aws

Entwicklerhandbuch

AWS Manager für Netzwerksicherheit



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

AWS Manager für Netzwerksicherheit: Entwicklerhandbuch

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

Die Handelsmarken und die Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist AWS Network Security Manager? 1
Wie AWS Network Security Manager funktioniert auf einen Blick 1
Funktionen von AWS Manager für Netzwerksicherheit 1
Anwendungsfälle 2
Zugehörige Services 3
Zugriff AWS Network Security Manager 4
Preisgestaltung 4
Verwenden Sie zum ersten Mal? 5
Wie funktioniert AWS Network Security Manager 6
AWS Network Security Manager-Ressourcenmodell 6
AWS Lebenszyklus, Zusammenführung und Synchronisation von Network Security Manager-Ressourcen 7
Entwurf und aktiver Lebenszyklus 8
Versionsverwaltung 9
Priority-based Zusammenführung von Richtlinien 9
Ressourcenerkennung mit AWS Config 11
Synchronisation und Problembehebung 11
Administrator- und Mitgliedskonten 13
Service-linked Rolle 14
AWS Network Security Manager einrichten 15
Wählen Sie Ihr Organisationsmodell 15
Einrichtung für die Verwendung mit einem einzigen Konto 15
Einrichtung für die Verwendung mehrerer Konten mit AWS Organizations 16
Erstellen eines AWS Network Security Manager-Administratorkonto 17
Erstellen Sie eine IAM-Identität mit AWS Network Security Manager-Berechtigungen 19
Melden Sie sich an für ein AWS-Konto 20
Verwenden AWS Network Security Manager in Regionen, die standardmäßig deaktiviert sind 20
Tutorial: Implementieren Sie Ihren ersten Netzwerksicherheitsschutz 21
Voraussetzungen 21
Schritt 1: Erstellen Sie eine Regel 22
Schritt 2: Erstellen Sie eine Vorlage 23
Schritt 3: Erstellen Sie eine Richtlinie 24
Schritt 4: Erstellen Sie einen Bereich 25
Schritt 5: Eine Bereitstellung erstellen und veröffentlichen 26

Schritt 6: Synchronisierungsstatus überwachen ... 26
Schritt 7: Bereinigen ... 27
Nächste Schritte ... 29
Verwaltung von Firewalls und Sicherheitsdiensten ... 30
Verwaltung von Web-ACLs für WAF AWS ... 30
AWS WAF-Konzepte ... 30
Quick Create für AWS WAF ... 34
Standarderstellungsprozess für AWS WAF ... 39
Verwaltung des DDoS-Schutzes für Shield Advanced AWS ... 45
Quick Create für AWS Shield Advanced ... 46
Standarderstellungsprozess für AWS Shield Advanced ... 50
AWS Netzwerksicherheitsmanager und Firewall Manager ... 55
Koexistenz mit AWS Firewall Manager ... 55
Vorrang bei der Problembehebung ... 55
Geplante Migration von AWS Firewall Manager ... 55
Sicherheit ... 57
Datenschutz ... 58
Verschlüsselung im Ruhezustand ... 59
Verschlüsselung während der Übertragung ... 59
Schlüsselverwaltung ... 59
Identity and Access Management ... 59
Zielgruppe ... 60
Authentifizierung mit Identitäten ... 60
Verwalten des Zugriffs mit Richtlinien ... 62
Wie AWS Network Security Manager funktioniert mit IAM ... 63
Identity-based Beispiele für Richtlinien ... 70
Fehlerbehebung ... 74
Service-linked Rollen ... 76
Service-linked Rollenberechtigungen ... 77
Erstellen einer serviceverknüpften Rolle ... 88
Bearbeiten einer serviceverknüpften Rolle ... 88
Löschen einer serviceverknüpften Rolle ... 88
Unterstützte Regionen ... 89
Compliance-Validierung ... 89
Ausfallsicherheit ... 90
Infrastruktursicherheit ... 90

Bewährte Methoden für die Gewährleistung der Sicherheit 91
Präventive Kontrollen 91
Detektivische Kontrollen 91
Überwachen AWS Manager für Netzwerksicherheit 92
Synchronisierungsstatus überwachen 92
Vorgänge mit dem Synchronisierungsstatus 92
Grundlegendes zu Synchronisationsstatuswerten 93
Die Zeitstempel der Evaluierung verstehen 93
Cross-account Sichtbarkeit 93
Diagnose von Ressourcen, die nicht synchron sind 94
CloudTrail protokolliert 94
AWS Informationen zum Network Security Manager in CloudTrail 95
Beispiel: Ereignis CreatePolicy 96
Kontingente 99
Ressourcenkontingente 99
Kontingente für die Zusammensetzung von 99
Umfang der Konfigurationskontingente 100
Kontingente für Administratorkonten 100
Kontingente für API-Paginierung 101
Einstellbarkeit der Quote 101
Dokumentverlauf 102
..... ciii

Was ist AWS Manager für Netzwerksicherheit?

Mit AWS Network Security Manager können Sie Netzwerksicherheitsmaßnahmen — wie AWS WAF- und AWS Shield Advanced-Regeln — zentral für ein oder mehrere Konten und Ressourcen in Ihrem Unternehmen definieren und bereitstellen. Anstatt mit jeder Ressource einzeln zu arbeiten, definieren Sie wiederverwendbare Richtlinienobjekte (Regeln, Vorlagen und Richtlinien) einmal und stellen sie dann in großem Umfang bereit. Dabei erfolgt eine kontinuierliche Überwachung, um Richtlinienabweichungen zu erkennen und zu beheben.

Wie AWS Network Security Manager funktioniert auf einen Blick

Sie definieren eine Reihe von hierarchischen Richtlinienobjekten und wenden sie auf bestimmte Bereiche an. Die unterste Ebene von Richtlinienobjekten sind Regeln. Sie können Regeln in Vorlagen gruppieren, die Sie zu Richtlinien mit prioritätsbasierter Konfliktlösung kombinieren können. Anschließend wählen Sie die zu schützenden Konten und Ressourcen mit einem bestimmten Geltungsbereich aus und setzen Ihre Richtlinien durch, indem Sie eine Bereitstellung veröffentlichen.

Nach der Bereitstellung überwacht AWS Network Security Manager kontinuierlich die Umgebung mit dem Geltungsbereich und die bereitgestellten Richtlinien, um zu überprüfen, ob sie den beabsichtigten Definitionen entsprechen. Falls nicht, kann AWS Network Security Manager optional Ressourcen korrigieren, die von der geplanten Konfiguration abweichen. Vollständige Informationen zum Ressourcenmodell, zum Lebenszyklus und zur Architektur finden Sie unterWie funktioniert AWS Network Security Manager.

Funktionen von AWS Manager für Netzwerksicherheit

- Support für mehrere Firewalltypen — AWS Network Security Manager unterstützt AWS WAF für Web-ACL-Konfigurationen und Regelgruppen. Zu den geschützten Ressourcentypen gehören CloudFront Amazon-Distributionen, Application Load Balancers und Amazon API Gateway-Stufen. AWS Network Security Manager unterstützt auch AWS Shield Advanced für den DDoS-Schutz von CloudFront Amazon-Distributionen, Application Load Balancers, Classic Load Balancers und Elastic IP-Adressen.
- Wiederverwendbare Sicherheitskonfigurationen — Definieren Sie Richtlinienobjekte einmal als Regeln, gruppieren Sie sie in Vorlagen und erstellen Sie Bereiche für Zielressourcen. Verwenden Sie Regeln, Vorlagen und Bereiche für mehrere Richtlinien und Bereitstellungen wieder.

- Priority-based Zusammenführung von Richtlinien — Wenn mehrere Richtlinien dieselbe Ressource schützen, führt AWS Network Security Manager ihre Konfigurationen auf der Grundlage der Richtlinienpriorität zusammen und sorgt so für eine vorhersehbare Konfliktlösung.
- Single-account und Unterstützung mehrerer Administratoren — Verwenden Sie AWS Network Security Manager in einem einzigen Konto oder weisen Sie mehrere Administratorkonten zu, jedes mit einer Prioritätsstufe. Wenn sich die Richtlinien von Administratoren überschneiden, löst AWS Network Security Manager Konflikte zuerst nach Administratorpriorität und dann nach Richtlinienpriorität innerhalb jedes Kontos.
- Status „Entwurf“ und „Aktiv“ — Jede AWS Network Security Manager-Ressource, einschließlich Regeln, Vorlagen, Richtlinien, Bereichen und Bereitstellungen, unterstützt den Status Entwurf und Aktiv. Speichern Sie Ressourcen als Entwurf, ohne den aktuellen Schutz zu beeinträchtigen, und veröffentlichen Sie sie dann, wenn Sie bereit sind, sie durchzusetzen.
- Versionierte Snapshots — Jede AWS Network Security Manager-Ressource, einschließlich Regeln, Vorlagen, Richtlinien, Bereichen und Bereitstellungen, unterstützt unveränderliche Snapshots mit Versionsnummern. Verwenden Sie die Versionierung, um zweifelsfrei funktionierende Network Security Manager-Ressourcenkonfigurationen beizubehalten. AWS
- Protected-resource Synchronisationsdiagnose — Sehen Sie sich für jede Ressource im Gültigkeitsbereich genau an, welche Einstellungen nicht synchron sind und warum. Dabei werden die erwarteten Einstellungen mit den tatsächlichen Werten für jedes Konfigurationsfeld verglichen.
- Automatische Korrektur — Aktivieren Sie optional AWS Network Security Manager, um Ressourcen, die nicht synchron sind, automatisch zu korrigieren und sie ohne manuelles Eingreifen an die vorgesehene Konfiguration anzupassen.
- Natural-language Regelgenerierung — Verwenden Sie den `GenerateRuleConfiguration` Vorgang, um eine Regel in einfacher Sprache zu beschreiben und die entsprechende Konfigurations-JSON zu erhalten, bereitgestellt von Amazon Bedrock.

Anwendungsfälle

Im Folgenden finden Sie häufig Anwendungsfälle für AWS Network Security Manager:

- AWS WAF-Basisregeln für alle Konten durchsetzen — Definieren Sie eine Reihe von AWS WAF-Regelgruppen, die jede mit dem Internet verbundene Anwendung verwenden muss, und stellen Sie sie dann in Ihrem gesamten Unternehmen bereit. AWS Network Security Manager wendet die Regeln automatisch auf neue Ressourcen an, die in den Geltungsbereich fallen, sobald sie in den Geltungsbereich fallen.

- Erstellen Sie spezifische benutzerdefinierte WAF-Regeln oder AWS WAF-Ausnahmeregeln für bestimmte Ressourcen — Definieren Sie eine Reihe von AWS WAF-Regeln, die nur für eine bestimmte Gruppe von Ressourcen gelten. Bei diesem Set kann es sich um eine bestimmte Geschäftseinheit oder Anwendung handeln, die Sie anhand von AWS Konto-ID, OU, Tag oder Amazon Resource Names (ARNs) identifizieren.
- Überprüfen Sie den DDoS-Schutz für mit dem Internet verbundene Ressourcen — Erstellen Sie eine AWS Shield Advanced-Richtlinie, die auf öffentliche Ressourcentypen beschränkt ist, und stellen Sie sie unternehmensweit bereit, sodass der DDoS-Schutz für kritische Ressourcen aktiviert ist.
- Konfigurationsabweichungen erkennen und beheben — Verwenden Sie die Überwachung des Synchronisierungsstatus, um Ressourcen zu identifizieren, deren Firewallkonfigurationen vom vorgesehenen Zustand abweichen, und aktivieren Sie optional automatische Problembehebungen, um sie wieder auf die Konformität zu bringen.
- Delegieren Sie das Sicherheitsmanagement an mehrere Teams — Weisen Sie mehrere Administratorkonten mit unterschiedlichen Prioritätsstufen und Zugriffsberechtigungen für bestimmte Konten, Organisationseinheiten oder Firewalltypen zu, sodass Teams ihre eigenen Sicherheitsrichtlinien innerhalb definierter Grenzen verwalten können.

Zugehörige Services

- AWS WAF — Verwenden Sie AWS WAF, um Ihre Webanwendungen und APIs vor gängigen Web-Exploits und Bots zu schützen, die die Verfügbarkeit beeinträchtigen, die Sicherheit gefährden oder übermäßig viele Ressourcen verbrauchen könnten. AWS Network Security Manager verwendet AWS WAF, um Web-ACLs und Regelgruppen für Ressourcen in einem einzigen Konto oder kontenübergreifend in Ihrem Unternehmen zu erstellen und zu verwalten.
- AWS Shield Advanced — Ein verwalteter DDoS-Schutzdienst, der erweiterten Schutz für Ihre Anwendungen bietet, auf denen ausgeführt wird. AWS AWS Network Security Manager verwendet Shield Advanced, um DDoS-Schutz für Ressourcen in einem einzelnen Konto oder für mehrere Konten in Ihrem Unternehmen bereitzustellen.
- AWS Organizations — Hilft Ihnen dabei, Ihre Umgebung zentral zu verwalten und zu steuern, während Sie Ihre AWS Ressourcen erweitern und skalieren. AWS Network Security Manager verlangt von AWS Organizations, den Schutz aller Mitgliedskonten zu verwalten.
- AWS Config — Ein Service, mit dem Sie die Konfigurationen Ihrer AWS Ressourcen bewerten, prüfen und auswerten können. AWS Network Security Manager verwendet einen serviceverknüpften AWS Config-Recorder, um Ressourcen in Ihren Mitgliedskonten zu ermitteln.

Zugriff AWS Network Security Manager

Sie können über die folgenden Schnittstellen auf AWS Network Security Manager zugreifen:

AWS Management-Konsole

Eine webbasierte Oberfläche zur Verwaltung der AWS Network Security Manager-Ressourcen.

Öffnen Sie die AWS Network Security Manager-Konsole unter https://console.aws.amazon.com/network-security-manager/.

AWS Befehlszeilenschnittstelle (AWS CLI)

Stellt Befehle für AWS Network Security Manager-Operationen bereit. Weitere Informationen finden Sie in der AWS CLI Befehlsreferenz.

AWS SDKs

AWS stellt SDKs bereit, die aus Bibliotheken und Beispielcode für verschiedene Programmiersprachen und Plattformen bestehen. Die SDKs bieten eine bequeme Möglichkeit, programmatischen Zugriff auf AWS Network Security Manager zu erstellen. Weitere Informationen finden Sie unter Tools für Amazon Web Services.

AWS Network Security Manager-API

Eine REST-API, die JSON über HTTPS verwendet. Das API-Endpunktformat ist`network-security-manager.{region}.api.aws`. Weitere Informationen finden Sie in der AWS Network Security Manager API-Referenz.

Informationen zu den ersten Schritten mit AWS Network Security Manager finden Sie unter AWS Network Security Manager einrichten undTutorial: Implementieren Sie Ihren ersten Netzwerksicherheitsschutz.

Preisgestaltung

Sie zahlen für jede im Leistungsumfang enthaltene Ressource, die AWS Network Security Manager überwacht und schützt. Für die zugrunde liegenden Sicherheitsdienste, die Sie bereitstellen, wie AWS WAF und AWS Shield Advanced, fallen zusätzliche Gebühren an. Detaillierte Preisinformationen finden Sie auf der AWS Website unter AWS Network Security Manager-Preise.

Verwenden Sie zum ersten Mal?

Wenn Sie AWS Network Security Manager zum ersten Mal verwenden, empfehlen wir Ihnen, die folgenden Themen der Reihe nach zu lesen:

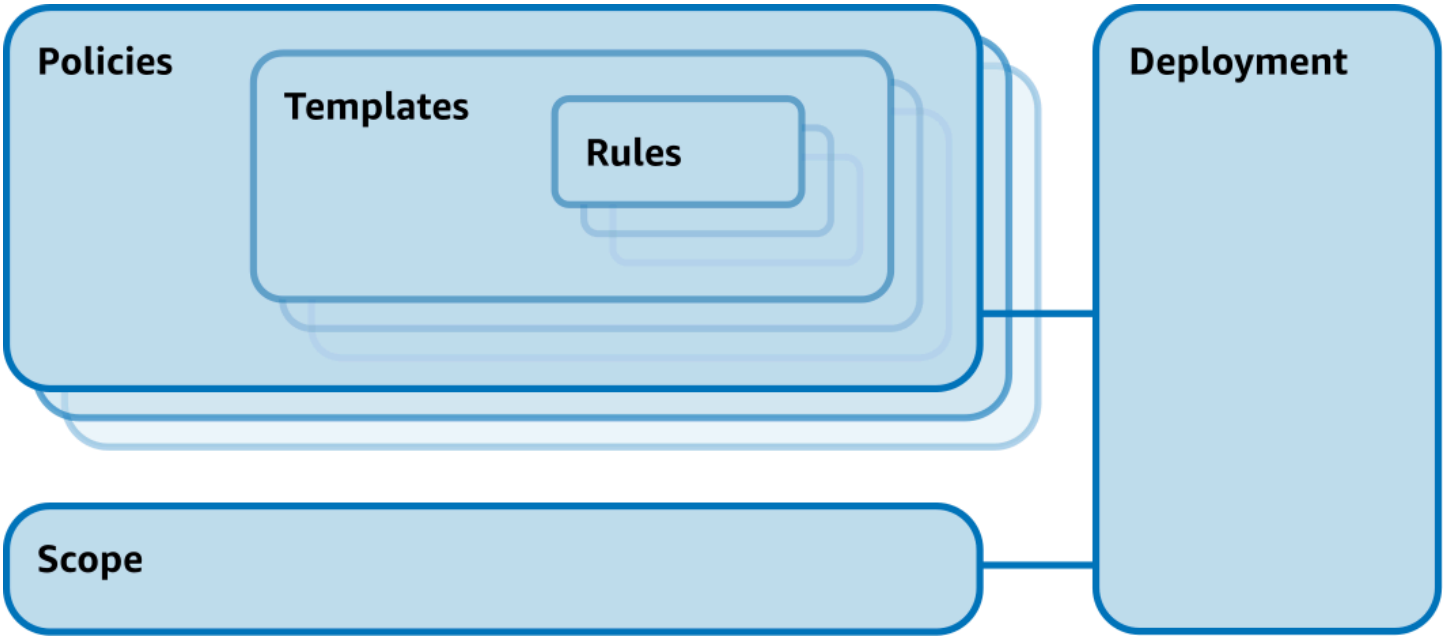
1. Wie funktioniert AWS Network Security Manager— Erfahren Sie mehr über das Ressourcenmodell, den Lebenszyklusstatus, die Zusammenführung von Richtlinien und die Synchronisation.
2. AWS Network Security Manager einrichten— Erfüllen Sie die Voraussetzungen für die Verwendung von AWS Network Security Manager.
3. Tutorial: Implementieren Sie Ihren ersten Netzwerksicherheitsschutz— Sehen Sie sich ein umfassendes Tutorial an, in dem Sie Ihre erste Implementierung erstellen.

Wie AWS Network Security Manager funktioniert

Verwenden Sie das AWS Network Security Manager-Ressourcenmodell, um Netzwerksicherheitsmaßnahmen für Ressourcen in einem einzigen Konto oder für mehrere Konten in Ihrem Unternehmen zu entwerfen und zu verwalten. In diesem Kapitel werden die fünf Ressourcentypen, ihre Hierarchiebildung und die wichtigsten Konzepte erläutert, die ihr Verhalten bestimmen.

AWS Network Security Manager-Ressourcenmodell

AWS Network Security Manager verwendet fünf Ressourcentypen, die in einer Kompositionshierarchie angeordnet sind:



Ressourcen verweisen in der Hierarchie nach oben aufeinander. Regeln werden in Vorlagen und Richtlinien verwendet. Vorlagen, Regeln oder beides werden in Richtlinien verwendet. Ein Geltungsbereich bezieht sich auf die Ressourcen, die Richtlinien innerhalb einer Bereitstellung schützen.

In den folgenden Abschnitten werden die einzelnen Ressourcentypen in der Hierarchie beschrieben.

Regel — Die atomare Einheit der Netzwerksicherheitskonfiguration. Es gibt zwei Arten von Regeln: Regeln zur Überprüfung des Datenverkehrs und Regeln für die Firewall-Konfiguration. Die Verkehrsinspektion konzentriert sich darauf, wie der Sicherheitsdienst mit dem Verkehr umgeht. Eine

Konfigurationsregel spezifiziert Systemvorgänge außerhalb der Verkehrsinspektion. Die Struktur einer Regel variiert je nach Firewalltyp.

Vorlage — Eine geordnete, wiederverwendbare Gruppe von Regeln für einen einzelnen Firewalltyp. Verwenden Sie Vorlagen, um verwandte Regeln zu bündeln und sie für mehrere Richtlinien gemeinsam zu nutzen. Vorlagen sind optional.

Richtlinie — Kombiniert einen geordneten Satz von Vorlagen und Regeln mit Erzwingungseinstellungen für einen Firewalltyp. Jede Richtlinie hat eine Priorität (eine niedrigere Zahl bedeutet eine höhere Priorität). Wenn mehrere Richtlinien dieselbe Ressource schützen, bestimmt die Priorität, wie Konflikte gelöst werden. Bei Regeln für Verkehrsinspektionen bestimmt die Priorität die Reihenfolge, in der die Regeln zusammengefasst werden. Bei Firewall-Konfigurationsregeln bestimmt die Priorität, welche Konfiguration für jede Ressource und die darin enthaltenen Richtlinien gilt.

Geltungsbereich — Eine deklarative Auswahl der Bereiche, in denen Schutzmaßnahmen gelten. Ein Bereich gibt an, welche Ressourcentypen geschützt werden sollen, und Sie können Ressourcen optional nach Tag oder Konfigurationsattribut filtern. Im Modus mit mehreren Konten gibt ein Bereich auch an, welche Konten oder Organisationseinheiten ein- oder ausgeschlossen werden sollen. Im Einzelkontenmodus bezieht sich der Geltungsbereich auf das Konto selbst. Der Modus eines Bereichs ist festgelegt, wenn Sie ihn erstellen. Sie können einen Bereich in keiner der beiden Richtungen zwischen dem Modus für mehrere Konten und dem Modus für ein einzelnes Konto wechseln, sodass aus einem Bereich mit mehreren Konten niemals ein Bereich mit einem einzigen Konto werden kann oder umgekehrt.

Bereitstellung — Bindet eine oder mehrere Richtlinien an einen Geltungsbereich. Durch die Veröffentlichung einer Bereitstellung wird die Durchsetzung aktiviert. AWS Network Security Manager erkennt Ressourcen im Bereich, berechnet die vorgesehene Konfiguration und korrigiert optional nicht synchronisierte Ressourcen.

Grenzwerte für die Ressourcenzusammensetzung finden Sie unter. Kontingente

AWS Lebenszyklus, Zusammenführung und Synchronisation von Network Security Manager-Ressourcen

In den folgenden Abschnitten werden die Verhaltensweisen und Mechanismen erläutert, die bestimmen, wie AWS Network Security Manager-Ressourcen funktionieren, nachdem Sie sie erstellt haben.

Entwurf und aktiver Lebenszyklus

Jede AWS Network Security Manager-Ressource — einschließlich Regeln, Vorlagen, Richtlinien, Bereichen und Bereitstellungen — hat den Status Entwurf oder Aktiv:

- Aktiv — Der Standardstatus. Die Ressource ist veröffentlicht und kann verwendet werden. Andere Ressourcen können auf sie verweisen, und Bereitstellungen, die sie enthalten, setzen ihre Konfiguration durch.
- Entwurf — Die Ressource wurde gespeichert, ist aber noch nicht aktiv. Entwurfsressourcen werden nicht erzwungen und können nicht von anderen Ressourcen referenziert werden. Wenn Sie eine Ressource erstellen oder aktualisieren, wählen Sie Entwurf speichern, um sie im Entwurfsstatus zu belassen.

Standardmäßig erstellt AWS Network Security Manager Ressourcen als Aktiv. Um eine Ressource mithilfe der API als Entwurf zu erstellen, setzen Sie den `isPublished` Parameter `false` im Erstellungs- oder Aktualisierungsvorgang auf.

Wenn Sie eine Ressource aktualisieren, gelten die folgenden Szenarien:

Aktueller Status	Action	Ergebnis
Entwurf	Wählen Sie Entwurf speichern	Aktualisieren Sie den Entwurf (bleibt Entwurf)
Entwurf	Wählen Sie Veröffentlichen	Veröffentlichen Sie den Entwurf (wird aktiv)
Aktiv	Wählen Sie Veröffentlichen	Aktualisieren und aktiv bleiben (Aktiv)
Aktiv	Wählen Sie Entwurf speichern	Erstellen Sie ein Entwurf-Overlay (wird zu Entwurf mit einer aktiven Ressource darunter)

Das `hasPublishedVersion` Feld erscheint in der Liste und Sie erhalten Antworten. In diesem Feld erfahren Sie, ob unter einem Entwurf eine veröffentlichte aktive Ressource vorhanden ist. Wenn eine

Ressource den Status Entwurf hat und `hasPublishedVersion: true` ein ausstehender Entwurf über einer aktiven, veröffentlichten aktiven Ressource steht.

Sie können keine aktive Ressource löschen, auf die eine andere aktive Ressource verweist.

Versionsverwaltung

Jede AWS Network Security Manager-Ressource — einschließlich Regeln, Vorlagen, Richtlinien, Bereichen und Bereitstellungen — kann versioniert werden. Um eine Version einer aktiven Ressource zu erstellen, wählen Sie die Ressource aus, klicken Sie auf Aktion und anschließend auf Versionierten Snapshot erstellen. Versionen werden nicht bei jedem Update automatisch erstellt.

> **AWS CLI-Alternative**
>
> Sie können eine Version auch mithilfe des `Create{Resource}Snapshot` API-Vorgangs für eine aktive Ressource erstellen.

Die wichtigsten Eigenschaften der Version:

- Jede Version hat eine eindeutige Nummer (eine sequentielle Ganzzahl) und einen versionsqualifizierten ARN (z. B.). `arn:aws:network-security-manager:us-east-1:123456789012:rule:abc123:3`
- Versionen sind unveränderlich. Sie können nicht aktualisiert werden.
- Sie können bis zu 10 Versionen pro Ressource erstellen.
- Versionen können mit Tags versehen werden.

Verwenden Sie Versionen, um die gewünschten Konfigurationsvarianten beizubehalten. Um eine Ressource rückgängig zu machen, lesen Sie eine Version und aktualisieren Sie dann die Live-Ressource mit der gewünschten Konfiguration der Version.

Priority-based Zusammenführung von Richtlinien

Wenn mehrere Richtlinien dieselbe Ressource schützen, führt AWS Network Security Manager ihre Konfigurationen zu einem einzigen Ergebnis zusammen. Eine niedrigere Prioritätszahl steht für eine höhere Priorität (Priorität 1 hat Vorrang vor Priorität 2). Wenn AWS Network Security Manager Richtlinien zusammenführt, die Regeln zur Überprüfung des Datenverkehrs enthalten,

bestimmt die Priorität die Reihenfolge, in der die Regeln zusammengefasst werden. Bei Firewall-Konfigurationsregeln bestimmt die Richtlinie mit höherer Priorität, welche Konfiguration gilt.

AWS Network Security Manager bewertet die Priorität auf zwei Ebenen, und zwar in dieser Reihenfolge:

1. Administratorpriorität — AWS Network Security Manager bewertet zuerst die Administratorpriorität. Jedem Organisationsadministrator wird eine Priorität zugewiesen, wie unter beschriebenthe section called “Administrator- und Mitgliedskonten”. Wenn AWS Network Security Manager Richtlinien zusammenführt, stuft er eine Administratorrichtlinie höher ein als die Einzelkonto-Richtlinie eines Mitgliedskontos. Wenn sowohl eine Administratorrichtlinie als auch die Einzelkonto-Richtlinie eines Mitgliedskontos für eine Ressource gelten und ein Konflikt entsteht, gewinnt die Konfiguration der Administratorrichtlinie. Ein Mitgliedskonto kann sich nicht von einer Administratorrichtlinie abmelden, sie außer Kraft setzen oder sich selbst davon ausnehmen.
2. Richtlinienpriorität — Innerhalb jedes Kontos verwendet AWS Network Security Manager dann die Richtlinienpriorität, um verbleibende Konflikte zu lösen. Die Werte für die Richtlinienpriorität sind ganze Zahlen, die bei 1 beginnen und für jedes Konto eindeutig sein müssen.

Sie legen die Administratorpriorität mit dem erforderlichen `priority` Feld für den `PutAdminAccount` Vorgang fest, einer Ganzzahl zwischen 1 und 10. Prioritätswerte sind einzigartig, sodass zwei Administratoren nie dieselbe Priorität haben und es ist auch kein Gleichstand erforderlich. Weitere Informationen finden Sie in der AWS Network Security Manager API-Referenz.

Das zusammengeführte Ergebnis aller geltenden Richtlinien für eine Ressource ist die effektive Firewall-Konfiguration. AWS Network Security Manager berechnet diese Konfiguration, vergleicht sie mit der tatsächlichen Konfiguration der Ressource und meldet alle Unterschiede als Synchronisierungsstatus.

Wenn Richtlinien kollidieren, vergleicht AWS Network Security Manager jedes Attribut und wendet den Wert aus der Richtlinie mit höherer Priorität an. Wenn die Richtlinie mit der höheren Priorität kein Attribut definiert, gilt der Richtlinienwert mit niedrigerer Priorität. Eine Ressource, die der effektiven Konfiguration entspricht, ist IN_SYNC. Eine Ressource, die durch eine Richtlinie mit niedrigerer Priorität geschützt ist, deren Einstellungen durch eine Richtlinie mit höherer Priorität außer Kraft gesetzt wurden, wird für die Bereitstellung mit niedrigerer Priorität als OUT_OF_SYNC gemeldet. Dies ist ein erwartetes Verhalten, kein Fehler.

Ressourcenerkennung mit AWS Config

AWS Network Security Manager erkennt geschützte Ressourcen in Ihren Konten mithilfe eines serviceverknüpften AWS Config-Konfigurationsrekorders. Dieser Rekorder wird automatisch für jedes Konto erstellt, wenn dieses Konto in den Geltungsbereich einer Bereitstellung fällt. Im Gegensatz zu AWS Firewall Manager müssen Sie keine zusätzlichen Einstellungen vornehmen. AWS Die Nutzung der Config durch AWS Network Security Manager wird dem AWS Network Security Manager-Kunden nicht in Rechnung gestellt.

Hauptmerkmale des serviceverknüpften Rekorders:

- Sie heißt `AWSConfigurationRecorderForNetworkSecurityManager`.
- Er ist unabhängig von allen vom Kunden verwalteten Konfigurationsrekordern im Konto.
- Es zeichnet nur die Ressourcentypen auf, die für Ihre aktiven Bereiche und Bereitstellungen relevant sind.
- Sie müssen AWS Config nicht einrichten oder einen Konfigurationsrekorder erstellen. AWS Network Security Manager verwaltet dies automatisch. AWS Die Nutzung der Config durch AWS Network Security Manager wird dem Kunden nicht in Rechnung gestellt.
- Sie können den Rekorder nicht ändern oder löschen, während er verwendet wird. AWS Network Security Manager verwaltet seinen Lebenszyklus automatisch.

Sie müssen AWS Config nicht manuell aktivieren oder konfigurieren, damit AWS Network Security Manager funktioniert. Der Dienst führt die Ressourcenerkennung automatisch durch, nachdem Sie eine Bereitstellung veröffentlicht haben.

Synchronisation und Problembehebung

Die Durchsetzung in AWS Network Security Manager erfolgt asynchron und letztlich konsistent. Nachdem Sie eine Einrichtung veröffentlicht haben oder wenn sich eine Ressource ändert, finden die folgenden Phasen statt:

1. Ressourcenerkennung — AWS Network Security Manager erkennt Ressourcen im Gültigkeitsbereich mithilfe eines serviceverknüpften AWS Config-Recorders.
2. Berechnung der Konfiguration — Für jede erkannte Ressource berechnet AWS Network Security Manager die effektive Firewall-Konfiguration, indem er alle geltenden Richtlinien nach Priorität zusammenführt.

3. Bewertung der Synchronisation — AWS Network Security Manager vergleicht die effektive Konfiguration mit der tatsächlichen Konfiguration der Ressource und zeichnet einen Synchronisierungsstatus auf.
4. Korrektur (optional) — Wenn Sie die Richtlinie aktivieren`remediationEnabled`, korrigiert AWS Network Security Manager nicht synchronisierte Ressourcen, sodass sie der effektiven Konfiguration entsprechen.

Jede Phase ist asynchron. Konsequenzen für Ihren Arbeitsablauf:

- Es gibt eine Verzögerung zwischen der Veröffentlichung einer Bereitstellung und dem Schutz der Ressourcen.
- Es gibt eine Verzögerung zwischen der Erstellung einer neuen Ressource im Geltungsbereich und ihrem Schutz.
- Der `Last Checked` Zeitstempel auf den Einträgen zum Synchronisierungsstatus gibt an, wann AWS Network Security Manager eine Ressource zuletzt bewertet hat.

Bei der Problembehebung und der Säuberung von Ressourcen handelt es sich um Einstellungen auf Richtlinienebene. Sie konfigurieren jede Richtlinie pro Richtlinie im Objekt. `policyConfiguration`

`remediationEnabled`

Gibt an, ob AWS Network Security Manager nicht konforme Ressourcen automatisch behebt. Wenn Sie diese Einstellung aktivieren, korrigiert AWS Network Security Manager Ressourcen, die nicht synchron sind, sodass sie der aktuellen Konfiguration entsprechen.

`resourcesCleanUp`

Gibt an, ob AWS Network Security Manager die von ihm erstellten Ressourcen automatisch entfernt, wenn sie nicht mehr benötigt werden. AWS Network Security Manager löscht eine Firewall, die er erstellt hat, wenn Sie die Bereitstellung entfernen oder wenn das Konto oder die Ressource den Gültigkeitsbereich überschreitet.

Die `resourcesCleanUp` Einstellungen `remediationEnabled` und beide sind standardmäßig auf `false` eingestellt. AWS Network Security Manager repariert oder bereinigt Ressourcen erst, wenn Sie diese Einstellungen aktivieren. Das `policyConfiguration` Objekt gilt auch`wafConfig`, was für AWS WAF-Richtlinien gilt. Weitere Informationen finden Sie in der AWS Network Security Manager API-Referenz.

Wenn eine Ressource nicht synchron ist, enthält der Synchronisierungsstatus Gründe für die Nichtsynchronisierung sowie Details zu den einzelnen Einstellungen, die erwartete Werte im Vergleich zu den tatsächlichen Werten zeigen. Die Gründe sind in die folgenden Kategorien unterteilt:

- `missingFirewall`— Der Ressource ist kein Firewall-Schutz zugeordnet.
- `invalidFirewall`— Eine Firewall ist vorhanden, aber ihre Konfiguration unterscheidet sich von der effektiven Konfiguration. Dazu gehören sechs Detailbereiche:`incorrectSingleValueConfigurations`,`missingAppendableConfigurationVal` `incorrectAppendableConfigurationOrdermissingMergeableConfigurationValues`, undunexpectedMergeableConfigurationValues.

Wenn die Problembehebung aktiviert ist, AWS Network Security Manager jedoch eine Ressource nicht reparieren kann, enthält das `remediationIssues` Feld eine `message` Beschreibung des Problems und einen `correctiveAction` Vorschlag zur Lösung des Problems. `issueType`

AWS Network Security Manager bewertet keine Einstellungen, die er nicht verwaltet. Wenn ein Feld in keiner beitragenden Regel vorkommt, ignoriert AWS Network Security Manager es bei der Synchronisierungsauswertung.

Administrator- und Mitgliedskonten

AWS Network Security Manager verwendet ein kontenübergreifendes Verwaltungsmodell, das auf AWS Organizations basiert:

- Administratorkonto — Das Konto, mit dem Sie AWS Network Security Manager-Ressourcen (Regeln, Vorlagen, Richtlinien, Bereiche und Bereitstellungen) erstellen und verwalten. Sie bestimmen ein oder mehrere Administratorkonten mit jeweils einer Priorität von 1 bis 10.
- Mitgliedskonten — Die Konten, bei denen AWS Network Security Manager Ressourcen erkennt, den Synchronisierungsstatus auswertet und optional nicht synchronisierte Konfigurationen korrigiert. AWS Network Security Manager agiert in Mitgliedskonten über eine dienstbezogene Rolle. Weitere Informationen finden Sie unter the section called “Service-linked Rolle”.

Sie können jeden Administrator optional auf eine Untergruppe von Konten, Organisationseinheiten und Firewalltypen beschränken. Verwenden Sie diese Funktion, um die Verwaltung bestimmter Bereiche an verschiedene Teams zu delegieren.

AWS Network Security Manager ist ein regionaler Dienst. Sie erstellen Ressourcen und Bereitstellungen pro Region ohne regionsübergreifende Abhängigkeiten.

Service-linked Rolle

AWS Network Security Manager verwendet eine mit dem IAM-Dienst verknüpfte Rolle, die so benannt ist`AWSServiceRoleForNetworkSecurityManager`, dass sie in Ihrem Namen in den Mitgliedskonten Ihrer Organisation agiert. Diese Rolle vertraut dem Dienstprinzipal. `network-security-manager.amazonaws.com` Sie verwendet die `NetworkSecurityManagerServiceRolePolicy` AWS verwaltete Richtlinie.

AWS Network Security Manager erstellt diese Rolle automatisch, wenn Sie den Dienst aktivieren, sodass keine manuelle Einrichtung erforderlich ist. Mit dieser Rolle kann AWS Network Security Manager die AWS WAF- und AWS Shield Advanced-Schutzmaßnahmen verwalten, geschützte Ressourcen über AWS Config ermitteln und kontenübergreifende Operationen ausführen. Weitere Informationen finden Sie unter the section called “Service-linked Rollen”.

Einrichtung AWS Manager für Netzwerksicherheit

Mit AWS Network Security Manager können Sie in zwei Organisationsmodellen arbeiten. Verwenden Sie es direkt in einem einzigen Konto oder verwenden Sie es mit AWS Organizations, um den Schutz für mehrere Konten zu verwalten. Die Einrichtungsschritte hängen davon ab, welches Modell Sie wählen.

Topics

- Wählen Sie Ihr Organisationsmodell
- Einrichtung für die Verwendung mit einem einzigen Konto
- Einrichtung für die Verwendung mehrerer Konten mit AWS Organizations
- Erstellen eines AWS Network Security Manager-Administratorkonto
- Erstellen Sie eine IAM-Identität mit AWS Network Security Manager-Berechtigungen
- Verwenden AWS Network Security Manager in Regionen, die standardmäßig deaktiviert sind

Wählen Sie Ihr Organisationsmodell

Wählen Sie aus den folgenden Organisationsmodellen:

- Single-account— Verwenden Sie AWS Network Security Manager, um Ressourcen in einem Konto zu schützen. Sie benötigen weder AWS Organizations noch ein Administratorkonto. Erstellen Sie eine IAM-Identität mit AWS Network Security Manager-Berechtigungen und beginnen Sie direkt mit der Nutzung des Dienstes. AWS Network Security Manager erstellt automatisch eine dienstbezogene Rolle in Ihrem Konto.
- Multi-account— Verwenden Sie AWS Network Security Manager with AWS Organizations, um Ressourcen über mehrere Konten hinweg zu schützen. In diesem Modus müssen AWS Organizations eingerichtet, vertrauenswürdiger Zugriff aktiviert und ein Administratorkonto erstellt werden.

Einrichtung für die Verwendung mit einem einzigen Konto

Um AWS Network Security Manager in einem einzigen Konto zu verwenden, erstellen Sie eine IAM-Identität mit den entsprechenden Berechtigungen und beginnen Sie direkt mit der Nutzung des Dienstes. Sie müssen kein Administratorkonto erstellen. AWS Network Security Manager erstellt im

Hintergrund automatisch eine dienstbezogene Rolle in Ihrem Konto. Fahren Sie mit the section called “Erstellen Sie eine IAM-Identität mit AWS Network Security Manager-Berechtigungen” fort.

Einrichtung für die Verwendung mehrerer Konten mit AWS Organizations

Um den Schutz für mehrere Konten zu verwalten, richten Sie die erforderliche Mitgliedschaft und Konfiguration der AWS Organizations ein.

1. Wählen Sie ein Konto, das Sie als AWS Network Security Manager-Administrator für die Organisation verwenden möchten. Dies ist das Konto, von dem aus Sie AWS Network Security Manager-Ressourcen erstellen und verwalten.
2. Überprüfen Sie die Mitgliedschaft in der Organisation — Falls das von Ihnen gewählte Konto noch kein Mitglied der Organisation ist, lassen Sie es beitreten. Folgen Sie den Anweisungen unter Einladen eines AWS Kontos zum Beitritt zu Ihrer Organisation im Benutzerhandbuch für AWS Organizations.
3. Aktivieren Sie alle Funktionen in Ihrer Organisation — AWS Organizations verfügt über zwei verfügbare Funktionen: Funktionen zur konsolidierten Abrechnung und alle Funktionen. Um AWS Network Security Manager verwenden zu können, muss Ihr Unternehmen für alle Funktionen aktiviert sein. Wenn Ihre Organisation nur für die konsolidierte Fakturierung konfiguriert ist, folgen Sie den Anweisungen unter Aktivieren aller Funktionen in Ihrer Organisation im Benutzerhandbuch für AWS Organizations.
4. Vertrauenswürdigen Zugriff für AWS Network Security Manager aktivieren — Aktivieren Sie vertrauenswürdigen Zugriff für AWS Network Security Manager in AWS Organizations. Wenn der vertrauenswürdige Zugriff aktiviert ist, kann AWS Network Security Manager eine dienstbezogene Rolle in Mitgliedskonten erstellen und Ressourcen in deren Namen verwalten.
5. Ein delegiertes Administratorkonto registrieren — Registrieren Sie das von Ihnen gewählte Konto als delegierten Administrator für AWS Network Security Manager in AWS Organizations. Verwenden Sie das Verwaltungskonto für Organizations, um diesen Schritt abzuschließen.

⚠ Multi-account Schutzmaßnahmen wurden deaktiviert, wenn der vertrauenswürdige Zugriff deaktiviert wurde

Wenn Sie den vertrauenswürdigen Zugriff für AWS Network Security Manager in AWS Organizations deaktivieren oder die Registrierung eines delegierten Administratorkontos

aufheben, setzt AWS Network Security Manager den Umfang und die Bereitstellung mehrerer Konten auf einen `DISABLED` Status und bereinigt die von ihm verwalteten Schutzmaßnahmen.

Erstellen eines AWS Network Security Manager-Administratorkonto

Dieser Schritt gilt nur für den Modus mit mehreren Konten. Nur das Verwaltungskonto der Organisation kann AWS Network Security Manager-Administratorkonten erstellen.

Nachdem Sie das Organisations-Setup abgeschlossen haben, registrieren Sie Ihr Konto als AWS Network Security Manager-Administrator. Sie können dies von der Konsole oder der AWS Befehlszeilenschnittstelle (AWS CLI) aus tun.

Wenn Sie ein Administratorkonto erstellen, erstellt AWS Network Security Manager automatisch eine dienstbezogene Rolle für alle Konten in Ihrer Organisation. Mit dieser Rolle erkennt AWS Network Security Manager Ressourcen und verwaltet die Schutzmaßnahmen in den Mitgliedskonten.

Mit AWS Network Security Manager können Sie mehrere Administratoren haben, die die Firewall-Ressourcen Ihres Unternehmens verwalten. Wenn Sie mehrere Administratoren in Ihrer Organisation einsetzen möchten, können Sie für jeden Administrator Bedingungen für den administrativen Geltungsbereich festlegen, um die Ressourcen zu definieren, die er verwalten kann. Dies gibt Ihnen die Flexibilität, innerhalb Ihrer Organisation unterschiedliche Administratorrollen zu haben, und hilft Ihnen, das Prinzip des geringsten Zugriffs beizubehalten. Beispielsweise kann ein Administrator eine Reihe von Organisationseinheiten (OUs) verwalten. Ein anderer Administrator kann nur bestimmte Richtlinientypen verwalten.

Die maximale Anzahl von Administratoren, die Sie pro Organisation haben können, finden Sie unterKontingente.

Registrierung der Region

Sie registrieren ein AWS Network Security Manager-Administratorkonto in einer einzigen AWS Region. Um AWS Network Security Manager in weiteren Regionen zu verwenden, wiederholen Sie diesen Schritt in jeder Region.

Um ein Administratorkonto mit der Konsole zu erstellen

1. Öffnen Sie die AWS Network Security Manager-Konsole unter https://console.aws.amazon.com/network-security-manager/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie Administrator hinzufügen.
4. Wählen Sie das Konto aus und geben Sie einen Prioritätswert ein (1 bis 10).
5. Wählen Sie zur Bestätigung Administrator hinzufügen aus.

Um ein Administratorkonto zu erstellen, verwenden Sie AWS CLI

Aufrufen der `PutAdminAccount`-Operation. Sie müssen einen Prioritätswert (1 bis 10) angeben.

Das folgende AWS CLI-Beispiel registriert ein Konto als AWS Network Security Manager-Administrator mit Priorität 1:

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

Sie können mehrere Administratorkonten mit jeweils unterschiedlicher Priorität festlegen. Optional können Sie jeden Administrator auf bestimmte Konten, Organisationseinheiten oder Firewalltypen beschränken, indem Sie einen `adminScope` Parameter angeben.

Um ein Administratorkonto mithilfe der Konsole zu entfernen

> ⚠ Multi-account Der Schutz wurde beim Entfernen eines Administrators deaktiviert
>
> Wenn Sie ein Administratorkonto entfernen, setzt AWS Network Security Manager den Geltungsbereich und die Bereitstellung mehrerer Konten auf einen `DISABLED` Status und bereinigt die von ihm verwalteten Schutzmaßnahmen.

1. Öffnen Sie die AWS Network Security Manager-Konsole unter. https://console.aws.amazon.com/network-security-manager/
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie das Administratorkonto aus, das Sie entfernen möchten.

4. Wählen Sie Remove administrator (Administrator entfernen) aus.
5. Wählen Sie zur Bestätigung die Option Administratorlöschung bestätigen aus.

Erstellen Sie eine IAM-Identität mit AWS Network Security Manager-Berechtigungen

Um AWS Network Security Manager verwenden zu können, benötigen Sie eine IAM-Identität (Benutzer oder Rolle) mit Berechtigungen zum Aufrufen von AWS Network Security Manager-Vorgängen. Die IAM-Aktionen verwenden das Präfix. `network-security-manager`

Das folgende Beispiel für eine IAM-Richtlinie enthält drei Anweisungen. Die erste Anweisung gewährt vollen Zugriff auf alle AWS Network Security Manager-Vorgänge. Die zweite Anweisung gewährt die zusätzlichen AWS Organizations- und AWS WAF-Berechtigungen, die AWS Network Security Manager benötigt. AWS Network Security Manager verwendet diese Berechtigungen, um die Konten und Organisationseinheiten (OUs) in Ihrer Organisation zu identifizieren und die verfügbaren WAF-Regelgruppen und verwalteten Produkte aufzulisten. Diese Berechtigungen ermöglichen AWS es Network Security Manager auch, vertrauenswürdigen Zugriff zu aktivieren und einen delegierten Administrator in AWS Organizations zu registrieren. Die dritte Anweisung erteilt AWS Network Security Manager die `iam:CreateServiceLinkedRole` Berechtigung, die er benötigt, um seine dienstbezogene Rolle zu erstellen, die sowohl für die Verwendung mit einem Konto als auch für die Verwendung mit mehreren Konten erforderlich ist.

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

Für den produktiven Einsatz empfehlen wir, nur die erforderlichen Mindestberechtigungen zu gewähren. Weitere Informationen finden Sie unter the section called “Identity and Access Management”.

Melden Sie sich an für ein AWS-Konto

Um loszulegen AWS, benötigen Sie eine AWS-Konto. Informationen zum Erstellen eines AWS-Konto finden Sie unter Erste Schritte mit einem AWS-Konto im AWS -Kontenverwaltung Referenzhandbuch.

Verwenden AWS Network Security Manager in Regionen, die standardmäßig deaktiviert sind

Um AWS Network Security Manager in einer Region zu verwenden, die standardmäßig deaktiviert ist, müssen Sie die Region sowohl für das Verwaltungskonto Ihrer Organisation als auch für das AWS Network Security Manager-Administratorkonto aktivieren. Informationen zu Regionen, die standardmäßig deaktiviert sind, und zu deren Aktivierung finden Sie unter AWS Regionen verwalten in der AWS allgemeinen Referenz.

So aktivieren Sie eine deaktivierte Region

Folgen Sie sowohl für das Organisationsverwaltungskonto als auch für das AWS Network Security Manager-Administratorkonto den Anweisungen unter Region aktivieren in der AWS Allgemeinen Referenz.

Implementieren Sie Ihren ersten Netzwerksicherheitsschutz

Dieses Tutorial führt Sie durch die Bereitstellung einer AWS WAF-Web-ACL mithilfe der AWS Network Security Manager-Konsole. Sie führen die folgenden Schritte aus:

1. Erstellen einer Regel
2. Erstellen Sie eine Vorlage
3. Erstellen einer Richtlinie
4. Erstellen eines Geltungsbereichs
5. Erstellen und veröffentlichen Sie ein Deployment
6. Überwachen Sie den Synchronisierungsstatus

In diesem Tutorial erstellen Sie eine AWS WAF-Web-ACL, die Application Load Balancer für Ihre ausgewählten Konten schützt. Dieser Vorgang ist für alle Sicherheitsdienste und Firewalls, die von AWS Network Security Manager unterstützt werden, weitgehend identisch.

Zeit bis zur Fertigstellung: ca. 10 Minuten

Kosten: In diesem Tutorial werden AWS Dienste verwendet, für die möglicherweise Gebühren anfallen. Aktuelle Preise finden Sie auf der AWS Website unter AWS Network Security Manager-Preise.

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen:

- Die Einrichtungsschritte wurden wie unter beschrieben abgeschlossen AWS Network Security Manager einrichten.
- Eine AWS Identity and Access Management (IAM) -Identität mit AWS Network Security Manager-Berechtigungen.
- Eine AWS Organizations mit allen aktivierten Funktionen und einem bestimmten AWS Network Security Manager-Administratorkonto (erforderlich für Bereitstellungen mit mehreren Konten).
- Zugriff auf die AWS Network Security Manager-Konsole.

Schritt 1: Erstellen Sie eine Regel

Eine Regel ist der Baustein Ihrer Sicherheitskonfiguration. In diesem Schritt erstellen Sie zwei AWS WAF-Regeln: eine, die die Standardaktion festlegt, und eine, die die Sichtbarkeitskonfiguration festlegt. Standardaktion und VisibilityConfig sind Pflichtfelder für eine AWS WAF-Web-ACL.

Gehen Sie folgendermaßen vor, um die Standardaktionsregel zu erstellen:

1. Öffnen Sie die AWS Network Security Manager-Konsole unter https://console.aws.amazon.com/network-security-manager/.
2. Wählen Sie im Navigationsbereich Overview (Übersicht) aus.
3. Wählen Sie auf der Übersichtsseite die Option Regel erstellen aus.
4. Geben Sie unter Regelname einen aussagekräftigen Namen ein, z. B. `my-default-action-rule`
5. Wählen Sie im Abschnitt Regeldefinition für Firewalltyp die Option AWS WAF aus.
6. Wählen Sie für Regeltyp auswählen die Option Konfiguration aus.
7. Wählen Sie Konfigurationstypen einfügen und anschließend Standardaktion aus. Ein JSON-Editor mit einer Standardkonfiguration wird angezeigt.
8. Entfernen Sie im JSON-Editor den `Block` Abschnitt und behalten Sie nur den `Allow` Abschnitt bei.
9. Wählen Sie Regel erstellen aus.

Gehen Sie folgendermaßen vor, um die VisibilityConfig Regel zu erstellen:

1. Wählen Sie im Navigationsbereich Overview (Übersicht) aus.
2. Wählen Sie auf der Übersichtsseite die Option Regel erstellen aus.
3. Geben Sie unter Regelname einen aussagekräftigen Namen ein, z. B. `my-visibility-config-rule`
4. Wählen Sie im Abschnitt Regeldefinition für Firewalltyp die Option AWS WAF aus.
5. Wählen Sie für Regeltyp auswählen die Option Konfiguration aus.
6. Wählen Sie Konfigurationstypen einfügen und wählen Sie dann aus VisibilityConfig. Ein JSON-Editor mit einer Standardkonfiguration wird angezeigt.
7. Wählen Sie Regel erstellen aus.

AWS CLI-Alternative

Sie können Regeln auch mit der AWS CLI erstellen:

```
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
```

Schritt 2: Erstellen Sie eine Vorlage

Eine Vorlage gruppiert eine oder mehrere Regeln für die richtlinienübergreifende Wiederverwendung. In diesem Schritt erstellen Sie eine Vorlage, die die Regel aus Schritt 1 enthält:

1. Wählen Sie im Navigationsbereich Overview (Übersicht) aus.
2. Wählen Sie auf der Übersichtsseite die Option Vorlage erstellen aus.
3. Geben Sie als Vorlagenname einen aussagekräftigen Namen ein, z. B. `my-waf-template`
4. Wählen Sie als Firewalltyp AWS WAF aus.
5. Wählen Sie im Abschnitt Regeln die Option Regel hinzufügen und wählen Sie die Regeln aus, die Sie in Schritt 1 erstellt haben.
6. Wählen Sie Create template (Vorlage erstellen) aus.

AWS CLI-Alternative

Sie können auch eine Vorlage mit der AWS CLI erstellen:

```
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
```

Schritt 3: Erstellen Sie eine Richtlinie

Eine Richtlinie kombiniert Vorlagen mit Durchsetzungseinstellungen. In diesem Schritt erstellen Sie eine Richtlinie, die auf Ihre Vorlage verweist und automatische Problembehebungen ermöglicht:

1. Wählen Sie im Navigationsbereich Overview (Übersicht) aus.
2. Wählen Sie auf der Übersichtsseite die Option Richtlinie erstellen aus.
3. Geben Sie als Richtlinienname einen aussagekräftigen Namen ein, z. B. `my-waf-policy`
4. Wählen Sie als Firewall-Typ AWS WAF aus.
5. Im Abschnitt Richtlinienpriorität werden die vorhandenen Richtlinien und ihre Prioritäten angezeigt. Überprüfen Sie die Priorität der neuen Richtlinie. Wenn Sie sie anpassen müssen, wählen Sie das Prioritätsfeld aus und ändern Sie den Wert in 1 oder eine ungenutzte Prioritätsnummer.
6. Wählen Sie im Abschnitt Vorlagen und Regeln die Option Vorlage hinzufügen und wählen Sie die Vorlage aus, die Sie in Schritt 2 erstellt haben.
7. Wählen Sie für Korrektur die Option Aktiviert aus.
8. Wählen Sie für die Web-ACL-Auflösung für bestehende Kunden die Option Keine Korrektur aus.
9. Wählen Sie Richtlinie erstellen aus.

AWS CLI-Alternative

Sie können eine Richtlinie auch mit der AWS CLI erstellen:

```
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
```

Schritt 4: Erstellen Sie einen Bereich

Ein Geltungsbereich definiert, wo Ihre Schutzmaßnahmen gelten. In diesem Schritt erstellen Sie einen Bereich, der auf Application Load Balancer in Ihren Konten abzielt:

1. Wählen Sie im Navigationsbereich Overview (Übersicht) aus.
2. Wählen Sie auf der Übersichtsseite die Option Bereich erstellen aus.
3. Geben Sie als Bereichsname einen beschreibenden Namen ein, z. B. `my-alb-scope`
4. (Optional) Wählen Sie im Abschnitt Auswahl von Konten und Organisationseinheiten für Methode zur Steuerung des administrativen Geltungsbereichs die Option Gültigkeitsbereich für die gesamte AWS Organisation (alle Organisationseinheiten und Konten) aus. Überspringen Sie diesen Schritt bei Bereitstellungen mit einem einzigen Konto.
5. Wählen Sie im Abschnitt Ressourcen für Ressourcentypen die Option Application Load Balancer aus.
6. Wählen Sie Create scope (Bereich erstellen).

AWS CLI-Alternative

Sie können einen Bereich auch mit der AWS CLI erstellen:

```
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
```

Schritt 5: Eine Bereitstellung erstellen und veröffentlichen

Eine Bereitstellung bindet Richtlinien an einen Geltungsbereich und aktiviert deren Durchsetzung. So erstellen und veröffentlichen Sie eine Bereitstellung:

1. Wählen Sie im Navigationsbereich Overview (Übersicht) aus.
2. Wählen Sie auf der Übersichtsseite die Option Bereitstellung erstellen aus.
3. Geben Sie als Bereitstellungsname einen aussagekräftigen Namen ein, z. B. `my-first-deployment`
4. Wählen Sie im Abschnitt Richtlinien die Option Richtlinie hinzufügen und wählen Sie die Richtlinie aus, die Sie in Schritt 3 erstellt haben.
5. Wählen Sie im Abschnitt Bereiche die Option Bereich hinzufügen und wählen Sie den Bereich aus, den Sie in Schritt 4 erstellt haben.
6. Wählen Sie Create deployment.

AWS Network Security Manager beginnt mit der Suche nach Ressourcen und der Anwendung von Schutzmaßnahmen. Dieser Vorgang ist asynchron und kann einige Minuten dauern.

AWS CLI-Alternative

Sie können eine Bereitstellung auch mit der AWS CLI erstellen und veröffentlichen:

```
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
```

Schritt 6: Synchronisierungsstatus überwachen

Nachdem Sie eine Bereitstellung veröffentlicht haben, erkennt AWS Network Security Manager Ressourcen und synchronisiert deren Konfigurationen. Um den Status der einzelnen Ressourcen zu überwachen, gehen Sie wie folgt vor:

1. Wählen Sie im Navigationsbereich Overview (Übersicht) aus.
2. Wählen Sie die Registerkarte Bereitstellen.
3. Wählen Sie die Bereitstellung aus, die Sie in Schritt 5 erstellt haben.
4. Wählen Sie die Registerkarte Synchronisation.
5. Überprüfen Sie den Synchronisierungsstatus für jede Ressource:
   - IN_SYNC — Die Ressourcenkonfiguration entspricht Ihren beabsichtigten Schutzeinstellungen.
   - OUT_OF_SYNC — Die Ressourcenkonfiguration stimmt nicht überein. AWS Network Security Manager behebt dies automatisch, wenn die Wiederherstellung aktiviert ist.
   - NOT_APPLICABLE — Die Ressource befindet sich im Gültigkeitsbereich, kann aber durch diese Bereitstellung nicht bewertet werden.

> **AWS CLI-Alternative**
>
> Sie können den Synchronisationsstatus auch mit der AWS CLI überprüfen:

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

Schritt 7: Bereinigen

Wenn Sie die von Ihnen erstellten Ressourcen nicht mehr benötigen, löschen Sie sie in umgekehrter Reihenfolge, um die Durchsetzung zu verhindern und den Schutz für Ressourcen aufzuheben, die in den Geltungsbereich fallen:

Die umgekehrte Reihenfolge ist wichtig, da diese Ressourcen aufeinander verweisen.
Um zu sehen, was mit einer Ressource verknüpft ist, bevor Sie sie löschen, rufen Sie `ListResourceAssociations` mit dem ARN dieser Ressource auf. Es gibt den ARN und den Ressourcentyp jeder zugehörigen Ressource zurück. Weitere Informationen finden Sie in der AWS Network Security Manager API-Referenz.

1. Wählen Sie im Navigationsbereich Overview (Übersicht) aus. Wählen Sie die Registerkarte Bereitstellen. Wählen Sie Ihre Bereitstellung aus, klicken Sie auf Aktion und anschließend auf Löschen.

2. Wählen Sie die Registerkarte Bereiche aus. Wählen Sie Ihren Bereich aus, klicken Sie auf Aktion und anschließend auf Löschen.
3. Wählen Sie die Registerkarte Policies. Wählen Sie Ihre Richtlinie aus, wählen Sie Aktion und dann Löschen aus.
4. Wählen Sie die Registerkarte Templates (Vorlagen) aus. Wählen Sie Ihre Vorlage aus, wählen Sie Aktion und anschließend Löschen aus.
5. Wählen Sie die Registerkarte Rules (Regeln). Wählen Sie Ihre Regel aus, wählen Sie Aktion und dann Löschen.

AWS CLI-Alternative

Bevor Sie eine Ressource löschen, überprüfen Sie ihre Verknüpfungen, um die Löschreihenfolge zu planen:

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

Wenn eine Ressource immer noch Verknüpfungen hat, entfernen oder löschen Sie zuerst die zugehörigen Ressourcen.
Sie können Ressourcen mit der AWS CLI in umgekehrter Reihenfolge löschen:

```
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"
```

Nächste Schritte

Nachdem Sie nun über eine funktionierende Bereitstellung verfügen, sollten Sie die folgenden Möglichkeiten zur Erweiterung Ihres Netzwerksicherheitsschutzes erkunden:

- Erfahren Sie mehr über das Ressourcenmodell und den Lebenszyklus inWie funktioniert AWS Network Security Manager.
- Verwenden Sie den draft/publish Workflow, um Änderungen zu implementieren, bevor sie wirksam werden. Weitere Informationen finden Sie unter the section called “Entwurf und aktiver Lebenszyklus”.
- Erstellen Sie Schnappschüsse, um zweifelsfrei funktionierende Konfigurationen beizubehalten. Weitere Informationen finden Sie unter the section called “Versionsverwaltung”.
- Wird verwendet`GenerateRuleConfiguration`, um Regeln aus Beschreibungen in natürlicher Sprache zu erstellen. Weitere Informationen finden Sie in der AWS Network Security Manager API-Referenz.
- Erfahren Sie mehr über die Verwaltung von AWS WAF- und AWS Shield Advanced-Schutzmaßnahmen in Ihrem Unternehmen. Weitere Informationen finden Sie unter Verwaltung von Firewalls und Sicherheitsdiensten.

Verwaltung von Firewalls und Sicherheitsdiensten

Mit AWS Network Security Manager definieren und implementieren Sie Sicherheitsrichtlinien für mehrere Firewalls und Sicherheitsdienste. Obwohl das AWS Netzwerksicherheitsportfolio gemeinsame Elemente umfasst, gibt es wichtige Variationen, die Sie in AWS Network Security Manager berücksichtigen müssen.

Für jeden unterstützten Netzwerksicherheitsdienst werden in den folgenden Unterabschnitten die einzelnen Elemente und Schritte sowohl für eine Schnellerstellung als auch für einen detaillierten Standarderstellungsprozess beschrieben.

Verwaltung von Web-ACLs für AWS WAF

Mit AWS Network Security Manager können Sie AWS WAF-Web-Zugriffskontrolllisten (Web-ACLs) für Konten und Ressourcen in Ihrem Unternehmen zentral konfigurieren und bereitstellen. Sie können AWS Network Security Manager-Regeln für AWS WAF definieren, sie in Schutzvorlagen gruppieren und sie mithilfe von AWS Network Security Manager-Richtlinien und -Bereitstellungen in großem Umfang durchsetzen.

AWS WAF-Konzepte

Die folgenden Konzepte sind spezifisch für die Verwendung von AWS Network Security Manager mit AWS WAF. Weitere Informationen zur Funktionsweise von AWS Network Security Manager finden Sie unterWie funktioniert AWS Network Security Manager.

AWS WAF-Regeltypen

Für AWS WAF gibt es zwei Arten von Regeln:

- INSPEKTION — Enthält eine Regelgruppendefinition mit `PreProcessFirewallManagerRuleGroups` (Regeln, die vor kundendefinierten Regeln ausgeführt werden) oder `PostProcessFirewallManagerRuleGroups` (Regeln, die danach ausgeführt werden).
- KONFIGURATION — Enthält eine einzige Web-ACL-Konfigurationseinstellung. Die Konfigurations-JSON muss genau einen Schlüssel der obersten Ebene enthalten, der einer unterstützten Einstellung entspricht (z. B. `Description` `DefaultActionVisibilityConfig`,`LoggingConfiguration`,`CaptchaConfig`,,`ChallengeConfig` `OnSourceDDoSProtectionConfigTokenDomains`, oder`MonetizationConfig`).

Die meisten Web-ACL-Konfigurationseinstellungen entsprechen den Parametern des AWS WAF-Vorgangs`CreateWebACL`. Weitere Informationen zu diesen Einstellungen und ihren Definitionen finden Sie unter CreateWebACL in der AWS WAF-API-Referenz.

Die Ausnahme ist`LoggingConfiguration`, was Sie separat konfigurieren. Weitere Informationen finden Sie unter the section called “Protokollierung”.

AWS Zusammenführung von WAF-Richtlinien

Für AWS WAF verwendet jede Konfigurationseinstellung eine der folgenden Zusammenführungsstrategien:

SingleValue

Einstellungen, die nur einen Wert haben können. Die Richtlinie mit der höchsten Priorität gewinnt. Prioritätswerte sind einzigartig, sodass zwei Richtlinien nicht unterschiedliche Werte mit derselben Priorität definieren können. Weitere Informationen darüber, wie AWS Network Security Manager Prioritäten löst, finden Sie unterthe section called “Priority-based Zusammenführung von Richtlinien”. Die folgenden Einstellungen verwenden SingleValue:`DefaultAction`,`VisibilityConfig`,`CaptchaConfig`,`ChallengeConfig`,`OnSourceDI` `LoggingConfiguration`,`MonetizationConfig`, und`Description`.

Anhängen (und AppendAndSort)

Einträge aus allen Richtlinien werden in der Reihenfolge ihrer Priorität an die Liste angehängt. `TokenDomains`und `DataProtectionConfig.DataProtections` verwenden Sie Append. `PreProcessFirewallManagerRuleGroups`und `PostProcessFirewallManagerRuleGroups` use AppendAndSort, wodurch Regelgruppen aus allen Richtlinien angehängt und nach Priorität sortiert werden. Die Reihenfolge ist wichtig, da die AWS WAF Regelgruppen sequentiell auswertet.

Mischen von

Einträge aus allen Richtlinien werden unabhängig von ihrer Priorität zu einem einzigen Satz zusammengeführt. `CustomResponseBodies`und `AssociationConfig.RequestBody` verwenden Sie Merge.

Die Strategien Append AppendAndSort, Merge und Append entfernen doppelte Einträge. Wenn zwei Richtlinien zur identischen Konfiguration beitragen, behält AWS Network Security Manager den Eintrag aus der Richtlinie mit der höheren Priorität bei. Die tatsächliche Konfiguration enthält daher eine Kopie dieses Eintrags, nicht eine Kopie pro beitragender Richtlinie.

Bestehende Web-ACL-Auflösung

Verwenden Sie die `existingCustomerWebACLResolution` Einstellung für eine AWS WAF-Richtlinie, um anzugeben, wie AWS Network Security Manager mit Ressourcen umgeht, die bereits über eine vom Kunden verwaltete Web-ACL verfügen:

- `RETROFIT`— Aktualisieren Sie Ihre bestehende Web-ACL, um sie an die aktuelle Konfiguration anzupassen.
- `OVERRIDE_ASSOCIATION`— Ordnen Sie der Ressource stattdessen eine von AWS Network Security Manager verwaltete Web-ACL zu.
- `NO_REMEDIATION`— Korrigieren Sie nicht, wenn Ihre Web-ACL vorhanden ist.

Protokollieren des ACL-Datenverkehrs

Sie steuern die Web-ACL-Protokollierung mit der `LoggingConfiguration` Einstellung in einer Richtlinie. AWS Network Security Manager wendet diese Einstellung mithilfe der AWS `PutLoggingConfiguration` WAF-Operation an. Sie können ein Protokollierungs-Ziel pro Web-ACL definieren. Weitere Informationen finden Sie PutLoggingConfigurationin der AWS WAF-API-Referenz.

Jede in den Geltungsbereich fallende Web-ACL, die von der Richtlinie verwaltet wird, sendet ihre Protokolle an das in der Richtlinie angegebene Ziel. Auf diese Weise erhalten Sie eine zentralisierte Protokollierung aller Konten in Ihrer Organisation. Verwenden Sie es, um detaillierte Informationen über den Datenverkehr zu erhalten, den Ihre Web-ACLs unternehmensweit analysieren.

Für eine zentralisierte Protokollierung über mehrere Konten hinweg können Sie Protokolle an einen Amazon S3 S3-Bucket oder einen Amazon Data Firehose-Lieferstream senden. Für jeden Zieltyp ist eine zusätzliche Konfiguration erforderlich, die Sie abschließen müssen, bevor AWS Network Security Manager die AWS WAF-Protokollierung für Ihre Ressourcen und Konten verwalten kann. Der Zielname muss mit beginnen. `aws-waf-logs-`

Amazon Data Firehose

Erstellen Sie den Delivery Stream mit den folgenden Eigenschaften:

- Mit Ihrem AWS Network Security Manager-Administratorkonto erstellt
- Ein Name, der `aws-waf-logs-` beispielsweise mit beginnt `aws-waf-logs-network-security-manager-central`

- Eine PUT Quelle
- Erstellt in der Region, in der Sie tätig sind, oder in der Region USA Ost (Nord-Virginia), wenn Sie Logs für Amazon erfassen CloudFront

Bevor Sie den Delivery Stream verwenden, testen Sie ihn, um sicherzustellen, dass er über einen ausreichenden Durchsatz für die Logs Ihrer Organisation verfügt. Weitere Informationen finden Sie unter Creating a Amazon Data Firehose Delivery Stream im Amazon Data Firehose Developer Guide.

Amazon S3

Erstellen Sie den Bucket gemäß der Amazon S3 S3-Anleitung im AWS WAF Developer Guide. Sie müssen den Bucket auch mit den Berechtigungen konfigurieren, die es der Protokollzustellung ermöglichen, in ihn zu schreiben. Die folgende Bucket-Richtlinie gewährt diese Berechtigungen.

```
{
    "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*Ersetzen Sie es durch Ihr eigenes Bucket-Namensuffix und *policy-id* ersetzen Sie es durch die ID Ihrer Richtlinie.

> **CloudWatch Logs unterstützt nur die Verwendung eines einzelnen Kontos**
>
> Wenn Sie AWS Network Security Manager für mehrere Konten verwenden, können Sie keine Amazon CloudWatch Logs-Protokollgruppe als Protokollierungsziel verwenden. Die Protokollgruppe muss sich im selben AWS Konto und in derselben Region wie die Web-ACL befinden. Verwenden Sie für Bereitstellungen mit mehreren Konten stattdessen einen Amazon S3 S3-Bucket oder einen Amazon Data Firehose-Lieferstream.

Quick Create für AWS WAF

Mit Quick Create definieren und implementieren Sie AWS WAF-Schutzmaßnahmen in einem einzigen geführten Arbeitsablauf. Verwenden Sie Quick Create, wenn Sie einen vollständigen Web-ACL-Schutz von Regeln bis hin zur Bereitstellung in einer Sitzung einrichten möchten.

Um einen AWS WAF-Schutz mit Quick Create zu definieren und bereitzustellen, führen Sie die folgenden Verfahren der Reihe nach durch.

Um die Richtlinie zu erstellen und Schutzmaßnahmen hinzuzufügen

1. Öffnen Sie die AWS Network Security Manager-Konsole unter https://console.aws.amazon.com/network-security-manager/.
2. Wählen Sie im Navigationsbereich Overview (Übersicht) aus.
3. Wählen Sie oben rechts auf der Übersichtsseite die Option Schnelles Erstellen und Bereitstellen aus. Die Seite „Schnelles Erstellen und Bereitstellen“ wird mit mehreren Bereichen angezeigt.
4. Geben Sie im Bereich mit den Richtliniendetails für Name einen Richtliniennamen ein. (Optional) Geben Sie unter Description (Beschreibung) eine Beschreibung ein.
5. Wählen Sie im Bereich Schutzmaßnahmen definieren den Firewalltyp aus, mit dem Sie arbeiten möchten. Wählen Sie AWS WAF aus. Ein Unterbereich Vorlagen und Regeln wird angezeigt, in dem Sie Regeln oder Vorlagen hinzufügen können.

6. Um Regeln hinzuzufügen, wählen Sie Regeln hinzufügen oder verwalten. Wählen Sie im daraufhin angezeigten Fenster unter Regeltyp auswählen eine der folgenden Optionen aus:
   - AWS Verwaltete Regeln — Die Tabelle zeigt alle AWS verwalteten Regeln, die AWS WAF unterstützt.
   - Regeln — Die Tabelle zeigt die AWS WAF-Regelgruppen, deren Eigentümer Sie sind, mit Ausnahme der AWS verwalteten Regeln.

   Aktivieren Sie die Kontrollkästchen für die Regeln, die Sie zu Ihrer Richtlinie hinzufügen möchten. Wählen Sie dann Regeln hinzufügen.
7. Um Vorlagen hinzuzufügen, wählen Sie Vorlagen hinzufügen. Im daraufhin angezeigten Fenster Vorlagen hinzufügen werden in der Tabelle alle verfügbaren Vorlagen angezeigt. Wählen Sie die Vorlagen aus, die Sie möchten, zusammen mit der Version, die in die Richtlinie aufgenommen werden soll. Wählen Sie dann Vorlagen hinzufügen.

Um die Richtlinie zu konfigurieren

1. Überprüfen Sie Ihre Auswahl in der Tabelle Vorlagen und Regeln. Die Ganzzahl in der Spalte Position bestimmt die Bewertungsreihenfolge der Regeln und Vorlagen. Um die Bewertungsreihenfolge zu ändern, wählen Sie den Positionswert in der Spalte Position aus. Verwenden Sie die Pfeile, um den Wert zu ändern. Um die Änderung zu akzeptieren, wählen Sie Bestätigen. Um die Änderung rückgängig zu machen, wählen Sie Abbrechen.
2. Legen Sie unter Richtlinienkonfiguration im Bereich Schutzmaßnahmen definieren fest, welche automatisierten Aktionen AWS Network Security Manager im Zielbereich durchführt:
   - Bei der Wiederherstellung wird die definierte Richtlinie auf alle Ressourcen angewendet, deren Sicherheitsstatus nicht mit dem gewünschten Status synchronisiert ist, der in AWS Network Security Manager beschrieben ist.
   - Die Ressourcensäuberung löscht die Firewall, die AWS Network Security Manager für eine Ressource erstellt hat, wenn die Bereitstellung entfernt wird oder wenn das Konto oder die Ressource außerhalb des Gültigkeitsbereichs liegt.
   - Die WebACL-Lösung für bestehende Kunden bestimmt, wie Konflikte zwischen der Richtlinie, die Sie definieren, und den möglicherweise bereits bereitgestellten Richtlinien gelöst werden. Wählen Sie im Menü eine der folgenden Optionen aus:
     - Keine Standardisierung überspringt die Standardisierung für alle Ressourcen, die bereits über eine Web-ACL verfügen.

- Durch die Override-Zuordnung wird die vorhandene Web-ACL durch die von AWS Network Security Manager erstellte Web-ACL ersetzt.
- Retrofit passt seine Regeln an jede bestehende Web-ACL an und behält die der Ressource zugeordnete Web-ACL bei.

3. Legen Sie im Bereich Richtlinienpriorität die Priorität fest. AWS Network Security Manager bewertet Richtlinien nach ihrer Priorität, um Konflikte zu lösen. Niedrigere Positionen (niedrigere Ganzzahlen) haben eine höhere Priorität. Um die Priorität zu bearbeiten, wählen Sie den Wert Position. Erhöhen Sie ihn dann mit den Pfeilen oder geben Sie direkt einen Wert ein. Um die Auswahl zu bestätigen, wählen Sie Bestätigen. Um die Änderung zu verwerfen, wählen Sie Abbrechen.

Um den Geltungsbereich festzulegen

1. Definieren Sie im Bereich Umfang festlegen die Gruppe von Ressourcen, für die die Richtlinien gelten. Geben Sie unter Bereichsname einen Namen ein. (Optional) Geben Sie unter Description (Beschreibung) eine Beschreibung ein.
2.
> **Multi-account nur Modus**
>
> Dieser Schritt gilt nur für den Modus mit mehreren Konten. Verwenden Sie im Modus mit mehreren Konten den Unterbereich zur Auswahl von Konten und Organisationseinheiten, um auszuwählen, welche Konten oder Organisationseinheiten ein- oder ausgeschlossen werden sollen. Im Einzelkontenmodus wird dieser Unterbereich nicht in der Konsole angezeigt. Überspringen Sie diesen Schritt also.

   Wählen Sie im Unterbereich zur Auswahl von Konten und Organisationseinheiten eine der folgenden Optionen aus:

   - Geltungsbereich für die gesamte AWS Organisation. Es ist keine weitere Definition erforderlich.
   - Geltungsbereich für das gesamte AWS Unternehmen, ausgenommen sind jedoch bestimmte Organisationseinheiten und Konten. Ein Unterbereich für Organisationseinheiten und ein Unterbereich für Konten werden angezeigt. Um Organisationseinheiten auszuschließen, wählen Sie Organisationseinheiten hinzufügen. Wählen Sie die Organisationseinheiten in der Organisationsstruktur aus und klicken Sie dann auf Organisationseinheiten hinzufügen. Um einzelne Konten auszuschließen, wählen Sie Konten hinzufügen. Wählen Sie die Konten in der Organisationsstruktur aus und klicken Sie dann auf Konten hinzufügen.

- Erfassen Sie nicht die gesamte AWS Organisation, sondern beziehen Sie nur bestimmte Organisationseinheiten und Konten ein. Verwenden Sie denselben Mechanismus zum Hinzufügen von Organisationseinheiten und zum Hinzufügen von Konten, um die gewünschten Organisationseinheiten und Konten einzubeziehen.

3. Wählen Sie im Unterbereich Ressourcen für Ressourcentypen alle oder bestimmte AWS WAF-Ressourcentypen aus. Es stehen eine oder mehrere der folgenden Optionen zur Verfügung:
   - Application Load Balancer
   - Amazon API Gateway API-Gateway-REST-API
   - CloudFront Verteilung

> **CloudFront Anforderung an die Region**
>
> Verwenden Sie zum Schutz der CloudFront Vertriebsressourcen die Region USA Ost (Nord-Virginia) (`us-east-1`).

> **Globale und regionale Ressourcentypen**
>
> Sie können den globalen Ressourcentyp (CloudFront Distribution) oder die regionalen Ressourcentypen (Application Load Balancer und Amazon API Gateway REST API) auswählen, aber nicht beide. Nachdem Sie einen Ressourcentyp ausgewählt haben, können Sie bei der Aktualisierung der Konfiguration nicht zwischen den Ressourcentypen CloudFront Distribution und Regional wechseln.

> **Nicht verwaltete Ressourcen CloudFront**
>
> AWS Network Security Manager verwaltet keine CloudFront Distributionen, die den CloudFront Pauschalpreis oder CloudFront Staging-Distributionen verwenden. Diese Ressourcen scheinen nicht synchron zu sein.

4. Wählen Sie für jeden ausgewählten Ressourcentyp eine der folgenden Optionen, die sich gegenseitig ausschließen:
   - Alle Ressourcen einbeziehen
   - Spezifische Ressourcen einbeziehen

- Schließen Sie bestimmte Ressourcen aus

5. Wenn Sie Bestimmte Ressourcen einbeziehen wählen, wählen Sie einen der folgenden Ausdruckstypen und erstellen Sie dann die entsprechenden Kombinationen von Tags oder ARNs:
   - Einzelne Kriterien
   - Erfüllen Sie alle Kriterien (UND)
   - Entspricht allen Kriterien (ODER)
   - NICHT

   Alle Ressourcentypen haben die Tag - und ARN-Einschlusskriterien. Wenn Sie Tag wählen, geben Sie einen Schlüssel und optional einen Wert ein. Sie können mehrere Tags identifizieren. Wenn es sich bei Ihrem Ressourcentyp um einen Application Load Balancer handelt, wird ein zusätzliches Konfigurationskriterium angezeigt. Wählen Sie unter Konfiguration ein Schema aus, das die Optionen Internet-facingoder Intern enthält.

Um die Richtlinie zu überprüfen und umzusetzen

1. Geben Sie im Bereich Überprüfen und Bereitstellen einen Namen für den Bereitstellungsnamen ein. (Optional) Geben Sie unter Description (Beschreibung) eine Beschreibung ein. Um festzustellen, ob der Inhalt Ihrer Bereitstellung für andere Konten in Ihrer Organisation sichtbar ist, wählen Sie Kontoübergreifende Sichtbarkeit für diese Bereitstellung aktivieren aus.
2. (Optional) Um Ihrer Ressource Tags hinzuzufügen, wählen Sie Neues Tag hinzufügen und geben Sie dann Kombinationen aus Schlüssel und optionalen Werten ein.
3. Um das, was Sie definiert haben, auszuführen, wählen Sie Create and deploy. Wenn der Vorgang abgeschlossen ist, wird die Seite Bereitstellungen angezeigt, auf der Sie die Details der erstellten Elemente sehen können.

⚠ Für Bereitstellungen können Gebühren anfallen

Bei einer Bereitstellung werden Netzwerksicherheitsdienste erstellt und an eine geschützte Ressource angehängt. AWS Network Security Manager berechnet Gebühren für geschützte Ressourcen. Die Sicherheitsdienste selbst schützen die Ressource, wofür zusätzliche Gebühren anfallen. Lesen Sie vor der Bereitstellung die Preisinformationen für AWS Network Security Manager und die AWS WAF-Preisseite.

Standarderstellungsprozess für AWS WAF

Beim Standarderstellungsprozess erstellen Sie jede AWS WAF-Komponente — Regeln, Vorlagen, Richtlinien, Bereiche und Bereitstellungen — einzeln, um vollständige Kontrolle zu haben. Verwenden Sie diesen Ansatz, wenn Sie wiederverwendbare Komponenten erstellen und diese nach Bedarf kombinieren möchten.

Eine AWS Network Security Manager AWS WAF-Richtlinie kann Regeln und Vorlagen enthalten. Wenn Sie die Richtlinie anwenden, erstellt AWS Network Security Manager für jedes in den Geltungsbereich fallende Konto eine Web-ACL.

So erstellen Sie eine Regel (Konsole)

1. Melden Sie sich mit Ihrem AWS Network Security Manager-Administratorkonto bei der AWS Management-Konsole an und öffnen Sie dann die AWS Network Security Manager-Konsole unter https://console.aws.amazon.com/network-security-manager/.

   > **Einrichtung des Administratorkontos**
   >
   > Informationen zur Einrichtung eines AWS Network Security Manager-Administratorkontos finden Sie unter AWS Network Security Manager einrichten.

2. Wählen Sie im Navigationsbereich AWS Network Security Manager und anschließend Overview aus.
3. Wählen Sie im Bereich Übersicht die Option Regel erstellen aus. Geben Sie einen aussagekräftigen Namen und anschließend optional eine Beschreibung ein.
4. Wählen Sie im Bereich Regeldefinition für Firewalltyp die Option AWS WAF aus.
5. Wählen Sie als Regeltyp entweder Inspektion oder Konfiguration aus.

   Wenn Sie Inspektion wählen, wird ein JSON-Editorbereich mit dem Namen Regelgruppenreferenz definieren mit den folgenden Optionen angezeigt:

   - Vorlage einfügen — Wählen Sie eine JSON-Vorlage für erste Regeln (vor der Verarbeitung) oder Letzte Regeln (nach der Verarbeitung) aus. Wenn Sie eine Auswahl treffen, fügt AWS Network Security Manager das entsprechende JSON zusammen mit Warnsymbolen in den Editor ein, falls Eingaben erforderlich sind, um die Vorlage zu vervollständigen.
   - Regelgruppe einfügen — Zeigt eine Auswahlliste mit drei Optionen an:
     - Eine Regelgruppe mit AWS verwalteten Regeln (AMR)

- Eine bestehende benutzerdefinierte Regelgruppe
- Eine AWS Marketplace-Regelgruppe

  AWS Network Security Manager präsentiert die Regelgruppen, die Ihrer Wahl zugeordnet sind, und Sie können eine einzelne Instanz für die Aufnahme auswählen. Nachdem Sie die Auswahl getroffen haben, wählen Sie Regelgruppe auswählen. AWS Network Security Manager fügt Verweise auf die Inspektionsregel mit der richtigen Syntax in den JSON-Editor ein.

- Mit KI einfügen — Öffnet ein Overlay-Fenster mit dem Namen AI Configuration Generator. Verwenden Sie dieses Tool, um Ihre Regel in einfacher Sprache zu beschreiben, und AWS Network Security Manager generiert das zugehörige JSON im Editor. Anschließend können Sie den generierten Code überprüfen und entscheiden, ob Sie die Ausgabe akzeptieren, ändern oder löschen möchten.

6. (Optional) Nachdem Ihre JSON-Regeldefinition abgeschlossen ist, können Sie Ihrer Regel ein Tag zuordnen. Wählen Sie Add new tag (Neues Tag hinzufügen) und geben Sie dann einen Key (Schlüssel) und einen optionalen Value (Wert) ein.
7. Wenn Sie mit Ihren Definitionen fertig sind, wählen Sie entweder Entwurf speichern, um ein inaktives, potenziell unvollständiges Objekt zu speichern, oder Regel erstellen.

> ⚠ Web-ACL-Namen sind permanent
>
> Sie können einen Web-ACL-Namen nicht ändern, nachdem Sie ihn erstellt haben. Wenn Sie den Namen Ihrer Richtlinie aktualisieren, aktualisiert AWS Network Security Manager den zugehörigen Web-ACL-Namen nicht. Damit AWS Network Security Manager eine Web-ACL mit einem anderen Namen erstellt, müssen Sie eine neue Richtlinie erstellen.

Um eine Vorlage (Konsole) zu erstellen

In einer Vorlage werden Regeln in der Reihenfolge ihrer Priorität zusammengestellt, damit sie innerhalb einer Richtlinie ausgewertet werden können. Sie können Ihre Regeltypen in Gruppen organisieren, die Ihren Sicherheitszielen entsprechen. Sie können auch verschiedene Teams Anweisungen zur Sicherheitskontrolle erstellen lassen, die ihren Verantwortlichkeiten und Fähigkeiten entsprechen.

1. Wählen Sie auf der Übersichtsseite im Bereich Übersicht die Option Vorlage erstellen aus. Geben Sie auf der Seite „Vorlage erstellen“ einen Vorlagennamen und optional eine Beschreibung ein und wählen Sie einen Firewalltyp (in diesem Fall AWS WAF) aus.
2. Wenn Sie einen Firewalltyp auswählen, wird der Bereich Regeln angezeigt. Wählen Sie eine der beiden Schaltflächen Regeln hinzufügen, um eine Liste der verfügbaren Regeln zu öffnen. Aktivieren Sie das Kontrollkästchen links neben dem Namen einer Regel, um sie der Vorlage hinzuzufügen. Um eine bestimmte Version einer Regel auszuwählen, wählen Sie das Feld Version der Regel aus. Wenn mehrere Versionen verfügbar sind, wählen Sie die gewünschte Version aus und klicken Sie dann auf Bestätigen.
3. (Optional) Erstellen Sie ein Tag für die Vorlage. Wenn Sie fertig sind, wählen Sie entweder Entwurf speichern oder Vorlage erstellen. Um mit der Erstellung einer Richtlinie fortzufahren, wählen Sie Vorlage erstellen.

So erstellen Sie eine -Richtlinie (Konsole):

Dies ist der letzte Schritt der Richtliniendefinition und der Vorbereitung für die Implementierung.

1. Wählen Sie auf der Übersichtsseite im Bereich Übersicht die Option Richtlinie erstellen aus. Geben Sie auf der Seite Richtlinie erstellen einen Namen und optional eine Beschreibung ein und wählen Sie dann einen Firewalltyp (in diesem Fall AWS WAF) aus.
2. Legen Sie im Bereich Richtlinienpriorität die Priorität fest. AWS Network Security Manager bewertet Richtlinien nach ihrer Priorität, um Konflikte zu lösen. Niedrigere Positionen (niedrigere Ganzzahlen) haben eine höhere Priorität. Um die Priorität zu bearbeiten, wählen Sie den Wert Position. Erhöhen Sie ihn dann mit den Pfeilen oder geben Sie direkt einen Wert ein. Um die Auswahl zu bestätigen, wählen Sie Bestätigen. Um die Änderung zu verwerfen, wählen Sie Abbrechen.
3. Legen Sie im Bereich Richtlinienkonfiguration fest, welche automatisierten Aktionen AWS Network Security Manager im Zielbereich durchführt:
   - Bei der Wiederherstellung wird die definierte Richtlinie auf alle Ressourcen angewendet, deren Sicherheitsstatus nicht mit dem gewünschten Status synchronisiert ist, der in AWS Network Security Manager beschrieben ist.
   - Die Ressourcensäuberung löscht die Firewall, die AWS Network Security Manager für eine Ressource erstellt hat, wenn die Bereitstellung entfernt wird oder wenn das Konto oder die Ressource außerhalb des Gültigkeitsbereichs liegt.

- Die WebACL-Lösung für bestehende Kunden bestimmt, wie Konflikte zwischen der Richtlinie, die Sie definieren, und der möglicherweise bereits implementierten Richtlinie gelöst werden. Wählen Sie im Menü eine der folgenden Optionen:
  - Keine Standardisierung überspringt die Standardisierung für alle Ressourcen, die bereits über eine Web-ACL verfügen.
  - Durch die Override-Zuordnung wird die vorhandene Web-ACL durch die von AWS Network Security Manager erstellte Web-ACL ersetzt.
  - Retrofit passt seine Regeln an jede bestehende Web-ACL an und behält die der Ressource zugeordnete Web-ACL bei.

4. Nachdem diese Konfigurationseinstellungen abgeschlossen sind, wählen Sie die Regeln und Vorlagen aus, die Sie der Richtlinie hinzufügen möchten. Wählen Sie im Bereich Vorlagen und Regeln die Option Regeln hinzufügen oder Vorlagen hinzufügen aus, um die Richtlinie auszufüllen. Beide Prozesse öffnen ein Fenster, das genauso funktioniert wie der weiter oben in diesem Abschnitt beschriebene Regelauswahlprozess.

Um einen Bereich zu erstellen (Konsole)

1. Sie können diesen Schritt auf der Übersichtsseite oder in anderen Bereichen des Tools starten. Geben Sie im Bereich mit den Bereichsdetails einen Bereichsnamen und optional eine Beschreibung ein.
2.
   > **Multi-account nur Modus**
   >
   > Dieser Schritt gilt nur für den Modus mit mehreren Konten. Verwenden Sie im Modus mit mehreren Konten den Unterbereich zur Auswahl von Konten und Organisationseinheiten, um auszuwählen, welche Konten oder Organisationseinheiten ein- oder ausgeschlossen werden sollen. Im Einzelkontenmodus wird dieser Unterbereich nicht in der Konsole angezeigt. Überspringen Sie diesen Schritt also.

   Wählen Sie im Auswahlbereich Konto und Organisationseinheit eine von drei Methoden zur Steuerung des administrativen Bereichs aus:

   - Geltungsbereich für die gesamte AWS Organisation (alle Organisationseinheiten und Konten) — Es ist keine weitere Definition erforderlich.

- Geltungsbereich für die gesamte AWS Organisation, jedoch ohne spezifische Organisationseinheiten und Konten — Es werden zwei Unterbereiche angezeigt, einer für Organisationseinheiten und einer für Konten. Wählen Sie „Organisationseinheiten hinzufügen“, um das Fenster „Organisationseinheiten hinzufügen“ zu öffnen. Wählen Sie im Organisationsbaum die benötigten Organisationseinheiten aus und klicken Sie dann auf Organisationseinheiten hinzufügen. Um einzelne Konten hinzuzufügen, wählen Sie im Unterbereich Konten die Option Konten hinzufügen, wählen Sie die Konten aus der Organisationsstruktur aus und klicken Sie dann auf Konten hinzufügen.
- Erfassen Sie nicht die gesamte AWS Organisation, sondern beziehen Sie nur bestimmte Organisationseinheiten und Konten ein. Verwenden Sie dieselben Unterbereiche, um Organisationseinheiten oder Konten hinzuzufügen, und zwar mit demselben Mechanismus, der für die vorherige Option beschrieben wurde.

3. Wählen Sie als Nächstes Ressourcen im Unterbereich Ressourcen aus. Wählen Sie im Auswahlfeld Ressourcentypen alle oder bestimmte AWS WAF-Ressourcentypen aus. Für AWS WAF stehen eine oder alle der folgenden Optionen zur Verfügung:
   - Application Load Balancer
   - Amazon API Gateway API-Gateway-REST-API
   - CloudFront Verteilung

> **CloudFront Anforderung an die Region**
>
> Verwenden Sie zum Schutz der CloudFront Vertriebsressourcen die Region USA Ost (Nord-Virginia) (`us-east-1`).

> **Globale und regionale Ressourcentypen**
>
> Sie können den globalen Ressourcentyp (CloudFront Distribution) oder die regionalen Ressourcentypen (Application Load Balancer und Amazon API Gateway REST API) auswählen, aber nicht beide. Nachdem Sie einen Ressourcentyp ausgewählt haben, können Sie bei der Aktualisierung der Konfiguration nicht zwischen den Ressourcentypen CloudFront Distribution und Regional wechseln.

> **Nicht verwaltete Ressourcen CloudFront**
>
> AWS Network Security Manager verwaltet keine CloudFront Distributionen, die den CloudFront Pauschalpreis oder CloudFront Staging-Distributionen verwenden. Diese Ressourcen scheinen nicht synchron zu sein.

4. Wählen Sie für jeden ausgewählten Ressourcentyp eine der folgenden Optionen, die sich gegenseitig ausschließen:
   - Alle Ressourcen einbeziehen
   - Spezifische Ressourcen einbeziehen
   - Schließen Sie bestimmte Ressourcen aus
5. Wenn Sie Bestimmte Ressourcen einbeziehen wählen, wählen Sie einen der folgenden Ausdruckstypen aus:
   - Einzelne Kriterien
   - Erfüllen Sie alle Kriterien (UND)
   - Entspricht allen Kriterien (ODER)
   - NICHT
6. Jeder Ausdruckstyp unterstützt einzelne oder mehrere Einschlusskriterien und ARNs, sodass Sie Kombinationen von Tags oder ARNs erstellen können. Alle Ressourcentypen unterstützen die Tag - und ARN-Einschlusskriterien. Wenn Sie Tag wählen, identifizieren Sie einen Schlüssel und einen optionalen Wert. Sie können mehrere Tags identifizieren.
7. Für einen Application Load Balancer wird ein zusätzliches Konfigurationskriterium angezeigt. In der Konfiguration können Sie ein Schema mit den Optionen Intern Internet-facingoder Intern festlegen.

Um ein Deployment zu erstellen (Konsole)

Eine Bereitstellung bindet Ihre Richtlinien an einen Geltungsbereich und aktiviert die Durchsetzung, wodurch AWS Network Security Manager Ihre AWS WAF-Regeln auf die im Geltungsbereich enthaltenen Ressourcen anwendet.

1. Wählen Sie auf der Übersichtsseite im Bereich Übersicht die Option Einrichtung erstellen aus. Sie können diesen Schritt auch in anderen Bereichen des Tools starten.
2. Wählen Sie die Richtlinie aus, die Sie bereitstellen möchten.

3. Wählen Sie den Bereich, der die Konten und Ressourcen definiert, auf die AWS Network Security Manager die Richtlinie anwendet.
4. Geben Sie unter Bereitstellungsname einen Namen ein. (Optional) Geben Sie unter Description (Beschreibung) eine Beschreibung ein.
5. (Optional) Um die Bereitstellung für andere Konten in Ihrer Organisation sichtbar zu machen, wählen Sie Kontoübergreifende Sichtbarkeit für diese Bereitstellung aktivieren aus.
6. (Optional) Um Tags hinzuzufügen, wählen Sie Neues Tag hinzufügen und geben Sie dann Kombinationen aus Schlüssel und optionalen Werten ein.
7. Wählen Sie Create and deploy (Erstellen und bereitstellen) aus. Die Seite Bereitstellungen wird angezeigt, auf der Sie die Details dessen sehen können, was AWS Network Security Manager erstellt hat.

> **Für Bereitstellungen können Gebühren anfallen**
>
> Bei einer Bereitstellung werden Netzwerksicherheitsdienste erstellt und an eine geschützte Ressource angehängt. AWS Network Security Manager berechnet Gebühren für geschützte Ressourcen. Die Sicherheitsdienste selbst schützen die Ressource, wofür zusätzliche Gebühren anfallen. Lesen Sie vor der Bereitstellung die Preisinformationen für AWS Network Security Manager und die AWS WAF-Preisseite.

Verwaltung des DDoS-Schutzes für AWS Shield Advanced

Mit AWS Network Security Manager konfigurieren und implementieren Sie den AWS Shield Advanced-Schutz zentral für Konten und Ressourcen in Ihrem Unternehmen. Sie können DDoS-Schutzrichtlinien definieren und diese mithilfe von AWS Network Security Manager-Richtlinien und -Bereitstellungen in großem Umfang durchsetzen.

> **AWS Network Security Manager wird separat in Rechnung gestellt**
>
> AWS Network Security Manager ist nicht Teil des AWS Shield Advanced-Angebots. Weitere Informationen zu den Preisen finden Sie unter AWS Network Security Manager-Preise und AWS Shield Advanced-Preise.

⚠ AWS Shield Advanced-Abonnement

Wenn eine aktive Bereitstellung ein Konto in ihren Geltungsbereich einschließt, abonniert AWS Network Security Manager dieses Konto bei AWS Shield Advanced. AWS Network Security Manager kündigt das Abonnement nicht, wenn das Konto den Gültigkeitsbereich verlässt oder wenn Sie die Bereitstellung entfernen. Informationen zur Kündigung eines AWS Shield Advanced-Abonnements finden Sie unter AWS Shield Advanced abonnieren im AWS WAF Developer Guide.

Quick Create für AWS Shield Advanced

Mit Quick Create definieren und implementieren Sie AWS Shield Advanced-Schutzmaßnahmen in einem einzigen geführten Arbeitsablauf. Verwenden Sie Quick Create, wenn Sie den DDoS-Schutz von Richtlinien bis hin zur Bereitstellung in einer Sitzung einrichten möchten.

Um einen AWS Shield Advanced-Schutz mit Quick Create zu definieren und bereitzustellen, führen Sie die folgenden Verfahren der Reihe nach durch.

Um die Richtlinie zu erstellen und Schutzmaßnahmen zu konfigurieren

Führen Sie folgende Schritte aus:

1. Öffnen Sie die AWS Network Security Manager-Konsole unter https://console.aws.amazon.com/network-security-manager/.
2. Wählen Sie im Navigationsbereich Overview (Übersicht) aus.
3. Wählen Sie auf der Übersichtsseite die Option Schnelles Erstellen und Bereitstellen aus. Die Seite „Schnelles Erstellen und Bereitstellen“ wird mit mehreren Bereichen angezeigt.
4. Geben Sie im Bereich mit den Richtliniendetails für Name einen Richtliniennamen ein. (Optional) Geben Sie unter Description (Beschreibung) eine Beschreibung ein.
5. Wählen Sie im Bereich Schutzmaßnahmen definieren den Firewalltyp aus, mit dem Sie arbeiten möchten. Wählen Sie AWS Shield Advanced aus.
6. Legen Sie unter Richtlinienkonfiguration im Bereich Schutzmaßnahmen definieren fest, welche automatisierten Aktionen AWS Network Security Manager im Zielbereich durchführt:
   - Bei der Behebung wird die definierte Richtlinie auf alle Ressourcen angewendet, deren Sicherheitsstatus nicht dem gewünschten Status entspricht, den AWS Network Security Manager beschreibt.

- Die Ressourcenbereinigung löscht den DDoS-Schutz, den AWS Network Security Manager für eine Ressource erstellt hat, wenn die Bereitstellung entfernt wird oder wenn das Konto oder die Ressource außerhalb des Gültigkeitsbereichs liegt.
- Die DDoS-Lösung für bestehende Kunden bestimmt, wie Konflikte zwischen der Richtlinie, die Sie definieren, und der möglicherweise bereits implementierten Richtlinie gelöst werden. Wählen Sie im Menü eine der folgenden Optionen aus:
  - Bei der Nichtbehebung wird die Behebung aller Ressourcen übersprungen, die bereits über einen DDoS-Schutz verfügen.
  - Override Association ersetzt den vorhandenen DDoS-Schutz durch den von AWS Network Security Manager erstellten DDoS-Schutz.
  - Retrofit passt seine Regeln an jeden vorhandenen DDoS-Schutz an und behält den DDoS-Schutz bei, der mit der Ressource verknüpft ist.

7. Legen Sie im Bereich Richtlinienpriorität die Priorität fest. AWS Network Security Manager bewertet Richtlinien nach ihrer Priorität, um Konflikte zu lösen. Niedrigere Positionen (niedrigere Ganzzahlen) haben eine höhere Priorität.

   Um die Priorität zu bearbeiten, wählen Sie den Wert Position. Erhöhen Sie ihn dann mit den Pfeilen oder geben Sie direkt einen Wert ein. Um die Auswahl zu bestätigen, wählen Sie Bestätigen. Um die Änderung zu verwerfen, wählen Sie Abbrechen.

Um den Geltungsbereich festzulegen

Führen Sie folgende Schritte aus:

1. Definieren Sie im Bereich Umfang festlegen die Gruppe von Ressourcen, für die die Richtlinien gelten. Geben Sie unter Bereichsname einen Namen ein. (Optional) Geben Sie unter Description (Beschreibung) eine Beschreibung ein.
2.
   > **Multi-account nur Modus**
   >
   > Dieser Schritt gilt nur für den Modus mit mehreren Konten. Verwenden Sie im Modus mit mehreren Konten den Unterbereich zur Auswahl von Konten und Organisationseinheiten, um auszuwählen, welche Konten oder Organisationseinheiten ein- oder ausgeschlossen werden sollen. Im Einzelkontenmodus wird dieser Unterbereich nicht in der Konsole angezeigt. Überspringen Sie diesen Schritt also.

Wählen Sie im Unterbereich zur Auswahl von Konten und Organisationseinheiten eine der folgenden Optionen aus:

- Geltungsbereich für die gesamte AWS Organisation. Es ist keine weitere Definition erforderlich.
- Geltungsbereich für das gesamte AWS Unternehmen, ausgenommen sind jedoch bestimmte Organisationseinheiten und Konten. Es werden ein Unterbereich „Organisationseinheiten“ und ein Unterbereich „Konten“ angezeigt. Um Organisationseinheiten auszuschließen, wählen Sie Organisationseinheiten hinzufügen. Wählen Sie die Organisationseinheiten in der Organisationsstruktur aus und klicken Sie dann auf Organisationseinheiten hinzufügen. Um einzelne Konten auszuschließen, wählen Sie Konten hinzufügen. Wählen Sie die Konten in der Organisationsstruktur aus und klicken Sie dann auf Konten hinzufügen.
- Erfassen Sie nicht die gesamte AWS Organisation, sondern beziehen Sie nur bestimmte Organisationseinheiten und Konten ein. Verwenden Sie denselben Mechanismus zum Hinzufügen von Organisationseinheiten und zum Hinzufügen von Konten, um die gewünschten Organisationseinheiten und Konten einzubeziehen.

3. Wählen Sie im Unterbereich Ressourcen für Ressourcentypen alle oder bestimmte AWS Shield Advanced-Ressourcentypen aus. Es stehen eine oder mehrere der folgenden Optionen zur Verfügung:
   - Application Load Balancer
   - CloudFront Verteilung
   - Classic Load Balancer
   - Elastic IP-Adresse
4. Wählen Sie für jeden ausgewählten Ressourcentyp eine der folgenden Optionen, die sich gegenseitig ausschließen:
   - Alle Ressourcen einbeziehen
   - Spezifische Ressourcen einbeziehen
   - Schließen Sie bestimmte Ressourcen aus
5. Wenn Sie Bestimmte Ressourcen einbeziehen wählen, wählen Sie einen der folgenden Ausdruckstypen und erstellen Sie dann die entsprechenden Kombinationen von Tags oder ARNs:
   - Einzelne Kriterien
   - Erfüllen Sie alle Kriterien (UND)
   - Entspricht allen Kriterien (ODER)
   - NICHT

Alle Ressourcentypen haben die Tag - und ARN-Einschlusskriterien. Wenn Sie Tag wählen, geben Sie einen Schlüssel und optional einen Wert ein. Sie können mehrere Tags identifizieren.

> **CloudFront Anforderung an die Region**
>
> Verwenden Sie zum Schutz der CloudFront Vertriebsressourcen die Region USA Ost (Nord-Virginia) (`us-east-1`).

Um die Richtlinie zu überprüfen und umzusetzen

Führen Sie folgende Schritte aus:

1. Geben Sie im Bereich Überprüfen und Bereitstellen einen Namen für den Bereitstellungsnamen ein. (Optional) Geben Sie unter Description (Beschreibung) eine Beschreibung ein. Um festzustellen, ob der Inhalt Ihrer Bereitstellung für andere Konten in Ihrer Organisation sichtbar ist, wählen Sie Kontoübergreifende Sichtbarkeit für diese Bereitstellung aktivieren aus.
2. (Optional) Um Ihrer Ressource Tags hinzuzufügen, wählen Sie Neues Tag hinzufügen und geben Sie dann Kombinationen aus Schlüssel und optionalen Werten ein.
3. Um die Richtlinie und den Geltungsbereich zu erstellen und bereitzustellen, wählen Sie Create and deploy aus. Wenn der Vorgang abgeschlossen ist, wird die Seite Bereitstellungen angezeigt, auf der Sie die Details der von AWS Network Security Manager erstellten Elemente sehen können.

> **Für Bereitstellungen können Gebühren anfallen**
>
> Bei einer Bereitstellung werden Netzwerksicherheitsdienste erstellt und an eine geschützte Ressource angehängt. AWS Network Security Manager berechnet Gebühren für geschützte Ressourcen. Die Sicherheitsdienste selbst schützen die Ressource, wofür zusätzliche Gebühren anfallen. Lesen Sie vor der Bereitstellung die Preisseite für AWS Network Security Manager und die Preisseite für AWS Shield Advanced.

Standarderstellungsprozess für AWS Shield Advanced

Beim standardmäßigen Erstellungsprozess richten Sie jede AWS Shield Advanced-Komponente — Richtlinien, Geltungsbereiche und Bereitstellungen — einzeln ein, um die volle Kontrolle zu haben. Verwenden Sie diesen Ansatz, wenn Sie wiederverwendbare Komponenten erstellen und diese nach Bedarf kombinieren möchten.

Eine AWS Shield Advanced-Richtlinie ist einfach und enthält keine Regeln, Regelgruppen oder Vorlagen. Wenn Sie die Richtlinie anwenden, erstellt AWS Network Security Manager für jedes in den Geltungsbereich fallende Konto einen AWS Shield Advanced-DDoS-Schutz. Informationen zur Funktionsweise von AWS Network Security Manager finden Sie unter. Wie funktioniert AWS Network Security Manager

So erstellen Sie eine -Richtlinie (Konsole):

Führen Sie folgende Schritte aus:

1. Melden Sie sich mit Ihrem AWS Network Security Manager-Administratorkonto bei der AWS Management-Konsole an, und öffnen Sie dann die AWS Network Security Manager-Konsole unter https://console.aws.amazon.com/network-security-manager/.

   > Einrichtung des Administratorkontos
   >
   > Informationen zur Einrichtung eines AWS Network Security Manager-Administratorkontos finden Sie unter AWS Network Security Manager einrichten.

2. Wählen Sie im Navigationsbereich AWS Network Security Manager und anschließend Overview aus.
3. Wählen Sie im Bereich Übersicht die Option Richtlinie erstellen aus. Geben Sie einen Namen und optional eine Beschreibung ein und wählen Sie dann einen Firewall-Typ aus (in diesem Fall AWS Shield Advanced).
4. Legen Sie im Bereich Richtlinienpriorität die Priorität fest. AWS Network Security Manager bewertet Richtlinien nach ihrer Priorität, um Konflikte zu lösen. Niedrigere Positionen (niedrigere Ganzzahlen) haben eine höhere Priorität.

   Um die Priorität zu bearbeiten, wählen Sie den Wert Position. Erhöhen Sie ihn dann mit den Pfeilen oder geben Sie direkt einen Wert ein. Um die Auswahl zu bestätigen, wählen Sie Bestätigen. Um die Änderung zu verwerfen, wählen Sie Abbrechen.

5. Legen Sie im Bereich Richtlinienkonfiguration fest, welche automatisierten Aktionen AWS Network Security Manager im Zielbereich durchführt:
   - Bei der Korrektur wird die definierte Richtlinie auf alle Ressourcen angewendet, deren Sicherheitsstatus nicht dem gewünschten Status entspricht, den AWS Network Security Manager beschreibt.
   - Die Ressourcenbereinigung löscht den DDoS-Schutz, den AWS Network Security Manager für eine Ressource erstellt hat, wenn die Bereitstellung entfernt wird oder wenn das Konto oder die Ressource außerhalb des Gültigkeitsbereichs liegt.
   - Die DDoS-Lösung für bestehende Kunden bestimmt, wie Konflikte zwischen der Richtlinie, die Sie definieren, und der möglicherweise bereits implementierten Richtlinie gelöst werden. Wählen Sie im Menü eine der folgenden Optionen:
     - Bei der Nichtbehebung wird die Behebung aller Ressourcen übersprungen, die bereits über einen DDoS-Schutz verfügen.
     - Override Association ersetzt den vorhandenen DDoS-Schutz durch den von AWS Network Security Manager erstellten DDoS-Schutz.
     - Retrofit passt seine Regeln an jeden bestehenden DDoS-Schutz an und behält den DDoS-Schutz bei, der mit der Ressource verknüpft ist.

Um einen Bereich zu erstellen (Konsole)

Führen Sie folgende Schritte aus:

1. Geben Sie im Bereich mit den Bereichsdetails einen Bereichsnamen und optional eine Beschreibung ein.
2. Multi-account nur Modus

   Dieser Schritt gilt nur für den Modus mit mehreren Konten. Verwenden Sie im Modus für mehrere Konten den Unterbereich zur Auswahl von Konten und Organisationseinheiten, um auszuwählen, welche Konten oder Organisationseinheiten ein- oder ausgeschlossen werden sollen. Im Einzelkontenmodus wird dieser Unterbereich nicht in der Konsole angezeigt. Überspringen Sie diesen Schritt also.

   Wählen Sie im Auswahlbereich Konto und Organisationseinheit eine von drei Methoden zur Steuerung des administrativen Bereichs aus:

- Geltungsbereich für die gesamte AWS Organisation (alle Organisationseinheiten und Konten) — Es ist keine weitere Definition erforderlich.
- Geltungsbereich für die gesamte AWS Organisation, jedoch ohne spezifische Organisationseinheiten und Konten — Es werden zwei Unterbereiche angezeigt, einer für Organisationseinheiten und einer für Konten. Wählen Sie „Organisationseinheiten hinzufügen“, um das Fenster „Organisationseinheiten hinzufügen“ zu öffnen, wählen Sie die benötigten Organisationseinheiten aus und klicken Sie dann auf Organisationseinheiten hinzufügen. Um einzelne Konten hinzuzufügen, wählen Sie im Unterbereich Konten hinzufügen aus, wählen Sie die Konten aus und klicken Sie dann auf Konten hinzufügen.
- Erfassen Sie nicht die gesamte AWS Organisation, sondern beziehen Sie nur bestimmte Organisationseinheiten und Konten ein. Verwenden Sie dieselben Unterbereiche, um Organisationseinheiten oder Konten hinzuzufügen.

3. Wählen Sie als Nächstes Ressourcen im Unterbereich Ressourcen aus. Wählen Sie im Auswahlfeld Ressourcentypen alle oder bestimmte AWS Shield Advanced-Ressourcentypen aus. Für AWS Shield Advanced stehen eine oder alle der folgenden Optionen zur Verfügung:
   - Application Load Balancer
   - CloudFront Verteilung
   - Classic Load Balancer
   - Elastic IP-Adresse
4. Wählen Sie für jeden ausgewählten Ressourcentyp eine der folgenden Optionen, die sich gegenseitig ausschließen:
   - Alle Ressourcen einbeziehen
   - Spezifische Ressourcen einbeziehen
   - Schließen Sie bestimmte Ressourcen aus
5. Wenn Sie Bestimmte Ressourcen einbeziehen wählen, wählen Sie einen der folgenden Ausdruckstypen aus:
   - Einzelne Kriterien
   - Erfüllen Sie alle Kriterien (UND)
   - Entspricht allen Kriterien (ODER)
   - NICHT
6. Jeder Ausdruckstyp unterstützt einzelne oder mehrere Einschlusskriterien und ARNs, sodass Sie Kombinationen von Tags oder ARNs erstellen können. Alle Ressourcentypen unterstützen die Tag

- und ARN-Einschlusskriterien. Wenn Sie Tag wählen, identifizieren Sie einen Schlüssel und einen optionalen Wert. Sie können mehrere Tags identifizieren.

> **CloudFront Anforderung an die Region**
>
> Verwenden Sie zum Schutz der CloudFront Vertriebsressourcen die Region USA Ost (Nord-Virginia) (`us-east-1`).

Um eine Bereitstellung zu erstellen (Konsole)

Eine Bereitstellung bindet Ihre Richtlinien an einen bestimmten Geltungsbereich und aktiviert deren Durchsetzung. AWS Network Security Manager wendet dann Ihren AWS Shield Advanced-DDoS-Schutz auf die im Leistungsumfang enthaltenen Ressourcen an.

Führen Sie folgende Schritte aus:

1. Wählen Sie auf der Übersichtsseite im Bereich Übersicht die Option Einrichtung erstellen aus.
2. Wählen Sie die Richtlinie aus, die Sie bereitstellen möchten.
3. Wählen Sie den Bereich, der die Konten und Ressourcen definiert, auf die AWS Network Security Manager die Richtlinie anwendet.
4. Geben Sie unter Bereitstellungsname einen Namen ein. (Optional) Geben Sie unter Description (Beschreibung) eine Beschreibung ein.
5. (Optional) Um die Bereitstellung für andere Konten in Ihrer Organisation sichtbar zu machen, wählen Sie Kontoübergreifende Sichtbarkeit für diese Bereitstellung aktivieren aus.
6. (Optional) Um Tags hinzuzufügen, wählen Sie Neues Tag hinzufügen und geben Sie dann Kombinationen aus Schlüssel und optionalen Werten ein.
7. Wählen Sie Create and deploy (Erstellen und bereitstellen) aus. Die Seite Bereitstellungen wird angezeigt, auf der Sie die Details dessen sehen können, was AWS Network Security Manager erstellt hat.

> **Für Bereitstellungen können Gebühren anfallen**
>
> Bei einer Bereitstellung werden Netzwerksicherheitsdienste erstellt und an eine geschützte Ressource angehängt. AWS Network Security Manager berechnet Gebühren für geschützte

Ressourcen. Die Sicherheitsdienste selbst schützen die Ressource, wofür zusätzliche Gebühren anfallen. Lesen Sie vor der Bereitstellung die Preisseite für AWS Network Security Manager und die Preisseite für AWS Shield Advanced.

AWS Network Security Manager und AWS Firewall Manager

AWS Network Security Manager ist der Dienst, der AWS Firewall Manager ersetzt. Bei den beiden handelt es sich um völlig separate Dienste mit jeweils einzigartigen Funktionen und einem unterschiedlichen Preismodell. Wenn Sie derzeit AWS Firewall Manager verwenden, müssen Sie keine Maßnahmen ergreifen — Ihre vorhandenen Firewalls und Richtlinien funktionieren weiterhin. In diesem Kapitel wird beschrieben, wie die beiden Dienste koexistieren, wie die Rangfolge funktioniert, wenn Sie beide verwenden, und wie die Migration funktioniert, sobald sie verfügbar ist.

AWS Network Security Manager und AWS Firewall Manager arbeiten Seite an Seite und unabhängig voneinander. Irgendwann wird AWS Firewall Manager nicht mehr verkauft und dann nicht mehr betrieben.

Koexistenz mit AWS Firewall Manager

AWS Network Security Manager wirkt sich nicht auf Firewalls aus, die Sie mit AWS Firewall Manager erstellt haben, es sei denn, Sie initiieren eine Aktion, um sie zu ändern. Firewalls und Richtlinien, die Sie mit AWS Firewall Manager erstellt haben, funktionieren weiter, sofern Sie sie nicht beenden. Dies gilt auch nach der AWS Stilllegung von Firewall Manager.

Vorrang bei der Problembehebung

Während beide Dienste funktionieren, können Sie Aktionen ergreifen, die sich auf Firewalls auswirken, die Sie mit AWS Firewall Manager erstellt haben. Wenn Sie AWS Network Security Manager-Richtlinien erstellen, wenden Sie sie auf einen Bereich an, bei dem es sich um eine Reihe von Zielressourcen handelt. Wenn dieser Bereich Ressourcen umfasst, für die eine AWS Firewall Manager Manager-Richtlinie bereits gilt, hat AWS Network Security Manager bei der Wiederherstellung Vorrang. In diesem Fall haben die AWS Network Security Manager-Richtlinie und der Geltungsbereich Vorrang vor der bestehenden AWS Firewall Manager Manager-Firewall und -Richtlinie. Das spezifische Verhalten hängt von den ausgewählten Auflösungsoptionen ab.

Geplante Migration von AWS Firewall Manager

Durch die Migration von AWS Firewall Manager zu AWS Network Security Manager wird Ihr Firewall-Management in einem einzigen Dienst konsolidiert, sodass Sie dessen Funktionen nutzen können. Die Migration ist geplant, aber noch nicht verfügbar. Sobald die Migration verfügbar ist, können Sie

Ihre AWS Firewall Manager Manager-Richtlinien auf AWS Network Security Manager verschieben. Für die Migration sind neue Aktionen in beiden Diensten erforderlich, die noch nicht eingerichtet wurden.

Der geplante Prozess kopiert eine ausgewählte Richtlinie aus dem AWS Firewall Manager, überträgt sie an AWS Network Security Manager und übersetzt sie in die neue Richtlinienstruktur. Dieser Vorgang hat keine Auswirkungen auf Ihre ursprüngliche Richtlinie oder die zugehörigen Firewalls in AWS Firewall Manager.

Sicherheit bei AWS Manager für Netzwerksicherheit

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Third-party Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für AWS Network Security Manager gelten, finden Sie unter AWS Services im Umfang nach Compliance-Programm AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, einschließlich der Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von AWS Network Security Manager anwenden können. In den folgenden Themen erfahren Sie, wie Sie AWS Network Security Manager so konfigurieren, dass Sie Ihre Sicherheits- und Compliance-Ziele erreichen. Sie lernen auch, wie Sie andere AWS Dienste verwenden können, die Sie bei der Überwachung und Sicherung Ihrer AWS Network Security Manager-Ressourcen unterstützen.

Topics

- Datenschutz in AWS Manager für Netzwerksicherheit
- Identitäts- und Zugriffsmanagement für AWS Manager für Netzwerksicherheit
- Verwenden von serviceverknüpften Rollen für AWS Manager für Netzwerksicherheit
- Konformitätsprüfung für AWS Manager für Netzwerksicherheit
- Resilienz in AWS Manager für Netzwerksicherheit
- Sicherheit der Infrastruktur in AWS Manager für Netzwerksicherheit
- Bewährte Sicherheitsmethoden für AWS Manager für Netzwerksicherheit

Datenschutz in AWS Manager für Netzwerksicherheit

Das AWS Modell der gilt für den Datenschutz in AWS Network Security Manager. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz . Weitere Informationen zum Datenschutz in Europa finden Sie im Zentrum für die Datenschutz-Grundverordnung (DSGVO).

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit AWS Network Security Manager oder anderen Geräten arbeiten und die Konsole, die API oder SDKs AWS-Services verwenden. AWS CLI AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet

werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Verschlüsselung im Ruhezustand

AWS Network Security Manager verschlüsselt alle ruhenden Daten mithilfe von AWS Key Management Service (AWS KMS) -Schlüsseln. Service-managed KMS-Schlüssel schützen Ihre Ressourcenkonfigurationen, Ihren Bereitstellungsstatus und Ihre Synchronisationsdaten. Sie müssen diese Schlüssel nicht konfigurieren oder verwalten.

Verschlüsselung während der Übertragung

AWS Network Security Manager verschlüsselt alle Daten während der Übertragung mit Transport Layer Security (TLS). Alle API-Anfragen erfordern TLS 1.2 oder höher. Verbindungen zu den AWS Network Security Manager-API-Endpunkten verwenden ausschließlich HTTPS.

Schlüsselverwaltung

AWS Network Security Manager verwendet vom Service verwaltete AWS KMS-Schlüssel für die Verschlüsselung im Ruhezustand. Sie können derzeit keine eigenen KMS-Schlüssel bereitstellen.

Identitäts- und Zugriffsmanagement für AWS Manager für Netzwerksicherheit

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um AWS Network Security Manager-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- Wie AWS Network Security Manager funktioniert mit IAM

- Identity-based Richtlinienbeispiele für AWS Manager für Netzwerksicherheit
- Fehlerbehebung AWS Network Security Manager: Identität und Zugriff

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe Fehlerbehebung AWS Network Security Manager: Identität und Zugriff).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe Wie AWS Network Security Manager funktioniert mit IAM).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe Identity-based Richtlinienbeispiele für AWS Manager für Netzwerksicherheit).

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der

Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Verbundidentität

Es hat sich bewährt, dass menschliche Benutzer für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden müssen.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Ihrem Directory Service Web-Identitätsanbieter oder der AWS-Services mithilfe von Anmeldeinformationen aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zugreifen zu können.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln AWS CLI oder einen AWS API-Vorgang aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für den Verbundbenutzer-Zugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, serviceübergreifenden Zugriff und Anwendungen, die auf Amazon EC2 laufen. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWS bewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcenund unter welchen Bedingungendurchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identity-based Richtlinien

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität (Benutzer, Gruppe oder Rolle) anhängen. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identity-based Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mehreren Identitäten zugeordnet sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Resource-based Richtlinien

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen und Amazon S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

Resource-based Richtlinien sind Inline-Richtlinien, die sich in diesem Dienst befinden. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- Berechtigungsgrenzen – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im -IAM-Benutzerhandbuch.
- Service-Kontrollrichtlinien (SCPs) – SCPs legen die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in AWS Organizations fest. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Ressourcen-Kontrollrichtlinien (RCPs) – RCPs definieren die maximale Anzahl an Berechtigungen, die Ressourcen in Ihren Konten zur Verfügung stehen. Weitere Informationen finden Sie unter Ressourcen-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere Arten von Richtlinien für eine Anfrage gelten, sind die sich daraus ergebenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

Wie AWS Network Security Manager funktioniert mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf AWS Network Security Manager verwenden, sollten Sie sich darüber informieren, welche IAM-Funktionen für die Verwendung mit AWS Network Security Manager verfügbar sind.

IAM-Feature	AWS Unterstützung für Network Security Manager
Identity-based Richtlinien	Ja
Resource-based Richtlinien	Nein

IAM-Feature	AWS Unterstützung für Network Security Manager
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Ja
Service-linked Rollen	Ja

Einen allgemeinen Überblick darüber, wie AWS Network Security Manager und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identity-based Richtlinien für AWS Manager für Netzwerksicherheit

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität anhängen können, z. B. an einen IAM-Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Informationen zu sämtlichen Elementen, die Sie

in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Resource-based Richtlinien innerhalb AWS Manager für Netzwerksicherheit

Unterstützt ressourcenbasierte Richtlinien: Nein

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

AWS Network Security Manager unterstützt keine ressourcenbasierten Richtlinien.

Richtlinienaktionen für AWS Manager für Netzwerksicherheit

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Eine Liste der AWS Network Security Manager-Aktionen finden Sie unter Von AWS Network Security Manager definierte Aktionen in der Serviceautorisierungsreferenz.

Richtlinienaktionen in AWS Network Security Manager verwenden vor der Aktion das folgende Präfix:

```
network-security-manager
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

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

AWS Network Security Manager definiert IAM-Aktionen für alle Ressourcentypen. Dazu gehören CRUD-Operationen (Create, Read, Update und Delete) für Regeln, Vorlagen, Richtlinien, Bereiche und Bereitstellungen sowie Snapshot-, Tagging-, Verwaltungs-, Synchronisierungsstatus- und Ressourcenzuordnungsvorgänge.

Richtlinienressourcen für AWS Manager für Netzwerksicherheit

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Eine Liste der AWS Network Security Manager-Ressourcentypen und ihrer ARNs finden Sie unter Von AWS Network Security Manager definierte Ressourcen in der Serviceautorisierungsreferenz. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von AWS Network Security Manager definierte Aktionen.

AWS Network Security Manager definiert einen IAM-Ressourcentyp für jede seiner Ressourcen (Regel, Vorlage, Richtlinie, Bereich und Bereitstellung) sowie einen Snapshot-Typ für jede Ressource (z. B.`rule-snapshot`). Das ARN-Format ist:

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

Entwurfs-ARNs werden angehängt `:DRAFT` und Snapshot-ARNs fügen die Versionsnummer hinzu (z. B.). `:3`

Entwürfe sind keine separaten IAM-Ressourcentypen. Bei der Autorisierung wird ein Entwurf als untergeordnetes Element seiner aktiven Ressource behandelt, bei der es sich um die übergeordnete Ressource handelt. Ein `:DRAFT` -qualifizierter ARN autorisiert gegen die aktive Ressource. Die Erlaubnis, auf einen Entwurf zu reagieren, ergibt sich also aus der Genehmigung, mit dieser aktiven Ressource zu arbeiten.

Schnappschüsse unterscheiden sich von Entwürfen. Jeder Snapshot hat seinen eigenen IAM-Ressourcentyp, sodass ein versionsqualifizierter ARN direkt für diesen Snapshot-Ressourcentyp autorisiert, nicht für die übergeordnete aktive Ressource.

Richtlinien-Bedingungsschlüssel für AWS Manager für Netzwerksicherheit

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der AWS Network Security Manager-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Network Security Manager in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von AWS Network Security Manager definierte Aktionen.

AWS Network Security Manager unterstützt die folgenden AWS globalen Tag-Bedingungsschlüssel für die attributebasierte Zugriffskontrolle (ABAC):

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

Tag-based Bedingungsschlüssel gelten für aktive Ressourcen und Snapshots. Ressourcenentwürfe können nicht markiert werden und unterstützen keine Bedingungen. `aws:ResourceTag`

ACLs in AWS Manager für Netzwerksicherheit

Unterstützt ACLs: Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

AWS Network Security Manager unterstützt keine Zugriffskontrolllisten (ACLs).

ABAC mit AWS Manager für Netzwerksicherheit

Unterstützt ABAC (Tags in Richtlinien): Ja

Attribute-based Access Control (ABAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert, die als Tags bezeichnet werden. Sie können Tags an IAM-Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien entwerfen, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

AWS Network Security Manager unterstützt die attributbasierte Zugriffskontrolle unter Verwendung aller drei AWS globalen Tag-Bedingungsschlüssel. Sie können den Zugriff auf AWS Network Security Manager-Ressourcen anhand der mit diesen Ressourcen verknüpften Tags einschränken.

Verwenden temporärer Anmeldeinformationen mit AWS Manager für Netzwerksicherheit

Unterstützt temporäre Anmeldeinformationen: Ja

Temporäre Anmeldeinformationen ermöglichen kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie einen Verbund verwenden oder die Rollen wechseln. AWS empfiehlt,

temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Anmeldeinformationen in IAM und AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Cross-service Hauptberechtigungen für AWS Manager für Netzwerksicherheit

Unterstützt Forward Access Sessions (FAS): Ja

Forward Access Sessions (FAS) verwenden die Berechtigungen des Principals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen AWS-Service an nachgeschaltete Dienste zu stellen. Einzelheiten zu den Richtlinien für FAS-Anforderungen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AWS Manager für Netzwerksicherheit

Unterstützt Servicerollen: Ja

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität von AWS Network Security Manager beeinträchtigt werden. Bearbeiten Sie Dienstrollen nur, wenn AWS Network Security Manager Sie dazu anleitet.

Service-linked Rollen für AWS Manager für Netzwerksicherheit

Unterstützt serviceverknüpfte Rollen: Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer AWS-Service verknüpft ist. Der Dienst kann die Rolle übernehmen, eine Aktion in Ihrem Namen auszuführen. Service-linked Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

AWS Network Security Manager verwendet eine dienstbezogene Rolle, um in Mitgliedskonten Ihrer Organisation zu agieren. AWS Network Security Manager erstellt die dienstbezogene Rolle automatisch, wenn Sie den Dienst aktivieren. Die Rolle gewährt AWS Network Security Manager die

Berechtigung, AWS WAF- und AWS Shield Advanced-Ressourcen zu verwalten. Die Rolle gewährt auch Zugriff auf AWS Config für die Ressourcenerkennung und die Erlaubnis, kontenübergreifende Operationen durchzuführen.

Einzelheiten zum Erstellen und Verwalten von dienstbezogenen AWS Network Security Manager-Rollen finden Sie unter. the section called “Service-linked Rollen”

Identity-based Richtlinienbeispiele für AWS Manager für Netzwerksicherheit

Standardmäßig sind Benutzer und Rollen nicht berechtigt, AWS Network Security Manager-Ressourcen zu erstellen oder zu ändern. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von AWS Network Security Manager definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für jeden Ressourcentyp, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Network Security Manager in der Service Authorization Reference.

Themen

- Best Practices für Richtlinien
- Verwendung der AWS Network Security Manager-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Read-only Zugriff auf AWS Manager für Netzwerksicherheit
- Nur Regeln und Vorlagen verwalten

Best Practices für Richtlinien

Identity-based Richtlinien legen fest, ob jemand AWS Network Security Manager-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder diese löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Beachten Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für

viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien oder Von AWS verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.

- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Best Practices für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwendung der AWS Network Security Manager-Konsole

Um auf die AWS Network Security Manager-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS Network Security Manager-Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um auf die AWS Network Security Manager-Konsole zugreifen zu können, benötigt ein Principal mindestens Berechtigungen für die `network-security-manager:Get*` Aktionen `network-security-manager:List*` und.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie beinhaltet Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI AWS OR-API.

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

```
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Read-only Zugriff auf AWS Manager für Netzwerksicherheit

Die folgende Richtlinie gewährt einem Prinzipal nur Lesezugriff auf alle AWS Network Security Manager-Ressourcen. Dies ist nützlich für Prüfer oder Überwacher, die Konfigurationen und den Synchronisierungsstatus einsehen müssen, ohne Änderungen vorzunehmen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "network-security-manager:Get*",
                "network-security-manager:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Nur Regeln und Vorlagen verwalten

Die folgende Richtlinie ermöglicht es einem Prinzipal, Regeln und Vorlagen zu erstellen, zu aktualisieren und zu löschen, ohne Zugriff auf Richtlinien, Bereiche oder Bereitstellungen zu gewähren. Dies ist nützlich für Teams, die Sicherheitskonfigurationen erstellen, aber nicht die Durchsetzung kontrollieren.

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

Fehlerbehebung AWS Network Security Manager: Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS Network Security Manager und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Manager für Netzwerksicherheit
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb meines AWS-Konto um auf meine zuzugreifen AWS Ressourcen für Network Security Manager

Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Manager für Netzwerksicherheit

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `network-security-manager:`*`GetWidget`*-Berechtigungen verfügt.

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

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `network-security-manager:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht autorisiert sind, die `iam:PassRole` Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an AWS Network Security Manager übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AWS Network Security Manager auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

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

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meines AWS-Konto um auf meine zuzugreifen AWS Ressourcen für Network Security Manager

Sie können eine Rolle erstellen, mit der Benutzer mit anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob AWS Network Security Manager diese Funktionen unterstützt, finden Sie unterWie AWS Network Security Manager funktioniert mit IAM.
- Informationen darüber, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwenden von serviceverknüpften Rollen für AWS Manager für Netzwerksicherheit

AWS Network Security Manager verwendet dienstverknüpfte IAM-Rollen. Eine dienstverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, die direkt mit Network Security Manager verknüpft ist. AWS Service-linked Rollen sind von AWS Network Security Manager vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle erleichtert die Einrichtung von AWS Network Security Manager, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Network Security Manager definiert die Berechtigungen seiner dienstbezogenen Rollen. Sofern nicht anders definiert, kann nur AWS Network Security Manager seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Sie können diese Berechtigungsrichtlinie keiner anderen IAM-Entität zuordnen.

Sie können eine dienstbezogene Rolle erst löschen, nachdem Sie zuerst die zugehörigen Ressourcen gelöscht haben. Dadurch werden Ihre AWS Network Security Manager-Ressourcen geschützt, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entziehen können.

Informationen zu anderen Diensten, die dienstbezogene Rollen unterstützen, finden Sie unter AWS Dienste, die mit IAM funktionieren. Suchen Sie nach den Diensten, die in der Rollenspalte Ja enthalten. Service-linked Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Service-linked Rollenberechtigungen für AWS Manager für Netzwerksicherheit

AWS Network Security Manager verwendet die mit dem Dienst verknüpfte Rolle namens`AWSServiceRoleForNetworkSecurityManager`. Diese dienstbezogene Rolle vertraut darauf, dass der `network-security-manager.amazonaws.com` Dienstprinzipal die Rolle übernimmt.

Bei der genannten Rollenberechtigungsrichtlinie `NetworkSecurityManagerServiceRolePolicy` handelt es sich um eine AWS verwaltete Richtlinie, die es AWS Network Security Manager ermöglicht, Aktionen an den angegebenen Ressourcen durchzuführen.

Die folgende Vertrauensrichtlinie ermöglicht es dem `network-security-manager.amazonaws.com` Dienstprinzipal, die Rolle zu übernehmen.

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

```
            "Action": "sts:AssumeRole"
        }
    ]
}
```

> **Note**
>
> Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Service-linked Rollenberechtigungen.

Details zu Berechtigungen

AWS Network Security Manager benötigt jede Gruppe von Berechtigungen, um Ressourcen in Ihrem Konto und Ihrer Organisation zu schützen und zu erkennen. Die `NetworkSecurityManagerServiceRolePolicy` verwaltete Richtlinie gewährt die folgenden Berechtigungen, gruppiert nach Diensten:

- `wafv2`— Web-ACLs und Firewall Manager Manager-Regelgruppen erstellen, lesen, aktualisieren und löschen. Ordnen Sie Web-ACLs geschützten Ressourcen zu und trennen Sie die Zuweisung. Verwalten Sie Web-ACL-Protokollierungskonfigurationen und Richtlinien für Regelgruppenberechtigungen. Ressourcen kennzeichnen und deren Markierung aufheben Überprüfen Sie die Web ACL- und Regelkonfigurationen von AWS Network Security Manager.
- `shield`— AWS Shield Advanced-Schutzmaßnahmen erstellen, beschreiben, auflisten und löschen. Erstellen und beschreiben Sie das AWS Shield Advanced-Abonnement.
- `elasticloadbalancing`— Beschreiben Sie Application Load Balancer und Tags. Web-ACL-Zuordnungen auf Application Load Balancers erstellen, löschen und einrichten.
- `cloudfront`— Abrufen und Auflisten von CloudFront Amazon-Distributionen, -Konfigurationen und -Tags. Zuordnen und Trennen der Zuordnung von Distribution-Web-ACLs. Lesen Sie VPC-Ursprünge.
- `apigateway`— Lesen Sie die REST-APIs, Stufen und Tags von Amazon API Gateway. Stellen Sie die Web-ACL auf einer API-Phase ein.
- `ec2`— Lesen Sie Web-ACLs und Zuordnungen für Amazon EC2 Verified Access-Instances. Beschreiben Sie Elastic IP-Adressen für AWS Shield Advanced-Schutz.

- `cognito-idp`,, `apprunner` `appsyncamplify`, und `bedrock-agentcore` — Lesen Sie Web-ACL-Verknüpfungen für Amazon Cognito Cognito-Benutzerpools, AWS App Runner Dienste, AWS AppSync GraphQL-APIs, AWS Amplify Apps und Amazon AgentCore Bedrock-Gateways, damit AWS Network Security Manager geschützte Ressourcen finden kann.
- `config`— Wählen Sie Ressourcenkonfigurationen aus und verwalten Sie den serviceverknüpften AWS Config Konfigurationsrekorder, den AWS Network Security Manager verwendet, um Ressourcen zu ermitteln, die im Leistungsumfang enthalten sind.
- `organizations`— Lesen Sie Ihre Organisation, Konten, Stammverzeichnisse, Organisationseinheiten und delegierte Administratoren, damit AWS Network Security Manager unternehmensweit eingesetzt werden kann.
- `logs`— Protokollzustellungen für die Web-ACL-Protokollierung erstellen, lesen, aktualisieren, löschen und auflisten.
- `s3`— Rufen Sie Bucket-Richtlinien ab und fügen Sie sie in Amazon S3 S3-Buckets ein, deren Namen mit beginnen, `aws-waf-logs-` damit Web-ACL-Protokolle übermittelt werden können.
- `iam`— Erstellen Sie die serviceverknüpften Rollen, die AWS Shield Advanced und AWS WAF benötigen, im Bereich des Bedingungsschlüssels. AWS Config`iam:AWSServiceName`

Die folgende JSON-Datei zeigt die vollständige Berechtigungsrichtlinie. `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"
        }
      }
    }
```

```
  ]
}
```

Erstellen einer serviceverknüpften Rolle für AWS Manager für Netzwerksicherheit

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie AWS Network Security Manager aktivieren, erstellt AWS Network Security Manager die dienstbezogene Rolle für Sie. Es muss kein manueller Schritt ausgeführt werden.

Wenn Sie diese dienstbezogene Rolle löschen und sie dann erneut erstellen müssen, erstellt AWS Network Security Manager die Rolle neu, wenn Sie den Dienst das nächste Mal verwenden. Sie müssen keine Maßnahmen ergreifen.

Weitere Informationen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Bearbeiten einer serviceverknüpften Rolle für AWS Manager für Netzwerksicherheit

Sie können die Berechtigungen der `AWSServiceRoleForNetworkSecurityManager` serviceverknüpften Rolle nicht ändern. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten.

Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für AWS Manager für Netzwerksicherheit

Wenn Sie AWS Network Security Manager nicht mehr verwenden müssen, empfehlen wir, die `AWSServiceRoleForNetworkSecurityManager` dienstbezogene Rolle zu löschen.

Bevor Sie die dienstverknüpfte Rolle löschen, sollten Sie die von AWS Network Security Manager verwalteten Ressourcen bereinigen. Deaktivieren Sie AWS Network Security Manager und entfernen Sie die Richtlinien und Bereiche, sodass keine von AWS Network Security Manager verwalteten Ressourcen in Ihrem Konto verbleiben. Anschließend können Sie die Rolle manuell löschen.

> **Note**
>
> Wenn AWS Network Security Manager die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

So löschen Sie die -servicegebundene Rolle mit IAM

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Rollen.
3. Geben Sie `AWSServiceRoleForNetworkSecurityManager` im Suchfeld die Rolle ein und wählen Sie sie aus.
4. Wählen Sie Löschen aus.
5. Um den Löschvorgang zu bestätigen, geben Sie den Rollennamen ein und wählen Sie dann Löschen aus.

Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für AWS Mit dem Dienst verknüpfte Rollen von Network Security Manager

AWS Network Security Manager unterstützt die Verwendung von dienstbezogenen Rollen in allen AWS Regionen, in denen AWS Network Security Manager verfügbar ist.

Konformitätsprüfung für AWS Manager für Netzwerksicherheit

Unser neues AWS Anmeldeerlebnis ist nicht für regulierte Workloads konzipiert. Wenn Sie unser neues AWS Anmeldeformular nutzen, es aber AWS für regulierte Workloads nutzen möchten, können Sie sich für AWS (erweiterte) Funktionen registrieren oder erweiterte Funktionen für Ihre Umgebung aktivieren. AWS

Informationen darüber, ob AWS-Service ein in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter AWS-Services Umfang nach Compliance-Programm unter Umfang nach Compliance-Programm AWS-Services das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. Weitere Informationen zu Ihrer Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services finden Sie in der AWS Sicherheitsdokumentation.

Resilienz in AWS Manager für Netzwerksicherheit

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur bietet AWS Network Security Manager mehrere Funktionen zur Unterstützung Ihrer Datenausfallsicherheit und Backup-Anforderungen.

Sicherheit der Infrastruktur in AWS Manager für Netzwerksicherheit

Als verwalteter Service ist AWS Network Security Manager durch die AWS globalen Netzwerksicherheitsverfahren geschützt, die im Whitepaper Amazon Web Services: Sicherheitsprozesse im Überblick beschrieben sind.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über AWS das Netzwerk auf Network Security Manager zuzugreifen. Kunden müssen Transport Layer Security (TLS) 1.0 oder neuer unterstützen. Wir empfehlen TLS 1.2 oder neuer. Die Clients müssen außerdem Cipher Suites mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) unterstützen. Diffie-Hellman Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS

-Security-Token-Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Bewährte Sicherheitsmethoden für AWS Manager für Netzwerksicherheit

Die folgenden bewährten Methoden helfen Ihnen dabei, eine sichere AWS Network Security Manager-Konfiguration aufrechtzuerhalten.

Präventive Kontrollen

- Geringste IAM-Rechte verwenden — Gewähren Sie nur die Berechtigungen, die für jeden Benutzer oder jede Rolle erforderlich sind, um ihre AWS Network Security Manager-Aufgaben auszuführen. Verwenden Sie nach Möglichkeit IAM-Bedingungsschlüssel, um den Zugriff auf bestimmte Ressourcen einzuschränken.
- Dienstbezogene Rollen verwenden — AWS Network Security Manager verwendet dienstverknüpfte Rollen, um Aktionen in Ihrem Namen auszuführen. Diese Rollen verfügen über vordefinierte Berechtigungen, die auf den erforderlichen Mindestzugriff beschränkt sind.
- Bereiche sorgfältig konfigurieren -- Definieren Sie Bereichskonfigurationen, die nur auf die Konten und Ressourcentypen abzielen, die geschützt werden müssen. Ein zu breiter Geltungsbereich kann zu unbeabsichtigten Durchsetzungsmaßnahmen führen.

Detektivische Kontrollen

- AWS CloudTrail Protokollierung aktivieren — CloudTrail zeichnet alle AWS Network Security Manager API-Aufrufe auf. Überprüfen Sie diese Protokolle, um zu überprüfen, wer wann Änderungen an Ihren Sicherheitskonfigurationen vorgenommen hat.
- Synchronisierungsstatus überwachen — Überprüfen Sie regelmäßig den Synchronisierungsstatus Ihrer Bereitstellungen, um festzustellen, ob Ressourcen nicht mit Ihrem beabsichtigten Sicherheitsstatus synchron sind.

Überwachen AWS Manager für Netzwerksicherheit

Durch die Überwachung von AWS Network Security Manager können Sie nachvollziehen, ob Ihre Ressourcen wie vorgesehen geschützt sind. AWS Network Security Manager bietet die folgenden Überwachungsfunktionen:

- APIs für den Synchronisierungsstatus — Fragen Sie den Schutzstatus einzelner Ressourcen in Ihren Bereitstellungen ab.
- AWS CloudTrail-- Zeichnet alle AWS Network Security Manager-API-Aufrufe zur Prüfung, Einhaltung von Vorschriften und zur betrieblichen Fehlerbehebung auf.

Synchronisierungsstatus überwachen

Die wichtigste Methode, um zu überwachen, ob Ihre Ressourcen geschützt sind, sind die APIs für den Synchronisierungsstatus. AWS Network Security Manager bewertet jede Ressource im Geltungsbereich und zeichnet auf, ob ihre tatsächliche Firewall-Konfiguration mit der beabsichtigten Konfiguration übereinstimmt.

Vorgänge mit dem Synchronisierungsstatus

AWS Network Security Manager bietet zwei Operationen zum Abfragen des Synchronisationsstatus:

ListResourceSynchronizationStatuses

Gibt den Status pro Ressource für eine bestimmte Bereitstellung zurück. Erfordert einen `deploymentIdentifier` Parameter. Filtern Sie optional nach `synchronizationStatus` (IN_SYNC, OUT_OF_SYNC oder NOT_APPLICABLE).

ListAggregateResourceSynchronizationStatuses

Gibt den aggregierten Status pro Ressource für all Ihre Bereitstellungen zurück. Filtern Sie optional nach. `synchronizationStatus` Dieser Vorgang zeigt das kombinierte Ergebnis aller Richtlinien, die für jede Ressource gelten.

Beide Operationen unterstützen die Paginierung mit `maxResults` (1 bis 100) und`nextToken`.

Grundlegendes zu Synchronisationsstatuswerten

IN_SYNC

Die tatsächliche Firewallkonfiguration der Ressource entspricht der effektiven Konfiguration, die anhand aller geltenden Richtlinien berechnet wurde.

OUT_OF_SYNC

Die tatsächliche Konfiguration der Ressource unterscheidet sich von der effektiven Konfiguration. Das `outOfSyncReasons` Feld enthält Details zu den einzelnen Einstellungen, in denen die erwarteten Werte im Vergleich zu den tatsächlichen Werten dargestellt werden.

NOT_APPLICABLE

Das Konto und der Ressourcentyp der Ressource befinden sich im Gültigkeitsbereich, aber die Ressource selbst entspricht nicht den Bereichsfiltern (z. B. schließt sie ein Tagfilter aus). Keine Aktion erforderlich.

Wenn eine Ressource überhaupt nicht in den Ergebnissen erscheint, ist das Konto oder der Ressourcentyp nicht im Bereich der Bereitstellung enthalten. Überprüfen Sie Ihre Bereichskonfiguration.

Die Zeitstempel der Evaluierung verstehen

Jeder Synchronisationsstatuseintrag enthält zwei Zeitstempel:

- `evaluatedAt`-- Wann AWS Network Security Manager die Konfiguration der Ressource zuletzt bewertet hat. Ein veralteter `evaluatedAt` Wert gibt an, dass die Evaluierung der letzten Änderungen noch nicht durchgeführt wurde.
- `updatedAt`— Wann der Synchronisationsstatusdatensatz selbst zuletzt geändert wurde. Wenn älter als `updatedAt` ist`evaluatedAt`, ist der Status seit der letzten Auswertung stabil.

Cross-account Sichtbarkeit

Wenn mehrere Administratoren dieselbe Ressource schützen, hängt der Einblick in den aggregierten Synchronisierungsstatus von den `enableCrossAccountVisibility` Einstellungen in der jeweiligen Bereitstellung ab.

- Wenn für alle Bereitstellungen, die eine Ressource abdecken, die kontenübergreifende Sichtbarkeit aktiviert ist, kann jeder Administrator den vollständigen Aggregatstatus und die Gründe für die Nichtsynchronisierung einsehen.
- Wenn bei einer Bereitstellung die kontoübergreifende Sichtbarkeit deaktiviert ist, sehen andere Administratoren statt detaillierter Gründe eine `NOT_VISIBLE` Markierung. Dies weist darauf hin, dass ein anderer Administrator die Ressource ebenfalls schützt, aber keine gemeinsame Sichtbarkeit hat.

Diagnose von Ressourcen, die nicht synchron sind

Wenn eine Ressource OUT_OF_SYNC meldet, identifiziert das Feld die `outOfSyncReasons` spezifischen Konfigurationsunterschiede. Der Grund auf oberster Ebene ist einer der folgenden:

- `missingFirewall`-- Der Ressource ist kein Firewall-Schutz zugeordnet.
- `invalidFirewall`-- Eine Firewall ist vorhanden, aber ihre Konfiguration entspricht nicht den Erwartungen. Spezifische Unterschiede sind in kategorisierten Kategorien aufgeführt.

Wenn die Problembehebung aktiviert ist, die Ressource aber nicht repariert werden kann, enthält das `remediationIssues` Feld eine `correctiveAction` Anleitung, wie das Problem manuell gelöst werden kann. Bei der Behebung handelt es sich um eine Einstellung auf Richtlinienebene, die standardmäßig deaktiviert ist. Weitere Informationen finden Sie unter the section called “Synchronisation und Problembehebung”.

Mehrere Bereitstellungen mit unterschiedlichen Konfigurationen können auf dieselbe Ressource abzielen. In diesem Fall kann der Synchronisationsstatus pro Bereitstellung OUT_OF_SYNC sein, während der aggregierte Synchronisationsstatus IN_SYNC lautet. Dies ist ein erwartetes Verhalten, kein Fehler. Die Einstellungen einer Richtlinie mit höherer Priorität hatten beim Zusammenführen Vorrang. Infolgedessen entspricht die Ressource der effektiven Konfiguration, obwohl sie nicht der Konfiguration der Bereitstellung mit niedrigerer Priorität entspricht.

Protokollierung AWS Network Security Manager API-Aufrufe mit AWS CloudTrail

AWS Network Security Manager ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS Dienst ausgeführten Aktionen bereitstellt. CloudTrail erfasst alle API-Aufrufe für AWS Network Security Manager als Verwaltungsereignisse.

Zu den erfassten Aufrufen gehören Aufrufe von der AWS Network Security Manager-Konsole und programmatische Aufrufe der AWS Network Security Manager-API-Operationen.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für AWS Network Security Manager. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

AWS Informationen zum Network Security Manager in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn im AWS Network Security Manager eine Aktivität auftritt, wird diese Aktivität zusammen mit anderen CloudTrail AWS Dienstereignissen im Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem System AWS-Konto, einschließlich der Ereignisse für AWS Network Security Manager, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition. Es übermittelt die Protokolldateien an den Amazon S3 S3-Bucket, den Sie angeben. Sie können andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail

Alle AWS Network Security Manager-Vorgänge werden von CloudTrail protokolliert. Zu den öffentlichen Operationen gehören die folgenden:

- Operationen zum Erstellen, Lesen, Aktualisieren und Löschen (CRUD) für Regeln, Vorlagen, Richtlinien, Bereiche und Bereitstellungen
- Snapshot-Operationen
- Tagging-Operationen

- Vorgänge mit Administratorkonten
- Operationen mit dem Synchronisierungsstatus
- Operationen zur Zuordnung von Ressourcen
- Operationen zur Generierung von Regeln

Jeder Ereigniseintrag enthält die folgenden Informationen:

- Die Quelle des Ereignisses: `network-security-manager.amazonaws.com`
- Der Name des Ereignisses, bei dem es sich um den Namen der API-Operation handelt (z. B. `CreatePolicy` oder`ListDeployments`)
- Die betroffenen Ressourcen, identifiziert nach ARN und Ressourcentyp

Read-only Operationen (wie `GetPolicyListRules`, und`ListResourceSynchronizationStatuses`) werden mit protokolliert `readOnly: true` und enthalten keine Antwortelemente. Mutationsoperationen umfassen Anforderungsparameter und Antwortelemente.

> **Note**
>
> CloudTrail redigiert sensible Felder aus Ereignisdatensätzen. CloudTrail Redigiert beispielsweise den `prompt` Parameter in der `GenerateRuleConfiguration` Operation.

Beispiel: Ereignis CreatePolicy

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag für den `CreatePolicy` Vorgang.

```
{
  "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 Network Security Manager-Kontingente

Ihr AWS-Konto hat die folgenden Standardkontingente für AWS Network Security Manager. Sofern nicht anders angegeben, gilt jedes Kontingent pro Konto und Region.

Ressourcenkontingente

In der folgenden Tabelle ist die maximale Anzahl von AWS Network Security Manager-Ressourcen aufgeführt, die Sie pro Konto in jeder Region erstellen können.

Ressource	Standardkontingent	Einstellbar
Regeln pro -Konto	200	Nein
Vorlagen pro Konto	100	Nein
Richtlinien je Konto	100	Nein
Bereiche pro Konto	100	Nein
Bereitstellungen pro Konto	100	Nein
Schnappschüsse pro Ressource	10	Nein

Kontingente für die Zusammensetzung von

In der folgenden Tabelle sind die Kontingente aufgeführt, die angeben, wie AWS Network Security Manager-Ressourcen innerhalb der Ressourcenhierarchie aufeinander verweisen.

Kontingent	Wert
Regeln pro Vorlage	1 bis 50
Vorlagen pro AWS WAF-Richtlinie	1 bis 2

Kontingent	Wert
Regeln und Vorlagen werden pro AWS WAF-Richtlinie kombiniert	1 bis 100
Vorlagen oder Regeln gemäß AWS Shield Advanced-Richtlinie	0 (muss leer sein)
Richtlinien pro Bereitstellung	1 bis 2
Geltungsbereiche pro Bereitstellung	1 (genau einer)

Umfang der Konfigurationskontingente

In der folgenden Tabelle sind die Kontingente für Ausdrücke der Bereichskonfiguration aufgeführt.

Kontingent	Wert
Bereiche des Ressourcentyps pro Bereich	20
Tiefe des Ausdrucks im Geltungsbereich (verschachtelte Ebenen)	2
Breite des Ausdrucks für den Geltungsbereich (Kriterien pro Ebene)	20

Kontingente für Administratorkonten

In der folgenden Tabelle sind die Kontingente für die Prioritätsstufen von AWS Network Security Manager-Administratorkonten aufgeführt.

Kontingent	Wert
Prioritätsstufen für Administratoren	1 bis 10

Kontingente für API-Paginierung

In der folgenden Tabelle sind die Paginierungslimits für Listenoperationen aufgeführt.

Kontingent	Wert
Maximale Anzahl von Ergebnissen pro Seite () `maxResults`	100
Minimale Ergebnisse pro Seite (`maxResults`)	1

Einstellbarkeit der Quote

Die in den vorangegangenen Abschnitten aufgeführten Kontingente sind fest und können derzeit nicht erhöht werden.

Dokumentenhistorie für die AWS Network Security Manager Entwicklerhandbuch

In der folgenden Tabelle werden die Dokumentationsversionen für AWS Network Security Manager beschrieben.

Änderung	Beschreibung	Datum
Erstversion	Erste Version des AWS Network Security Manager-Entwicklerhandbuchs.	1. August 2026

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.