Guía para desarrolladores

AWS Gerente de seguridad de red

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

AWS Gerente de seguridad de red: Guía para desarrolladores

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

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es AWS Network Security Manager? ... 1
Cómo AWS Network Security Manager funciona de un vistazo ... 1
Características de AWS Administrador de seguridad de red ... 1
Casos de uso ... 2
Servicios relacionados ... 3
Acceso AWS Administrador de seguridad de red ... 4
Precios ... 4
¿Es la primera vez que usa ? ... 5
Cómo funciona AWS Network Security Manager ... 6
AWS Modelo de recursos de Network Security Manager ... 6
AWS Ciclo de vida de los recursos, fusión y sincronización de Network Security Manager ... 7
Borrador y ciclo de vida activo ... 7
Control de versiones ... 8
Priority-based fusión de políticas ... 9
Descubrimiento de recursos con AWS Config ... 10
Sincronización y corrección ... 11
Cuentas de administrador y de miembro ... 13
Service-linked rol ... 13
Configuración de AWS Network Security Manager ... 14
Elige tu modelo organizativo ... 14
Configuración para el uso de una sola cuenta ... 14
Se configura para el uso de varias cuentas con AWS Organizations ... 15
Crear un AWS Cuenta de administrador de Network Security Manager ... 16
Cree una identidad de IAM con AWS Permisos de Network Security Manager ... 18
Inscríbase para obtener una Cuenta de AWS ... 19
Utilización AWS Administrador de seguridad de red en las regiones que están deshabilitadas de forma predeterminada ... 19
Tutorial: Implemente su primera protección de seguridad de red ... 20
Requisitos previos ... 20
Paso 1: Crear una regla ... 21
Paso 2: Crear una plantilla ... 22
Paso 3: Crear una política ... 23
Paso 4: Crear un ámbito ... 24
Paso 5: Crear y publicar una implementación ... 25

Paso 6: Supervisar el estado de sincronización ... 25
Paso 7: limpiar ... 26
Siguientes pasos ... 27
Administración de firewalls y servicios de seguridad ... 29
Administrar las ACL web para WAF AWS ... 29
AWS Conceptos de WAF ... 29
Quick Create para AWS WAF ... 33
Proceso de creación estándar para AWS WAF ... 37
Gestión de las protecciones DDoS para AWS Shield Advanced ... 43
Creación rápida para AWS Shield Advanced ... 44
Proceso de creación estándar para AWS Shield Advanced ... 48
AWS Administrador de Seguridad de Red y Administrador de Firewall ... 52
Coexistencia con AWS Firewall Manager ... 52
Prioridad durante la corrección ... 52
Migración planificada desde AWS Firewall Manager ... 52
Seguridad ... 54
Protección de datos ... 55
Cifrado en reposo ... 56
Cifrado en tránsito ... 56
Administración de claves ... 56
Identity and Access Management ... 56
Público ... 57
Autenticación con identidades ... 57
Administración del acceso con políticas ... 58
Cómo AWS Network Security Manager funciona con IAM ... 60
Identity-based ejemplos de políticas ... 66
Resolución de problemas ... 71
Service-linked funciones ... 73
Service-linked permisos de rol ... 74
Crear un rol vinculado a servicios ... 84
Editar un rol vinculado a un servicio ... 85
Eliminar un rol vinculado a un servicio ... 85
Regiones admitidas ... 86
Validación de conformidad ... 86
Resiliencia ... 86
Seguridad de infraestructuras ... 87

Prácticas recomendadas de seguridad 87
Controles preventivos 87
Controles de detección 88
Supervisión AWS Gerente de seguridad de red 89
Supervisar el estado de sincronización 89
Estado de sincronización: operaciones 89
Comprensión de los valores del estado de sincronización 90
Comprenda las marcas de tiempo de la evaluación 90
Cross-account visibilidad 90
Diagnóstico de recursos no sincronizados 91
CloudTrail registros 91
AWS La información del administrador de seguridad de red en CloudTrail 92
Ejemplo: evento CreatePolicy 93
Cuotas 96
Cuotas de recursos 96
Cuotas de composición de recursos 96
Cuotas de configuración del alcance 97
Cuotas de cuentas de administrador 97
Cuotas de paginación de la API 97
Capacidad de ajuste de la cuota 98
Historial de revisión 99
..... c

¿Qué es? AWS ¿Administrador de seguridad de red?

Con AWS Network Security Manager, puede definir e implementar de forma centralizada las protecciones de seguridad de la red, como las reglas AWS WAF y AWS Shield Advanced, en una o más cuentas y recursos de su organización. En lugar de trabajar con cada recurso de forma individual, debe definir los objetos de política reutilizables (reglas, plantillas y políticas) de una sola vez y desplegarlos a escala, con una supervisión continua para detectar y corregir las desviaciones de las políticas.

Cómo AWS Network Security Manager funciona de un vistazo

Puede definir un conjunto de objetos de política jerárquicos y aplicarlos a los ámbitos específicos. El nivel más bajo de los objetos de política son las reglas. Puede agrupar las reglas en plantillas, que puede combinar en políticas con resolución de conflictos basada en prioridades. A continuación, selecciona las cuentas y los recursos para protegerlos con un alcance específico y aplica tus políticas publicando una implementación.

Tras la implementación, AWS Network Security Manager monitorea continuamente el entorno específico y las políticas implementadas para comprobar si coinciden con las definiciones previstas. De lo contrario, AWS Network Security Manager puede remediar, si lo desea, los recursos que se desvíen de la configuración prevista. Para obtener todos los detalles sobre el modelo de recursos, el ciclo de vida y la arquitectura, consulteCómo funciona AWS Network Security Manager.

Características de AWS Administrador de seguridad de red

- Soporte para varios tipos de firewall: AWS Network Security Manager admite AWS WAF para configuraciones de ACL web y grupos de reglas. Los tipos de recursos protegidos incluyen CloudFront las distribuciones de Amazon, los balanceadores de carga de aplicaciones y las etapas de Amazon API Gateway. AWS Network Security Manager también es compatible con AWS Shield Advanced para la protección DDoS de CloudFront las distribuciones de Amazon, los balanceadores de carga de aplicaciones, los balanceadores de carga clásicos y las direcciones IP elásticas.
- Configuraciones de seguridad reutilizables: defina los objetos de política una vez como reglas, agrúpelos en plantillas y cree ámbitos para destinar los recursos. Reutilice las reglas, las plantillas y los ámbitos en varias políticas e implementaciones.

- Priority-based fusión de políticas: cuando varias políticas protegen el mismo recurso, AWS Network Security Manager combina sus configuraciones en función de la prioridad de las políticas, lo que proporciona una resolución de conflictos predecible.
- Single-account y soporte para varios administradores: utilice AWS Network Security Manager en una sola cuenta o designe varias cuentas de administrador, cada una con un nivel de prioridad. Cuando las políticas de los administradores se superponen, AWS Network Security Manager resuelve los conflictos en función de la prioridad del administrador en primer lugar y, después, de acuerdo con la prioridad de la política dentro de cada cuenta.
- Estados provisional y activo: cada recurso de AWS Network Security Manager, incluidas las reglas, plantillas, políticas, ámbitos e implementaciones, admite los estados Borrador y Activo. Guarde los recursos como borrador sin que ello afecte a las protecciones activas y, a continuación, publíquelos cuando estén listos para aplicarlos.
- Instantáneas versionadas: cada recurso de AWS Network Security Manager, incluidas las reglas, las plantillas, las políticas, los ámbitos y las implementaciones, admite instantáneas numeradas por versiones inmutables. Utilice el control de versiones para conservar las configuraciones de recursos de Network Security Manager que se sabe que son correctas. AWS
- Protected-resource diagnósticos de sincronización: para cada recurso incluido en el ámbito de aplicación, compruebe exactamente qué ajustes están desincronizados y por qué, comparando los ajustes esperados con los valores reales de cada campo de configuración.
- Corrección automática: si lo desea, habilite AWS Network Security Manager para corregir automáticamente los recursos no sincronizados y alinearlos con la configuración deseada sin intervención manual.
- Natural-language generación de reglas: utilice la `GenerateRuleConfiguration` operación para describir una regla en un lenguaje sencillo y reciba el JSON de configuración correspondiente, con la tecnología de Amazon Bedrock.

Casos de uso

Los siguientes son casos de uso habituales de AWS Network Security Manager:

- Aplique las reglas básicas de AWS WAF en todas las cuentas: defina un conjunto de grupos de reglas de AWS WAF que todas las aplicaciones con acceso a Internet deben usar y, a continuación, impleméntelos en toda la organización. AWS Network Security Manager aplica automáticamente las reglas a los nuevos recursos incluidos en el ámbito de aplicación a medida que entran en el ámbito de aplicación.

- Cree reglas de AWS WAF específicas personalizadas o de excepción para recursos específicos: defina un conjunto de reglas de AWS WAF que se apliquen solo a un conjunto específico de recursos. Este conjunto puede ser una aplicación o unidad de negocio específica que se identifique mediante el ID de AWS cuenta, la OU, la etiqueta o los nombres de recursos de Amazon (ARN).
- Verifique la protección contra DDoS en los recursos con acceso a Internet: cree una política AWS Shield Advanced que abarque los tipos de recursos públicos e impleméntela en toda la organización para que los recursos críticos tengan habilitada la protección contra DDoS.
- Detecte y corrija los errores de configuración: utilice la supervisión del estado de sincronización para identificar los recursos cuyas configuraciones de firewall se hayan desviado del estado previsto y, si lo prefiere, habilite la corrección automática para que vuelvan a cumplir con las normas.
- Delegue la gestión de la seguridad a varios equipos: designe varias cuentas de administrador con diferentes niveles de prioridad y acceso limitado a cuentas, unidades organizativas o tipos de firewall específicos, lo que permitirá a los equipos gestionar sus propias políticas de seguridad dentro de unos límites definidos.

Servicios relacionados

- AWS WAF: utilice AWS WAF para proteger sus aplicaciones web y API contra los ataques web y los bots más comunes que pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos. AWS Network Security Manager usa AWS WAF para crear y administrar las ACL web y los grupos de reglas para los recursos en una sola cuenta o en todas las cuentas de la organización.
- AWS Shield Advanced: un servicio de protección DDoS gestionado que proporciona una mayor protección para las aplicaciones que se estén ejecutando en AWS ellas. AWS Network Security Manager utiliza Shield Advanced para proporcionar protección contra DDoS a los recursos de una sola cuenta o de todas las cuentas de su organización.
- AWS Organizations: le ayuda a administrar y gobernar su entorno de forma centralizada a medida que crece y escala sus AWS recursos. AWS Network Security Manager requiere que AWS Organizations administre las protecciones en todas las cuentas de los miembros.
- AWS Config: un servicio que le permite evaluar, auditar y evaluar las configuraciones de sus AWS recursos. AWS Network Security Manager utiliza una grabadora AWS Config vinculada a un servicio para detectar los recursos en las cuentas de los miembros.

Acceso AWS Administrador de seguridad de red

Puede acceder a AWS Network Security Manager a través de las siguientes interfaces:

AWS Consola de administración

Una interfaz basada en web para administrar los recursos de AWS Network Security Manager.

Abra la consola de AWS Network Security Manager en https://console.aws.amazon.com/network-security-manager/.

AWS Interfaz de línea de comandos (AWS CLI)

Proporciona comandos para las operaciones de AWS Network Security Manager. Para obtener más información, consulte la Referencia de comandos de CLI AWS.

AWS SDK

AWS proporciona SDK que constan de bibliotecas y códigos de muestra para varios lenguajes de programación y plataformas. Los SDK proporcionan una forma cómoda de crear un acceso programático a AWS Network Security Manager. Para obtener más información, consulte Herramientas para Amazon Web Services.

AWS API de Network Security Manager

Una API REST que usa JSON sobre HTTPS. El formato de punto final de la API es`network-security-manager.`*`{region}`*`.api.aws`. Para obtener más información, consulte la referencia de la API de AWS Network Security Manager.

Para empezar a utilizar AWS Network Security Manager, consulte Configuración de AWS Network Security Manager yTutorial: Implemente su primera protección de seguridad de red.

Precios

Usted paga por cada recurso incluido en el ámbito de aplicación que AWS Network Security Manager monitorea y protege. Se aplican cargos adicionales a los servicios de seguridad subyacentes que implemente, como AWS WAF y AWS Shield Advanced. Para obtener información detallada sobre los precios, consulte los precios de AWS Network Security Manager en el AWS sitio web.

¿Es la primera vez que usa ?

Si es la primera vez que utiliza AWS Network Security Manager, le recomendamos que lea los siguientes temas en orden:

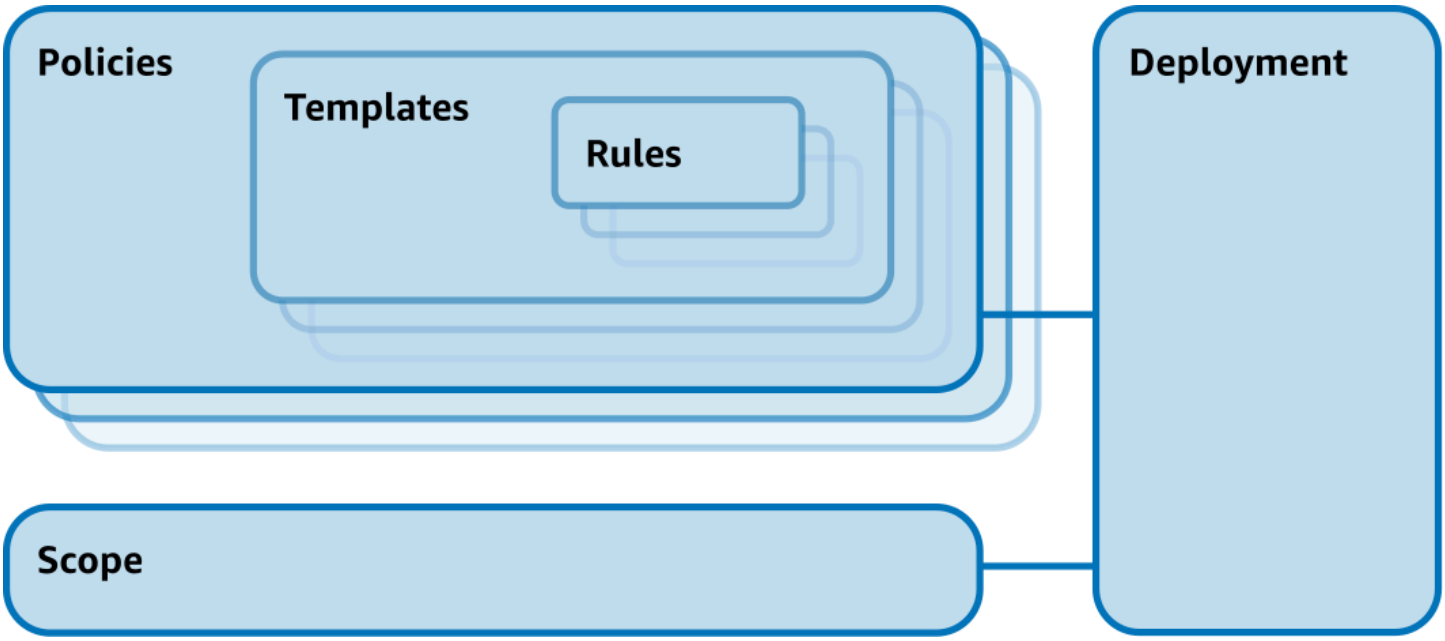
1. Cómo funciona AWS Network Security Manager— Obtenga información sobre el modelo de recursos, los estados del ciclo de vida, la fusión de políticas y la sincronización.
2. Configuración de AWS Network Security Manager— Complete los requisitos previos para usar AWS Network Security Manager.
3. Tutorial: Implemente su primera protección de seguridad de red— Siga un tutorial completo que le permitirá crear su primera implementación.

Cómo AWS Network Security Manager funciona

Utilice el modelo de recursos de AWS Network Security Manager para diseñar y administrar las protecciones de seguridad de la red para los recursos de una sola cuenta o de varias cuentas de su organización. En este capítulo se explican los cinco tipos de recursos, cómo forman una jerarquía y los conceptos clave que rigen su comportamiento.

AWS Modelo de recursos de Network Security Manager

AWS Network Security Manager utiliza cinco tipos de recursos organizados en una jerarquía de composición:



Los recursos hacen referencia entre sí hacia arriba en la jerarquía. Las reglas se utilizan en las plantillas y políticas. Las plantillas, las reglas o ambas se utilizan en las políticas. Un ámbito hace referencia a los recursos que las políticas protegen dentro de una implementación.

En las siguientes secciones se describe cada tipo de recurso de la jerarquía.

Regla: la unidad atómica de la configuración de seguridad de la red. Existen dos tipos de reglas: reglas de inspección de tráfico y reglas de configuración de firewall. La inspección de tráfico se centra en la forma en que el servicio de seguridad aborda el tráfico. Una regla de configuración especifica las operaciones del sistema fuera de la inspección de tráfico. La estructura de una regla varía según el tipo de firewall.

Plantilla: grupo de reglas ordenadas y reutilizables para un único tipo de firewall. Utilice plantillas para empaquetar las reglas relacionadas y compartirlas en varias políticas. Las plantillas son opcionales.

Política: combina un conjunto ordenado de plantillas y reglas con la configuración de aplicación de un tipo de firewall. Cada política tiene una prioridad (un número más bajo indica una prioridad más alta). Cuando varias políticas protegen el mismo recurso, la prioridad determina cómo se resuelven los conflictos. En el caso de las reglas de inspección de tráfico, la prioridad determina el orden en que se agregan las reglas. En el caso de las reglas de configuración del firewall, la prioridad determina qué configuración se aplica a cada recurso y sus políticas incluidas en el ámbito de aplicación.

Alcance: una selección declarativa de los lugares en los que se aplican las protecciones. Un ámbito especifica los tipos de recursos que se deben proteger y, si lo desea, puede filtrar los recursos por etiqueta o atributo de configuración. En el modo multicuenta, un ámbito también especifica qué cuentas u OU se deben incluir o excluir. En el modo de cuenta única, el alcance se aplica a la propia cuenta. El modo de un osciloscopio es fijo al crearlo. No puedes cambiar un ámbito entre el modo multicuenta y el modo de cuenta única en ninguna dirección, por lo que un ámbito multicuenta nunca puede convertirse en uno de cuenta única, ni al revés.

Implementación: vincula una o más políticas a un ámbito. La publicación de una implementación activa su aplicación. AWS Network Security Manager descubre los recursos del ámbito, calcula la configuración prevista y, de forma opcional, corrige los recursos no sincronizados.

Para conocer los límites de composición de los recursos, consulte. Cuotas

AWS Ciclo de vida de los recursos, fusión y sincronización de Network Security Manager

En las siguientes secciones se explican los comportamientos y los mecanismos que rigen el funcionamiento de los recursos de AWS Network Security Manager una vez creados.

Borrador y ciclo de vida activo

Todos los recursos de AWS Network Security Manager, incluidas las reglas, las plantillas, las políticas, los ámbitos y las implementaciones, tienen el estado Borrador o Activo:

- Activo: el estado predeterminado. El recurso está publicado y disponible para su uso. Otros recursos pueden hacer referencia a él, y las implementaciones que lo incluyen imponen su configuración.

- Borrador: el recurso está guardado pero aún no está activo. Los borradores de recursos no se aplican y otros recursos no pueden hacer referencia a ellos. Al crear o actualizar un recurso, seleccione Guardar borrador para mantenerlo en estado de borrador.

De forma predeterminada, AWS Network Security Manager crea los recursos como activos. Para crear un recurso como borrador mediante la API, defina el `isPublished` parámetro `false` en la operación de creación o actualización.

Al actualizar un recurso, se aplican los siguientes escenarios:

Estado actual	Action	Resultado
Borrador	Seleccione Guardar borrador	Actualice el borrador (sigue siendo borrador)
Borrador	Elija Publicar	Publica el borrador (pasa a estar activo)
Activo	Elija Publicar	Actualizar y permanecer activo (activo)
Activo	Elija Guardar borrador	Crea un borrador superpuesto (se convierte en borrador con un recurso activo debajo)

El `hasPublishedVersion` campo aparece en la lista y obtiene las respuestas. Este campo indica si existe un recurso activo publicado debajo de un borrador. Cuando un recurso tiene el estado Borrador y `hasPublishedVersion: true` un borrador pendiente se coloca encima de un recurso activo publicado y activo.

No puede eliminar un recurso activo al que haga referencia otro recurso activo.

Control de versiones

Se pueden versionar todos los recursos de AWS Network Security Manager, incluidas las reglas, las plantillas, las políticas, los ámbitos y las implementaciones. Para crear una versión de un recurso activo, seleccione el recurso, elija Acción y, a continuación, elija Crear instantánea versionada. Las versiones no se crean automáticamente en cada actualización.

> **AWS Alternativa CLI**
>
> También puede crear una versión mediante la operación de `Create{Resource}Snapshot` API en un recurso activo.

Propiedades clave de la versión:

- Cada versión tiene un número único (un entero secuencial) y un ARN compatible con la versión (por ejemplo,). `arn:aws:network-security-manager:us-east-1:123456789012:rule:abc123:3`
- Las versiones son inmutables. No se pueden actualizar.
- Puede crear hasta 10 versiones por recurso.
- Las versiones se pueden etiquetar.

Utilice las versiones para conservar las variantes de configuración deseadas. Para revertir un recurso, lea una versión y, a continuación, actualice el recurso activo con la configuración deseada de la versión.

Priority-based fusión de políticas

Cuando varias políticas protegen el mismo recurso, AWS Network Security Manager combina sus configuraciones en un único resultado. Un número de prioridad más bajo indica una prioridad más alta (la prioridad 1 tiene prioridad sobre la prioridad 2). Cuando AWS Network Security Manager combina políticas que contienen reglas de inspección de tráfico, la prioridad determina el orden en que se agregan las reglas. En el caso de las reglas de configuración del firewall, la política de mayor prioridad determina qué configuración se aplica.

AWS Network Security Manager evalúa la prioridad en dos niveles, en este orden:

1. Prioridad del administrador: AWS Network Security Manager evalúa primero la prioridad del administrador. A cada administrador de la organización se le asigna una prioridad, tal y como se describe enthe section called “Cuentas de administrador y de miembro”. Cuando AWS Network Security Manager combina políticas, clasifica una política de administrador por encima de la política de cuenta única de un miembro. Si una política de administrador y la política de cuenta única de un miembro se aplican a un recurso y entran en conflicto, prevalece la configuración

de la política de administrador. Una cuenta de miembro no puede excluirse de una política de administrador, anularla ni eximirse de ella.

2. Prioridad de política: dentro de cada cuenta, AWS Network Security Manager utiliza la prioridad de política para resolver los conflictos pendientes. Los valores de prioridad de la política son números enteros a partir de 1 y deben ser únicos por cuenta.

La prioridad del administrador se establece con el `priority` campo obligatorio de la `PutAdminAccount` operación, un número entero comprendido entre 1 y 10. Los valores de prioridad son únicos, por lo que dos administradores nunca comparten una prioridad y no es necesario establecer un empate. Para obtener más información, consulte la referencia de la API de AWS Network Security Manager.

El resultado combinado de todas las políticas aplicables a un recurso es la configuración efectiva del firewall. AWS Network Security Manager calcula esta configuración, la compara con la configuración real del recurso e informa de cualquier diferencia en el estado de sincronización.

Cuando las políticas entran en conflicto, AWS Network Security Manager compara cada atributo y aplica el valor de la política de mayor prioridad. Si la política de mayor prioridad no define un atributo, se aplica el valor de la política de menor prioridad. Un recurso que coincide con la configuración efectiva es IN_SYNC. Un recurso protegido por una política de menor prioridad cuya configuración fue anulada por una política de mayor prioridad se presenta como OUT_OF_SYNC para la implementación de menor prioridad. Se trata de un comportamiento esperado, no de un error.

Descubrimiento de recursos con AWS Config

AWS Network Security Manager descubre los recursos protegidos en sus cuentas mediante un grabador de configuración AWS Config vinculado a un servicio. Esta grabadora se crea automáticamente en cada cuenta cuando esa cuenta entra en el ámbito de una implementación. A diferencia del AWS Firewall Manager, no es necesario realizar ninguna configuración adicional. AWS El uso de Config por parte de AWS Network Security Manager no se cobra al cliente de AWS Network Security Manager.

Características principales de la grabadora vinculada a un servicio:

- Su nombre es `AWSConfigurationRecorderForNetworkSecurityManager`.
- Es independiente de cualquier grabador de configuración gestionado por el cliente de la cuenta.
- Registra solo los tipos de recursos relevantes para sus ámbitos e implementaciones activos.

- No es necesario configurar AWS Config ni crear una grabadora de configuración. AWS Network Security Manager lo gestiona automáticamente. AWS El uso de Config por parte de AWS Network Security Manager no se cobra al cliente.
- No puede modificar ni eliminar la grabadora mientras está en uso. AWS Network Security Manager gestiona su ciclo de vida automáticamente.

No necesita habilitar ni configurar AWS Config manualmente para que AWS Network Security Manager funcione. El servicio gestiona la detección de recursos automáticamente después de publicar una implementación.

Sincronización y corrección

La aplicación en AWS Network Security Manager es asincrónica y, en última instancia, coherente. Después de publicar una implementación, o cuando un recurso cambia, se producen las siguientes etapas:

1. Descubrimiento de recursos: AWS Network Security Manager descubre los recursos dentro del alcance mediante una grabadora AWS Config vinculada a un servicio.
2. Cálculo de configuración: para cada recurso descubierto, AWS Network Security Manager calcula la configuración efectiva del firewall combinando todas las políticas aplicables por prioridad.
3. Evaluación de la sincronización: AWS Network Security Manager compara la configuración efectiva con la configuración real del recurso y registra el estado de la sincronización.
4. Solución (opcional): si establece **`remediationEnabled`** la política, AWS Network Security Manager corrige los recursos no sincronizados para que coincidan con la configuración efectiva.

Cada etapa es asíncrona. Consecuencias para su flujo de trabajo:

- Hay un retraso entre la publicación de una implementación y la protección de los recursos.
- Hay un retraso entre la creación de un nuevo recurso en el ámbito de aplicación y su protección.
- La `Last Checked` marca de tiempo de las entradas del estado de sincronización indica cuándo fue la última vez que AWS Network Security Manager evaluó un recurso.

La corrección y la limpieza de recursos son configuraciones a nivel de políticas. Cada una de ellas se configura por política del objeto. `policyConfiguration`

`remediationEnabled`

Especifica si AWS Network Security Manager corrige automáticamente los recursos no conformes. Al habilitar esta configuración, AWS Network Security Manager corrige los recursos no sincronizados para que coincidan con la configuración efectiva.

`resourcesCleanUp`

Especifica si AWS Network Security Manager eliminará automáticamente los recursos que creó cuando ya no sean necesarios. AWS Network Security Manager elimina un firewall que creó al eliminar la implementación o cuando la cuenta o el recurso quedan fuera del alcance.

Los `resourcesCleanUp` valores `remediationEnabled` y son los valores predeterminados. `false` AWS Network Security Manager no corrige ni limpia los recursos hasta que habilite esta configuración. El `policyConfiguration` objeto también es válido`wafConfig`, lo que se aplica a las políticas de AWS WAF. Para obtener más información, consulte la referencia de la API de AWS Network Security Manager.

Cuando un recurso no está sincronizado, el estado de sincronización incluye los motivos de desincronización con detalles por configuración que muestran los valores esperados en comparación con los valores reales. Los motivos se organizan en las siguientes categorías:

- `missingFirewall`— No hay ninguna protección de firewall asociada al recurso.
- `invalidFirewall`— Existe un firewall, pero su configuración es diferente de la configuración efectiva. Esto incluye seis grupos de detalles: `incorrectSingleValueConfigurationsmissingAppendableConfigurationValues`,`unexpect` `incorrectAppendableConfigurationOrdermissingMergeableConfigurationValues`, `yunexpectedMergeableConfigurationValues`.

Si la corrección está habilitada pero AWS Network Security Manager no puede reparar un recurso, el `remediationIssues` campo proporciona una `issueType` `message` descripción del problema y una `correctiveAction` sugerencia de cómo resolverlo.

AWS Network Security Manager no evalúa la configuración que no administra. Si un campo no aparece en ninguna regla contributiva, AWS Network Security Manager lo ignora durante la evaluación de la sincronización.

Cuentas de administrador y de miembro

AWS Network Security Manager utiliza un modelo de administración multicuenta basado en AWS Organizations:

- Cuenta de administrador: la cuenta en la que se crean y administran los recursos de AWS Network Security Manager (reglas, plantillas, políticas, ámbitos e implementaciones). Usted designa una o más cuentas de administrador, cada una con una prioridad de 1 a 10.
- Cuentas de miembro: las cuentas en las que AWS Network Security Manager descubre los recursos, evalúa el estado de la sincronización y, de forma opcional, corrige las configuraciones no sincronizadas. AWS Network Security Manager actúa en las cuentas de los miembros mediante una función vinculada al servicio. Para obtener más información, consulte the section called "Service-linked rol".

Si lo desea, puede asignar a cada administrador un subconjunto de cuentas, unidades organizativas y tipos de firewall. Utilice esta capacidad para delegar la administración de áreas específicas a diferentes equipos.

AWS Network Security Manager es un servicio regional. Los recursos y las implementaciones se crean por región sin dependencias entre regiones.

Service-linked rol

AWS Network Security Manager utiliza un rol vinculado al servicio de IAM denominado `AWSServiceRoleForNetworkSecurityManager` para actuar en las cuentas de los miembros de su organización en su nombre. Este rol confía en el director del servicio`network-security-manager.amazonaws.com`. Utiliza la política `NetworkSecurityManagerServiceRolePolicy` AWS gestionada.

AWS Network Security Manager crea esta función automáticamente al habilitar el servicio, por lo que no se realiza una configuración manual. Esta función permite a AWS Network Security Manager gestionar las protecciones AWS WAF y AWS Shield Advanced, descubrir los recursos protegidos mediante AWS Config y realizar operaciones entre cuentas. Para obtener más información, consulte the section called "Service-linked funciones".

Configuración AWS Gerente de seguridad de red

Con AWS Network Security Manager, puede trabajar en dos modelos organizativos. Úselo directamente en una sola cuenta o úselo con AWS Organizations para administrar las protecciones en varias cuentas. Los pasos de configuración dependen del modelo que elija.

Temas

- Elige tu modelo organizativo
- Configuración para el uso de una sola cuenta
- Se configura para el uso de varias cuentas con AWS Organizations
- Crear un AWS Cuenta de administrador de Network Security Manager
- Cree una identidad de IAM con AWS Permisos de Network Security Manager
- Utilización AWS Administrador de seguridad de red en las regiones que están deshabilitadas de forma predeterminada

Elige tu modelo organizativo

Elige entre los siguientes modelos organizativos:

- Single-account— Utilice AWS Network Security Manager para proteger los recursos de una cuenta. No necesita AWS Organizations ni una cuenta de administrador. Cree una identidad de IAM con los permisos de AWS Network Security Manager y comience a utilizar el servicio directamente. AWS Network Security Manager crea automáticamente un rol vinculado al servicio en su cuenta.
- Multi-account— Utilice AWS Network Security Manager with AWS Organizations para proteger los recursos de varias cuentas. Este modo requiere configurar AWS Organizations, habilitar el acceso confiable y crear una cuenta de administrador.

Configuración para el uso de una sola cuenta

Para usar AWS Network Security Manager en una sola cuenta, cree una identidad de IAM con los permisos adecuados y comience a usar el servicio directamente. No necesita crear una cuenta de administrador. AWS Network Security Manager crea automáticamente un rol vinculado a un servicio

en su cuenta en segundo plano. Vaya a the section called “Cree una identidad de IAM con AWS Permisos de Network Security Manager”.

Se configura para el uso de varias cuentas con AWS Organizations

Para administrar las protecciones en varias cuentas, establezca la membresía y la configuración de AWS Organizations requeridas.

1. Elija una cuenta para usarla como administrador de AWS Network Security Manager para la organización: esta es la cuenta desde la que se crean y administran los recursos de AWS Network Security Manager.
2. Compruebe la pertenencia a la organización: si la cuenta que ha elegido aún no es miembro de la organización, haga que se una. Sigue las instrucciones que aparecen en Cómo invitar a una AWS cuenta a unirse a tu organización en la AWS Guía del usuario de Organizations.
3. Habilite todas las funciones de su organización: AWS Organizations tiene dos conjuntos de funciones disponibles: funciones de facturación consolidada y todas las funciones. Para utilizar AWS Network Security Manager, su organización debe tener habilitadas todas las funciones. Si su organización está configurada solo para la facturación unificada, siga las instrucciones de Habilitar todas las funciones de su organización en la Guía del AWS usuario de Organizations.
4. Habilite el acceso confiable para AWS Network Security Manager: habilite el acceso confiable para AWS Network Security Manager en AWS Organizations. Con el acceso de confianza activado, AWS Network Security Manager puede crear un rol vinculado al servicio en las cuentas de los miembros y administrar los recursos en su nombre.
5. Registrar una cuenta de administrador delegado: registre la cuenta que elija como administrador delegado de AWS Network Security Manager in Organizations AWS . Use la cuenta de administración de Organizations para completar este paso.

> **Multi-account las protecciones están deshabilitadas al desactivar el acceso confiable**
>
> Si desactiva el acceso de confianza de AWS Network Security Manager en AWS Organizations o anula el registro de una cuenta de administrador delegado, AWS Network Security Manager establece el alcance y la implementación de múltiples cuentas en un `DISABLED` estado y limpia las protecciones que administra.

Crear un AWS Cuenta de administrador de Network Security Manager

Este paso se aplica únicamente al modo multicuenta. Solo la cuenta de administración de la organización puede crear cuentas de administrador de AWS Network Security Manager.

Tras completar la configuración de Organizations, registre su cuenta como administrador AWS de Network Security Manager. Puede hacerlo desde la consola o la interfaz de línea de AWS comandos (AWS CLI).

Al crear una cuenta de administrador, AWS Network Security Manager crea automáticamente un rol vinculado al servicio en todas las cuentas de la organización. Con esta función, AWS Network Security Manager descubre los recursos y administra las protecciones de las cuentas de los miembros.

Con AWS Network Security Manager, puede tener varios administradores que administren los recursos de firewall de su organización. Si desea utilizar varios administradores en su organización, puede aplicar condiciones de ámbito administrativo a cada administrador para definir los recursos que pueden administrar. Esto le da la flexibilidad de tener diferentes funciones de administrador en su organización y le ayuda a mantener el principio del acceso con menos privilegios. Por ejemplo, un administrador puede administrar un conjunto de unidades organizativas (OU). Otro administrador solo puede administrar tipos de políticas específicos.

Para ver el número máximo de administradores que puede tener por organización, consulte Cuotas.

> **Registro regional**
>
> Registra una cuenta de administrador de AWS Network Security Manager en una sola AWS región. Para usar AWS Network Security Manager en otras regiones, repita este paso en cada región.

Para crear una cuenta de administrador mediante la consola

1. Abra la consola de AWS Network Security Manager en https://console.aws.amazon.com/network-security-manager/.
2. En el panel de navegación, seleccione Configuración.

3. Seleccione Agregar administrador.
4. Seleccione la cuenta e introduzca un valor de prioridad (del 1 al 10).
5. Seleccione Añadir administrador para confirmar.

Para crear una cuenta de administrador mediante el AWS CLI

Llame a la operación `PutAdminAccount`. Debe proporcionar un valor de prioridad (del 1 al 10).

El siguiente ejemplo de AWS CLI registra una cuenta como administrador de AWS Network Security Manager con prioridad 1:

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

Puede designar varias cuentas de administrador, cada una con una prioridad diferente. Si lo desea, puede limitar a cada administrador a cuentas, unidades organizativas o tipos de firewall específicos proporcionando un `adminScope` parámetro.

Para eliminar una cuenta de administrador mediante la consola

> **Multi-account las protecciones están deshabilitadas al eliminar a un administrador**
>
> Al eliminar una cuenta de administrador, AWS Network Security Manager establece el alcance y el despliegue de las cuentas múltiples en un `DISABLED` estado y limpia las protecciones que administra.

1. Abra la consola AWS de Network Security Manager en. https://console.aws.amazon.com/network-security-manager/
2. En el panel de navegación, seleccione Configuración.
3. Seleccione la cuenta de administrador que desee eliminar.
4. Seleccione Remove administrator (Eliminar administrador).
5. Para confirmar, selecciona Confirmar la eliminación del administrador.

Cree una identidad de IAM con AWS Permisos de Network Security Manager

Para usar AWS Network Security Manager, necesita una identidad de IAM (usuario o rol) con permisos para llamar a las operaciones de AWS Network Security Manager. Las acciones de IAM utilizan el prefijo. `network-security-manager`

El siguiente ejemplo de política de IAM contiene tres declaraciones. La primera declaración otorga acceso total a todas las operaciones AWS de Network Security Manager. La segunda declaración otorga los permisos adicionales de AWS Organizations y AWS WAF que AWS Network Security Manager necesita. AWS Network Security Manager utiliza estos permisos para identificar las cuentas y las unidades organizativas (OU) de su organización y para enumerar los grupos de reglas de WAF y los productos gestionados disponibles. Estos permisos también permiten a AWS Network Security Manager habilitar el acceso confiable y registrar un administrador delegado en AWS Organizations. La tercera declaración otorga el `iam:CreateServiceLinkedRole` permiso que AWS Network Security Manager necesita para crear su función vinculada al servicio, que se requiere tanto para el uso de una sola cuenta como de varias cuentas.

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

Para uso en producción, le recomendamos que conceda únicamente los permisos mínimos necesarios. Para obtener más información, consulte the section called “Identity and Access Management”.

Inscríbase para obtener una Cuenta de AWS

Para empezar AWS, necesitas un Cuenta de AWS. Para obtener información sobre cómo crear un Cuenta de AWS, consulte Cómo empezar con un Cuenta de AWS en la Guía de AWS Account Management referencia.

Utilización AWS Administrador de seguridad de red en las regiones que están deshabilitadas de forma predeterminada

Para usar AWS Network Security Manager en una región que está deshabilitada de forma predeterminada, debe habilitar la región tanto para la cuenta de administración de su organización como para la cuenta de administrador de AWS Network Security Manager. Para obtener información sobre las regiones que están deshabilitadas de forma predeterminada y cómo habilitarlas, consulte Gestión de AWS regiones en la Referencia AWS general.

Habilitación de una región deshabilitada

Tanto para la cuenta de administración de Organizations como para la cuenta de administrador de AWS Network Security Manager, siga las instrucciones de Habilitar una región en la Referencia AWS general.

Implemente su primera protección de seguridad de red

En este tutorial, se explica cómo implementar una ACL web de AWS WAF mediante la consola de AWS Network Security Manager. Debe completar los siguientes pasos:

1. Creación de una regla
2. Crear una plantilla
3. Crear una política.
4. Creación de un ámbito
5. Crear y publicar una implementación
6. Supervise el estado de sincronización

En este tutorial, creará una ACL web de AWS WAF que proteja los balanceadores de carga de aplicaciones en las cuentas seleccionadas. Este proceso es prácticamente idéntico para todos los servicios de seguridad y firewalls compatibles con AWS Network Security Manager.

Tiempo de finalización: aproximadamente 10 minutos

Costo: este tutorial utiliza AWS servicios que pueden implicar cargos. Para conocer los precios actuales, consulte los precios de AWS Network Security Manager en el AWS sitio web.

Requisitos previos

Antes de empezar, compruebe que cumple los siguientes requisitos:

- Se han completado los pasos de configuración tal y como se describe enConfiguración de AWS Network Security Manager.
- Una AWS identidad de Identity and Access Management (IAM) con permisos de AWS Network Security Manager.
- Una organización de AWS Organizations con todas las funciones habilitadas y una cuenta de administrador de AWS Network Security Manager designada (necesaria para las implementaciones de varias cuentas).
- Acceso a la consola de AWS Network Security Manager.

Paso 1: Crear una regla

Una regla es el elemento fundamental de la configuración de seguridad. En este paso, se crean dos reglas de AWS WAF: una que establece la acción predeterminada y otra que establece la configuración de visibilidad. Acción predeterminada y VisibilityConfig son campos obligatorios para una ACL web de AWS WAF.

Para crear la regla de acción predeterminada, siga estos pasos:

1. Abra la consola de AWS Network Security Manager en https://console.aws.amazon.com/network-security-manager/.
2. En el panel de navegación, elija Overview (Información general).
3. En la página de información general, elija Crear regla.
4. En Nombre de regla, introduzca un nombre descriptivo, como `my-default-action-rule`.
5. En la sección Definición de reglas, en Tipo de firewall, elija AWS WAF.
6. En Seleccione el tipo de regla, elija Configuración.
7. Elige Insertar tipos de configuración y, a continuación, selecciona Acción predeterminada. Aparece un editor de JSON con una configuración predeterminada.
8. En el editor JSON, elimina la `Block` sección y conserva solo la `Allow` sección.
9. Seleccione Creación de regla.

Para crear la VisibilityConfig regla, sigue estos pasos:

1. En el panel de navegación, elija Overview (Información general).
2. En la página de descripción general, selecciona Crear regla.
3. En Nombre de regla, introduzca un nombre descriptivo, como `my-visibility-config-rule`.
4. En la sección Definición de reglas, en Tipo de firewall, elija AWS WAF.
5. En Seleccione el tipo de regla, elija Configuración.
6. Elija Insertar tipos de configuración y, a continuación, seleccione VisibilityConfig. Aparece un editor de JSON con una configuración predeterminada.
7. Seleccione Creación de regla.

AWS Alternativa CLI

También puede crear reglas con la AWS CLI:

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

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

Paso 2: Crear una plantilla

Una plantilla agrupa una o más reglas para su reutilización en todas las políticas. En este paso, creará una plantilla que incluya la regla del paso 1:

1. En el panel de navegación, elija Overview (Información general).
2. En la página de descripción general, selecciona Crear plantilla.
3. En Nombre de plantilla, introduzca un nombre descriptivo, como`my-waf-template`.
4. Para el tipo de firewall, elija AWS WAF.
5. En la sección Reglas, elija Agregar regla y seleccione las reglas que creó en el paso 1.
6. Seleccione Crear plantilla.

AWS Alternativa CLI

También puede crear una plantilla con la AWS CLI:

```
aws network-security-manager create-template \
```

```
    --template-name "my-waf-template" \
    --firewall-type WAF \
    --associated-rule-list '[{"ruleIdentifier": "rule-arn-from-step-1"}]' \
    --is-published true
```

Paso 3: Crear una política

Una política combina plantillas con configuraciones de aplicación. En este paso, crea una política que haga referencia a su plantilla y permita la corrección automática:

1. En el panel de navegación, elija Overview (Información general).
2. En la página de descripción general, elija Crear política.
3. En Nombre de la política, introduzca un nombre descriptivo, como `my-waf-policy`.
4. Para el tipo de firewall, selecciona AWS WAF.
5. En la sección Prioridad de la política, se muestran las políticas existentes y sus prioridades. Revise la prioridad de la nueva política. Si necesita ajustarlo, elija el campo de prioridad y cambie el valor por un número de prioridad no utilizado. 1
6. En la sección Plantillas y reglas, elige Añadir plantilla y selecciona la plantilla que creaste en el paso 2.
7. Para la corrección, seleccione Activado.
8. Para la resolución de ACL web para clientes existentes, elija Sin corrección.
9. Elija Crear política.

AWS Alternativa CLI

También puede crear una política con la AWS CLI:

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

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

Paso 4: Crear un ámbito

Un ámbito define dónde se aplican sus protecciones. En este paso, debe crear un ámbito dirigido a los balanceadores de carga de aplicaciones de sus cuentas:

1. En el panel de navegación, elija Overview (Información general).
2. En la página de descripción general, elija Crear ámbito.
3. En Nombre del ámbito, introduzca un nombre descriptivo, como`my-alb-scope`.
4. (Opcional) En la sección de selección de cuentas y unidades organizativas, en Seleccione el método de control del ámbito administrativo, seleccione Alcanzar a toda AWS la organización (todas las unidades organizativas y cuentas). Omita este paso para las implementaciones de una sola cuenta.
5. En la sección Recursos, para Tipos de recursos, seleccione Application Load Balancer.
6. Elija Create scope (Crear alcance).

AWS Alternativa CLI

También puede crear un ámbito con la AWS CLI:

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

Paso 5: Crear y publicar una implementación

Una implementación vincula las políticas a un ámbito y activa su aplicación. Para crear y publicar una implementación:

1. En el panel de navegación, elija Overview (Información general).
2. En la página de información general, elija Crear despliegue.
3. En Nombre de implementación, introduzca un nombre descriptivo, como`my-first-deployment`.
4. En la sección Políticas, elija Agregar política y seleccione la política que creó en el paso 3.
5. En la sección Ámbitos, elija Añadir ámbito y seleccione el ámbito que creó en el paso 4.
6. Elija Crear implementación.

AWS Network Security Manager comienza a descubrir los recursos y a aplicar las protecciones. Este proceso es asíncrono y puede tardar unos minutos en completarse.

> **AWS Alternativa CLI**
>
> También puede crear y publicar una implementación con la AWS CLI:

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

Paso 6: Supervisar el estado de sincronización

Tras publicar una implementación, AWS Network Security Manager descubre los recursos y sincroniza sus configuraciones. Para supervisar el estado de cada recurso:

1. En el panel de navegación, elija Overview (Información general).
2. Elija la pestaña Implementaciones.
3. Elija la implementación que creó en el paso 5.

4. Seleccione la pestaña Sincronización.
5. Revise el estado de sincronización de cada recurso:
   - IN_SYNC: la configuración del recurso coincide con la configuración de protección prevista.
   - OUT_OF_SYNC — La configuración del recurso no coincide. AWS Network Security Manager corrige esta situación automáticamente cuando la corrección está habilitada.
   - NOT_APPLICABLE: el recurso está dentro del alcance, pero esta implementación no lo puede evaluar.

> **AWS Alternativa CLI**
>
> También puede comprobar el estado de la sincronización con la AWS CLI:
>
> ```
> aws network-security-manager list-resource-synchronization-statuses \
>  --deployment-identifier "deployment-arn-from-step-5"
> ```

Paso 7: limpiar

Si ya no necesitas los recursos que creaste, elimínalos en orden inverso para detener la aplicación y eliminar las protecciones de los recursos incluidos en el ámbito de aplicación:

El orden inverso es importante porque estos recursos se refieren entre sí. Para ver qué está asociado a un recurso antes de eliminarlo, llame `ListResourceAssociations` con el ARN de ese recurso. Devuelve el ARN y el tipo de recurso de cada recurso asociado. Para obtener más información, consulte la referencia de la API de AWS Network Security Manager.

1. En el panel de navegación, elija Overview (Información general). Elija la pestaña Implementaciones. Seleccione su implementación, elija Acción y, a continuación, elija Eliminar.
2. Seleccione la pestaña Ámbitos. Selecciona tu ámbito, selecciona Acción y, a continuación, selecciona Eliminar.
3. Elija la pestaña Policies. Seleccione su política, elija Acción y, a continuación, elija Eliminar.
4. Elija la pestaña Plantillas. Selecciona tu plantilla, selecciona Acción y, a continuación, selecciona Eliminar.
5. Elija la pestaña Rules. Selecciona tu regla, selecciona Acción y, a continuación, selecciona Eliminar.

AWS Alternativa CLI

Antes de eliminar un recurso, compruebe sus asociaciones para planificar el orden de eliminación:

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

Si un recurso aún tiene asociaciones, quite o elimine primero los recursos asociados. Puede eliminar los recursos con la AWS CLI en orden inverso:

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

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

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

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

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

Siguientes pasos

Ahora que tiene una implementación en funcionamiento, explore las siguientes formas de ampliar la protección de seguridad de su red:

- Obtenga información sobre el modelo de recursos y el ciclo de vida enCómo funciona AWS Network Security Manager.
- Utilice el draft/publish flujo de trabajo para organizar los cambios antes de que surtan efecto. Para obtener más información, consulte the section called “Borrador y ciclo de vida activo”.
- Cree instantáneas para conservar las configuraciones de funcionalidad comprobada. Para obtener más información, consulte the section called “Control de versiones”.

- Se utiliza `GenerateRuleConfiguration` para crear reglas a partir de descripciones en lenguaje natural. Para obtener más información, consulte la referencia de la API de AWS Network Security Manager.
- Explore la gestión de las protecciones AWS WAF y AWS Shield Advanced en toda su organización. Para obtener más información, consulte Administración de firewalls y servicios de seguridad.

Administración de firewalls y servicios de seguridad

Con AWS Network Security Manager, puede definir e implementar una política de seguridad para varios firewalls y servicios de seguridad. Si bien los elementos comunes abarcan la cartera de seguridad de AWS red, existen variaciones importantes que debe abordar en AWS Network Security Manager.

Para cada servicio de seguridad de red compatible, en las siguientes subsecciones se describen los elementos y pasos únicos de un proceso de creación rápida y uno de creación detallada estándar.

Administración de ACL web para AWS WAF

Con AWS Network Security Manager, puede configurar e implementar de forma centralizada las listas de control de acceso web (ACL web) de AWS WAF en todas las cuentas y recursos de su organización. Puede definir las reglas de AWS Network Security Manager para el AWS WAF, agruparlas en plantillas de protección y hacerlas cumplir a escala mediante las políticas e implementaciones de AWS Network Security Manager.

AWS Conceptos de WAF

Los siguientes conceptos son específicos del uso de AWS Network Security Manager con AWS WAF. Para obtener más información sobre el funcionamiento AWS de Network Security Manager, consulteCómo funciona AWS Network Security Manager.

AWS Tipos de reglas WAF

En el AWS caso del WAF, una regla es de dos tipos:

- INSPECCIÓN: contiene una definición de grupo de reglas que utiliza `PreProcessFirewallManagerRuleGroups` (reglas que se ejecutan antes que las reglas definidas por el cliente) o `PostProcessFirewallManagerRuleGroups` (reglas que se ejecutan después).
- CONFIGURACIÓN: contiene un único parámetro de configuración de ACL web. El JSON de configuración debe contener exactamente una clave de nivel superior que coincida con una configuración compatible (por ejemplo `Description` `DefaultAction` `VisibilityConfigLoggingConfiguration`,`CaptchaConfig`,,`ChallengeConfig`,`CustomRespons` `OnSourceDDoSProtectionConfigTokenDomains`, `oMonetizationConfig`).

La mayoría de los ajustes de configuración de la ACL web corresponden a los parámetros del funcionamiento del AWS WAF. `CreateWebACL` Para obtener más información sobre estos ajustes y sus definiciones, consulte CreateWebACL en la referencia de la API de AWS WAF.

La excepción es que `LoggingConfiguration` se configura por separado. Para obtener más información, consulte the section called “Registro”.

AWS Fusión de políticas WAF

En el AWS caso de WAF, cada parámetro de configuración utiliza una de las siguientes estrategias de combinación:

SingleValue

Configuraciones que solo pueden tener un valor. La política de mayor prioridad gana. Los valores de prioridad son únicos, por lo que dos políticas no pueden definir valores diferentes con la misma prioridad. Para obtener más información sobre cómo AWS Network Security Manager resuelve la prioridad, consultethe section called “Priority-based fusión de políticas”. Las siguientes configuraciones utilizan SingleValue: `DefaultActionVisibilityConfig`,`CaptchaConfig`,`ChallengeConfig`, `OnSourceDDoSProtectionConfigLoggingConfiguration`,`MonetizationConfig`, y`Description`.

Añadir (y AppendAndSort)

Las entradas de todas las políticas se anexan a la lista por orden de prioridad. `TokenDomains`y `DataProtectionConfig.DataProtections` utilice Append. `PreProcessFirewallManagerRuleGroups`y `PostProcessFirewallManagerRuleGroups` use AppendAndSort, que agrega grupos de reglas de todas las políticas y los ordena por prioridad. El orden es importante porque el AWS WAF evalúa los grupos de reglas de forma secuencial.

Merge

Las entradas de todas las políticas se combinan en un único conjunto, independientemente de su prioridad. `CustomResponseBodies`y `AssociationConfig.RequestBody` usa Merge.

Las estrategias Adjuntar y Combinar eliminan las entradas duplicadas. AppendAndSort Cuando dos políticas aportan una configuración idéntica, AWS Network Security Manager mantiene la entrada de la política de mayor prioridad. Por lo tanto, la configuración efectiva contiene una copia de esa entrada, no una copia por política contributiva.

Resolución de ACL web existente

Utilice la `existingCustomerWebACLResolution` configuración de una política de AWS WAF para especificar cómo gestiona AWS Network Security Manager los recursos que ya tienen una ACL web gestionada por el cliente:

- `RETROFIT`— Actualice su ACL web existente para alinearla con la configuración efectiva.
- `OVERRIDE_ASSOCIATION`— En su lugar, asocie al recurso una ACL web gestionada por AWS Network Security Manager.
- `NO_REMEDIATION`— No lo corrija si su ACL web existe.

Registro del tráfico en la ACL web

Usted controla el registro de la ACL web con la `LoggingConfiguration` configuración de una política. AWS Network Security Manager aplica esta configuración mediante la `PutLoggingConfiguration` operación AWS WAF. Puede definir un destino de registro por ACL web. Para obtener más información, consulte la referencia PutLoggingConfigurationde la API AWS de WAF.

Cada ACL web incluida en el ámbito que administra la política envía sus registros al destino que especifique la política. Esto le permite centralizar el registro de todas las cuentas de su organización. Úselo para obtener información detallada sobre el tráfico que las ACL web analizan en toda la organización.

Para el registro centralizado en varias cuentas, puede enviar los registros a un bucket de Amazon S3 o a una transmisión de entrega de Amazon Data Firehose. Cada tipo de destino requiere una configuración adicional, que debe completar antes de que AWS Network Security Manager pueda gestionar el registro de AWS WAF en todos sus recursos y cuentas incluidos. El nombre del destino debe empezar por. `aws-waf-logs-`

Amazon Data Firehose

Cree el flujo de entrega con las siguientes características:

- Creado con su cuenta de administrador de AWS Network Security Manager
- Un nombre que comience por`aws-waf-logs-`, por ejemplo `aws-waf-logs-network-security-manager-central`
- Una PUT fuente

- Creado en la región en la que operas o en la región EE.UU. Este (Norte de Virginia) si capturas registros para Amazon CloudFront

Antes de usar el flujo de entrega, pruébelo para confirmar que tiene un rendimiento suficiente para los registros de su organización. Para obtener más información, consulte Creación de una transmisión de entrega de Amazon Data Firehose en la Guía para desarrolladores de Amazon Data Firehose.

Amazon S3

Cree el bucket siguiendo las instrucciones de Amazon S3 de la Guía para desarrolladores AWS de WAF. También debe configurar el depósito con los permisos que permiten a la entrega de registros escribir en él. La siguiente política de bucket concede esos permisos.

```
{
    "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*Sustitúyalos por el sufijo del nombre de su depósito y *policy-id* sustitúyalos por el ID de su política.

> **CloudWatch Logs solo admite el uso de una sola cuenta**
>
> Si usa AWS Network Security Manager en varias cuentas, no puede usar un grupo de CloudWatch registros de Amazon Logs como destino de registro. El grupo de registros debe estar en la misma AWS cuenta y región que la ACL web. Para las implementaciones con varias cuentas, utilice en su lugar un bucket de Amazon S3 o una transmisión de entrega de Amazon Data Firehose.

Creación rápida para AWS WAF

Con Quick Create, puede definir e implementar las protecciones AWS WAF en un único flujo de trabajo guiado. Utilice Quick Create cuando desee configurar una protección completa de las ACL web desde las reglas hasta el despliegue en una sola sesión.

Para definir e implementar una protección AWS WAF con Quick Create, complete los siguientes procedimientos en orden.

Para crear la política y añadir protecciones

1. Abra la consola de AWS Network Security Manager en https://console.aws.amazon.com/network-security-manager/.
2. En el panel de navegación, elija Overview (Información general).
3. En la parte superior derecha de la página de información general, seleccione Creación e implementación rápidas. La página de creación e implementación rápidas aparece con varios paneles.
4. En el panel de detalles de la política, en Nombre, introduzca un nombre de política. (Opcional) En Description (Descripción), introduzca una descripción.
5. En el panel Definir protecciones, elija el tipo de firewall con el que quiere trabajar. Seleccione AWS WAF. Aparece un subpanel de plantillas y reglas, en el que puede añadir reglas o plantillas.

6. Para agregar reglas, elija Agregar o administrar reglas. En la ventana que aparece, en Seleccionar el tipo de regla, elige una de las siguientes opciones:
   - AWS Reglas administradas: la tabla muestra todas las reglas AWS administradas que admite AWS WAF.
   - Reglas: la tabla muestra los grupos de reglas AWS de WAF que usted posee, además de las reglas AWS administradas.

   Seleccione las casillas de verificación de las reglas que desee añadir a su política. A continuación, selecciona Añadir reglas.
7. Para añadir plantillas, selecciona Añadir plantillas. En la ventana Añadir plantillas que aparece, la tabla muestra todas las plantillas disponibles. Seleccione las plantillas que desee, junto con la versión que desee incluir en la política. A continuación, selecciona Añadir plantillas.

Para configurar la política

1. Revise sus selecciones en la tabla de plantillas y reglas. El número entero de la columna Posición determina el orden de evaluación de las reglas y plantillas. Para cambiar el orden de evaluación, elija el valor de la posición en la columna Posición. Utilice las flechas para cambiar el valor. Para aceptar el cambio, selecciona Confirmar. Para revertir el cambio, selecciona Cancelar.
2. En Configuración de políticas, en el panel Definir protecciones, decida las acciones automatizadas que AWS Network Security Manager llevará a cabo en el ámbito objetivo:
   - La corrección aplica la política definida a todos los recursos cuyo estado de seguridad no esté sincronizado con el estado deseado, tal como se describe en AWS Network Security Manager.
   - La limpieza de recursos elimina el firewall que AWS Network Security Manager creó para un recurso cuando se elimina la implementación o cuando la cuenta o el recurso están fuera del alcance.
   - La resolución WebACL de los clientes actuales determina cómo resolver los conflictos entre la política que está definiendo y la que podría estar ya implementada. En el menú, elija una de las siguientes opciones:
     - Ninguna corrección omite la corrección de los recursos que ya tengan una ACL web.
     - La asociación de anulación reemplaza la ACL web existente por la ACL web creada por AWS Network Security Manager.
     - Retrofit adapta sus reglas a cada ACL web existente y mantiene la ACL web asociada al recurso.

3. En el panel de prioridades de la política, defina la prioridad. AWS Network Security Manager evalúa las políticas según su prioridad para resolver conflictos. Las posiciones más bajas (números enteros más bajos) tienen una prioridad más alta. Para editar la prioridad, elija el valor de posición. A continuación, increméntelo con las flechas o introduzca un valor directamente. Para confirmar la selección, elija Confirmar. Para descartar el cambio, selecciona Cancelar.

Para establecer el alcance

1. En el panel Definir el alcance, defina el conjunto de activos a los que se aplican las políticas. En Nombre del ámbito, introduzca un nombre. (Opcional) En Description (Descripción), introduzca una descripción.
2.

   > **Multi-account solo modo**
   >
   > Este paso se aplica únicamente al modo multicuenta. En el modo multicuenta, utiliza el subpanel de selección de cuentas y unidades organizativas para elegir qué cuentas u OU quieres incluir o excluir. En el modo de cuenta única, este subpanel no aparece en la consola, así que omita este paso.

   En el subpanel de selección de cuentas y unidades organizativas, selecciona una de las siguientes opciones:

   - Alcance para toda la AWS organización. No se requiere ninguna definición adicional.
   - Abarca a toda la AWS organización, pero excluye unidades organizativas y cuentas específicas. Aparecen un subpanel de unidades organizativas y un subpanel de cuentas. Para excluir las unidades organizativas, selecciona Añadir unidades organizativas. Seleccione las unidades organizativas en el árbol organizativo y, a continuación, elija Agregar unidades organizativas. Para excluir cuentas individuales, selecciona Añadir cuentas. Selecciona las cuentas en el árbol de la organización y, a continuación, selecciona Agregar cuentas.
   - No se extienda a toda la AWS organización y solo incluya unidades organizativas y cuentas específicas. Utilice el mismo mecanismo para añadir unidades organizativas y añadir cuentas para incluir las unidades organizativas y las cuentas que desee.
3. En el subpanel Recursos, en Tipos de recursos, seleccione todos los tipos de recursos de AWS WAF o algunos tipos específicos. Las opciones son una o varias de las siguientes:
   - Equilibrador de carga de aplicación
   - API REST de Amazon API Gateway

- CloudFront Distribución

> **CloudFront Requisito de región**
>
> Para proteger los recursos CloudFront de distribución, utilice la región EE. UU. Este (Virginia del Norte`us-east-1`) ().

> **Tipos de recursos globales y regionales**
>
> Puede seleccionar el tipo de recurso global (CloudFront Distribución) o los tipos de recursos regionales (Application Load Balancer y API REST de Amazon API Gateway), pero no ambos. Después de seleccionar un tipo de recurso, no podrá cambiar entre los tipos de recursos regionales y de CloudFront distribución al actualizar la configuración.

> **Recursos no gestionados CloudFront**
>
> AWS Network Security Manager no administra CloudFront las distribuciones que utilizan el plan de precios de CloudFront tarifa fija ni CloudFront las distribuciones provisionales. Estos recursos parecen estar desincronizados.

4. Para cada tipo de recurso seleccionado, elija una de las siguientes opciones que se excluyen mutuamente:
   - Cómo incluir todos los recursos
   - Incluya recursos específicos
   - Excluya recursos específicos
5. Si elige Incluir recursos específicos, elija uno de los siguientes tipos de expresión y, a continuación, cree las combinaciones adecuadas de etiquetas o ARN:
   - Criterio único
   - Cumple con todos los criterios (AND)
   - Cumple con cualquier criterio (OR)
   - NO

Todos los tipos de recursos tienen los criterios de inclusión de etiquetas y ARN. Si elige Etiqueta, introduzca una clave y un valor opcional. Puede identificar varias etiquetas. Si el tipo de recurso es Application Load Balancer, aparece un criterio de configuración adicional. En Configuración, elija un esquema, que tenga las opciones Internet-facingo Interno.

Para revisar e implementar la política

1. En el panel de revisión e implementación, en Nombre de implementación, introduzca un nombre. (Opcional) En Description (Descripción), introduzca una descripción. Para determinar si el contenido de la implementación es visible para otras cuentas de la organización, seleccione Habilitar la visibilidad entre cuentas para esta implementación.
2. (Opcional) Para añadir etiquetas a su recurso, elija Añadir nueva etiqueta y, a continuación, introduzca las combinaciones clave y valores opcionales.
3. Para ejecutar lo que ha definido, elija Crear e implementar. Cuando se complete el proceso, aparecerá la página de despliegues, donde podrá ver los detalles de lo que se creó.

> **Las implementaciones pueden conllevar cargos**
>
> Una implementación crea servicios de seguridad de red y los conecta a un recurso protegido. AWS Network Security Manager cobra por los recursos protegidos. Los propios servicios de seguridad protegen el recurso, lo que conlleva cargos adicionales. Antes de realizar la implementación, consulte la página de precios de AWS Network Security Manager y la página de precios de AWS WAF.

Proceso de creación de estándares para AWS WAF

Con el proceso de creación estándar, puede crear cada componente del AWS WAF (reglas, plantillas, políticas, ámbitos e implementaciones) de forma individual para tener un control total. Utilice este enfoque cuando desee crear componentes reutilizables y combínelos según sea necesario.

Una política AWS WAF de AWS Network Security Manager puede contener reglas y plantillas. Al aplicar la política, AWS Network Security Manager crea una ACL web en cada cuenta incluida.

Para crear una regla (consola)

1. Inicie sesión en la consola AWS de administración con su cuenta de administrador de AWS Network Security Manager y, a continuación, abra la consola de AWS Network Security Manager en https://console.aws.amazon.com/network-security-manager/.

   > **Configuración de la cuenta de administrador**
   >
   > Para obtener información sobre la configuración de una cuenta de administrador de AWS Network Security Manager, consulteConfiguración de AWS Network Security Manager.

2. En el panel de navegación, seleccione AWS Network Security Manager y, a continuación, Descripción general.
3. En el panel de información general, elija Crear regla. Introduzca un nombre descriptivo y, a continuación, introduzca una descripción opcional.
4. En el panel de definición de reglas, en Tipo de firewall, elija AWS WAF.
5. En Tipo de regla, elija Inspección o Configuración.

   Si selecciona Inspección, aparecerá un panel del editor de JSON denominado Definir referencia a un grupo de reglas con las siguientes opciones:

   - Insertar plantilla: seleccione una plantilla JSON para la primera regla (previa al proceso) o la última regla (posterior al proceso). Al realizar una selección, AWS Network Security Manager inserta el JSON correspondiente en el editor, junto con iconos de advertencia si es necesario introducir datos para completar la plantilla.
   - Insertar grupo de reglas: presenta una lista de selección basada en tres opciones:
     - Un grupo de reglas de reglas AWS administradas (AMR)
     - Un grupo de reglas personalizado existente
     - Un grupo de reglas de AWS Marketplace

     AWS Network Security Manager presenta los grupos de reglas asociados a su elección y puede seleccionar una sola instancia para incluirla. Tras realizar la selección, elija Seleccionar grupo de reglas. AWS Network Security Manager inserta referencias a la regla de inspección con la sintaxis correcta en el editor JSON.
   - Insertar con IA: abre una ventana superpuesta denominada generador de configuración de IA. Utilice esta herramienta para describir la regla en un lenguaje sencillo y AWS Network Security Manager generará el JSON asociado en el editor. A continuación, puede revisar el código generado y elegir aceptar, modificar o eliminar el resultado.

6. (Opcional) Una vez completada la definición de la regla de JSON, puedes asociar una etiqueta a la regla. Elija Agregar nueva etiqueta y, a continuación, escriba una clave y el valor opcional.
7. Cuando termines de definir, selecciona Guardar borrador para guardar un objeto inactivo o potencialmente incompleto o Crear regla.

> **Los nombres de las ACL web son permanentes**
>
> No puede cambiar el nombre de una ACL web después de crearla. Si actualiza el nombre de la política, AWS Network Security Manager no actualiza el nombre de la ACL web asociada. Para que AWS Network Security Manager cree una ACL web con un nombre diferente, debe crear una política nueva.

Para crear una plantilla (consola)

Una plantilla agrupa las reglas en orden de prioridad para su evaluación dentro de una política. Puede organizar los tipos de reglas en grupos que se ajusten a sus objetivos de seguridad. También puede permitir que diferentes equipos elaboren declaraciones de control de seguridad que se ajusten a sus responsabilidades y habilidades.

1. En la página de descripción general, en el panel de información general, elija Crear plantilla. En la página Crear plantilla, introduzca un nombre de plantilla, introduzca una descripción opcional y elija un tipo de firewall (en este caso, AWS WAF).
2. Al elegir un tipo de firewall, aparece el panel Reglas. Pulse uno de los dos botones Añadir reglas para abrir una lista de las reglas disponibles. Seleccione la casilla de verificación situada a la izquierda del nombre de una regla para añadirla a la plantilla. Para elegir una versión específica de una regla, seleccione el campo Versión de la regla. Si hay varias versiones disponibles, seleccione la versión que desee y, a continuación, elija Confirmar.
3. (Opcional) Crea una etiqueta para la plantilla. Cuando termines, selecciona Guardar borrador o Crear plantilla. Para seguir creando una política, elija Crear plantilla.

Para crear una política de de (consola)

Este es el último paso de la definición de la política y la preparación para su implementación.

1. En la página de información general, en el panel de información general, seleccione Crear política. En la página Crear política, introduzca un nombre y una descripción opcional y, a continuación, elija un tipo de firewall (en este caso, AWS WAF).
2. En el panel Prioridad de la política, defina la prioridad. AWS Network Security Manager evalúa las políticas según su prioridad para resolver conflictos. Las posiciones más bajas (números enteros más bajos) tienen una prioridad más alta. Para editar la prioridad, elija el valor de posición. A continuación, increméntelo con las flechas o introduzca un valor directamente. Para confirmar la selección, elija Confirmar. Para descartar el cambio, selecciona Cancelar.
3. En el panel de configuración de políticas, decida las acciones automatizadas que AWS Network Security Manager llevará a cabo en el ámbito objetivo:
   - La corrección aplica la política definida a todos los recursos cuyo estado de seguridad no esté sincronizado con el estado deseado, tal como se describe en AWS Network Security Manager.
   - La limpieza de recursos elimina el firewall que AWS Network Security Manager creó para un recurso cuando se elimina la implementación o cuando la cuenta o el recurso están fuera del alcance.
   - La resolución WebACL de los clientes actuales determina cómo resolver los conflictos entre la política que está definiendo y la que podría estar ya implementada. En el menú, elija una de las siguientes opciones:
     - Ninguna corrección omite la corrección de los recursos que ya tengan una ACL web.
     - La asociación de anulación reemplaza la ACL web existente por la ACL web creada por AWS Network Security Manager.
     - Retrofit adapta sus reglas a cada ACL web existente y mantiene la ACL web asociada al recurso.
4. Una vez completados estos ajustes de configuración, seleccione las reglas y plantillas que desee agregar a la política. En el panel Plantillas y reglas, elija Agregar reglas o Agregar plantillas para completar la política. Ambos procesos abren una ventana que funciona de la misma manera que el proceso de selección de reglas descrito anteriormente en esta sección.

Para crear un ámbito (consola)

1. Puede iniciar este paso desde la página de información general o desde otras áreas de la herramienta. En el panel de detalles del ámbito, introduzca un nombre del ámbito y una descripción opcional.

2. > **Multi-account solo modo**
   >
   > Este paso se aplica únicamente al modo multicuenta. En el modo multicuenta, utiliza el subpanel de selección de cuentas y unidades organizativas para elegir qué cuentas u OU quieres incluir o excluir. En el modo de cuenta única, este subpanel no aparece en la consola, así que omita este paso.

   En el panel de selección de cuentas y unidades organizativas, elige uno de los tres métodos para controlar el ámbito administrativo:

   - Alcance para toda AWS la organización (todas las unidades organizativas y cuentas): no es necesaria ninguna definición adicional.
   - Se aplica a toda AWS la organización, pero no incluye unidades organizativas y cuentas específicas: aparecen dos subpaneles, uno para las unidades organizativas y otro para las cuentas. Seleccione Añadir unidades organizativas para abrir la ventana Añadir unidades organizativas, seleccione las unidades organizativas que necesite en el árbol organizativo y, a continuación, seleccione Añadir unidades organizativas. Para agregar cuentas individuales, en el subpanel Cuentas, elija Agregar cuentas, seleccione las cuentas del árbol de la organización y, a continuación, elija Agregar cuentas.
   - No se extienda a toda AWS la organización, sino que incluya únicamente unidades organizativas y cuentas específicas: utilice los mismos subpaneles para añadir unidades organizativas o cuentas con el mismo mecanismo descrito en la opción anterior.

3. A continuación, seleccione los recursos en el subpanel Recursos. En el cuadro de selección de tipos de recursos, seleccione todos los tipos de recursos de AWS WAF o algunos específicos. En el caso AWS del WAF, las opciones son una o todas de las siguientes opciones:

   - Equilibrador de carga de aplicación
   - API REST de Amazon API Gateway
   - CloudFront Distribución

   > **CloudFront Requisito de región**
   >
   > Para proteger los recursos de CloudFront distribución, utilice la región EE.UU. Este (Norte de Virginia) (`us-east-1`).

> **Tipos de recursos globales y regionales**
>
> Puede seleccionar el tipo de recurso global (CloudFront Distribución) o los tipos de recursos regionales (Application Load Balancer y API REST de Amazon API Gateway), pero no ambos. Después de seleccionar un tipo de recurso, no podrá cambiar entre los tipos de recursos regionales y de CloudFront distribución al actualizar la configuración.

> **Recursos no administrados CloudFront**
>
> AWS Network Security Manager no administra CloudFront las distribuciones que utilizan el plan de precios CloudFront fijo ni CloudFront las distribuciones provisionales. Estos recursos parecen estar desincronizados.

4. Para cada tipo de recurso seleccionado, elija una de las siguientes opciones que se excluyen mutuamente:
   - Cómo incluir todos los recursos
   - Incluya recursos específicos
   - Excluya recursos específicos
5. Si elige Incluir recursos específicos, seleccione uno de los siguientes tipos de expresión:
   - Criterio único
   - Cumple con todos los criterios (AND)
   - Cumple con cualquier criterio (OR)
   - NO
6. Cada tipo de expresión admite uno o varios criterios de inclusión y ARN, por lo que puede crear combinaciones de etiquetas o ARN. Todos los tipos de recursos admiten los criterios de inclusión de etiquetas y ARN. Si elige Etiqueta, identifique una clave y un valor opcional. Puede identificar varias etiquetas.
7. Para un Application Load Balancer, aparece un criterio de configuración adicional. En Configuración, puede establecer un esquema con las opciones Internet-facingInterno.

Para crear un despliegue (consola)

Una implementación vincula las políticas a un ámbito y activa su aplicación, lo que hace que AWS Network Security Manager aplique las reglas de AWS WAF a los recursos incluidos en el ámbito.

1. En la página de información general, en el panel de información general, seleccione Crear despliegue. También puede iniciar este paso desde otras áreas de la herramienta.
2. Elija la política que desee implementar.
3. Elija el ámbito que defina las cuentas y los recursos en los que AWS Network Security Manager aplica la política.
4. En Nombre de implementación, introduzca un nombre. (Opcional) En Description (Descripción), introduzca una descripción.
5. (Opcional) Para que la implementación sea visible para otras cuentas de su organización, seleccione Habilitar la visibilidad multicuenta para esta implementación.
6. (Opcional) Para añadir etiquetas, selecciona Añadir nueva etiqueta y, a continuación, introduce las combinaciones clave y valores opcionales.
7. Elija Create and deploy (Crear e implementar). Aparece la página de despliegues, donde puede ver los detalles de lo que creó AWS Network Security Manager.

> **Las implementaciones pueden conllevar cargos**
>
> Una implementación crea servicios de seguridad de red y los conecta a un recurso protegido. AWS Network Security Manager cobra por los recursos protegidos. Los propios servicios de seguridad protegen el recurso, lo que conlleva cargos adicionales. Antes de realizar la implementación, consulte la página de precios de AWS Network Security Manager y la página de precios de AWS WAF.

Administración de las protecciones contra DDoS para AWS Shield Avanzado

Con AWS Network Security Manager, puede configurar e implementar de forma centralizada las protecciones AWS Shield Advanced en todas las cuentas y recursos de su organización. Puede definir políticas de protección contra ataques DDoS y aplicarlas a escala mediante las políticas e implementaciones de AWS Network Security Manager.

AWS Network Security Manager se factura por separado

AWS Network Security Manager no forma parte de la oferta AWS Shield Advanced. Para obtener más información sobre los precios, consulte los precios AWS de Network Security Manager y los precios de AWS Shield Advanced.

AWS Suscripción Shield Advanced

Cuando una implementación activa incluye una cuenta en su ámbito, AWS Network Security Manager suscribe esa cuenta a AWS Shield Advanced. AWS Network Security Manager no cancela la suscripción cuando la cuenta abandona el ámbito o cuando se elimina la implementación. Para cancelar una suscripción a AWS Shield Advanced, consulte Suscripción a AWS Shield Advanced en la Guía para desarrolladores de AWS WAF.

Creación rápida para AWS Shield Avanzado

Con Quick Create, puede definir e implementar las protecciones AWS Shield Advanced en un único flujo de trabajo guiado. Utilice Quick Create cuando desee configurar la protección contra DDoS desde las políticas hasta su implementación en una sola sesión.

Para definir e implementar una protección AWS Shield Advanced con Quick Create, complete los siguientes procedimientos en orden.

Para crear la política y configurar las protecciones

Realice los siguientes pasos:

1. Abra la consola de AWS Network Security Manager en https://console.aws.amazon.com/network-security-manager/.
2. En el panel de navegación, elija Overview (Información general).
3. En la página de información general, seleccione Creación e implementación rápidas. La página de creación e implementación rápidas aparece con varios paneles.
4. En el panel de detalles de la política, en Nombre, introduzca un nombre de política. (Opcional) En Description (Descripción), introduzca una descripción.

5. En el panel Definir protecciones, elija el tipo de firewall con el que quiere trabajar. Selecciona AWS Shield Advanced.
6. En Configuración de políticas, en el panel Definir protecciones, decida las acciones automatizadas que AWS Network Security Manager llevará a cabo en el ámbito objetivo:
   - La corrección aplica la política definida a todos los recursos cuyo estado de seguridad no coincida con el estado deseado descrito por AWS Network Security Manager.
   - La limpieza de recursos elimina la protección DDoS que AWS Network Security Manager creó para un recurso cuando se elimina la implementación o cuando la cuenta o el recurso están fuera del alcance.
   - La resolución de DDoS de los clientes actuales determina cómo resolver los conflictos entre la política que está definiendo y la que podría estar ya implementada. En el menú, elija una de las siguientes opciones:
     - Si no hay ninguna solución, se omite la reparación de los recursos que ya cuentan con una protección contra DDoS.
     - La asociación de anulación reemplaza la protección contra DDoS existente por la protección contra DDoS creada por AWS Network Security Manager.
     - Retrofit adapta sus reglas a cada protección DDoS existente y mantiene la protección DDoS asociada al recurso.
7. En el panel de prioridades de la política, defina la prioridad. AWS Network Security Manager evalúa las políticas según su prioridad para resolver conflictos. Las posiciones más bajas (números enteros más bajos) tienen una prioridad más alta.

   Para editar la prioridad, elija el valor de posición. A continuación, increméntelo con las flechas o introduzca un valor directamente. Para confirmar la selección, elija Confirmar. Para descartar el cambio, selecciona Cancelar.

Para establecer el alcance

Realice los siguientes pasos:

1. En el panel Definir el alcance, defina el conjunto de activos a los que se aplican las políticas. En Nombre del ámbito, introduzca un nombre. (Opcional) En Description (Descripción), introduzca una descripción.

2.

> **Multi-account solo modo**
>
> Este paso se aplica únicamente al modo multicuenta. En el modo multicuenta, utiliza el subpanel de selección de cuentas y unidades organizativas para elegir qué cuentas u OU quieres incluir o excluir. En el modo de cuenta única, este subpanel no aparece en la consola, así que omita este paso.

En el subpanel de selección de cuentas y unidades organizativas, selecciona una de las siguientes opciones:

- Alcance para toda la AWS organización. No se requiere ninguna definición adicional.
- Abarca a toda la AWS organización, pero excluye unidades organizativas y cuentas específicas. Aparecen un subpanel de unidades organizativas y un subpanel de cuentas. Para excluir las unidades organizativas, selecciona Añadir unidades organizativas. Seleccione las unidades organizativas en el árbol organizativo y, a continuación, elija Agregar unidades organizativas. Para excluir cuentas individuales, selecciona Añadir cuentas. Selecciona las cuentas en el árbol de la organización y, a continuación, selecciona Agregar cuentas.
- No se extienda a toda la AWS organización y solo incluya unidades organizativas y cuentas específicas. Utilice el mismo mecanismo para añadir unidades organizativas y añadir cuentas para incluir las unidades organizativas y las cuentas que desee.

3. En el subpanel Recursos, en Tipos de recursos, seleccione todos o algunos tipos de recursos de AWS Shield Advanced. Las opciones son una o varias de las siguientes:
   - Equilibrador de carga de aplicación
   - CloudFront Distribución
   - Equilibrador de carga clásico
   - dirección IP elástica
4. Para cada tipo de recurso seleccionado, elija una de las siguientes opciones que se excluyen mutuamente:
   - Cómo incluir todos los recursos
   - Incluya recursos específicos
   - Excluya recursos específicos
5. Si elige Incluir recursos específicos, elija uno de los siguientes tipos de expresión y, a continuación, cree las combinaciones adecuadas de etiquetas o ARN:
   - Criterio único

- Cumple con todos los criterios (AND)
- Cumple con cualquier criterio (OR)
- NO

Todos los tipos de recursos tienen los criterios de inclusión de etiquetas y ARN. Si elige Etiqueta, introduzca una clave y un valor opcional. Puede identificar varias etiquetas.

> **CloudFront Requisito de región**
>
> Para proteger los recursos CloudFront de distribución, utilice la región EE. UU. Este (Virginia del Norte`us-east-1`) ().

Para revisar e implementar la política

Realice los siguientes pasos:

1. En el panel de revisión e implementación, en Nombre de implementación, introduzca un nombre. (Opcional) En Description (Descripción), introduzca una descripción. Para determinar si el contenido de la implementación es visible para otras cuentas de la organización, seleccione Habilitar la visibilidad entre cuentas para esta implementación.
2. (Opcional) Para añadir etiquetas a su recurso, elija Añadir nueva etiqueta y, a continuación, introduzca las combinaciones clave y valores opcionales.
3. Para crear e implementar la política y el alcance, elija Crear e implementar. Cuando se complete el proceso, aparecerá la página de despliegues, donde podrá ver los detalles de lo que creó AWS Network Security Manager.

> **Las implementaciones pueden conllevar cargos**
>
> Una implementación crea servicios de seguridad de red y los conecta a un recurso protegido. AWS Network Security Manager cobra por los recursos protegidos. Los propios servicios de seguridad protegen el recurso, lo que conlleva cargos adicionales. Antes de realizar la implementación, consulte la página de precios de AWS Network Security Manager y la página de precios de AWS Shield Advanced.

Proceso de creación de estándares para AWS Shield Avanzado

Con el proceso de creación estándar, configuras cada componente de AWS Shield Advanced (políticas, ámbitos e implementaciones) de forma individual para tener un control total. Utilice este enfoque cuando desee crear componentes reutilizables y combínelos según sea necesario.

Una política de AWS Shield Advanced es sencilla y no contiene reglas, grupos de reglas ni plantillas. Al aplicar la política, AWS Network Security Manager crea una protección AWS Shield Advanced DDoS en cada cuenta incluida. Para obtener información sobre el funcionamiento AWS de Network Security Manager, consulte. Cómo funciona AWS Network Security Manager

Para crear una política de de (consola)

Realice los siguientes pasos:

1. Inicie sesión en la consola AWS de administración con su cuenta de administrador de AWS Network Security Manager y, a continuación, abra la consola de AWS Network Security Manager en https://console.aws.amazon.com/network-security-manager/.

   > **Configuración de la cuenta de administrador**
   >
   > Para obtener información sobre la configuración de una cuenta de administrador de AWS Network Security Manager, consulteConfiguración de AWS Network Security Manager.

2. En el panel de navegación, seleccione AWS Network Security Manager y, a continuación, Descripción general.
3. En el panel de información general, elija Crear política. Introduzca un nombre y una descripción opcional y, a continuación, elija un tipo de firewall (en este caso, AWS Shield Advanced).
4. En el panel de prioridades de la política, defina la prioridad. AWS Network Security Manager evalúa las políticas según su prioridad para resolver conflictos. Las posiciones más bajas (números enteros más bajos) tienen una prioridad más alta.

   Para editar la prioridad, elija el valor de posición. A continuación, increméntelo con las flechas o introduzca un valor directamente. Para confirmar la selección, elija Confirmar. Para descartar el cambio, selecciona Cancelar.
5. En el panel de configuración de políticas, decida las acciones automatizadas que AWS Network Security Manager llevará a cabo en el ámbito objetivo:

- La corrección aplica la política definida a todos los recursos cuyo estado de seguridad no coincida con el estado deseado descrito por AWS Network Security Manager.
- La limpieza de recursos elimina la protección DDoS que AWS Network Security Manager creó para un recurso cuando se elimina la implementación o cuando la cuenta o el recurso están fuera del alcance.
- La resolución de DDoS de los clientes actuales determina cómo resolver los conflictos entre la política que está definiendo y la que podría estar ya implementada. En el menú, elija una de las siguientes opciones:
  - Si no hay ninguna solución, se omite la reparación de los recursos que ya cuentan con una protección contra DDoS.
  - La asociación de anulación reemplaza la protección contra DDoS existente por la protección contra DDoS creada por AWS Network Security Manager.
  - Retrofit adapta sus reglas a cada protección DDoS existente y mantiene la protección DDoS asociada al recurso.

Para crear un ámbito (consola)

Realice los siguientes pasos:

1. En el panel de detalles del ámbito, introduzca un nombre del ámbito y una descripción opcional.
2.

   > **Multi-account solo modo**
   >
   > Este paso se aplica únicamente al modo multicuenta. En el modo multicuenta, utiliza el subpanel de selección de cuentas y unidades organizativas para elegir qué cuentas u OU quieres incluir o excluir. En el modo de cuenta única, este subpanel no aparece en la consola, así que omita este paso.

   En el panel de selección de cuentas y unidades organizativas, elige uno de los tres métodos para controlar el ámbito administrativo:

   - Alcance para toda AWS la organización (todas las unidades organizativas y cuentas): no es necesaria ninguna definición adicional.
   - Se aplica a toda AWS la organización, pero no incluye unidades organizativas y cuentas específicas: aparecen dos subpaneles, uno para las unidades organizativas y otro para las cuentas. Seleccione Añadir unidades organizativas para abrir la ventana Añadir unidades

organizativas, seleccione las unidades organizativas que necesite y, a continuación, seleccione Añadir unidades organizativas. Para agregar cuentas individuales, en el subpanel Cuentas, elija Agregar cuentas, seleccione las cuentas y, a continuación, elija Agregar cuentas.

- No se extienda a toda AWS la organización, sino que incluya únicamente unidades organizativas y cuentas específicas. Utilice los mismos subpaneles para añadir unidades organizativas o cuentas.

3. A continuación, seleccione los recursos en el subpanel Recursos. En el cuadro de selección de tipos de recursos, selecciona todos los tipos de recursos de AWS Shield Advanced o algunos de ellos específicos. En el caso de AWS Shield Advanced, las opciones son algunas de las siguientes o todas ellas:
   - Equilibrador de carga de aplicación
   - CloudFront Distribución
   - Equilibrador de carga clásico
   - dirección IP elástica
4. Para cada tipo de recurso seleccionado, elija una de las siguientes opciones que se excluyen mutuamente:
   - Cómo incluir todos los recursos
   - Incluya recursos específicos
   - Excluya recursos específicos
5. Si elige Incluir recursos específicos, seleccione uno de los siguientes tipos de expresión:
   - Criterio único
   - Cumple con todos los criterios (AND)
   - Cumple con cualquier criterio (OR)
   - NO
6. Cada tipo de expresión admite uno o varios criterios de inclusión y ARN, por lo que puede crear combinaciones de etiquetas o ARN. Todos los tipos de recursos admiten los criterios de inclusión de etiquetas y ARN. Si elige Etiqueta, identifique una clave y un valor opcional. Puede identificar varias etiquetas.

> **CloudFront Requisito de región**
>
> Para proteger los recursos CloudFront de distribución, utilice la región EE. UU. Este (Virginia del Norte`us-east-1`) ().

Para crear una implementación (consola)

Un despliegue vincula sus políticas a un ámbito y activa su aplicación. AWS A continuación, Network Security Manager aplica las protecciones DDoS de AWS Shield Advanced a los recursos incluidos en el ámbito de aplicación.

Realice los siguientes pasos:

1. En la página de información general, en el panel de información general, seleccione Crear despliegue.
2. Elija la política que desee implementar.
3. Elija el ámbito que defina las cuentas y los recursos en los que AWS Network Security Manager aplica la política.
4. En Nombre de implementación, introduzca un nombre. (Opcional) En Description (Descripción), introduzca una descripción.
5. (Opcional) Para que la implementación sea visible para otras cuentas de su organización, seleccione Habilitar la visibilidad multicuenta para esta implementación.
6. (Opcional) Para añadir etiquetas, selecciona Añadir nueva etiqueta y, a continuación, introduce las combinaciones clave y valores opcionales.
7. Elija Create and deploy (Crear e implementar). Aparece la página de despliegues, donde puede ver los detalles de lo que creó AWS Network Security Manager.

> **Las implementaciones pueden conllevar cargos**
>
> Una implementación crea servicios de seguridad de red y los conecta a un recurso protegido. AWS Network Security Manager cobra por los recursos protegidos. Los propios servicios de seguridad protegen el recurso, lo que conlleva cargos adicionales. Antes de realizar la implementación, consulte la página de precios de AWS Network Security Manager y la página de precios de AWS Shield Advanced.

AWS Administrador de seguridad de red y AWS Firewall Manager

AWS Network Security Manager es el servicio que reemplaza al AWS Firewall Manager. Los dos son servicios totalmente independientes, cada uno con capacidades únicas y un modelo de precios diferente. Si actualmente usa AWS Firewall Manager, no necesita realizar ninguna acción: sus firewalls y políticas actuales siguen funcionando. En este capítulo se describe cómo coexisten los dos servicios, cómo funciona la prioridad cuando se utilizan ambos y cómo funcionará la migración cuando esté disponible.

AWS Network Security Manager y AWS Firewall Manager funcionan uno al lado del otro y de forma independiente. En algún momento, AWS Firewall Manager dejará de venderse y, después, dejará de funcionar.

Coexistencia con AWS Firewall Manager

AWS Network Security Manager no afecta a los firewalls que haya creado con AWS Firewall Manager, a menos que inicie una acción para cambiarlos. Los firewalls y las políticas que creó con AWS Firewall Manager seguirán funcionando a menos que los cancele. Esto es cierto incluso después de retirar el AWS Firewall Manager.

Prioridad durante la corrección

Mientras estén en funcionamiento ambos servicios, puede tomar medidas que afecten a los firewalls que haya creado con AWS Firewall Manager. Al crear políticas de AWS Network Security Manager, las aplica a un ámbito, que es un conjunto de recursos de destino. Si ese ámbito incluye recursos que una política de AWS Firewall Manager ya aborda, AWS Network Security Manager tiene prioridad durante la corrección. En ese caso, la política y el alcance de AWS Network Security Manager anulan la política y el AWS firewall de Firewall Manager existentes. El comportamiento específico depende de las opciones de resolución que seleccione.

Migración planificada desde AWS Firewall Manager

La migración de AWS Firewall Manager a AWS Network Security Manager consolida la administración del firewall en un solo servicio y le permite utilizar sus capacidades. La migración

está planificada, pero aún no está disponible. Cuando la migración esté disponible, podrá mover las políticas de AWS Firewall Manager a AWS Network Security Manager. La migración requerirá nuevas acciones en ambos servicios que aún no están implementadas.

El proceso planificado copiará una política seleccionada del AWS Firewall Manager, la transferirá a AWS Network Security Manager y la traducirá a la nueva estructura de políticas. Este proceso no afecta a la política original ni a los firewalls asociados en AWS Firewall Manager.

Seguridad en AWS Administrador de seguridad de red

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El https://aws.amazon.com/compliance/shared-responsibility-model/ describe estos conceptos como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Third-party los auditores comprueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los programas de AWS cumplimiento, los programas de . Para obtener más información sobre los programas de conformidad que se aplican a AWS Network Security Manager, consulte AWS Servicios incluidos en el ámbito del programa de conformidad AWS .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos vigentes.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida al utilizar AWS Network Security Manager. En los temas siguientes se muestra cómo configurar AWS Network Security Manager para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger los recursos de AWS Network Security Manager.

Temas

- Protección de datos en AWS Administrador de seguridad de red
- Administración de identidad y acceso para AWS Administrador de seguridad de red
- Uso de funciones vinculadas a servicios para AWS Administrador de seguridad de red
- Validación de conformidad para AWS Administrador de seguridad de red
- Resiliencia en AWS Administrador de seguridad de redes
- Seguridad de la infraestructura en AWS Administrador de seguridad de redes
- Prácticas recomendadas de seguridad para AWS Administrador de seguridad de red

Protección de datos en AWS Administrador de seguridad de red

El modelo de se aplica a la protección de datos en AWS Network Security Manager. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre privacidad de datos y los . Para obtener más información sobre la protección de datos en Europa, consulte el Centro del Reglamento General de Protección de Datos (RGPD).

Para fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger la información confidencial almacenada en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con AWS Network Security Manager u otro Servicios de AWS mediante la consola, la API o los SDK. AWS CLI AWS Cualquier dato que

introduzca en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Cifrado en reposo

AWS Network Security Manager cifra todos los datos en reposo mediante las claves del Servicio de administración de AWS claves (AWS KMS). Service-managed Las claves KMS protegen las configuraciones de los recursos, el estado de la implementación y los datos de sincronización. No necesita configurar ni administrar estas claves.

Cifrado en tránsito

AWS Network Security Manager cifra todos los datos en tránsito mediante Transport Layer Security (TLS). Todas las solicitudes de API requieren TLS 1.2 o una versión posterior. Las conexiones a los puntos finales de la API de AWS Network Security Manager utilizan HTTPS exclusivamente.

Administración de claves

AWS Network Security Manager utiliza claves AWS KMS administradas por el servicio para el cifrado en reposo. No puede proporcionar sus propias claves de KMS en este momento.

Administración de identidad y acceso para AWS Administrador de seguridad de red

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de AWS Network Security Manager. La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración del acceso con políticas

- Cómo AWS Network Security Manager funciona con IAM
- Identity-based ejemplos de políticas para AWS Administrador de seguridad de red
- Resolución de problemas AWS Identidad y acceso a Network Security Manager

Público

La forma de usar AWS Identity and Access Management (IAM) varía según la función que desempeñes:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte Resolución de problemas AWS Identidad y acceso a Network Security Manager).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte Cómo AWS Network Security Manager funciona con IAM).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte Identity-based ejemplos de políticas para AWS Administrador de seguridad de red).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte Cómo iniciar sesión en la Cuenta de AWS en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM.

Cuenta de AWS usuario raíz

Al crear una Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz, que tiene acceso completo a todos los Servicios de AWS recursos. Se recomiendaencarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, se recomienda AWS IAM Identity Center. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales en la Guía del usuario de IAM.

Un grupo de IAM especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un Rol de IAM es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol cambiando de un rol de usuario a uno de IAM (consola) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuario federado, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Administración del acceso con políticas

AWS Para controlar el acceso, puede crear políticas y adjuntarlas a AWS identidades o recursos. Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa

estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte Información general de políticas de JSON en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Identity-based políticas

Identity-based las políticas son documentos de política de permisos de JSON que se adjuntan a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Identity-based las políticas pueden ser políticas integradas (integradas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte Selección entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Resource-based políticas

Resource-based las políticas son documentos de políticas de JSON que se adjuntan a un recurso. Los ejemplos incluyen las Políticas de confianza de roles de IAM y las Políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe especificar una entidad principal en una política basada en recursos.

Resource-based las políticas son políticas en línea que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations .
- Políticas de control de recursos (RCP): definen los permisos máximos disponibles para los recursos de las cuentas. Para obtener más información, consulte Políticas de control de recursos (RCP) en la Guía del usuario de AWS Organizations .
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo AWS Network Security Manager funciona con IAM

Antes de usar IAM para administrar el acceso a AWS Network Security Manager, averigüe qué funciones de IAM están disponibles para su uso con AWS Network Security Manager.

Característica de IAM	AWS Soporte de Network Security Manager
Identity-based políticas	Sí
Resource-based políticas	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACL	No

Característica de IAM	AWS Soporte de Network Security Manager
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	Sí
Service-linked roles	Sí

Para obtener una visión general de cómo funcionan AWS Network Security Manager y otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Identity-based políticas para AWS Administrador de seguridad de red

Compatibilidad con las políticas basadas en identidad: sí

Identity-based las políticas son documentos de política de permisos de JSON que puedes adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de la política de JSON de IAM en la Guía del usuario de IAM.

Resource-based políticas dentro AWS Administrador de seguridad de red

Admite políticas basadas en recursos: no

Resource-based las políticas son documentos de políticas de JSON que se adjuntan a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico.

Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política basada en recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

AWS Network Security Manager no admite políticas basadas en recursos.

Acciones políticas para AWS Administrador de seguridad de red

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de AWS Network Security Manager, consulte las acciones definidas por AWS Network Security Manager en la Referencia de autorización de servicios.

Las acciones políticas de AWS Network Security Manager utilizan el siguiente prefijo antes de la acción:

```
network-security-manager
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

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

AWS Network Security Manager define las acciones de IAM en todos sus tipos de recursos. Estas incluyen las operaciones de creación, lectura, actualización y eliminación (CRUD) para reglas, plantillas, políticas, ámbitos e implementaciones, junto con las operaciones de captura de imágenes, etiquetado, administrativas, de estado de sincronización y de asociación de recursos.

Recursos de políticas para AWS Administrador de seguridad de red

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de recursos de AWS Network Security Manager y sus ARN, consulte los recursos definidos por AWS Network Security Manager en la Referencia de autorización de servicios. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Network Security Manager.

AWS Network Security Manager define un tipo de recurso de IAM para cada uno de sus recursos (regla, plantilla, política, ámbito e implementación), además de un tipo de instantánea para cada uno de ellos (por ejemplo,`rule-snapshot`). El formato del ARN es el siguiente:

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

Los ARN en borrador agregan `:DRAFT` y los ARN instantáneos agregan el número de versión (por ejemplo,). `:3`

Los borradores no son tipos de recursos de IAM independientes. En el caso de la autorización, un borrador se considera un elemento secundario de su recurso activo, que es el principal. Un `:DRAFT` ARN calificado autoriza en contra del recurso activo, por lo que el permiso para actuar sobre un borrador proviene del permiso para actuar sobre ese recurso activo.

Las instantáneas se diferencian de los borradores. Cada instantánea tiene su propio tipo de recurso de IAM, por lo que un ARN cualificado por versión autoriza directamente contra ese tipo de recurso de instantánea, no contra el recurso activo principal.

Claves de condición de la política para AWS Administrador de seguridad de red

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de AWS Network Security Manager, consulte las claves de condición de AWS Network Security Manager en la Referencia de autorización de servicios. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por AWS Network Security Manager.

AWS Network Security Manager admite las siguientes claves de condición de etiquetas AWS globales para el control de acceso basado en atributos (ABAC):

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

Tag-based las claves de condición se aplican a los recursos activos y a las instantáneas. Los borradores de recursos no se pueden etiquetar y no admiten `aws:ResourceTag` condiciones.

Las ACL están AWS Administrador de seguridad de red

Compatibilidad con ACL: no

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

AWS Network Security Manager no admite listas de control de acceso (ACL).

ABAC con AWS Administrador de seguridad de redes

Admite ABAC (etiquetas en las políticas): sí

Attribute-based el control de acceso (ABAC) es una estrategia de autorización que define los permisos en función de unos atributos denominados etiquetas. Puede adjuntar etiquetas a las

entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del director coincida con la etiqueta del recurso.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

AWS Network Security Manager admite el control de acceso basado en atributos mediante las tres claves de condición de etiquetas AWS globales. Puede restringir el acceso a los recursos AWS de Network Security Manager en función de las etiquetas adjuntas a esos recursos.

Usar credenciales temporales con AWS Administrador de seguridad de red

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente cuando se utiliza la federación o se cambia de rol. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM y Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Cross-service permisos principales para AWS Administrador de seguridad de red

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos de la persona principal que llama Servicio de AWS, junto con los de solicitud, Servicio de AWS para realizar solicitudes a los servicios descendentes. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Sesiones de acceso directo.

Funciones de servicio para AWS Administrador de seguridad de red

Compatible con roles de servicio: sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Crear un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de AWS Network Security Manager. Edite las funciones de servicio únicamente cuando AWS Network Security Manager proporcione instrucciones para hacerlo.

Service-linked funciones para AWS Administrador de seguridad de red

Compatible con roles vinculados al servicio: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir la función de realizar una acción en su nombre. Service-linked las funciones aparecen en su nombre Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

AWS Network Security Manager utiliza un rol vinculado a un servicio para operar en las cuentas de los miembros de su organización. AWS Network Security Manager crea el rol vinculado al servicio automáticamente cuando se habilita el servicio. El rol otorga permiso a AWS Network Security Manager para administrar los recursos de AWS WAF y AWS Shield Advanced. El rol también otorga acceso a AWS Config para descubrir recursos y permiso para realizar operaciones entre cuentas.

Para obtener más información sobre la creación y administración de funciones vinculadas al servicio de AWS Network Security Manager, consulte. the section called “Service-linked funciones”

Identity-based ejemplos de políticas para AWS Administrador de seguridad de red

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de AWS Network Security Manager. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por AWS Network Security Manager, incluido el formato de los ARN de cada uno de los tipos de recursos, consulte las acciones, los recursos y las claves de condición de AWS Network Security Manager en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de AWS Consola de Network Security Manager
- Cómo permitir a los usuarios consultar sus propios permisos
- Read-only acceso a AWS Administrador de seguridad de red
- Administre únicamente reglas y plantillas

Prácticas recomendadas sobre las políticas

Identity-based las políticas determinan si alguien puede crear, acceder o eliminar los recursos AWS de Network Security Manager de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo

CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de AWS Consola de Network Security Manager

Para acceder a la consola de AWS Network Security Manager, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de AWS Network Security Manager que tiene en su Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para acceder a la consola de AWS Network Security Manager, un director necesita un mínimo de permisos para las `network-security-manager:Get*` acciones `network-security-manager:List*` y acciones.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política

incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

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

Read-only acceso a AWS Administrador de seguridad de red

La siguiente política otorga un acceso principal de solo lectura a todos los recursos de AWS Network Security Manager. Esto resulta útil para los auditores o las funciones de supervisión que necesitan ver las configuraciones y el estado de la sincronización sin realizar cambios.

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

Administre únicamente reglas y plantillas

La siguiente política permite a un director crear, actualizar y eliminar reglas y plantillas sin conceder acceso a las políticas, los ámbitos o las implementaciones. Esto resulta útil para los equipos que crean configuraciones de seguridad pero no controlan su aplicación.

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

Resolución de problemas AWS Identidad y acceso a Network Security Manager

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas más comunes que pueden surgir al trabajar con AWS Network Security Manager e IAM.

Temas

- No estoy autorizado a realizar ninguna acción en AWS Administrador de seguridad de red
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mi Cuenta de AWS para acceder a mi AWS Recursos de Network Security Manager

No estoy autorizado a realizar ninguna acción en AWS Administrador de seguridad de red

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `network-security-manager:`*`GetWidget`*.

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

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `network-security-manager:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un mensaje de error que indica que no está autorizado a realizar la `iam:PassRole` acción, sus políticas deben actualizarse para que pueda transferir una función a AWS Network Security Manager.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir la función al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS Network Security Manager. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir la función al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mi Cuenta de AWS para acceder a mi AWS Recursos de Network Security Manager

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si AWS Network Security Manager admite estas funciones, consulte Cómo AWS Network Security Manager funciona con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.

- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Uso de funciones vinculadas a servicios para AWS Administrador de seguridad de red

AWS Network Security Manager utiliza funciones vinculadas al servicio de IAM. Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Network Security Manager. AWS Service-linked Los roles están predefinidos por AWS Network Security Manager e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración de AWS Network Security Manager, ya que no es necesario añadir manualmente los permisos necesarios. AWS Network Security Manager define los permisos de sus funciones vinculadas al servicio. A menos que se defina lo contrario, solo AWS Network Security Manager puede asumir sus funciones. Los permisos definidos incluyen la política de confianza y la política de permisos. No puede adjuntar esa política de permisos a ninguna otra entidad de IAM.

Puede eliminar un rol vinculado a un servicio solo después de eliminar por primera vez los recursos relacionados. Esto protege los recursos AWS de Network Security Manager porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que admiten funciones vinculadas a servicios, consulte los AWS servicios que funcionan con IAM y busque los servicios que incluyen Sí en la columna de funciones. Service-linked Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Service-linked permisos de rol para AWS Administrador de seguridad de red

AWS Network Security Manager utiliza el rol vinculado al servicio denominado. `AWSServiceRoleForNetworkSecurityManager` Esta función vinculada al servicio confía en que el director del `network-security-manager.amazonaws.com` servicio asuma la función.

La política de permisos de roles denominada `NetworkSecurityManagerServiceRolePolicy` es una política AWS administrada que permite a AWS Network Security Manager realizar acciones en los recursos especificados.

La siguiente política de confianza permite que el director del `network-security-manager.amazonaws.com` servicio asuma la función.

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

> **Note**
>
> Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte los permisos de Service-linked rol en la Guía del usuario de IAM.

Detalles de los permisos

AWS Network Security Manager requiere cada grupo de permisos para proteger y descubrir los recursos de su cuenta y organización. La política `NetworkSecurityManagerServiceRolePolicy` administrada otorga los siguientes permisos, agrupados por servicio:

- `wafv2`— Cree, lea, actualice y elimine las ACL web y los grupos de reglas del Firewall Manager. Asocie y desasocie las ACL web con los recursos protegidos. Administre las configuraciones de registro de las ACL web y las políticas de permisos de los grupos de reglas. Etiquetar y desetiquetar recursos de . AWS Valide las configuraciones de reglas y ACL web de Network Security Manager.
- `shield`— Crear, describir, enumerar y eliminar las protecciones AWS Shield Advanced. Cree y describa la suscripción AWS Shield Advanced.
- `elasticloadbalancing`— Describa los balanceadores de carga de aplicaciones y las etiquetas. Cree, elimine y establezca asociaciones de ACL web en los balanceadores de carga de aplicaciones.
- `cloudfront`— Obtenga y enumere CloudFront las distribuciones, configuraciones y etiquetas de Amazon. Asocie y desasocie las ACL web de distribución. Lea los orígenes de la VPC.
- `apigateway`— Lea las API, etapas y etiquetas de REST de Amazon API Gateway. Configure la ACL web en un escenario de API.
- `ec2`— Lea las ACL web y las asociaciones de las instancias de Amazon EC2 Verified Access. Describa las direcciones IP elásticas para la protección de AWS Shield Advanced.
- `cognito-idp`,, `apprunner` `appsyncamplify`, y `bedrock-agentcore` — Lea las asociaciones de ACL web para los grupos de usuarios, los AWS App Runner servicios, las API de AWS AppSync GraphQL, las aplicaciones y las AgentCore puertas de enlace de Amazon Bedrock de Amazon Cognito para que AWS Network Security Manager pueda descubrir los recursos protegidos. AWS Amplify
- `config`— Seleccione las configuraciones de los recursos y gestione el grabador de AWS Config configuración vinculado al servicio que AWS Network Security Manager utiliza para detectar los recursos específicos.
- `organizations`— Lea su organización, cuentas, raíces, unidades organizativas y administradores delegados para que AWS Network Security Manager pueda funcionar en toda la organización.
- `logs`— Cree, lea, actualice, elimine y enumere las entregas de registros para el registro de ACL web.
- `s3`— Obtenga y coloque políticas de bucket en los buckets de Amazon S3 cuyos nombres comiencen `aws-waf-logs-` por, de modo que se puedan entregar los registros de ACL web.
- `iam`— Cree las funciones vinculadas a servicios que requieren AWS Shield, Advanced y AWS WAF AWS Config, con el alcance de la clave de condición. `iam:AWSServiceName`

El siguiente JSON muestra la política de permisos completa. `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"
        }
      }
    }
  ]
}
```

Creación de un rol vinculado a un servicio de AWS Administrador de seguridad de red

No necesita crear manualmente un rol vinculado a servicios. Al habilitar AWS Network Security Manager, AWS Network Security Manager crea automáticamente la función vinculada al servicio. No es necesario realizar ningún paso manual.

Si elimina este rol vinculado al servicio y, a continuación, necesita volver a crearlo, AWS Network Security Manager volverá a crearlo la función la próxima vez que utilice el servicio. No tiene que realizar ninguna acción.

Para obtener más información, consulte Creating a service-linked role en la Guía del usuario de IAM.

Modificación de un rol vinculado a un servicio de AWS Administrador de seguridad de red

No puede cambiar los permisos de la función `AWSServiceRoleForNetworkSecurityManager` vinculada al servicio. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol mediante IAM.

Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio de AWS Administrador de seguridad de red

Si ya no necesita usar AWS Network Security Manager, le recomendamos que elimine la función `AWSServiceRoleForNetworkSecurityManager` vinculada al servicio.

Antes de eliminar el rol vinculado al servicio, limpie los recursos que administra AWS Network Security Manager. Desactive AWS Network Security Manager y elimine las políticas y los ámbitos para que ningún recurso que AWS Network Security Manager administra permanezca en su cuenta. A continuación, puede eliminar el rol manualmente.

> **Note**
>
> Si AWS Network Security Manager utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. Seleccione Roles en el panel de navegación.
3. En el cuadro de búsqueda, escriba y`AWSServiceRoleForNetworkSecurityManager`, a continuación, seleccione el rol.
4. Elija Eliminar.
5. Para confirmar la eliminación, introduzca el nombre del rol y, a continuación, elija Eliminar.

Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones compatibles para AWS Funciones vinculadas al servicio de Network Security Manager

AWS Network Security Manager admite el uso de funciones vinculadas a servicios en todas las AWS regiones en las que AWS Network Security Manager esté disponible.

Validación de conformidad para AWS Administrador de seguridad de red

Nuestra nueva experiencia AWS de registro no está diseñada para cargas de trabajo reguladas. Si está utilizando nuestra nueva experiencia de AWS registro, pero quiere utilizarla AWS para cargas de trabajo reguladas, puede suscribirse a una experiencia AWS (avanzada) o activar funciones avanzadas para su entorno. AWS

Para saber si un programa de cumplimiento Servicio de AWS se encuentra dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. Para obtener más información sobre su responsabilidad de conformidad al utilizarlos Servicios de AWS, consulte AWS la documentación de seguridad.

Resiliencia en AWS Administrador de seguridad de redes

La infraestructura AWS global se basa en zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor

disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Además de la infraestructura AWS global, AWS Network Security Manager ofrece varias funciones para ayudarlo a satisfacer sus necesidades de respaldo y resiliencia de datos.

Seguridad de la infraestructura en AWS Administrador de seguridad de redes

Como servicio gestionado, AWS Network Security Manager está protegido por los procedimientos de seguridad de red AWS global que se describen en el documento técnico Amazon Web Services: Overview of Security Processes.

Utiliza las llamadas a la API AWS publicadas para acceder a AWS Network Security Manager a través de la red. Los clientes deben ser compatibles con la seguridad de la capa de transporte (TLS) 1.0 o una versión posterior. Recomendamos TLS 1.2 o una versión posterior. Los clientes también deben admitir conjuntos de cifrado con perfecto secreto directo (PFS), como DHE (Ephemeral) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Prácticas recomendadas de seguridad para AWS Administrador de seguridad de red

Las siguientes prácticas recomendadas le ayudan a mantener una configuración segura de AWS Network Security Manager.

Controles preventivos

- Utilice el privilegio mínimo de IAM: conceda únicamente los permisos necesarios para que cada usuario o función desempeñe sus tareas de administrador de seguridad de AWS red. Utilice las

claves de condición de IAM para restringir el acceso a recursos específicos siempre que sea posible.

- Utilice funciones vinculadas al servicio: AWS Network Security Manager utiliza funciones vinculadas al servicio para realizar acciones en su nombre. Estos roles tienen permisos predefinidos que se limitan al acceso mínimo requerido.
- Configure los ámbitos con cuidado: defina las configuraciones de los ámbitos que se dirijan únicamente a las cuentas y los tipos de recursos que requieren protección. Los ámbitos demasiado amplios pueden provocar una aplicación no intencionada.

Controles de detección

- Habilita el AWS CloudTrail registro: CloudTrail registra todas las llamadas a la API de AWS Network Security Manager. Revise estos registros para comprobar quién realizó cambios en sus configuraciones de seguridad y cuándo.
- Supervise el estado de sincronización: compruebe periódicamente el estado de sincronización de sus implementaciones para identificar los recursos que no están sincronizados con la postura de seguridad prevista.

Supervisión AWS Gerente de seguridad de red

La supervisión de AWS Network Security Manager le ayuda a comprender si sus recursos están protegidos según lo previsto. AWS Network Security Manager ofrece las siguientes funciones de supervisión:

- API de estado de sincronización: consulte el estado de protección de los recursos individuales en sus implementaciones.
- AWS CloudTrail-- Registre todas las llamadas a la API de AWS Network Security Manager para realizar auditorías, cumplir y solucionar problemas operativos.

Supervisar el estado de sincronización

La forma principal de supervisar si sus recursos están protegidos es mediante las API de estado de sincronización. AWS Network Security Manager evalúa cada recurso incluido en el ámbito de aplicación y registra si su configuración de firewall real coincide con la configuración prevista.

Estado de sincronización: operaciones

AWS Network Security Manager proporciona dos operaciones para consultar el estado de la sincronización:

ListResourceSynchronizationStatuses

Devuelve el estado de cada recurso para una implementación específica. Requiere un parámetro `deploymentIdentifier`. Opcionalmente, filtre por `synchronizationStatus` (IN_SYNC, OUT_OF_SYNC o NOT_APPLICABLE).

ListAggregateResourceSynchronizationStatuses

Devuelve el estado agregado por recurso en todas las implementaciones. Si lo desea, filtre por. `synchronizationStatus` Esta operación muestra el resultado combinado de todas las políticas que se aplican a cada recurso.

Ambas operaciones admiten la paginación con `maxResults` (1 a 100) y`nextToken`.

Comprensión de los valores del estado de sincronización

IN_SYNC

La configuración del firewall real del recurso coincide con la configuración efectiva calculada a partir de todas las políticas aplicables.

OUT_OF_SYNC

La configuración real del recurso difiere de la configuración efectiva. El `outOfSyncReasons` campo proporciona detalles por configuración que muestran los valores esperados frente a los reales.

NOT_APPLICABLE

La cuenta y el tipo de recurso del recurso están dentro del ámbito, pero el recurso en sí no coincide con los filtros del ámbito (por ejemplo, un filtro de etiquetas lo excluye). No es necesario ninguna acción.

Si un recurso no aparece en absoluto en los resultados, significa que la cuenta o el tipo de recurso no están incluidos en el ámbito de la implementación. Compruebe la configuración de su alcance.

Comprenda las marcas de tiempo de la evaluación

Cada entrada de estado de sincronización incluye dos marcas de tiempo:

- `evaluatedAt`-- La última vez que AWS Network Security Manager evaluó la configuración del recurso. Un `evaluatedAt` valor obsoleto indica que aún no se ha realizado la evaluación de los cambios recientes.
- `updatedAt`-- Cuándo se modificó por última vez el propio registro de estado de sincronización. Si `updatedAt` es anterior `aevaluatedAt`, el estado se ha mantenido estable desde la última evaluación.

Cross-account visibilidad

Cuando varios administradores protegen el mismo recurso, la visibilidad del estado de sincronización agregado depende de la `enableCrossAccountVisibility` configuración de cada implementación.

- Si todas las implementaciones que cubren un recurso tienen habilitada la visibilidad entre cuentas, cualquier administrador podrá ver el estado agregado completo y los motivos de falta de sincronización.
- Si alguna implementación tiene deshabilitada la visibilidad entre cuentas, los demás administradores verán un `NOT_VISIBLE` marcador en lugar de los motivos detallados. Esto indica que otro administrador también protege el recurso pero no ha compartido la visibilidad.

Diagnóstico de recursos no sincronizados

Cuando un recurso muestra OUT_OF_SYNC, el `outOfSyncReasons` campo identifica las diferencias de configuración específicas. El motivo principal es uno de los siguientes:

- `missingFirewall`-- No hay ninguna protección de firewall asociada al recurso.
- `invalidFirewall`-- Existe un firewall, pero su configuración no cumple con las expectativas. Las diferencias específicas se enumeran en los cubos categorizados.

Si la corrección está habilitada pero no se puede corregir el recurso, el `remediationIssues` campo `correctiveAction` proporciona una guía sobre cómo resolver el problema manualmente. La corrección es una configuración a nivel de política que está desactivada de forma predeterminada. Para obtener más información, consulte the section called “Sincronización y corrección”.

Varias implementaciones con diferentes configuraciones pueden dirigirse al mismo recurso. En este caso, el estado de sincronización por despliegue puede ser OUT_OF_SYNC, mientras que el estado de sincronización agregado es IN_SYNC. Se trata de un comportamiento esperado, no de un error. La configuración de una política de mayor prioridad prevaleció durante la fusión. Como resultado, el recurso coincide con la configuración efectiva, aunque no coincida con la configuración de la implementación de menor prioridad.

Registro AWS Llamadas a la API de Network Security Manager con AWS CloudTrail

AWS Network Security Manager está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio. CloudTrail captura todas las llamadas a la API de AWS Network Security Manager como eventos de administración. Las llamadas capturadas incluyen las llamadas desde la consola de AWS Network Security Manager y las llamadas programáticas a las operaciones de la API de AWS Network Security Manager.

Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de AWS Network Security Manager. Si no configura un registro, podrá ver los eventos más recientes de la CloudTrail consola en el historial de eventos. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

AWS La información del administrador de seguridad de red en CloudTrail

CloudTrail está habilitada en su cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en AWS Network Security Manager, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para obtener un registro continuo de sus eventos Cuenta de AWS, incluidos los eventos de AWS Network Security Manager, cree un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. El registro registra los eventos de todas las regiones de la AWS partición. Entrega los archivos de registro al bucket de Amazon S3 que especifique. Puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail

Todas las operaciones de AWS Network Security Manager se registran en. CloudTrail Entre las operaciones públicas se incluyen las siguientes:

- Operaciones de creación, lectura, actualización y eliminación (CRUD) para reglas, plantillas, políticas, ámbitos e implementaciones
- Operaciones instantáneas
- Operaciones de etiquetado
- Operaciones de cuentas de administrador
- Operaciones de estado de sincronización
- Operaciones de asociación de recursos

- Operaciones de generación de reglas

Cada entrada de evento incluye la siguiente información:

- La fuente del evento: `network-security-manager.amazonaws.com`
- El nombre del evento, que es el nombre de la operación de la API (por ejemplo, `CreatePolicy` o`ListDeployments`)
- Los recursos afectados, identificados por el ARN y el tipo de recurso

Read-only las operaciones (como `GetPolicyListRules`, y`ListResourceSynchronizationStatuses`) se registran con `readOnly: true` y no incluyen elementos de respuesta. Las operaciones de mutación incluyen parámetros de solicitud y elementos de respuesta.

> **Note**
>
> CloudTrail redacta los campos confidenciales de los registros de eventos. Por ejemplo, CloudTrail redacta el `prompt` parámetro de la operación. `GenerateRuleConfiguration`

Ejemplo: evento CreatePolicy

El siguiente ejemplo muestra una entrada de CloudTrail registro de la `CreatePolicy` operación.

```
{
  "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 Cuotas de Network Security Manager

Cuenta de AWS Tiene las siguientes cuotas predeterminadas para AWS Network Security Manager. A menos que se indique lo contrario, cada cuota es por cuenta y por región.

Cuotas de recursos

La siguiente tabla muestra la cantidad máxima de recursos de AWS Network Security Manager que puede crear por cuenta en cada región.

Recurso	Cuota predeterminada	Ajustable
Reglas por cuenta	200	No
Plantillas por cuenta	100	No
Políticas por cuenta	100	No
Ámbitos por cuenta	100	No
Implementaciones por cuenta	100	No
Instantáneas por recurso	10	No

Cuotas de composición de recursos

En la siguiente tabla se enumeran las cuotas según las cuales los recursos de AWS Network Security Manager se refieren entre sí dentro de la jerarquía de recursos.

Cuota	Valor
Reglas por plantilla	De 1 a 50
Plantillas según la política de la AWS WAF	De 1 a 2
Reglas y plantillas combinadas según la política de la AWS WAF	De 1 a 100

Cuota	Valor
Plantillas o reglas según la política de AWS Shield Advanced	0 (debe estar vacío)
Políticas por despliegue	De 1 a 2
Ámbitos por despliegue	1 (exactamente uno)

Cuotas de configuración del alcance

En la siguiente tabla se enumeran las cuotas de las expresiones de configuración del ámbito.

Cuota	Valor
Ámbitos de tipo de recurso por ámbito	20
Profundidad de expresión del ámbito (niveles anidados)	2
Amplitud de expresión del ámbito (criterios por nivel)	20

Cuotas de cuentas de administrador

En la siguiente tabla se enumeran las cuotas de los niveles de prioridad de las cuentas de administrador de AWS Network Security Manager.

Cuota	Valor
Niveles de prioridad de administrador	1 a 10

Cuotas de paginación de la API

En la siguiente tabla se enumeran los límites de paginación de las operaciones de List.

Cuota	Valor
Resultados máximos por página () `maxResults`	100
Resultados mínimos por página (`maxResults`)	1

Capacidad de ajuste de la cuota

Las cuotas enumeradas en las secciones anteriores son fijas y no se pueden aumentar en este momento.

Historial de documentos del AWS Guía para desarrolladores de Network Security Manager

En la siguiente tabla se describen las versiones de la documentación de AWS Network Security Manager.

Cambio	Descripción	Fecha
Versión inicial	Versión inicial de la guía para desarrolladores de AWS Network Security Manager.	1 de agosto de 2026

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.