove i campi sensibili dai record degli eventi. Ad esempio, CloudTrail oscura il `prompt` parametro dell'operazione. `GenerateRuleConfiguration`

Esempio: evento CreatePolicy

L'esempio seguente mostra una voce di CloudTrail registro per l'`CreatePolicy`operazione.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AROAEXAMPLEID:my-session",
      "arn": "arn:aws:sts::123456789012:assumed-role/AdminRole/my-session",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
          "sessionIssuer": {
              "type": "Role",
              "principalId": "AROAEXAMPLEID",
              "arn": "arn:aws:iam::123456789012:role/AdminRole",
              "accountId": "123456789012",
              "userName": "AdminRole"
          },
          "attributes": {
              "creationDate": "2026-08-10T18:22:41Z",
              "mfaAuthenticated": "false"
          }
```

```
      }
  },
  "eventTime": "2026-08-10T18:24:03Z",
  "eventSource": "network-security-manager.amazonaws.com",
  "eventName": "CreatePolicy",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.44",
  "userAgent": "aws-cli/2.17.0 Python/3.12.4 Darwin/24.6.0",
  "requestParameters": {
      "clientToken": "550e8400-e29b-41d4-a716-446655440001",
      "policyName": "production-web-acl-policy",
      "firewallType": "WAF",
      "priority": 1,
      "associatedTemplateAndRuleList": [
          {
              "templateIdentifier": "arn:aws:network-security-manager:us-
east-1:123456789012:template:t1a2b3c4d5"
          }
      ],
      "policyConfiguration": {
          "remediationEnabled": true,
          "resourcesCleanUp": false,
          "wafConfig": {
              "existingCustomerWebACLResolution": "RETROFIT",
              "conflictResolution": "MERGE_WHERE_APPLICABLE"
          }
      },
      "isPublished": true
  },
  "responseElements": {
      "policyId": "p9z8y7x6w5v4u3t2",
      "policyArn": "arn:aws:network-security-manager:us-
east-1:123456789012:policy:p9z8y7x6w5v4u3t2",
      "policyName": "production-web-acl-policy",
      "status": "ACTIVE",
      "version": "1"
  },
  "requestID": "b1c2d3e4-5f67-4890-a1b2-c3d4e5f6a7b8",
  "eventID": "f0e1d2c3-b4a5-4968-8776-5a4b3c2d1e0f",
  "readOnly": false,
  "resources": [
      {
          "accountId": "123456789012",
          "type": "AWS::NetworkSecurityManager::Policy",
```

```
          "ARN": "arn:aws:network-security-manager:us-
east-1:123456789012:policy:p9z8y7x6w5v4u3t2"
      }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management"
}
```

AWS Quote di Network Security Manager

Hai Account AWS le seguenti quote predefinite per AWS Network Security Manager. Salvo diversa indicazione, ogni quota è per account, per regione.

Quote delle risorse

La tabella seguente elenca il numero massimo di risorse di AWS Network Security Manager che è possibile creare per account in ciascuna regione.

Risorsa	Quota predefinita	Regolabile
Regole per account	200	No
Modelli per account	100	No
Policy per account	100	No
Ambiti per account	100	No
Distribuzioni per account	100	No
Istantanee per risorsa	10	No

Quote di composizione delle risorse

La tabella seguente elenca le quote relative al modo in cui le risorse di AWS Network Security Manager fanno riferimento l'una all'altra all'interno della gerarchia delle risorse.

Quota	Valore
Regole per modello	Da 1 a 50
Modelli per policy AWS WAF	Da 1 a 2
Regole e modelli combinati per policy AWS WAF	Da 1 a 100

Quota	Valore
Modelli o regole per policy AWS Shield Advanced	0 (deve essere vuoto)
Politiche per implementazione	Da 1 a 2
Ambiti per implementazione	1 (esattamente uno)

Quote di configurazione dell'ambito

La tabella seguente elenca le quote per le espressioni di configurazione dell'ambito.

Quota	Valore
Ambiti dei tipi di risorsa per ambito	20
Profondità dell'espressione dell'ambito (livelli annidati)	2
Ampiezza dell'espressione dell'ambito (criteri per livello)	20

Quote degli account di amministratore

La tabella seguente elenca le quote per i livelli di priorità degli account di amministratore di AWS Network Security Manager.

Quota	Valore
Livelli di priorità dell'amministratore	Da 1 a 10

Quote di impaginazione delle API

La tabella seguente elenca i limiti di impaginazione per le operazioni List.

Quota	Valore
Numero massimo di risultati per pagina () `maxResults`	100
Risultati minimi per pagina (`maxResults`)	1

Regolabilità delle quote

Le quote elencate nelle sezioni precedenti sono fisse e non possono essere aumentate in questo momento.

Cronologia dei documenti per il AWS Guida per gli sviluppatori di Network Security Manager

La tabella seguente descrive le versioni della documentazione per AWS Network Security Manager.

Modifica	Descrizione	Data
Versione iniziale	Versione iniziale della AWS Network Security Manager Developer Guide.	1 agosto 2026

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.