



Guide du développeur

AWS Responsable de la sécurité réseau



AWS Responsable de la sécurité réseau: Guide du développeur

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

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce que AWS Network Security Manager ?	1
Comment ? AWS Network Security Manager fonctionne en un coup d'œil	1
Caractéristiques de AWS Responsable de la sécurité réseau	1
Cas d'utilisation	2
Services connexes	3
Accès AWS Responsable de la sécurité réseau	4
Tarification	4
Est-ce votre première utilisation ?	5
Comment fonctionne AWS Network Security Manager	6
AWS Modèle de ressources Network Security Manager	6
AWS Cycle de vie, fusion et synchronisation des ressources de Network Security Manager	7
Brouillon et cycle de vie actif	7
Gestion des versions	9
Priority-based fusion de politiques	9
Découverte de ressources avec AWS Config	10
Synchronisation et correction	11
Comptes d'administrateur et de membre	13
Service-linked rôle	13
Configuration AWS du gestionnaire de sécurité réseau	15
Choisissez votre modèle d'organisation	15
Configuration pour une utilisation avec un seul compte	15
Configuration pour une utilisation multicompte avec AWS Organizations	16
Création d'un AWS Compte administrateur Network Security Manager	17
Créez une identité IAM avec AWS Autorisations du Network Security Manager	19
Inscrivez-vous pour un Compte AWS	20
Utilisation AWS Gestionnaire de sécurité réseau dans les régions désactivées par défaut	20
Tutoriel : Déployez votre première protection de sécurité réseau	21
Conditions préalables	21
Étape 1 : Création d'une règle	22
Étape 2 : Création d'un modèle	23
Étape 3 : Création d'une politique	24
Étape 4 : Création d'un scope	25
Étape 5 : créer et publier un déploiement	26
Étape 6 : Surveiller l'état de synchronisation	26

Étape 7 : nettoyer	27
Étapes suivantes	28
Gestion des pare-feux et des services de sécurité	30
Gestion des ACL Web pour WAF AWS	30
AWS Concepts du WAF	30
Création rapide pour AWS WAF	34
Processus de création standard pour AWS WAF	38
Gestion des protections DDoS pour AWS Shield Advanced	45
Création rapide pour AWS Shield Advanced	45
Processus de création standard pour AWS Shield Advanced	49
AWS Network Security Manager et Firewall Manager	54
Coexistence avec AWS Firewall Manager	54
Priorité lors de la correction	54
Migration planifiée depuis AWS Firewall Manager	54
Sécurité	56
Protection des données	57
Chiffrement au repos	58
Chiffrement en transit	58
Gestion des clés	58
Gestion des identités et des accès	58
Public ciblé	59
Authentification par des identités	59
Gestion de l'accès à l'aide de politiques	61
Comment ? AWS Network Security Manager fonctionne avec IAM	62
Identity-based exemples de politiques	69
Résolution des problèmes	74
Service-linked rôles	76
Service-linked autorisations de rôle	76
Création d'un rôle lié à un service	87
Modification d'un rôle lié à un service	87
Suppression d'un rôle lié à un service	88
Régions prises en charge	88
Validation de conformité	89
Résilience	89
Sécurité de l'infrastructure	90
Bonnes pratiques de sécurité	90

Contrôles préventifs	90
Contrôles de détection	91
Contrôle AWS Responsable de la sécurité réseau	92
Surveillance de l'état de synchronisation	92
Opérations d'état de synchronisation	92
Comprendre les valeurs d'état de synchronisation	93
Comprendre les horodatages d'évaluation	93
Cross-account visibilité	93
Diagnostic des ressources désynchronisées	94
CloudTrail journaux	94
AWS Informations relatives au Network Security Manager dans CloudTrail	95
Exemple : CreatePolicy événement	96
Quotas	99
Quotas de ressources	99
Quotas de composition des ressources	99
Quotas de configuration du périmètre	100
Quotas de comptes d'administrateur	100
Quotas de pagination des API	100
Ajustement des quotas	101
Historique de la documentation	102
.....	ciii

Qu'est-ce que AWS Responsable de la sécurité réseau ?

Avec AWS Network Security Manager, vous pouvez définir et déployer de manière centralisée des protections de sécurité réseau, telles que les règles AWS WAF et AWS Shield Advanced, sur un ou plusieurs comptes et ressources de votre organisation. Au lieu de travailler avec chaque ressource individuellement, vous définissez des objets de politique réutilisables (règles, modèles et politiques) une seule fois et vous les déployez à grande échelle, avec une surveillance continue pour détecter et corriger les dérives des politiques.

Comment ? AWS Network Security Manager fonctionne en un coup d'œil

Vous définissez un ensemble d'objets de politique hiérarchiques et vous les appliquez à des étendues ciblées. Le niveau le plus bas des objets de politique sont les règles. Vous pouvez regrouper les règles dans des modèles, que vous pouvez combiner dans des politiques avec une résolution des conflits basée sur les priorités. Vous sélectionnez ensuite les comptes et les ressources à protéger dans une certaine mesure, puis vous appliquez vos politiques en publiant un déploiement.

Après le déploiement, AWS Network Security Manager surveille en permanence l'environnement délimité et les politiques déployées pour vérifier si elles correspondent aux définitions prévues. Dans le cas contraire, AWS Network Security Manager peut éventuellement corriger les ressources qui s'écartent de la configuration prévue. Pour plus de détails sur le modèle de ressources, le cycle de vie et l'architecture, consultez [Comment fonctionne AWS Network Security Manager](#).

Caractéristiques de AWS Responsable de la sécurité réseau

- Support de plusieurs types de pare-feu : AWS Network Security Manager prend en charge le AWS WAF pour les configurations ACL Web et les groupes de règles. Les types de ressources protégées incluent les CloudFront distributions Amazon, les équilibreurs de charge d'application et les stages Amazon API Gateway. AWS Network Security Manager prend également en charge AWS Shield Advanced pour la protection contre les attaques DDoS des CloudFront distributions Amazon, des équilibreurs de charge d'application, des équilibreurs de charge classiques et des adresses IP élastiques.
- Configurations de sécurité réutilisables : définissez les objets de politique une seule fois sous forme de règles, regroupez-les dans des modèles et créez des étendues pour cibler les ressources.

Réutilisez les règles, les modèles et les étendues dans le cadre de plusieurs politiques et déploiements.

- **Priority-based fusion des politiques** : lorsque plusieurs politiques protègent la même ressource, AWS Network Security Manager fusionne leurs configurations en fonction de la priorité des politiques, ce qui permet une résolution prévisible des conflits.
- **Single-account et support multi-administrateurs** : utilisez AWS Network Security Manager dans un seul compte ou désignez plusieurs comptes administrateurs, chacun avec un niveau de priorité. Lorsque les politiques des administrateurs se chevauchent, AWS Network Security Manager résout les conflits par priorité d'administrateur d'abord, puis par priorité de stratégie au sein de chaque compte.
- **États brouillon et actif** : chaque ressource AWS Network Security Manager, y compris les règles, les modèles, les politiques, les champs d'application et les déploiements, prend en charge les états brouillon et actif. Enregistrez les ressources sous forme de brouillon sans affecter les protections en direct, puis publiez-les lorsque vous êtes prêt à les appliquer.
- **Instantanés versionnés** : chaque ressource AWS Network Security Manager, y compris les règles, les modèles, les politiques, les champs d'application et les déploiements, prend en charge les instantanés immuables portant un numéro de version. Utilisez la gestion des versions pour préserver les configurations de ressources de AWS Network Security Manager, dont le fonctionnement a été vérifié.
- **Protected-resource diagnostic de synchronisation** : pour chaque ressource concernée, déterminez exactement quels paramètres ne sont pas synchronisés et pourquoi, en comparant les paramètres attendus aux valeurs réelles de chaque champ de configuration.
- **Correction automatique** : activez éventuellement AWS Network Security Manager pour corriger automatiquement les ressources désynchronisées et les aligner sur la configuration prévue sans intervention manuelle.
- **Natural-language génération de règles** — Utilisez l'`GenerateRuleConfiguration` opération pour décrire une règle en langage clair et recevoir le JSON de configuration correspondant, développé par Amazon Bedrock.

Cas d'utilisation

Les cas d'utilisation courants de AWS Network Security Manager sont les suivants :

- **Appliquez les règles AWS WAF de base à tous les comptes** : définissez un ensemble de groupes de règles AWS WAF que chaque application connectée à Internet doit utiliser, puis déployez-les

dans l'ensemble de votre organisation. AWS Network Security Manager applique automatiquement les règles aux nouvelles ressources incluses dans le champ d'application au fur et à mesure qu'elles entrent dans le champ d'application.

- Créez des règles AWS WAF personnalisées ou d'exception spécifiques pour des ressources spécifiques : définissez un ensemble de règles AWS WAF qui ne s'appliquent qu'à un ensemble spécifique de ressources. Cet ensemble peut être une unité commerciale ou une application spécifique que vous identifiez par un ID de AWS compte, une unité d'organisation, un tag ou des Amazon Resource Names (ARN).
- Vérifiez la protection contre les attaques DDoS sur les ressources connectées à Internet : créez une politique AWS Shield Advanced adaptée aux types de ressources publiques et déployez-la à l'échelle de l'organisation afin que la protection DDoS soit activée sur les ressources critiques.
- Détectez et corrigez les dérives de configuration : utilisez la surveillance de l'état de synchronisation pour identifier les ressources dont la configuration du pare-feu s'est éloignée de l'état prévu, et activez éventuellement la correction automatique pour les remettre en conformité.
- Déléguez la gestion de la sécurité à plusieurs équipes : désignez plusieurs comptes administrateurs avec différents niveaux de priorité et un accès limité à des comptes, des unités organisationnelles ou des types de pare-feu spécifiques, permettant aux équipes de gérer leurs propres politiques de sécurité dans des limites définies.

Services connexes

- AWS WAF — Utilisez le AWS WAF pour protéger vos applications Web et vos API contre les exploits Web courants et les robots susceptibles d'affecter la disponibilité, de compromettre la sécurité ou de consommer des ressources excessives. AWS Network Security Manager utilise le AWS WAF pour créer et gérer des ACL Web et des groupes de règles pour les ressources d'un seul compte ou de plusieurs comptes de votre organisation.
- AWS Shield Advanced — Un service de protection DDoS géré qui fournit des protections étendues pour vos applications exécutées sur AWS. AWS Network Security Manager utilise Shield Advanced pour protéger les ressources d'un seul compte ou de plusieurs comptes de votre organisation contre les attaques DDoS.
- AWS Organisations : vous aide à gérer et à gouverner de manière centralisée votre environnement à mesure que vous développez et faites évoluer vos AWS ressources. AWS Network Security Manager oblige AWS les Organisations à gérer les protections entre les comptes des membres.

- **AWS Config** : service qui vous permet d'évaluer, d'auditer et d'évaluer les configurations de vos AWS ressources. AWS Network Security Manager utilise un enregistreur de AWS configuration lié à un service pour découvrir les ressources de vos comptes membres.

Accès AWS Responsable de la sécurité réseau

Vous pouvez accéder à AWS Network Security Manager via les interfaces suivantes :

AWS Console de gestion

Interface Web pour gérer les ressources AWS du Network Security Manager.

Ouvrez la console AWS Network Security Manager à l'adresse <https://console.aws.amazon.com/network-security-manager/>.

AWS Interface de ligne de commande (AWS CLI)

Fournit des commandes pour les opérations de AWS Network Security Manager. Pour plus d'informations, consultez la [AWS Référence de commande CLI](#).

AWS SDK

AWS fournit des SDK composés de bibliothèques et d'exemples de code pour différents langages de programmation et plateformes. Les SDK constituent un moyen pratique de créer un accès programmatique à AWS Network Security Manager. Pour plus d'informations, consultez [Outils pour Amazon Web Services](#).

AWS API du gestionnaire de sécurité réseau

Une API REST qui utilise JSON sur HTTPS. Le format du point de terminaison de l'API est `network-security-manager.{region}.api.aws`. Pour plus d'informations, consultez le manuel de [référence de l'API AWS Network Security Manager](#).

Pour commencer à utiliser AWS Network Security Manager, reportez-vous aux sections [Configuration AWS du gestionnaire de sécurité réseau](#) et [Tutoriel : Déployez votre première protection de sécurité réseau](#).

Tarification

Vous payez pour chaque ressource incluse que AWS Network Security Manager surveille et protège. Des frais supplémentaires s'appliquent pour les services de sécurité sous-jacents que vous déployez,

tels que AWS WAF et AWS Shield Advanced. Pour obtenir des informations détaillées sur les tarifs, consultez les [tarifs de AWS Network Security Manager](#) sur le AWS site Web.

Est-ce votre première utilisation ?

Si vous utilisez AWS Network Security Manager pour la première fois, nous vous recommandons de lire les rubriques suivantes dans l'ordre :

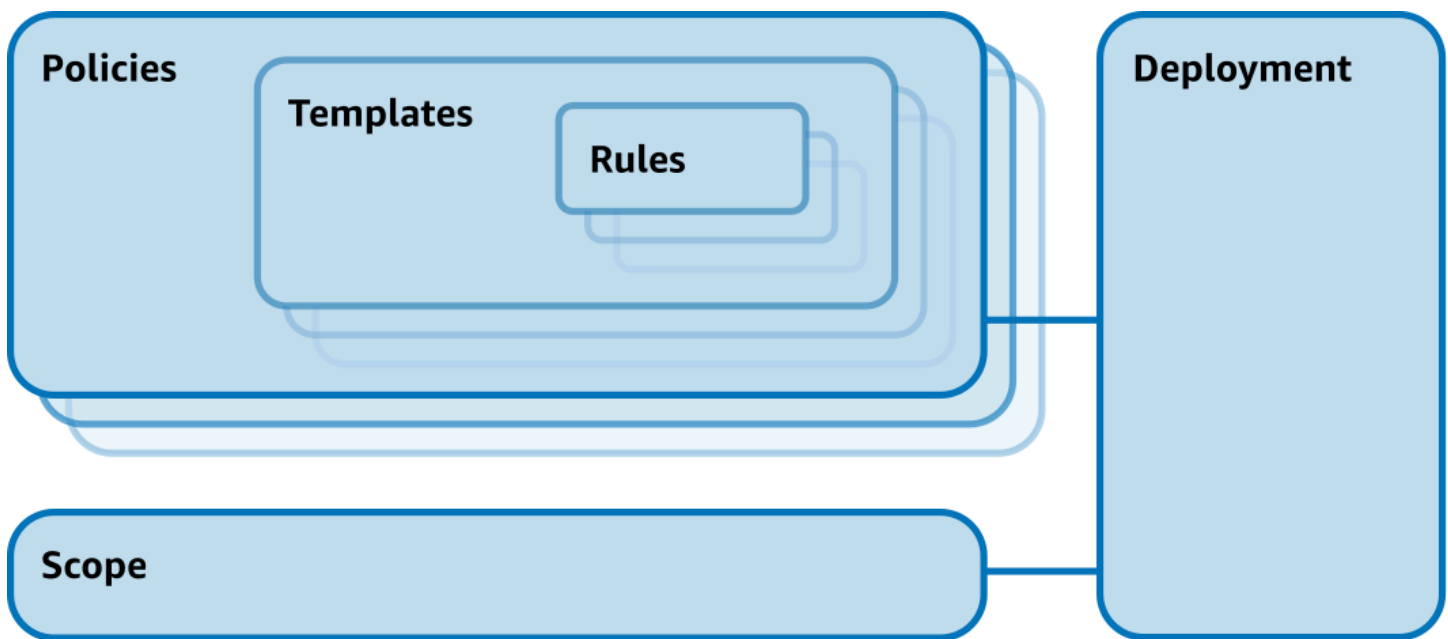
1. [Comment fonctionne AWS Network Security Manager](#)— Découvrez le modèle de ressources, les états du cycle de vie, la fusion des politiques et la synchronisation.
2. [Configuration AWS du gestionnaire de sécurité réseau](#)— Remplissez les conditions préalables à l'utilisation de AWS Network Security Manager.
3. [Tutoriel : Déployez votre première protection de sécurité réseau](#)— Parcourez un didacticiel de bout en bout qui crée votre premier déploiement.

Comment ? AWS Network Security Manager fonctionne

Utilisez le modèle de ressources AWS Network Security Manager pour concevoir et gérer les protections de sécurité réseau pour les ressources d'un seul compte ou de plusieurs comptes de votre organisation. Ce chapitre explique les cinq types de ressources, la manière dont ils forment une hiérarchie et les concepts clés qui régissent leur comportement.

AWS Modèle de ressources Network Security Manager

AWS Network Security Manager utilise cinq types de ressources organisés selon une hiérarchie de composition :



Les ressources se réfèrent mutuellement vers le haut dans la hiérarchie. Les règles sont utilisées dans les modèles et les politiques. Les modèles, les règles, ou les deux, sont utilisés dans les politiques. Une étendue fait référence aux ressources que les politiques protègent dans le cadre d'un déploiement.

Les sections suivantes décrivent chaque type de ressource de la hiérarchie.

Règle — Unité atomique de configuration de sécurité du réseau. Il existe deux types de règles : les règles d'inspection du trafic et les règles de configuration du pare-feu. L'inspection du trafic se concentre sur la manière dont le service de sécurité gère le trafic. Une règle de configuration définit les opérations du système en dehors de l'inspection du trafic. La structure d'une règle varie selon le type de pare-feu.

Modèle : groupe de règles ordonné et réutilisable pour un seul type de pare-feu. Utilisez des modèles pour regrouper les règles associées et les partager entre plusieurs politiques. Les modèles sont facultatifs.

Politique — Combine un ensemble ordonné de modèles et de règles avec des paramètres d'application pour un type de pare-feu. Chaque politique comporte une priorité (un chiffre inférieur indique une priorité plus élevée). Lorsque plusieurs politiques protègent la même ressource, la priorité détermine la manière dont les conflits sont résolus. Pour les règles d'inspection du trafic, la priorité détermine l'ordre dans lequel les règles sont agrégées. En ce qui concerne les règles de configuration du pare-feu, la priorité détermine la configuration qui s'applique à chaque ressource et à ses politiques incluses.

Champ d'application — Sélection déclarative des domaines dans lesquels les protections s'appliquent. Une étendue indique les types de ressources à protéger, et vous pouvez éventuellement filtrer les ressources par balise ou attribut de configuration. En mode multicompte, une étendue indique également les comptes ou les unités d'organisation à inclure ou à exclure. En mode compte unique, le champ d'application s'applique au compte lui-même. Le mode d'un scope est corrigé lorsque vous le créez. Vous ne pouvez pas changer d'étendue entre les modes multicompte et compte unique dans les deux sens. Une étendue multicompte ne peut donc jamais devenir une étendue mono-compte, ou l'inverse.

Déploiement : lie une ou plusieurs politiques à un périmètre. La publication d'un déploiement active l'application. AWS Network Security Manager découvre les ressources dans le périmètre, calcule la configuration prévue et corrige éventuellement les ressources désynchronisées.

Pour les limites de composition des ressources, voir [Quotas](#).

AWS Cycle de vie, fusion et synchronisation des ressources de Network Security Manager

Les sections suivantes expliquent les comportements et les mécanismes qui régissent le fonctionnement des ressources AWS Network Security Manager une fois que vous les avez créées.

Brouillon et cycle de vie actif

Chaque ressource AWS Network Security Manager, y compris les règles, les modèles, les politiques, les champs d'application et les déploiements, a le statut Brouillon ou Actif :

- **Actif** : statut par défaut. La ressource est publiée et peut être utilisée. D'autres ressources peuvent le référencer, et les déploiements qui l'incluent renforcent sa configuration.
- **Brouillon** — La ressource est enregistrée mais n'est pas encore active. Les ressources provisoires ne sont pas appliquées et ne peuvent pas être référencées par d'autres ressources. Lorsque vous créez ou mettez à jour une ressource, choisissez Enregistrer le brouillon pour conserver son statut de brouillon.

Par défaut, AWS Network Security Manager crée des ressources comme actives. Pour créer une ressource en tant que brouillon à l'aide de l'API, définissez le `isPublished` paramètre sur `false` lors de l'opération de création ou de mise à jour.

Lorsque vous mettez à jour une ressource, les scénarios suivants s'appliquent :

État actuel	Action	Résultat
Ébauche	Choisissez Enregistrer le brouillon	Mettre à jour le brouillon (reste le brouillon)
Ébauche	Choisissez Publier	Publier le brouillon (devient actif)
Actif	Choisissez Publier	Mettre à jour et rester actif (actif)
Actif	Choisissez Enregistrer le brouillon	Créez une superposition de brouillon (devient une ébauche avec une ressource active en dessous)

Le `hasPublishedVersion` champ apparaît dans la liste et reçoit des réponses. Ce champ indique si une ressource active publiée existe sous un brouillon. Lorsqu'une ressource a le statut de brouillon et `hasPublishedVersion: true` qu'un brouillon en attente se trouve au-dessus d'une ressource active publiée en ligne.

Vous ne pouvez pas supprimer une ressource active à laquelle une autre ressource active fait référence.

Gestion des versions

Chaque ressource AWS Network Security Manager, y compris les règles, les modèles, les politiques, les champs d'application et les déploiements, peut être versionnée. Pour créer une version d'une ressource active, sélectionnez la ressource, choisissez Action, puis choisissez Créer un instantané versionné. Les versions ne sont pas créées automatiquement à chaque mise à jour.

AWS Alternative à la CLI

Vous pouvez également créer une version à l'aide de l'opération `Create{Resource}SnapshotAPI` sur une ressource active.

Principales propriétés de la version :

- Chaque version possède un numéro unique (un entier séquentiel) et un ARN qualifié par version (par exemple `arn:aws:network-security-manager:us-east-1:123456789012:rule:abc123:3`).
- Les versions sont immuables. Ils ne peuvent pas être mis à jour.
- Vous pouvez créer jusqu'à 10 versions par ressource.
- Les versions peuvent être étiquetées.

Utilisez les versions pour conserver les variantes de configuration souhaitées. Pour annuler une ressource, lisez une version, puis mettez à jour la ressource active avec la configuration souhaitée pour la version.

Priority-based fusion de politiques

Lorsque plusieurs politiques protègent la même ressource, AWS Network Security Manager fusionne leurs configurations en un seul résultat. Un numéro de priorité inférieur indique une priorité plus élevée (la priorité 1 a priorité sur la priorité 2). Lorsque AWS Network Security Manager fusionne des politiques contenant des règles d'inspection du trafic, la priorité détermine l'ordre dans lequel les règles sont agrégées. Pour les règles de configuration du pare-feu, la politique de priorité la plus élevée détermine la configuration qui s'applique.

AWS Network Security Manager évalue la priorité à deux niveaux, dans l'ordre suivant :

1. **Priorité de l'administrateur** : AWS Network Security Manager évalue d'abord la priorité de l'administrateur. Une priorité est attribuée à chaque administrateur de l'organisation, comme décrit dans [the section called “Comptes d'administrateur et de membre”](#). Lorsque AWS Network Security Manager fusionne des politiques, il classe une politique d'administrateur plus haut que la politique de compte unique propre à un compte membre. Si une politique d'administrateur et la politique de compte unique d'un compte membre s'appliquent toutes deux à une ressource et à un conflit, la configuration de la politique d'administrateur l'emporte. Un compte de membre ne peut pas se soustraire à une politique d'administrateur, l'annuler ou s'en exempter.
2. **Priorité de politique** — Au sein de chaque compte, AWS Network Security Manager utilise ensuite la priorité de politique pour résoudre les conflits restants. Les valeurs de priorité des politiques sont des nombres entiers commençant à 1 et doivent être uniques par compte.

Vous définissez la priorité de l'administrateur avec le `priority` champ obligatoire de l'`PutAdminAccount` opération, un entier compris entre 1 et 10. Les valeurs de priorité étant uniques, deux administrateurs ne partagent jamais la même priorité et aucune rupture d'égalité n'est requise. Pour plus d'informations, consultez le manuel de [référence de l'API AWS Network Security Manager](#).

Le résultat combiné de toutes les politiques applicables à une ressource est la configuration effective du pare-feu. AWS Network Security Manager calcule cette configuration, la compare à la configuration réelle de la ressource et signale toute différence sous forme d'état de synchronisation.

En cas de conflit entre les politiques, AWS Network Security Manager compare chaque attribut et applique la valeur de la stratégie de priorité la plus élevée. Si la stratégie de priorité supérieure ne définit aucun attribut, la valeur de stratégie de priorité inférieure s'applique. Une ressource correspondant à la configuration effective est `IN_SYNC`. Une ressource protégée par une politique de priorité inférieure dont les paramètres ont été remplacés par une politique de priorité supérieure est signalée comme `OUT_OF_SYNC` pour le déploiement de priorité inférieure. Il s'agit d'un comportement attendu et non d'un échec.

Découverte de ressources avec AWS Config

AWS Network Security Manager découvre les ressources protégées de vos comptes à l'aide d'un enregistreur de configuration AWS Config lié à un service. Cet enregistreur est créé automatiquement dans chaque compte lorsque ce compte entre dans le cadre d'un déploiement. Contrairement à AWS Firewall Manager, vous n'avez pas besoin d'effectuer de configuration supplémentaire. AWS L'utilisation de la configuration par AWS Network Security Manager n'est pas facturée au client AWS Network Security Manager.

Principales caractéristiques de l'enregistreur lié au service :

- Il est nommé `AWSConfigurationRecorderForNetworkSecurityManager`.
- Il est distinct de tout enregistreur de configuration géré par le client dans le compte.
- Il enregistre uniquement les types de ressources correspondant à vos étendues actives et à vos déploiements.
- Il n'est pas nécessaire de configurer AWS Config ni de créer un enregistreur de configuration. AWS Network Security Manager gère cela automatiquement. AWS L'utilisation de la configuration par AWS Network Security Manager n'est pas facturée au client.
- Vous ne pouvez pas modifier ou supprimer l'enregistreur lorsqu'il est en cours d'utilisation. AWS Network Security Manager gère automatiquement son cycle de vie.

Il n'est pas nécessaire d'activer ou de configurer AWS Config manuellement pour que AWS Network Security Manager fonctionne. Le service gère automatiquement la découverte des ressources après la publication d'un déploiement.

Synchronisation et correction

L'application dans AWS Network Security Manager est asynchrone et finalement cohérente. Après avoir publié un déploiement ou lorsqu'une ressource est modifiée, les étapes suivantes se produisent :

1. Découverte des ressources : AWS Network Security Manager découvre les ressources concernées à l'aide d'un enregistreur de AWS configuration lié à un service.
2. Calcul de configuration : pour chaque ressource découverte, AWS Network Security Manager calcule la configuration effective du pare-feu en fusionnant toutes les politiques applicables par priorité.
3. Évaluation de la synchronisation : AWS Network Security Manager compare la configuration effective à la configuration réelle de la ressource et enregistre l'état de synchronisation.
4. Correction (facultatif) : si vous définissez `remediationEnabled` cette politique, AWS Network Security Manager corrige les ressources désynchronisées pour qu'elles correspondent à la configuration effective.

Chaque étape est asynchrone. Conséquences pour votre flux de travail :

- Il y a un délai entre la publication d'un déploiement et la protection des ressources.

- Il y a un délai entre la création d'une nouvelle ressource dans le champ d'application et sa protection.
- L'`LastChecked` horodatage des entrées d'état de synchronisation indique la date à laquelle AWS Network Security Manager a évalué une ressource pour la dernière fois.

La correction et le nettoyage des ressources sont des paramètres définis au niveau des politiques. Vous configurez chacune d'elles par politique dans l'`policyConfiguration` objet.

`remediationEnabled`

Spécifie si AWS Network Security Manager corrige automatiquement les ressources non conformes. Lorsque vous activez ce paramètre, AWS Network Security Manager corrige les ressources désynchronisées pour qu'elles correspondent à la configuration effective.

`resourcesCleanUp`

Spécifie si AWS Network Security Manager supprime automatiquement les ressources qu'il a créées lorsqu'elles ne sont plus nécessaires. AWS Network Security Manager supprime le pare-feu qu'il a créé lorsque vous supprimez le déploiement ou lorsque le compte ou la ressource devient hors de portée.

Les `resourcesCleanUp` paramètres `remediationEnabled` et sont tous deux définis par défaut sur `false`. AWS Network Security Manager ne corrige ni ne nettoie les ressources tant que vous n'activez pas ces paramètres. L'`policyConfiguration` objet est également valide `wafConfig`, ce qui s'applique aux politiques AWS WAF. Pour plus d'informations, consultez le manuel de [référence de l'API AWS Network Security Manager](#).

Lorsqu'une ressource n'est pas synchronisée, l'état de synchronisation inclut les raisons de la désynchronisation avec des détails par paramètre qui montrent les valeurs attendues par rapport aux valeurs réelles. Les raisons sont classées dans les catégories suivantes :

- `missingFirewall`— Aucune protection par pare-feu n'est associée à la ressource.
- `invalidFirewall`— Un pare-feu existe mais sa configuration est différente de la configuration effective. Cela inclut six compartiments détaillés : `incorrectSingleValueConfigurations`, `missingAppendableConfigurationValues`, `incorrectAppendableConfigurationOrder`, `missingMergeableConfigurationValues`, et `unexpectedMergeableConfigurationValues`.

Si la correction est activée mais que AWS Network Security Manager ne peut pas réparer une ressource, le `remediationIssues` champ fournit un message `issueType`, une message description du problème et une `correctiveAction` suggestion de résolution.

AWS Network Security Manager n'évalue pas les paramètres qu'il ne gère pas. Si un champ n'apparaît dans aucune règle contributive, AWS Network Security Manager l'ignore lors de l'évaluation de la synchronisation.

Comptes d'administrateur et de membre

AWS Network Security Manager utilise un modèle de gestion multi-comptes basé sur AWS Organizations :

- **Compte administrateur** : compte sur lequel vous créez et gérez les ressources de AWS Network Security Manager (règles, modèles, politiques, champs d'application et déploiements). Vous désignez un ou plusieurs comptes d'administrateur, chacun ayant une priorité comprise entre 1 et 10.
- **Comptes membres** : comptes sur lesquels AWS Network Security Manager découvre les ressources, évalue l'état de synchronisation et corrige éventuellement les configurations désynchronisées. AWS Network Security Manager agit sur les comptes des membres par le biais d'un rôle lié à un service. Pour plus d'informations, consultez [the section called "Service-linked rôle"](#).

Vous pouvez éventuellement étendre la portée de chaque administrateur à un sous-ensemble de comptes, d'unités d'organisation et de types de pare-feu. Utilisez cette fonctionnalité pour déléguer la gestion de domaines spécifiques à différentes équipes.

AWS Network Security Manager est un service régional. Vous créez des ressources et des déploiements par région sans aucune dépendance entre régions.

Service-linked rôle

AWS Network Security Manager utilise un rôle lié au service IAM nommé `AWSServiceRoleForNetworkSecurityManager` pour agir en votre nom sur les comptes des membres de votre organisation. Ce rôle fait confiance au directeur du `network-security-manager.amazonaws.com` service. Il utilise la politique `NetworkSecurityManagerServiceRolePolicy` AWS gérée.

AWS Network Security Manager crée ce rôle automatiquement lorsque vous activez le service, il n'y a donc aucune configuration manuelle. Ce rôle permet à AWS Network Security Manager de gérer les protections AWS WAF et AWS Shield Advanced, de découvrir les ressources protégées via AWS Config et d'effectuer des opérations entre comptes. Pour plus d'informations, consultez [the section called “Service-linked rôles”](#).

Configuration AWS Responsable de la sécurité réseau

Avec AWS Network Security Manager, vous pouvez travailler selon deux modèles d'organisation. Utilisez-le directement dans un seul compte ou utilisez-le avec AWS Organizations pour gérer les protections sur plusieurs comptes. Les étapes de configuration dépendent du modèle que vous choisissez.

Rubriques

- [Choisissez votre modèle d'organisation](#)
- [Configuration pour une utilisation avec un seul compte](#)
- [Configuration pour une utilisation multicompte avec AWS Organizations](#)
- [Création d'un AWS Compte administrateur Network Security Manager](#)
- [Créez une identité IAM avec AWS Autorisations du Network Security Manager](#)
- [Utilisation AWS Gestionnaire de sécurité réseau dans les régions désactivées par défaut](#)

Choisissez votre modèle d'organisation

Choisissez parmi les modèles d'organisation suivants :

- **Single-account**— Utilisez AWS Network Security Manager pour protéger les ressources d'un seul compte. Vous n'avez pas besoin d' AWS Organizations ou d'un compte administrateur. Créez une identité IAM avec les autorisations AWS du Network Security Manager et commencez à utiliser le service directement. AWS Network Security Manager crée automatiquement un rôle lié à un service dans votre compte.
- **Multi-account**— Utilisez AWS Network Security Manager with AWS Organizations pour protéger les ressources de plusieurs comptes. Ce mode nécessite la configuration d' AWS Organizations, l'activation d'un accès sécurisé et la création d'un compte administrateur.

Configuration pour une utilisation avec un seul compte

Pour utiliser AWS Network Security Manager dans un seul compte, créez une identité IAM avec les autorisations appropriées et commencez à utiliser le service directement. Il n'est pas nécessaire de créer un compte administrateur. AWS Network Security Manager crée automatiquement un rôle lié

à un service dans votre compte en arrière-plan. Passez à [the section called “Créez une identité IAM avec AWS Autorisations du Network Security Manager”](#).

Configuration pour une utilisation multicompte avec AWS Organizations

Pour gérer les protections sur plusieurs comptes, définissez l'adhésion et la configuration requises pour les AWS Organizations.

1. Choisissez un compte à utiliser en tant qu'administrateur du AWS Network Security Manager pour l'organisation : il s'agit du compte à partir duquel vous créez et gérez les ressources AWS du Network Security Manager.
2. Vérifier l'adhésion à l'organisation : si le compte que vous avez choisi n'est pas déjà membre de l'organisation, faites-le adhérer. Suivez les instructions de la section [Inviter un AWS compte à rejoindre votre organisation](#) dans le Guide de l'utilisateur AWS des Organizations.
3. Activez toutes les fonctionnalités de votre organisation — AWS Organizations propose deux ensembles de fonctionnalités : les fonctionnalités de facturation consolidée et toutes les fonctionnalités. Pour utiliser AWS Network Security Manager, votre organisation doit être activée pour toutes les fonctionnalités. Si votre organisation est configurée uniquement pour la facturation consolidée, suivez les instructions de la section [Activer toutes les fonctionnalités de votre organisation dans](#) le Guide de l'utilisateur AWS des Organizations.
4. Activer l'accès sécurisé pour AWS Network Security Manager — Activez l'accès sécurisé pour AWS Network Security Manager dans AWS les Organizations. Lorsque l'accès sécurisé est activé, AWS Network Security Manager peut créer un rôle lié à un service dans les comptes des membres et gérer les ressources en leur nom.
5. Enregistrer un compte d'administrateur délégué : enregistrez le compte que vous avez choisi en tant qu'administrateur délégué pour AWS Network Security Manager in AWS Organizations. Utilisez le compte de gestion des Organizations pour effectuer cette étape.



Multi-account protections désactivées lors de la désactivation de l'accès sécurisé

Si vous désactivez l'accès sécurisé pour AWS Network Security Manager dans AWS Organizations, ou si vous annulez l'enregistrement d'un compte d'administrateur délégué, AWS Network Security Manager définit l'étendue et le déploiement de plusieurs comptes sur un DISABLED état et nettoie les protections qu'il gère.

Création d'un AWS Compte administrateur Network Security Manager

Cette étape s'applique uniquement au mode multi-comptes. Seul le compte de gestion de l'organisation peut créer des comptes d'administrateur AWS Network Security Manager.

Après avoir terminé la configuration des Organizations, enregistrez votre compte en tant qu'administrateur AWS Network Security Manager. Vous pouvez le faire à partir de la console ou de l'interface de ligne de commande (AWS CLI).

Lorsque vous créez un compte administrateur, AWS Network Security Manager crée automatiquement un rôle lié à un service dans tous les comptes de votre organisation. Grâce à ce rôle, le responsable de la sécurité AWS réseau découvre les ressources et gère les protections des comptes des membres.

AWS Network Security Manager permet à plusieurs administrateurs de gérer les ressources de pare-feu de votre entreprise. Si vous souhaitez utiliser plusieurs administrateurs dans votre organisation, vous pouvez appliquer des conditions d'étendue administrative à chaque administrateur afin de définir les ressources qu'il peut gérer. Cela vous donne la flexibilité d'avoir différents rôles d'administrateur au sein de votre organisation et vous aide à maintenir le principe de l'accès le moins privilégié. Par exemple, un administrateur peut gérer un ensemble d'unités organisationnelles (UO). Un autre administrateur ne peut gérer que des types de politiques spécifiques.

Pour connaître le nombre maximal d'administrateurs que vous pouvez avoir par organisation, consultez [Quotas](#).

Enregistrement de la région

Vous enregistrez un compte administrateur AWS Network Security Manager dans une seule AWS région. Pour utiliser AWS Network Security Manager dans d'autres régions, répétez cette étape dans chaque région.

Pour créer un compte administrateur à l'aide de la console

1. Ouvrez la console AWS Network Security Manager à l'adresse <https://console.aws.amazon.com/network-security-manager/>.

2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Choisissez Ajouter un administrateur.
4. Sélectionnez le compte et entrez une valeur de priorité (1 à 10).
5. Choisissez Ajouter un administrateur pour confirmer.

Pour créer un compte administrateur à l'aide du AWS INTERFACE DE LIGNE DE COMMANDE (CLI)

Appelez l'opération PutAdminAccount. Vous devez fournir une valeur de priorité (1 à 10).

L'exemple de AWS CLI suivant enregistre un compte en tant qu'administrateur de AWS Network Security Manager avec la priorité 1 :

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

Vous pouvez désigner plusieurs comptes d'administrateur, chacun ayant une priorité différente. Vous pouvez éventuellement limiter chaque administrateur à des comptes, des unités d'organisation ou des types de pare-feu spécifiques en fournissant un adminScope paramètre.

Pour supprimer un compte administrateur à l'aide de la console

 **Multi-account protections désactivées lors de la suppression d'un administrateur**
Lorsque vous supprimez un compte administrateur, AWS Network Security Manager définit la portée et le déploiement de plusieurs comptes sur un DISABLED état et nettoie les protections qu'il gère.

1. Ouvrez la console AWS Network Security Manager à l'adresse <https://console.aws.amazon.com/network-security-manager/>.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Sélectionnez le compte administrateur que vous souhaitez supprimer.
4. Choisissez Remove administrator (Supprimer l'administrateur).
5. Pour confirmer, choisissez Confirmer la suppression par l'administrateur.

Créez une identité IAM avec AWS Autorisations du Network Security Manager

Pour utiliser AWS Network Security Manager, vous avez besoin d'une identité IAM (utilisateur ou rôle) autorisée à appeler les opérations de AWS Network Security Manager. Les actions IAM utilisent le préfixe `network-security-manager`.

L'exemple de politique IAM suivant contient trois instructions. La première instruction accorde un accès complet à toutes les opérations de AWS Network Security Manager. La deuxième déclaration accorde les AWS Organizations et les autorisations AWS WAF supplémentaires dont AWS Network Security Manager a besoin. AWS Network Security Manager utilise ces autorisations pour identifier les comptes et les unités organisationnelles (UO) de votre organisation et pour répertorier les groupes de règles WAF et les produits gérés disponibles. Ces autorisations permettent également à AWS Network Security Manager d'activer un accès sécurisé et d'enregistrer un administrateur délégué dans AWS Organizations. La troisième déclaration accorde l'`iam:CreateServiceLinkedRole` autorisation dont AWS Network Security Manager a besoin pour créer son rôle lié à un service, dont il a besoin pour une utilisation à compte unique ou multicompte.

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

Pour une utilisation en production, nous vous recommandons de n'accorder que les autorisations minimales requises. Pour plus d'informations, consultez [the section called “Gestion des identités et des accès”](#).

Inscrivez-vous pour un Compte AWS

Pour commencer AWS, vous avez besoin d'un Compte AWS. Pour plus d'informations sur la création d'un Compte AWS, voir [Getting started with an Compte AWS](#) dans le Guide de Gestion de compte AWS référence.

Utilisation AWS Gestionnaire de sécurité réseau dans les régions désactivées par défaut

Pour utiliser AWS Network Security Manager dans une région désactivée par défaut, vous devez activer la région à la fois pour le compte de gestion de votre organisation et pour le compte administrateur AWS Network Security Manager. Pour plus d'informations sur les régions désactivées par défaut et sur la manière de les activer, consultez [la section Gestion des AWS régions](#) dans le manuel de référence AWS général.

Pour activer une région désactivée

Pour le compte de gestion des Organisations et le compte administrateur de AWS Network Security Manager, suivez les instructions de la section [Activation d'une région](#) dans le manuel de référence AWS général.

Déployez votre première protection de sécurité réseau

Ce didacticiel explique comment déployer une ACL Web AWS WAF à l'aide de la console AWS Network Security Manager. Vous devez effectuer les étapes suivantes :

1. Création d'une règle
2. Création d'un modèle
3. Créer une politique
4. Créer une portée
5. Création et publication d'un déploiement
6. Surveiller l'état de synchronisation

Dans ce didacticiel, vous allez créer une ACL Web AWS WAF qui protège les équilibres de charge d'application sur les comptes que vous avez sélectionnés. Ce processus est largement identique pour tous les services de sécurité et pare-feux pris en charge par AWS Network Security Manager.

Temps de réalisation : environ 10 minutes

Coût : ce didacticiel utilise des AWS services susceptibles d'entraîner des frais. Pour connaître les tarifs actuels, consultez les [tarifs de AWS Network Security Manager](#) sur le AWS site Web.

Conditions préalables

Avant de commencer, vérifiez que vous répondez aux exigences suivantes :

- Étapes de configuration terminées, comme décrit dans [Configuration AWS du gestionnaire de sécurité réseau](#).
- Une AWS identité Identity and Access Management (IAM) avec les autorisations du AWS Network Security Manager.
- AWS Organisations disposant de toutes les fonctionnalités activées et disposant d'un compte administrateur AWS Network Security Manager désigné (obligatoire pour les déploiements multi-comptes).
- Accès à la console AWS Network Security Manager.

Étape 1 : Création d'une règle

Une règle est la pierre angulaire de votre configuration de sécurité. Au cours de cette étape, vous créez deux règles AWS WAF : l'une qui définit l'action par défaut et l'autre qui définit la configuration de visibilité. Action par défaut et champs VisibilityConfig obligatoires pour une ACL Web AWS WAF.

Pour créer la règle d'action par défaut, procédez comme suit :

1. Ouvrez la console AWS Network Security Manager à l'adresse <https://console.aws.amazon.com/network-security-manager/>.
2. Dans le panneau de navigation, sélectionnez Présentation.
3. Sur la page Vue d'ensemble, choisissez Créer une règle.
4. Pour Nom de la règle, entrez un nom descriptif, tel que `quemy-default-action-rule`.
5. Dans la section Définition des règles, pour Type de pare-feu, choisissez AWS WAF.
6. Pour Sélectionner le type de règle, choisissez Configuration.
7. Choisissez Insérer des types de configuration, puis sélectionnez Action par défaut. Un éditeur JSON apparaît avec une configuration par défaut.
8. Dans l'éditeur JSON, supprimez la Block section et conservez uniquement la Allow section.
9. Choisissez Créer une règle.

Pour créer la VisibilityConfig règle, procédez comme suit :

1. Dans le panneau de navigation, sélectionnez Présentation.
2. Sur la page Vue d'ensemble, choisissez Créer une règle.
3. Pour Nom de la règle, entrez un nom descriptif, tel que `quemy-visibility-config-rule`.
4. Dans la section Définition des règles, pour Type de pare-feu, choisissez AWS WAF.
5. Pour Sélectionner le type de règle, choisissez Configuration.
6. Choisissez Insérer des types de configuration, puis sélectionnez VisibilityConfig. Un éditeur JSON apparaît avec une configuration par défaut.
7. Choisissez Créer une règle.

AWS Alternative à la CLI

Vous pouvez également créer des règles à l'aide de 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
```

Étape 2 : Création d'un modèle

Un modèle regroupe une ou plusieurs règles à réutiliser entre les politiques. Au cours de cette étape, vous allez créer un modèle qui inclut la règle de l'étape 1 :

1. Dans le panneau de navigation, sélectionnez Présentation.
2. Sur la page Vue d'ensemble, choisissez Créer un modèle.
3. Dans Nom du modèle, entrez un nom descriptif, tel que `my-waf-template`.
4. Pour le type de pare-feu, choisissez AWS WAF.
5. Dans la section Règles, choisissez Ajouter une règle et sélectionnez les règles que vous avez créées à l'étape 1.
6. Sélectionnez Create template (Créer un modèle).

AWS Alternative à la CLI

Vous pouvez également créer un modèle à l'aide de 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
```

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

Étape 3 : Création d'une politique

Une politique combine des modèles avec des paramètres d'application. Au cours de cette étape, vous créez une politique qui fait référence à votre modèle et active la correction automatique :

1. Dans le panneau de navigation, sélectionnez Présentation.
2. Sur la page Vue d'ensemble, choisissez Créer une politique.
3. Pour Nom de la politique, entrez un nom descriptif, tel `quemy-waf-policy`.
4. Pour le type de pare-feu, choisissez AWS WAF.
5. Dans la section Priorité des politiques, les politiques existantes et leurs priorités s'affichent. Passez en revue la priorité de la nouvelle politique. Si vous devez l'ajuster, choisissez le champ de priorité et remplacez la valeur par 1 un numéro de priorité non utilisé.
6. Dans la section Modèles et règles, choisissez Ajouter un modèle et sélectionnez le modèle que vous avez créé à l'étape 2.
7. Pour la correction, sélectionnez Activé.
8. Pour la résolution ACL Web d'un client existant, sélectionnez Aucune correction.
9. Choisissez Create Policy (Créer une politique).

AWS Alternative à la CLI

Vous pouvez également créer une politique à l'aide de 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
```

Étape 4 : Création d'un scope

Un champ d'application définit les domaines dans lesquels vos protections s'appliquent. Au cours de cette étape, vous créez un périmètre qui cible les équilibres de charge d'application dans vos comptes :

1. Dans le panneau de navigation, sélectionnez Présentation.
2. Sur la page Vue d'ensemble, choisissez Create scope.
3. Pour Nom de l'étendue, entrez un nom descriptif, tel quemy-alb-scope.
4. (Facultatif) Dans la section Sélection du compte et de l'unité organisationnelle, pour Sélectionner la méthode de contrôle de l'étendue administrative, sélectionnez Étendue à AWS l'ensemble de l'organisation (toutes les unités d'organisation et tous les comptes). Ignorez cette étape pour les déploiements à compte unique.
5. Dans la section Ressources, pour les types de ressources, sélectionnez Application Load Balancer.
6. Choisissez Create scope (Créer une portée).

AWS Alternative à la CLI

Vous pouvez également créer une portée à l'aide de 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
```

Étape 5 : créer et publier un déploiement

Un déploiement lie les politiques à un périmètre et active leur application. Pour créer et publier un déploiement, procédez comme suit :

1. Dans le panneau de navigation, sélectionnez Présentation.
2. Sur la page Vue d'ensemble, choisissez Créer un déploiement.
3. Dans Nom du déploiement, entrez un nom descriptif, tel quemy-first-deployment.
4. Dans la section Politiques, choisissez Ajouter une politique et sélectionnez la politique que vous avez créée à l'étape 3.
5. Dans la section Étendue, choisissez Ajouter une étendue et sélectionnez la portée que vous avez créée à l'étape 4.
6. Choisissez Créer un déploiement.

AWS Network Security Manager commence à découvrir les ressources et à appliquer des protections. Ce processus est asynchrone et peut prendre quelques minutes.

AWS Alternative à la CLI

Vous pouvez également créer et publier un déploiement à l'aide de 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
```

Étape 6 : Surveiller l'état de synchronisation

Après avoir publié un déploiement, AWS Network Security Manager découvre les ressources et synchronise leurs configurations. Pour surveiller l'état de chaque ressource :

1. Dans le panneau de navigation, sélectionnez Présentation.
2. Choisissez l'onglet Déploiements.

3. Choisissez le déploiement que vous avez créé à l'étape 5.
4. Choisissez l'onglet Synchronisation.
5. Vérifiez l'état de synchronisation pour chaque ressource :
 - IN_SYNC — La configuration des ressources correspond à vos paramètres de protection prévus.
 - OUT_OF_SYNC — La configuration des ressources ne correspond pas. AWS Network Security Manager corrige ce problème automatiquement lorsque la correction est activée.
 - NOT_APPLICABLE — La ressource est comprise dans le champ d'application mais ne peut pas être évaluée par ce déploiement.

AWS Alternative à la CLI

Vous pouvez également vérifier l'état de synchronisation à l'aide de la AWS CLI :

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

Étape 7 : nettoyer

Si vous n'avez plus besoin des ressources que vous avez créées, supprimez-les dans l'ordre inverse pour mettre fin à leur application et supprimer les protections des ressources concernées :

L'ordre inverse est important car ces ressources se réfèrent les unes aux autres. Pour voir ce qui est associé à une ressource avant de la supprimer, appelez `ListResourceAssociations` l'ARN de cette ressource. Il renvoie l'ARN et le type de ressource de chaque ressource associée. Pour plus d'informations, consultez le manuel de [référence de l'API AWS Network Security Manager](#).

1. Dans le panneau de navigation, sélectionnez Présentation. Choisissez l'onglet Déploiements. Sélectionnez votre déploiement, choisissez Action, puis Supprimer.
2. Choisissez l'onglet Étendue. Sélectionnez votre champ d'application, choisissez Action, puis choisissez Supprimer.
3. Choisissez l'onglet Politiques. Sélectionnez votre politique, choisissez Action, puis Supprimer.
4. Sélectionnez l'onglet Modèles . Sélectionnez votre modèle, choisissez Action, puis Supprimer.
5. Choisissez l'onglet Règles. Sélectionnez votre règle, choisissez Action, puis Supprimer.

AWS Alternative à la CLI

Avant de supprimer une ressource, vérifiez ses associations pour planifier l'ordre de suppression :

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

Si une ressource possède toujours des associations, supprimez ou supprimez d'abord les ressources associées.

Vous pouvez supprimer des ressources à l'aide de la AWS CLI dans l'ordre inverse :

```
aws network-security-manager delete-deployment \  
  --deployment-identifiant "deployment-arn"  
  
aws network-security-manager delete-scope \  
  --scope-identifiant "scope-arn"  
  
aws network-security-manager delete-policy \  
  --policy-identifiant "policy-arn"  
  
aws network-security-manager delete-template \  
  --template-identifiant "template-arn"  
  
aws network-security-manager delete-rule \  
  --rule-identifiant "rule-arn"
```

Étapes suivantes

Maintenant que votre déploiement est opérationnel, explorez les méthodes suivantes pour étendre la protection de sécurité de votre réseau :

- Découvrez le modèle de ressources et le cycle de vie dans [Comment fonctionne AWS Network Security Manager](#).
- Utilisez le draft/publish flux de travail pour échelonner les modifications avant qu'elles ne prennent effet. Pour plus d'informations, consultez [the section called "Brouillon et cycle de vie actif"](#).
- Créez des instantanés pour préserver les configurations dont le fonctionnement a été vérifié. Pour plus d'informations, consultez [the section called "Gestion des versions"](#).

- Permet `GenerateRuleConfiguration` de créer des règles à partir de descriptions en langage naturel. Pour plus d'informations, consultez le manuel de [référence de l'API AWS Network Security Manager](#).
- Découvrez comment gérer les protections AWS WAF et AWS Shield Advanced au sein de votre entreprise. Pour plus d'informations, consultez [Gestion des pare-feux et des services de sécurité](#).

Gestion des pare-feux et des services de sécurité

Avec AWS Network Security Manager, vous définissez et déployez une politique de sécurité pour plusieurs pare-feux et services de sécurité. Bien que les éléments communs couvrent l' AWS ensemble du portefeuille de solutions de sécurité réseau, il existe des variations importantes auxquelles vous devez remédier dans AWS Network Security Manager.

Pour chaque service de sécurité réseau pris en charge, les sous-sections suivantes décrivent les éléments uniques et les étapes d'un processus de création rapide et d'un processus de création détaillé standard.

Gestion des ACL Web pour AWS WAF

Avec AWS Network Security Manager, vous configurez et déployez de manière centralisée les listes de contrôle d'accès Web (ACL Web) AWS WAF sur les comptes et les ressources de votre organisation. Vous pouvez définir des règles AWS Network Security Manager pour le AWS WAF, les regrouper dans des modèles de protection et les appliquer à grande échelle grâce aux politiques et aux déploiements de AWS Network Security Manager.

AWS Concepts du WAF

Les concepts suivants sont spécifiques à l'utilisation de AWS Network Security Manager avec AWS WAF. Pour plus d'informations sur le fonctionnement de AWS Network Security Manager, consultez [Comment fonctionne AWS Network Security Manager](#).

AWS Types de règles WAF

Pour AWS WAF, une règle est de deux types :

- **INSPECTION** — Contient une définition de groupe de règles utilisant `PreProcessFirewallManagerRuleGroups` (règles exécutées avant les règles définies par le client) ou `PostProcessFirewallManagerRuleGroups` (règles exécutées après).
- **CONFIGURATION** — Contient un seul paramètre de configuration ACL Web. Le JSON de configuration doit contenir exactement une clé de niveau supérieur correspondant à un paramètre pris en charge (par exemple `Description`, `DefaultAction`, `VisibilityConfig`, `LoggingConfiguration`, `CaptchaConfig`, `ChallengeConfig`, `CustomResponseBodies`, `DataProtection`, `OnSourceDDoSProtectionConfig`, `TokenDomains`, ou `MonetizationConfig`).

La plupart des paramètres de configuration ACL Web correspondent aux paramètres de l'CreateWebACL opération AWS WAF. Pour plus d'informations sur ces paramètres et leurs définitions, consultez la section [CreateWebACL](#) dans la référence de l'API AWS WAF.

L'exception est LoggingConfiguration que vous configurez séparément. Pour plus d'informations, consultez [the section called "Logging"](#).

AWS Fusion des politiques du WAF

Pour AWS WAF, chaque paramètre de configuration utilise l'une des stratégies de fusion suivantes :

SingleValue

Réglages ne pouvant avoir qu'une seule valeur. La politique la plus prioritaire l'emporte. Les valeurs de priorité étant uniques, deux politiques ne peuvent pas définir des valeurs différentes avec la même priorité. Pour plus d'informations sur la façon dont AWS Network Security Manager résout les problèmes de priorité, consultez [the section called "Priority-based fusion de politiques"](#). Les paramètres suivants utilisent SingleValue : DefaultActionVisibilityConfig, CaptchaConfig, ChallengeConfig, OnSourceDDoSProtection et Description.

Ajouter (et AppendAndSort)

Les entrées de toutes les politiques sont ajoutées à la liste par ordre de priorité. TokenDomain et DataProtectionConfig.DataProtections utilisent Ajouter. PreProcessFirewallManagerRuleGroup et PostProcessFirewallManagerRuleGroups use AppendAndSort, qui ajoute des groupes de règles à toutes les politiques et les trie par priorité. L'ordre est important car le AWS WAF évalue les groupes de règles de manière séquentielle.

Fusionner

Les entrées de toutes les politiques sont fusionnées en un seul ensemble, quelle que soit leur priorité. CustomResponseBodies et AssociationConfig.RequestBody utilisent Merge.

Les stratégies Ajouter et Fusionner suppriment les doublons. AppendAndSort Lorsque deux politiques fournissent une configuration identique, AWS Network Security Manager conserve l'entrée de la stratégie de priorité la plus élevée. La configuration effective contient donc une copie de cette entrée, et non une copie par politique contributive.

Résolution ACL Web existante

Utilisez le `existingCustomerWebACLResolution` paramètre d'une politique AWS WAF pour spécifier comment AWS Network Security Manager gère les ressources qui disposent déjà d'une ACL Web gérée par le client :

- **RETROFIT**— Mettez à jour votre ACL Web existante pour l'aligner sur la configuration effective.
- **OVERRIDE_ASSOCIATION**— Associez plutôt une ACL Web gérée par AWS Network Security Manager à la ressource.
- **NO_REMEDIATION**— Ne corrigez pas si votre ACL Web existe.

Journalisation du trafic ACL Web

Vous contrôlez la journalisation des ACL Web à l'aide du `LoggingConfiguration` paramètre d'une politique. AWS Network Security Manager applique ce paramètre à l'aide de l'`PutLoggingConfiguration` opération AWS WAF. Vous pouvez définir une destination de journalisation par liste ACL web. Pour plus d'informations, consultez [PutLoggingConfiguration](#) la référence de l'API AWS WAF.

Chaque ACL Web intégrée gérée par la politique envoie ses journaux à la destination spécifiée par la politique. Cela vous permet de centraliser la journalisation entre les comptes de votre organisation. Utilisez-le pour obtenir des informations détaillées sur le trafic que vos ACL Web analysent à l'échelle de l'organisation.

Pour une journalisation centralisée sur plusieurs comptes, vous pouvez envoyer les journaux vers un compartiment Amazon S3 ou un flux de diffusion Amazon Data Firehose. Chaque type de destination nécessite une configuration supplémentaire, que vous devez effectuer avant que AWS Network Security Manager puisse gérer la journalisation AWS WAF sur l'ensemble de vos ressources et comptes concernés. Le nom de destination doit commencer par `aws-waf-logs-`.

Amazon Data Firehose

Créez le flux de diffusion avec les caractéristiques suivantes :

- Créé à l'aide de votre compte administrateur AWS Network Security Manager
- Un nom commençant par `aws-waf-logs-`, par exemple `aws-waf-logs-network-security-manager-central`
- Une PUT source

- Créé dans la région où vous exercez vos activités, ou dans la région de l'est des États-Unis (Virginie du Nord) si vous capturez des journaux pour Amazon CloudFront

Avant d'utiliser le flux de diffusion, testez-le pour vérifier qu'il dispose d'un débit suffisant pour les journaux de votre organisation. Pour plus d'informations, consultez la section [Création d'un flux de diffusion Amazon Data Firehose](#) dans le manuel du développeur Amazon Data Firehose.

Amazon S3

Créez le compartiment en suivant les instructions Amazon S3 du guide du développeur AWS WAF. Vous devez également configurer le compartiment avec les autorisations permettant à la livraison du journal d'y écrire. La politique de compartiment suivante accorde ces autorisations.

```
{
  "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 Remplacez-le par votre propre suffixe de nom de compartiment et remplacez-le *policy-id* par l'ID de votre politique.

 CloudWatch Logs ne prend en charge que l'utilisation d'un seul compte

Si vous utilisez AWS Network Security Manager sur plusieurs comptes, vous ne pouvez pas utiliser un groupe de CloudWatch journaux Amazon Logs comme destination de journalisation. Le groupe de journaux doit se trouver dans le même AWS compte et dans la même région que l'ACL Web. Pour les déploiements multicomptes, utilisez plutôt un compartiment Amazon S3 ou un flux de diffusion Amazon Data Firehose.

Création rapide pour AWS WAF

Avec Quick Create, vous définissez et déployez les protections AWS WAF dans un seul flux de travail guidé. Utilisez Quick Create lorsque vous souhaitez configurer une protection ACL Web complète, des règles au déploiement en une seule session.

Pour définir et déployer une protection AWS WAF avec Quick Create, suivez les procédures suivantes dans l'ordre.

Pour créer la politique et ajouter des protections

1. Ouvrez la console AWS Network Security Manager à l'adresse <https://console.aws.amazon.com/network-security-manager/>.
2. Dans le panneau de navigation, sélectionnez Présentation.
3. En haut à droite de la page de présentation, choisissez Création et déploiement rapides. La page de création et de déploiement rapides s'affiche avec plusieurs volets.
4. Dans le volet Détails de la stratégie, pour Nom, entrez le nom de la politique. (Facultatif) Sous Description, entrez une description.
5. Dans le volet Définir les protections, choisissez le type de pare-feu avec lequel vous souhaitez travailler. Sélectionnez AWS WAF. Un sous-volet Modèles et règles apparaît, dans lequel vous pouvez ajouter des règles ou des modèles.
6. Pour ajouter des règles, choisissez Ajouter ou gérer des règles. Dans la fenêtre qui apparaît, pour Sélectionner le type de règle, sélectionnez l'une des options suivantes :

- **AWS Règles gérées** — Le tableau présente toutes les règles AWS gérées prises en charge par AWS WAF.
- **Règles** — Le tableau indique les groupes de règles AWS WAF que vous possédez, autres que les règles AWS gérées.

Cochez les cases correspondant aux règles que vous souhaitez ajouter à votre politique.

Choisissez ensuite **Ajouter des règles**.

7. Pour ajouter des modèles, choisissez **Ajouter des modèles**. Dans la fenêtre **Ajouter des modèles** qui apparaît, le tableau affiche tous les modèles disponibles. Sélectionnez les modèles que vous souhaitez, ainsi que la version à inclure dans la politique. Choisissez ensuite **Ajouter des modèles**.

Pour configurer la politique

1. Passez en revue vos sélections dans le tableau **Modèles et règles**. Le nombre entier dans la colonne **Position** détermine l'ordre d'évaluation des règles et des modèles. Pour modifier l'ordre d'évaluation, choisissez la valeur de la position dans la colonne **Position**. Utilisez les flèches pour modifier la valeur. Pour accepter la modification, choisissez **Confirmer**. Pour annuler la modification, choisissez **Annuler**.
2. Sous **Configuration des politiques** dans le volet **Définir les protections**, déterminez les actions automatisées que AWS Network Security Manager exécute dans le périmètre ciblé :
 - La correction applique la politique définie à toutes les ressources dont l'état de sécurité n'est pas synchronisé avec l'état souhaité décrit dans AWS Network Security Manager.
 - Le nettoyage des ressources supprime le pare-feu créé par AWS Network Security Manager pour une ressource lorsque le déploiement est supprimé ou lorsque le compte ou la ressource est hors de portée.
 - La résolution WebACL du client existant détermine comment résoudre les conflits entre la politique que vous définissez et celle qui est peut-être déjà déployée. Dans le menu, choisissez l'une des options suivantes :
 - **Aucune correction** n'ignore la correction sur les ressources déjà dotées d'une ACL Web.
 - **L'association Override** remplace l'ACL Web existante par l'ACL Web créée par AWS Network Security Manager.
 - **Retrofit** adapte ses règles à chaque ACL Web existante et conserve l'ACL Web associée à la ressource.

3. Dans le volet **Priorité des politiques**, définissez la priorité. AWS Network Security Manager évalue les politiques en fonction de leur priorité afin de résoudre les conflits. Les positions inférieures (nombres entiers inférieurs) ont une priorité plus élevée. Pour modifier la priorité, choisissez la valeur de position. Puis incrémentez-le à l'aide des flèches ou entrez directement une valeur. Pour confirmer la sélection, choisissez **Confirmer**. Pour annuler la modification, choisissez **Annuler**.

Pour définir le champ d'application

1. Dans le volet **Définir le champ d'application**, définissez l'ensemble des actifs auxquels les politiques s'appliquent. Pour **Nom de l'étendue**, entrez un nom. (Facultatif) Sous **Description**, entrez une description.

2.

 Multi-account mode uniquement

Cette étape s'applique uniquement au mode multi-comptes. En mode multicompte, utilisez le sous-volet de sélection des comptes et des unités organisationnelles pour choisir les comptes ou les unités d'organisation à inclure ou à exclure. En mode compte unique, ce sous-volet n'apparaît pas dans la console. Ignorez donc cette étape.

Dans le sous-volet de sélection des comptes et des unités organisationnelles, sélectionnez l'une des options suivantes :

- Portée à l'ensemble de AWS l'organisation. Aucune autre définition n'est requise.
- S'applique à l'ensemble de AWS l'organisation, mais exclut des unités d'organisation et des comptes spécifiques. Un sous-volet **Unités organisationnelles** et un sous-volet **Comptes** apparaissent. Pour exclure des unités organisationnelles, choisissez **Ajouter des unités d'organisation**. Sélectionnez les unités organisationnelles dans l'arborescence organisationnelle, puis choisissez **Ajouter des unités d'organisation**. Pour exclure des comptes individuels, choisissez **Ajouter des comptes**. Sélectionnez les comptes dans l'arborescence organisationnelle, puis choisissez **Ajouter des comptes**.
- Ne vous limitez pas à l'ensemble de AWS l'organisation et incluez uniquement des unités d'organisation et des comptes spécifiques. Utilisez le même mécanisme d'ajout d'unités d'organisation et d'ajout de comptes pour inclure les unités organisationnelles et les comptes que vous souhaitez.

3. Dans le sous-volet Ressources, pour les types de ressources, sélectionnez tous les types de ressources AWS WAF ou des types spécifiques. Les options sont l'une ou plusieurs des options suivantes :

- Application Load Balancer
- API REST d'Amazon API Gateway
- CloudFront Distribution

 CloudFront Exigence de région

Pour protéger les ressources de CloudFront distribution, utilisez la région USA Est (Virginie du Nord) (us-east-1).

 Types de ressources mondiaux et régionaux

Vous pouvez sélectionner le type de ressource global (CloudFront distribution) ou les types de ressources régionaux (Application Load Balancer et API REST Amazon API Gateway), mais pas les deux. Une fois que vous avez sélectionné un type de ressource, vous ne pouvez pas basculer entre les types de ressources de CloudFront distribution et régionaux lorsque vous mettez à jour la configuration.

 Ressources non gérées CloudFront

AWS Network Security Manager ne gère pas les CloudFront distributions qui utilisent le plan tarifaire CloudFront forfaitaire ou les distributions CloudFront intermédiaires. Ces ressources semblent désynchronisées.

4. Pour chaque type de ressource sélectionné, choisissez l'une des options mutuellement exclusives suivantes :

- Inclure toutes les ressources
- Inclure des ressources spécifiques
- Exclure des ressources spécifiques

5. Si vous choisissez Inclure des ressources spécifiques, choisissez l'un des types d'expression suivants, puis créez les combinaisons appropriées de balises ou d'ARN :

- Critères uniques
- Correspond à tous les critères (ET)
- Répondez à tous les critères (OU)
- NON

Tous les types de ressources ont les critères d'inclusion Tag et ARN. Si vous choisissez Tag, entrez une clé et une valeur facultative. Vous pouvez identifier plusieurs balises. Si votre type de ressource est un Application Load Balancer, un critère de configuration supplémentaire apparaît. Dans Configuration, choisissez un schéma comportant les options Internet-facing ou Interne.

Pour revoir et déployer la politique

1. Dans le volet Révision et déploiement, pour Nom du déploiement, entrez un nom. (Facultatif) Sous Description, entrez une description. Pour déterminer si le contenu de votre déploiement est visible pour les autres comptes de votre organisation, sélectionnez Activer la visibilité entre comptes pour ce déploiement.
2. (Facultatif) Pour ajouter des balises à votre ressource, choisissez Ajouter une nouvelle balise, puis entrez les combinaisons clé et valeur facultatives.
3. Pour exécuter ce que vous avez défini, choisissez Create and deploy. Lorsque le processus est terminé, la page Déploiements apparaît, où vous pouvez voir les détails de ce qui a été créé.

 Les déploiements peuvent entraîner des frais

Un déploiement crée des services de sécurité réseau et les associe à une ressource protégée. AWS Network Security Manager facture les ressources protégées. Les services de sécurité eux-mêmes protègent la ressource, ce qui entraîne des frais supplémentaires. Avant de procéder au déploiement, consultez la page de [tarification de AWS Network Security Manager](#) et la page de [tarification du AWS WAF](#).

Processus de création standard pour AWS WAF

Avec le processus de création standard, vous créez chaque composant AWS WAF (règles, modèles, politiques, étendues et déploiements) individuellement pour un contrôle total. Utilisez cette approche lorsque vous souhaitez créer des composants réutilisables et les combiner selon vos besoins.

Une politique AWS WAF de AWS Network Security Manager peut contenir des règles et des modèles. Lorsque vous appliquez la politique, AWS Network Security Manager crée une ACL Web dans chaque compte concerné.

Pour créer une règle (console)

1. Connectez-vous à la console AWS de gestion à l'aide de votre compte d'administrateur AWS Network Security Manager, puis ouvrez la console AWS Network Security Manager à l'adresse <https://console.aws.amazon.com/network-security-manager/>.

 Configuration du compte administrateur

Pour plus d'informations sur la configuration d'un compte administrateur AWS Network Security Manager, consultez [Configuration AWS du gestionnaire de sécurité réseau](#).

2. Dans le volet de navigation, choisissez AWS Network Security Manager, puis Overview.
3. Dans le volet Vue d'ensemble, choisissez Create rule. Entrez un nom descriptif, puis entrez une description facultative.
4. Dans le volet de définition des règles, pour Type de pare-feu, choisissez AWS WAF.
5. Pour Type de règle, sélectionnez Inspection ou Configuration.

Si vous choisissez Inspection, un volet de l'éditeur JSON nommé Définir une référence de groupe de règles apparaît avec les options suivantes :

- Insérer un modèle : sélectionnez un modèle JSON pour les premières règles (pré-traitement) ou les dernières règles (post-traitement). Lorsque vous effectuez une sélection, AWS Network Security Manager insère le JSON correspondant dans l'éditeur, ainsi que des icônes d'avertissement si des entrées sont nécessaires pour compléter le modèle.
- Insérer un groupe de règles : présente une liste de sélection composée de trois options :
 - Un AWS groupe de règles gérées (AMR)
 - Un groupe de règles personnalisées existant
 - Un groupe de règles AWS Marketplace

AWS Network Security Manager présente les groupes de règles associés à votre choix, et vous pouvez sélectionner une seule instance à inclure. Après avoir effectué la sélection, choisissez Sélectionner un groupe de règles. AWS Network Security Manager insère des références à la règle d'inspection avec la syntaxe correcte dans l'éditeur JSON.

- Insérer avec IA — Ouvrez une fenêtre de superposition nommée générateur de configuration AI. Utilisez cet outil pour décrire votre règle en langage clair, et AWS Network Security Manager génère le JSON associé dans l'éditeur. Vous pouvez ensuite consulter le code généré et choisir d'accepter, de modifier ou de supprimer la sortie.
6. (Facultatif) Une fois la définition de votre règle JSON terminée, vous pouvez associer une balise à votre règle. Pour cela, choisissez Ajouter une balise, puis saisissez une clé et éventuellement une valeur.
 7. Lorsque vous avez terminé vos définitions, choisissez Enregistrer le brouillon pour enregistrer un objet inactif potentiellement incomplet ou Créer une règle.

 Les noms d'ACL Web sont permanents

Vous ne pouvez pas modifier le nom d'une ACL Web après l'avoir créée. Si vous mettez à jour le nom de votre politique, AWS Network Security Manager ne met pas à jour le nom de l'ACL Web associé. Pour que AWS Network Security Manager crée une ACL Web portant un nom différent, vous devez créer une nouvelle politique.

Pour créer un modèle (console)

Un modèle assemble les règles par ordre de priorité en vue de leur évaluation dans le cadre d'une politique. Vous pouvez organiser vos types de règles en groupes correspondant à vos objectifs de sécurité. Vous pouvez également laisser les différentes équipes élaborer des déclarations de contrôle de sécurité correspondant à leurs responsabilités et à leurs compétences.

1. Sur la page Vue d'ensemble, dans le volet Vue d'ensemble, choisissez Créer un modèle. Sur la page Créer un modèle, entrez un nom de modèle, entrez une description facultative et choisissez un type de pare-feu (dans ce cas, AWS WAF).
2. Lorsque vous choisissez un type de pare-feu, le volet Règles apparaît. Cliquez sur l'un des deux boutons Ajouter des règles pour ouvrir la liste des règles disponibles. Cochez la case située à gauche du nom d'une règle pour l'ajouter au modèle. Pour choisir une version spécifique d'une règle, sélectionnez le champ Version de la règle. Si plusieurs versions sont disponibles, sélectionnez la version souhaitée, puis cliquez sur Confirmer.
3. (Facultatif) Créez une balise pour le modèle. Lorsque vous avez terminé, choisissez Enregistrer le brouillon ou Créer un modèle. Pour continuer à créer une politique, choisissez Créer un modèle.

Pour créer une stratégie (console)

Il s'agit de l'étape finale de la définition de la politique et de la préparation du déploiement.

1. Sur la page Vue d'ensemble, dans le volet Vue d'ensemble, choisissez Create policy. Sur la page Créer une politique, entrez un nom et une description facultative, puis choisissez un type de pare-feu (dans ce cas, AWS WAF).
2. Dans le volet Priorité des politiques, définissez la priorité. AWS Network Security Manager évalue les politiques en fonction de leur priorité afin de résoudre les conflits. Les positions inférieures (nombres entiers inférieurs) ont une priorité plus élevée. Pour modifier la priorité, choisissez la valeur de position. Puis incrémentez-le à l'aide des flèches ou entrez directement une valeur. Pour confirmer la sélection, choisissez Confirmer. Pour annuler la modification, choisissez Annuler.
3. Dans le volet de configuration des politiques, déterminez les actions automatisées que AWS Network Security Manager exécute dans le périmètre ciblé :
 - La correction applique la politique définie à toutes les ressources dont l'état de sécurité n'est pas synchronisé avec l'état souhaité décrit dans AWS Network Security Manager.
 - Le nettoyage des ressources supprime le pare-feu créé par AWS Network Security Manager pour une ressource lorsque le déploiement est supprimé ou lorsque le compte ou la ressource est hors de portée.
 - La résolution WebACL du client existant détermine comment résoudre les conflits entre la politique que vous définissez et celle qui est peut-être déjà déployée. Dans le menu, choisissez l'une des options suivantes :
 - Aucune correction n'ignore la correction sur les ressources déjà dotées d'une ACL Web.
 - L'association Override remplace l'ACL Web existante par l'ACL Web créée par AWS Network Security Manager.
 - Retrofit adapte ses règles à chaque ACL Web existante et conserve l'ACL Web associée à la ressource.
4. Une fois ces paramètres de configuration définis, sélectionnez les règles et les modèles que vous souhaitez ajouter à la politique. Dans le volet Modèles et règles, choisissez Ajouter des règles ou Ajouter des modèles pour renseigner la politique. Les deux processus ouvrent une fenêtre qui fonctionne de la même manière que le processus de sélection des règles décrit plus haut dans cette section.

Pour créer un scope (console)

1. Vous pouvez démarrer cette étape depuis la page Vue d'ensemble ou depuis d'autres zones de l'outil. Dans le volet Détails de l'étendue, entrez un nom de portée et une description facultative.

2.

 Multi-account mode uniquement

Cette étape s'applique uniquement au mode multi-comptes. En mode multicompte, utilisez le sous-volet de sélection des comptes et des unités organisationnelles pour choisir les comptes ou les unités d'organisation à inclure ou à exclure. En mode compte unique, ce sous-volet n'apparaît pas dans la console. Ignorez donc cette étape.

Dans le volet de sélection du compte et de l'unité organisationnelle, choisissez l'une des trois méthodes de contrôle de l'étendue administrative :

- Portée à AWS l'ensemble de l'organisation (toutes les unités d'organisation et tous les comptes)
— Aucune autre définition n'est requise.
 - Portez sur AWS l'ensemble de l'organisation, mais excluez des unités d'organisation et des comptes spécifiques : deux sous-volets apparaissent, l'un pour les unités organisationnelles et l'autre pour les comptes. Choisissez Ajouter des unités d'organisation pour ouvrir la fenêtre Ajouter des unités organisationnelles, sélectionnez les unités organisationnelles dont vous avez besoin dans l'arborescence organisationnelle, puis choisissez Ajouter des unités d'organisation. Pour ajouter des comptes individuels, dans le sous-volet Comptes, choisissez Ajouter des comptes, sélectionnez les comptes dans l'arborescence organisationnelle, puis choisissez Ajouter des comptes.
 - Ne pas couvrir l'ensemble de AWS l'organisation, inclure uniquement des unités d'organisation et des comptes spécifiques. Utilisez les mêmes sous-volets pour ajouter des unités d'organisation ou des comptes avec le même mécanisme que celui décrit pour l'option précédente.
3. Sélectionnez ensuite les ressources dans le sous-volet Ressources. Dans la zone de sélection des types de ressources, sélectionnez tous les types de ressources AWS WAF ou des types spécifiques. Pour AWS WAF, les options sont l'une ou l'ensemble des options suivantes :
- Application Load Balancer
 - API REST d'Amazon API Gateway
 - CloudFront Distribution

CloudFront Exigence de région

Pour protéger les ressources de CloudFront distribution, utilisez la région USA Est (Virginie du Nord) (us-east-1).

Types de ressources mondiaux et régionaux

Vous pouvez sélectionner le type de ressource global (CloudFront distribution) ou les types de ressources régionaux (Application Load Balancer et API REST Amazon API Gateway), mais pas les deux. Une fois que vous avez sélectionné un type de ressource, vous ne pouvez pas basculer entre les types de ressources de CloudFront distribution et régionaux lorsque vous mettez à jour la configuration.

Ressources non gérées CloudFront

AWS Network Security Manager ne gère pas les CloudFront distributions qui utilisent le plan tarifaire CloudFront forfaitaire ou les distributions CloudFront intermédiaires. Ces ressources semblent désynchronisées.

4. Pour chaque type de ressource sélectionné, choisissez l'une des options mutuellement exclusives suivantes :
 - Inclure toutes les ressources
 - Inclure des ressources spécifiques
 - Exclure des ressources spécifiques
5. Si vous choisissez Inclure des ressources spécifiques, sélectionnez l'un des types d'expression suivants :
 - Critères uniques
 - Correspond à tous les critères (ET)
 - Répondez à tous les critères (OU)
 - NON
6. Chaque type d'expression prend en charge un ou plusieurs critères d'inclusion et ARN, ce qui vous permet de créer des combinaisons de balises ou d'ARN. Tous les types de ressources prennent en

charge les critères d'inclusion des balises et des ARN. Si vous choisissez Tag, identifiez une clé et une valeur facultative. Vous pouvez identifier plusieurs balises.

7. Pour un Application Load Balancer, un critère de configuration supplémentaire apparaît. Dans Configuration, vous pouvez définir un schéma avec les options Internet-facing ou Interne.

Pour créer un déploiement (console)

Un déploiement lie vos politiques à un périmètre et active leur application, ce qui oblige AWS Network Security Manager à appliquer vos règles AWS WAF aux ressources incluses dans le périmètre.

1. Sur la page Vue d'ensemble, dans le volet Vue d'ensemble, choisissez Créer un déploiement. Vous pouvez également démarrer cette étape depuis d'autres zones de l'outil.
2. Choisissez la politique que vous souhaitez déployer.
3. Choisissez l'étendue qui définit les comptes et les ressources auxquels AWS Network Security Manager applique la politique.
4. Dans Nom du déploiement, entrez un nom. (Facultatif) Sous Description, entrez une description.
5. (Facultatif) Pour rendre le déploiement visible pour les autres comptes de votre organisation, sélectionnez Activer la visibilité entre comptes pour ce déploiement.
6. (Facultatif) Pour ajouter des balises, choisissez Ajouter une nouvelle balise, puis entrez les combinaisons clé et valeur facultatives.
7. Choisissez Create and deploy (Créer et déployer). La page Déploiements apparaît, où vous pouvez voir les détails de ce que AWS Network Security Manager a créé.

Les déploiements peuvent entraîner des frais

Un déploiement crée des services de sécurité réseau et les associe à une ressource protégée. AWS Network Security Manager facture les ressources protégées. Les services de sécurité eux-mêmes protègent la ressource, ce qui entraîne des frais supplémentaires. Avant le déploiement, consultez la page de [tarification de AWS Network Security Manager et la page de tarification du AWS WAF](#).

Gestion des protections DDoS pour AWS Shield Advanced

Avec AWS Network Security Manager, vous configurez et déployez de manière centralisée les protections AWS Shield Advanced sur les comptes et les ressources de votre organisation. Vous pouvez définir des politiques de protection contre les attaques DDoS et les appliquer à grande échelle grâce aux politiques et aux déploiements de AWS Network Security Manager.

AWS Network Security Manager est facturé séparément

AWS Network Security Manager ne fait pas partie de l'offre AWS Shield Advanced. Pour plus d'informations sur les tarifs, consultez les sections Tarification [de AWS Network Security Manager et Tarification](#) de [AWS Shield Advanced](#).

AWS Abonnement Shield Advanced

Lorsqu'un déploiement actif inclut un compte dans son champ d'application, AWS Network Security Manager abonne ce compte à AWS Shield Advanced. AWS Network Security Manager n'annule pas l'abonnement lorsque le compte quitte le champ d'application ou lorsque vous supprimez le déploiement. Pour annuler un abonnement à AWS Shield Advanced, consultez la section [S'abonner à AWS Shield Advanced](#) dans le guide du développeur AWS WAF.

Création rapide pour AWS Shield Advanced

Avec Quick Create, vous définissez et déployez les protections AWS Shield Advanced dans le cadre d'un flux de travail guidé unique. Utilisez Quick Create lorsque vous souhaitez configurer la protection contre les attaques DDoS contre les politiques par le biais d'un déploiement en une seule session.

Pour définir et déployer une protection AWS Shield Advanced avec Quick Create, suivez les procédures suivantes dans l'ordre.

Pour créer la politique et configurer les protections

Procédez comme suit :

1. Ouvrez la console AWS Network Security Manager à l'adresse <https://console.aws.amazon.com/network-security-manager/>.

2. Dans le panneau de navigation, sélectionnez Présentation.
3. Sur la page Vue d'ensemble, choisissez Création et déploiement rapides. La page de création et de déploiement rapides s'affiche avec plusieurs volets.
4. Dans le volet Détails de la stratégie, pour Nom, entrez le nom de la politique. (Facultatif) Sous Description, entrez une description.
5. Dans le volet Définir les protections, choisissez le type de pare-feu avec lequel vous souhaitez travailler. Sélectionnez AWS Shield Advanced.
6. Sous Configuration des politiques dans le volet Définir les protections, déterminez les actions automatisées que AWS Network Security Manager exécute dans le périmètre ciblé :
 - La correction applique la politique définie à toutes les ressources dont l'état de sécurité ne correspond pas à l'état souhaité décrit par AWS Network Security Manager.
 - Le nettoyage des ressources supprime la protection DDoS créée par AWS Network Security Manager pour une ressource lorsque le déploiement est supprimé ou lorsque le compte ou la ressource est hors de portée.
 - La résolution des attaques DDoS par les clients existants détermine la manière de résoudre les conflits entre la politique que vous définissez et celle qui est peut-être déjà déployée. Dans le menu, choisissez l'une des options suivantes :
 - Aucune correction n'ignore la correction des ressources déjà protégées contre les attaques DDoS.
 - L'association Override remplace la protection DDoS existante par la protection DDoS créée par AWS Network Security Manager.
 - Retrofit adapte ses règles à chaque protection DDoS existante et conserve la protection DDoS associée à la ressource.
7. Dans le volet Priorité des politiques, définissez la priorité. AWS Network Security Manager évalue les politiques en fonction de leur priorité afin de résoudre les conflits. Les positions inférieures (nombres entiers inférieurs) ont une priorité plus élevée.

Pour modifier la priorité, choisissez la valeur de position. Puis incrémentez-le à l'aide des flèches ou entrez directement une valeur. Pour confirmer la sélection, choisissez Confirmer. Pour annuler la modification, choisissez Annuler.

Pour définir le champ d'application

Procédez comme suit :

1. Dans le volet Définir le champ d'application, définissez l'ensemble des actifs auxquels les politiques s'appliquent. Pour Nom de l'étendue, entrez un nom. (Facultatif) Sous Description, entrez une description.

2.

 Multi-account mode uniquement

Cette étape s'applique uniquement au mode multi-comptes. En mode multicompte, utilisez le sous-volet de sélection des comptes et des unités organisationnelles pour choisir les comptes ou les unités d'organisation à inclure ou à exclure. En mode compte unique, ce sous-volet n'apparaît pas dans la console. Ignorez donc cette étape.

Dans le sous-volet de sélection des comptes et des unités organisationnelles, sélectionnez l'une des options suivantes :

- Portée à l'ensemble de AWS l'organisation. Aucune autre définition n'est requise.
 - S'applique à l'ensemble de AWS l'organisation, mais exclut des unités d'organisation et des comptes spécifiques. Un sous-volet Unités organisationnelles et un sous-volet Comptes apparaissent. Pour exclure des unités organisationnelles, choisissez Ajouter des unités d'organisation. Sélectionnez les unités organisationnelles dans l'arborescence organisationnelle, puis choisissez Ajouter des unités d'organisation. Pour exclure des comptes individuels, choisissez Ajouter des comptes. Sélectionnez les comptes dans l'arborescence organisationnelle, puis choisissez Ajouter des comptes.
 - Ne vous limitez pas à l'ensemble de AWS l'organisation et incluez uniquement des unités d'organisation et des comptes spécifiques. Utilisez le même mécanisme d'ajout d'unités d'organisation et d'ajout de comptes pour inclure les unités organisationnelles et les comptes que vous souhaitez.
3. Dans le sous-volet Ressources, pour les types de ressources, sélectionnez tous les types de ressources AWS Shield Advanced ou des types de ressources spécifiques. Les options sont l'une ou plusieurs des options suivantes :
- Application Load Balancer
 - CloudFront Distribution
 - Equilibreur de charge classique
 - Adresse IP Elastic
4. Pour chaque type de ressource sélectionné, choisissez l'une des options mutuellement exclusives suivantes :

- Inclure toutes les ressources
 - Inclure des ressources spécifiques
 - Exclure des ressources spécifiques
5. Si vous choisissez Inclure des ressources spécifiques, choisissez l'un des types d'expression suivants, puis créez les combinaisons appropriées de balises ou d'ARN :
- Critères uniques
 - Correspond à tous les critères (ET)
 - Répondez à tous les critères (OU)
 - NON

Tous les types de ressources ont les critères d'inclusion Tag et ARN. Si vous choisissez Tag, entrez une clé et une valeur facultative. Vous pouvez identifier plusieurs balises.

 CloudFront Exigence de région

Pour protéger les ressources de CloudFront distribution, utilisez la région USA Est (Virginie du Nord) (`us-east-1`).

Pour revoir et déployer la politique

Procédez comme suit :

1. Dans le volet Révision et déploiement, pour Nom du déploiement, entrez un nom. (Facultatif) Sous Description, entrez une description. Pour déterminer si le contenu de votre déploiement est visible pour les autres comptes de votre organisation, sélectionnez Activer la visibilité entre comptes pour ce déploiement.
2. (Facultatif) Pour ajouter des balises à votre ressource, choisissez Ajouter une nouvelle balise, puis entrez les combinaisons clé et valeur facultatives.
3. Pour créer et déployer la politique et le périmètre, choisissez Create and deploy. Lorsque le processus est terminé, la page Déploiements apparaît, où vous pouvez voir les détails de ce que AWS Network Security Manager a créé.

Les déploiements peuvent entraîner des frais

Un déploiement crée des services de sécurité réseau et les associe à une ressource protégée. AWS Network Security Manager facture les ressources protégées. Les services de sécurité eux-mêmes protègent la ressource, ce qui entraîne des frais supplémentaires. Avant de procéder au déploiement, consultez la page de [tarification de AWS Network Security Manager et la page de tarification de AWS Shield Advanced](#).

Processus de création standard pour AWS Shield Advanced

Avec le processus de création standard, vous configurez chaque composant de AWS Shield Advanced (politiques, champs d'application et déploiements) individuellement pour un contrôle total. Utilisez cette approche lorsque vous souhaitez créer des composants réutilisables et les combiner selon vos besoins.

Une politique AWS Shield Advanced est simple et ne contient pas de règles, de groupes de règles ou de modèles. Lorsque vous appliquez cette politique, AWS Network Security Manager crée une protection DDoS AWS Shield Advanced dans chaque compte concerné. Pour plus d'informations sur le fonctionnement de AWS Network Security Manager, consultez [Comment fonctionne AWS Network Security Manager](#).

Pour créer une stratégie (console)

Procédez comme suit :

1. Connectez-vous à la console AWS de gestion à l'aide de votre compte d'administrateur AWS Network Security Manager, puis ouvrez la console AWS Network Security Manager à l'adresse <https://console.aws.amazon.com/network-security-manager/>.

Configuration du compte administrateur

Pour plus d'informations sur la configuration d'un compte administrateur AWS Network Security Manager, consultez [Configuration AWS du gestionnaire de sécurité réseau](#).

2. Dans le volet de navigation, choisissez AWS Network Security Manager, puis Overview.
3. Dans le volet Vue d'ensemble, choisissez Create policy. Entrez un nom et une description facultative, puis choisissez un type de pare-feu (dans ce cas, AWS Shield Advanced).

4. Dans le volet Priorité des politiques, définissez la priorité. AWS Network Security Manager évalue les politiques en fonction de leur priorité afin de résoudre les conflits. Les positions inférieures (nombres entiers inférieurs) ont une priorité plus élevée.

Pour modifier la priorité, choisissez la valeur de position. Puis incrémentez-le à l'aide des flèches ou entrez directement une valeur. Pour confirmer la sélection, choisissez Confirmer. Pour annuler la modification, choisissez Annuler.

5. Dans le volet de configuration des politiques, déterminez les actions automatisées que AWS Network Security Manager exécute dans le périmètre ciblé :
 - La correction applique la politique définie à toutes les ressources dont l'état de sécurité ne correspond pas à l'état souhaité décrit par AWS Network Security Manager.
 - Le nettoyage des ressources supprime la protection DDoS créée par AWS Network Security Manager pour une ressource lorsque le déploiement est supprimé ou lorsque le compte ou la ressource est hors de portée.
 - La résolution des attaques DDoS par les clients existants détermine la manière de résoudre les conflits entre la politique que vous définissez et celle qui est peut-être déjà déployée. Dans le menu, choisissez l'une des options suivantes :
 - Aucune correction n'ignore la correction des ressources déjà protégées contre les attaques DDoS.
 - L'association Override remplace la protection DDoS existante par la protection DDoS créée par AWS Network Security Manager.
 - Retrofit adapte ses règles à chaque protection DDoS existante et conserve la protection DDoS associée à la ressource.

Pour créer un scope (console)

Procédez comme suit :

1. Dans le volet Détails de l'étendue, entrez un nom de portée et une description facultative.

2.  Multi-account mode uniquement

Cette étape s'applique uniquement au mode multi-comptes. En mode multicompte, utilisez le sous-volet de sélection des comptes et des unités organisationnelles pour choisir les

comptes ou les unités d'organisation à inclure ou à exclure. En mode compte unique, ce sous-volet n'apparaît pas dans la console. Ignorez donc cette étape.

Dans le volet de sélection du compte et de l'unité organisationnelle, choisissez l'une des trois méthodes de contrôle de l'étendue administrative :

- Portée à AWS l'ensemble de l'organisation (toutes les unités d'organisation et tous les comptes) — Aucune autre définition n'est requise.
 - Portez sur AWS l'ensemble de l'organisation, mais excluez des unités d'organisation et des comptes spécifiques : deux sous-volets apparaissent, l'un pour les unités organisationnelles et l'autre pour les comptes. Choisissez Ajouter des unités d'organisation pour ouvrir la fenêtre Ajouter des unités organisationnelles, puis choisissez Ajouter des unités d'organisation. Pour ajouter des comptes individuels, dans le sous-volet Comptes, choisissez Ajouter des comptes, sélectionnez les comptes, puis choisissez Ajouter des comptes.
 - Ne vous limitez pas à AWS l'ensemble de l'organisation, incluez uniquement des unités d'organisation et des comptes spécifiques. Utilisez les mêmes sous-volets pour ajouter des unités d'organisation ou des comptes.
3. Sélectionnez ensuite les ressources dans le sous-volet Ressources. Dans la zone de sélection des types de ressources, sélectionnez tous les types de ressources AWS Shield Advanced ou certains d'entre eux. Pour AWS Shield Advanced, les options sont l'une ou l'ensemble des options suivantes :
- Application Load Balancer
 - CloudFront Distribution
 - Equilibreur de charge classique
 - Adresse IP Elastic
4. Pour chaque type de ressource sélectionné, choisissez l'une des options mutuellement exclusives suivantes :
- Inclure toutes les ressources
 - Inclure des ressources spécifiques
 - Exclure des ressources spécifiques
5. Si vous choisissez Inclure des ressources spécifiques, sélectionnez l'un des types d'expression suivants :
- Critères uniques

- Correspond à tous les critères (ET)
 - Répondez à tous les critères (OU)
 - NON
6. Chaque type d'expression prend en charge un ou plusieurs critères d'inclusion et ARN, ce qui vous permet de créer des combinaisons de balises ou d'ARN. Tous les types de ressources prennent en charge les critères d'inclusion des balises et des ARN. Si vous choisissez Tag, identifiez une clé et une valeur facultative. Vous pouvez identifier plusieurs balises.

 CloudFront Exigence de région

Pour protéger les ressources de CloudFront distribution, utilisez la région USA Est (Virginie du Nord) (us-east-1).

Pour créer un déploiement (console)

Un déploiement lie vos politiques à un périmètre et active leur application. AWS Network Security Manager applique ensuite vos protections DDoS AWS Shield Advanced aux ressources concernées.

Procédez comme suit :

1. Sur la page Vue d'ensemble, dans le volet Vue d'ensemble, choisissez Créer un déploiement.
2. Choisissez la politique que vous souhaitez déployer.
3. Choisissez l'étendue qui définit les comptes et les ressources auxquels AWS Network Security Manager applique la politique.
4. Dans Nom du déploiement, entrez un nom. (Facultatif) Sous Description, entrez une description.
5. (Facultatif) Pour rendre le déploiement visible pour les autres comptes de votre organisation, sélectionnez Activer la visibilité entre comptes pour ce déploiement.
6. (Facultatif) Pour ajouter des balises, choisissez Ajouter une nouvelle balise, puis entrez les combinaisons clé et valeur facultatives.
7. Choisissez Create and deploy (Créer et déployer). La page Déploiements apparaît, où vous pouvez voir les détails de ce que AWS Network Security Manager a créé.

 Les déploiements peuvent entraîner des frais

Un déploiement crée des services de sécurité réseau et les associe à une ressource protégée. AWS Network Security Manager facture les ressources protégées. Les services de sécurité eux-mêmes protègent la ressource, ce qui entraîne des frais supplémentaires. Avant de procéder au déploiement, consultez la page de [tarification de AWS Network Security Manager et la page](#) de [tarification de AWS Shield Advanced](#).

AWS Responsable de la sécurité réseau et AWS Firewall Manager

AWS Network Security Manager est le service qui remplace AWS Firewall Manager. Les deux sont des services totalement distincts, chacun doté de capacités uniques et d'un modèle de tarification différent. Si vous utilisez actuellement AWS Firewall Manager, vous n'avez aucune action à effectuer : vos pare-feux et vos politiques existants continuent de fonctionner. Ce chapitre décrit comment les deux services coexistent, comment fonctionne la priorité lorsque vous utilisez les deux et comment fonctionnera la migration lorsqu'elle sera disponible.

AWS Network Security Manager et AWS Firewall Manager fonctionnent côte à côte et indépendamment l'un de l'autre. À un moment donné, AWS Firewall Manager cessera d'être vendu, puis cessera de fonctionner.

Coexistence avec AWS Firewall Manager

AWS Network Security Manager n'affecte pas les pare-feux que vous avez créés avec AWS Firewall Manager, sauf si vous lancez une action pour les modifier. Les pare-feux et les politiques que vous avez créés avec AWS Firewall Manager continuent de fonctionner à moins que vous ne les résiliiez. Cela est vrai même après le retrait de AWS Firewall Manager.

Priorité lors de la correction

Pendant le fonctionnement des deux services, vous pouvez prendre des mesures qui affectent les pare-feux que vous avez créés avec AWS Firewall Manager. Lorsque vous créez des politiques AWS Network Security Manager, vous les appliquez à une étendue, qui est un ensemble de ressources cibles. Si cette étendue inclut des ressources déjà prises en charge par une politique de AWS Firewall Manager, AWS Network Security Manager a la priorité lors de la correction. Dans ce cas, la politique et le champ d'application de AWS Network Security Manager remplacent le AWS pare-feu et la politique de Firewall Manager existants. Le comportement spécifique dépend des options de résolution que vous sélectionnez.

Migration planifiée depuis AWS Firewall Manager

La migration de AWS Firewall Manager vers AWS Network Security Manager consolide la gestion de votre pare-feu en un seul service et vous permet d'utiliser ses fonctionnalités. La migration est prévue

mais n'est pas encore disponible. Lorsque la migration sera disponible, vous pourrez transférer vos politiques de AWS Firewall Manager vers AWS Network Security Manager. La migration nécessitera de nouvelles actions dans les deux services qui ne sont pas encore en place.

Le processus planifié copiera une politique sélectionnée depuis AWS Firewall Manager, la transférera vers AWS Network Security Manager et la traduira dans la nouvelle structure de politique. Ce processus n'affecte pas votre politique d'origine ni les pare-feux associés dans AWS Firewall Manager.

Sécurité dans AWS Responsable de la sécurité réseau

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le [modèle de responsabilité partagée](#) décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Third-party les auditeurs testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de [AWS conformité Programmes](#) de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Network Security Manager, voir [AWS Services concernés par programme de conformitéAWS](#) .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise, ainsi que la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de AWS Network Security Manager. Les rubriques suivantes expliquent comment configurer AWS Network Security Manager pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser les ressources de votre AWS Network Security Manager.

Rubriques

- [Protection des données dans AWS Responsable de la sécurité réseau](#)
- [Gestion des identités et des accès pour AWS Responsable de la sécurité réseau](#)
- [Utilisation de rôles liés à un service pour AWS Responsable de la sécurité réseau](#)
- [Validation de conformité pour AWS Responsable de la sécurité réseau](#)
- [Résilience dans AWS Responsable de la sécurité réseau](#)
- [Sécurité de l'infrastructure dans AWS Responsable de la sécurité réseau](#)
- [Bonnes pratiques en matière de sécurité pour AWS Responsable de la sécurité réseau](#)

Protection des données dans AWS Responsable de la sécurité réseau

Le modèle de [responsabilité AWS partagée \(modèle de \)](#) s'applique à la protection des données dans AWS Network Security Manager. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la [FAQ sur la confidentialité des données](#) et les . Pour plus d'informations sur la protection des données en Europe, consultez le [Centre du règlement général sur la protection des données \(RGPD\)](#).

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section [Utilisation des CloudTrail sentiers](#) dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez [Norme FIPS \(Federal Information Processing Standard\) 140-3](#).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que

le champ Nom. Cela inclut lorsque vous travaillez avec AWS Network Security Manager ou un autre outil Services AWS à l'aide de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement au repos

AWS Network Security Manager chiffre toutes les données inactives à l'aide des AWS clés du service de gestion des clés (AWS KMS). Service-managed Les clés KMS protègent les configurations de vos ressources, l'état de déploiement et les données de synchronisation. Il n'est pas nécessaire de configurer ou de gérer ces clés.

Chiffrement en transit

AWS Network Security Manager chiffre toutes les données en transit à l'aide du protocole TLS (Transport Layer Security). Toutes les demandes d'API nécessitent le protocole TLS 1.2 ou version ultérieure. Les connexions aux points de terminaison de l'API AWS Network Security Manager utilisent exclusivement le protocole HTTPS.

Gestion des clés

AWS Network Security Manager utilise des clés AWS KMS gérées par le service pour le chiffrement au repos. Vous ne pouvez pas fournir vos propres clés KMS pour le moment.

Gestion des identités et des accès pour AWS Responsable de la sécurité réseau

Gestion des identités et des accès AWS (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources de AWS Network Security Manager. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- [Public ciblé](#)
- [Authentification par des identités](#)
- [Gestion de l'accès à l'aide de politiques](#)
- [Comment ? AWS Network Security Manager fonctionne avec IAM](#)
- [Identity-based exemples de politiques pour AWS Responsable de la sécurité réseau](#)
- [Résolution des problèmes AWS Identité et accès du Network Security Manager](#)

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir [Résolution des problèmes AWS Identité et accès du Network Security Manager](#))
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir [Comment ? AWS Network Security Manager fonctionne avec IAM](#))
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir [Identity-based exemples de politiques pour AWS Responsable de la sécurité réseau](#))

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), d'une authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations sur la connexion, consultez [Connexion à votre Compte AWS](#) dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une CLI pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez [Signature AWS Version 4 pour les demandes d'API](#) dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez [Tâches qui requièrent les informations d'identification de l'utilisateur racine](#) dans le Guide de l'utilisateur IAM.

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à Services AWS l'aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur provenant de l'annuaire de votre entreprise, de votre fournisseur d'identité Web ou Directory Service qui y accède à Services AWS l'aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées assument des rôles qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Pour plus d'informations, consultez [Qu'est-ce que IAM Identity Center ?](#) dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un [utilisateur IAM](#) est une identité qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir [Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires](#) dans le guide de l'utilisateur IAM.

[Les groupes IAM](#) spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez [Cas d'utilisation pour les utilisateurs IAM](#) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un [rôle IAM](#) est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en [passant d'un rôle d'utilisateur à un rôle IAM \(console\)](#) ou en appelant une opération d' AWS API AWS CLI ou d'API. Pour plus d'informations, consultez [Méthodes pour endosser un rôle](#) dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez [Vue d'ensemble des politiques JSON](#) dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Identity-based politiques

Identity-based les politiques sont des documents de politique d'autorisation JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez [Définition d'autorisations IAM personnalisées avec des politiques gérées par le client](#) dans le Guide de l'utilisateur IAM.

Identity-based les politiques peuvent être des politiques intégrées (intégrées directement dans une seule identité) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et en ligne, consultez [Choix entre les politiques gérées et les politiques en ligne](#) dans le Guide de l'utilisateur IAM.

Resource-based politiques

Resource-based les politiques sont des documents de politique JSON que vous attachez à une ressource. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de

compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Vous devez [spécifier un principal](#) dans une politique basée sur les ressources.

Resource-based les politiques sont des politiques intégrées qui se trouvent dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez [Limites d'autorisations pour des entités IAM](#) dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) : spécifient les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez [Politiques de contrôle de service](#) dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCP) : définissent les autorisations maximales disponibles pour les ressources de votre organisation. Pour plus d'informations, consultez [Politiques de contrôle des ressources \(RCP\)](#) dans le Guide de l'utilisateur AWS Organizations .
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez [Politiques de session](#) dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section [Logique d'évaluation des politiques](#) dans le guide de l'utilisateur IAM.

Comment ? AWS Network Security Manager fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à AWS Network Security Manager, découvrez quelles fonctionnalités IAM peuvent être utilisées avec AWS Network Security Manager.

Fonctionnalité IAM	AWS Support pour les responsables de la sécurité réseau
Identity-based politiques	Oui
Resource-based politiques	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique	Oui
ACL	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Rôles de service	Oui
Service-linked rôles	Oui

Pour obtenir une vue d'ensemble de la façon dont AWS Network Security Manager et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section [AWS Services compatibles avec IAM](#) dans le Guide de l'utilisateur IAM.

Identity-based politiques pour AWS Responsable de la sécurité réseau

Prend en charge les politiques basées sur l'identité : oui

Identity-based les politiques sont des documents de politique d'autorisation JSON que vous pouvez associer à une identité, telle qu'un utilisateur IAM, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez [Définition d'autorisations IAM personnalisées avec des politiques gérées par le client](#) dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez [Références des éléments de politique JSON IAM](#) dans le Guide de l'utilisateur IAM.

Resource-based politiques au sein de AWS Responsable de la sécurité réseau

Prend en charge les politiques basées sur les ressources : non

Resource-based les politiques sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez [spécifier un principal](#) dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. Pour plus d'informations, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

AWS Network Security Manager ne prend pas en charge les politiques basées sur les ressources.

Actions politiques pour AWS Responsable de la sécurité réseau

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions de AWS Network Security Manager, voir [Actions définies par AWS Network Security Manager](#) dans la référence d'autorisation de service.

Les actions de stratégie dans AWS Network Security Manager utilisent le préfixe suivant avant l'action :

```
network-security-manager
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

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

AWS Network Security Manager définit les actions IAM pour tous ses types de ressources. Il s'agit notamment des opérations de création, de lecture, de mise à jour et de suppression (CRUD) pour les règles, les modèles, les politiques, les étendues et les déploiements, ainsi que des opérations de capture instantanée, de balisage, d'administration, d'état de synchronisation et d'association de ressources.

Ressources politiques pour AWS Responsable de la sécurité réseau

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son [Amazon Resource Name \(ARN\)](#). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour consulter la liste des types de ressources AWS Network Security Manager et leurs ARN, consultez la section [Ressources définies par AWS Network Security Manager](#) dans la référence d'autorisation de service. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, voir [Actions définies par AWS Network Security Manager](#).

AWS Network Security Manager définit un type de ressource IAM pour chacune de ses ressources (règle, modèle, politique, étendue et déploiement), ainsi qu'un type de snapshot pour chacune d'entre elles (par exemple, `rule-snapshot`). Le format ARN est le suivant :

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

Les ARN brouillons : DRAFT et les ARN instantanés ajoutent le numéro de version (par exemple, `. : 3`) :

Les brouillons ne sont pas des types de ressources IAM distincts. Pour l'autorisation, un brouillon est traité comme un enfant de sa ressource active, qui est le parent. Un ARN : DRAFT qualifié autorise la ressource active, de sorte que l'autorisation d'agir sur un brouillon provient de l'autorisation d'agir sur cette ressource active.

Les instantanés sont différents des brouillons. Chaque instantané possède son propre type de ressource IAM, de sorte qu'un ARN qualifié par version autorise directement ce type de ressource instantané, et non la ressource active parent.

Clés de conditions de politique pour AWS Responsable de la sécurité réseau

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. Vous pouvez créer des expressions conditionnelles qui utilisent des [opérateurs de condition](#), tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande. Pour voir toutes les clés de condition AWS globales, voir les clés de [contexte de condition AWS globales](#) dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition de AWS Network Security Manager, voir [Clés de condition pour AWS Network Security Manager](#) dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, voir [Actions définies par AWS Network Security Manager](#).

AWS Network Security Manager prend en charge les clés de condition de balise AWS globales suivantes pour le contrôle d'accès basé sur les attributs (ABAC) :

- `aws:ResourceTag/${TagKey}`

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

Tag-based les clés de condition s'appliquent aux ressources actives et aux instantanés. Les brouillons de ressources ne sont pas balisables et ne prennent pas en charge `aws:ResourceTag` les conditions.

ACL dans AWS Responsable de la sécurité réseau

Prend en charge les ACL : non

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

AWS Network Security Manager ne prend pas en charge les listes de contrôle d'accès (ACL).

ABAC avec AWS Responsable de la sécurité réseau

Prise en charge d'ABAC (balises dans les politiques) : Oui

Attribute-based le contrôle d'accès (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction d'attributs appelés balises. Vous pouvez associer des balises aux entités et aux AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de la ressource.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans [l'élément de condition](#) d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur ABAC, consultez [Définition d'autorisations avec l'autorisation ABAC](#) dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez [Utilisation du contrôle d'accès par attributs \(ABAC\)](#) dans le Guide de l'utilisateur IAM.

AWS Network Security Manager prend en charge le contrôle d'accès basé sur les attributs à l'aide des trois clés de condition de balise AWS globales. Vous pouvez restreindre l'accès aux ressources de AWS Network Security Manager en fonction des balises associées à ces ressources.

Utilisation d'informations d'identification temporaires avec AWS Responsable de la sécurité réseau

Prend en charge les informations d'identification temporaires : oui

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez [Informations d'identification de sécurité temporaires dans IAM](#) et [Services AWS compatibles avec IAM](#) dans le Guide de l'utilisateur IAM.

Cross-service autorisations principales pour AWS Responsable de la sécurité réseau

Prend en charge les sessions d'accès direct (FAS) : oui

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant et Service AWS, combinées Service AWS à la demande d'envoi de demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section [Sessions de transmission d'accès](#).

Rôles de service pour AWS Responsable de la sécurité réseau

Prend en charge les rôles de service : oui

Un rôle de service est un [rôle IAM](#) qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez [Création d'un rôle pour la délégation d'autorisations à un Service AWS](#) dans le Guide de l'utilisateur IAM.

Warning

La modification des autorisations associées à un rôle de service peut perturber les fonctionnalités de AWS Network Security Manager. Modifiez les rôles de service uniquement lorsque AWS Network Security Manager fournit des instructions à cet effet.

Service-linked rôles pour AWS Responsable de la sécurité réseau

Prend en charge les rôles liés à un service : oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut assumer le rôle d'effectuer une action en votre nom. Service-linked les rôles apparaissent dans votre fichier Compte AWS et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

AWS Network Security Manager utilise un rôle lié à un service pour opérer sur les comptes des membres de votre organisation. AWS Network Security Manager crée automatiquement le rôle lié au service lorsque vous activez le service. Le rôle accorde à AWS Network Security Manager l'autorisation de gérer les ressources AWS WAF et AWS Shield Advanced. Le rôle accorde également l'accès à AWS Config pour la découverte de ressources et l'autorisation d'effectuer des opérations entre comptes.

Pour plus de détails sur la création et la gestion des rôles liés au service AWS Network Security Manager, consultez [the section called “Service-linked rôles”](#)

Identity-based exemples de politiques pour AWS Responsable de la sécurité réseau

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources AWS Network Security Manager. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez [Création de politiques IAM \(console\)](#) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par AWS Network Security Manager, y compris le format des ARN pour chacun des types de ressources, voir [Actions, ressources et clés de condition pour AWS Network Security Manager](#) dans la référence d'autorisation de service.

Rubriques

- [Bonnes pratiques en matière de politiques](#)
- [Utilisation de AWS Console Network Security Manager](#)
- [Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations](#)
- [Read-only accès à AWS Responsable de la sécurité réseau](#)

- [Gérer les règles et les modèles uniquement](#)

Bonnes pratiques en matière de politiques

Identity-based les politiques déterminent si quelqu'un peut créer, accéder ou supprimer des ressources AWS Network Security Manager dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez [politiques gérées par AWS](#) ou [politiques gérées par AWS pour les activités professionnelles](#) dans le Guide de l'utilisateur IAM.
- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez [politiques et autorisations dans IAM](#) dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que CloudFormation. Pour plus d'informations, consultez [Conditions pour éléments de politique JSON IAM](#) dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez [Validation de politiques avec IAM Access Analyzer](#) dans le Guide de l'utilisateur IAM.

- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez [Sécurisation de l'accès aux API avec MFA](#) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez [Bonnes pratiques de sécurité dans IAM](#) dans le Guide de l'utilisateur IAM.

Utilisation de AWS Console Network Security Manager

Pour accéder à la console AWS Network Security Manager, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher des informations détaillées sur les ressources AWS Network Security Manager de votre Compte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour accéder à la console AWS Network Security Manager, un principal a besoin d'autorisations minimales pour les `network-security-manager:Get*` actions `network-security-manager:List*` et.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or 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 accès à AWS Responsable de la sécurité réseau

La politique suivante accorde un accès principal en lecture seule à toutes les ressources de AWS Network Security Manager. Cela est utile pour les auditeurs ou les rôles de surveillance qui ont besoin de consulter les configurations et l'état de synchronisation sans apporter de modifications.

```

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

```

```

    }
  ]
}

```

Gérer les règles et les modèles uniquement

La politique suivante permet à un directeur de créer, de mettre à jour et de supprimer des règles et des modèles, sans accorder l'accès aux politiques, aux étendues ou aux déploiements. Cela est utile pour les équipes qui créent des configurations de sécurité mais n'en contrôlent pas l'application.

```

{
  "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": "*"
    }
  ]
}

```

Résolution des problèmes AWS Identité et accès du Network Security Manager

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation de AWS Network Security Manager et d'IAM.

Rubriques

- [Je ne suis pas autorisé à effectuer une action dans AWS Responsable de la sécurité réseau](#)
- [Je ne suis pas autorisé à effectuer iam : PassRole](#)
- [Je souhaite autoriser des personnes extérieures à mon Compte AWS pour accéder à mon AWS Ressources pour le responsable de la sécurité réseau](#)

Je ne suis pas autorisé à effectuer une action dans AWS Responsable de la sécurité réseau

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM mateojackson tente d'utiliser la console pour afficher des informations détaillées sur une ressource *my-example-widget* fictive, mais ne dispose pas des autorisations `network-security-manager:GetWidget` fictives.

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

Dans ce cas, la politique qui s'applique à l'utilisateur mateojackson doit être mise à jour pour autoriser l'accès à la ressource *my-example-widget* à l'aide de l'action `network-security-manager:GetWidget`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole` action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à AWS Network Security Manager.

Certains services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, vous devez disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans AWS Network Security Manager. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary n'est pas autorisée à transmettre le rôle au service.

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

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à mon Compte AWS pour accéder à mon AWS Ressources pour le responsable de la sécurité réseau

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si AWS Network Security Manager prend en charge ces fonctionnalités, consultez [Comment ? AWS Network Security Manager fonctionne avec IAM](#).
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section [Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez](#) dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section [Fournir un accès à des ressources Comptes AWS détenues par des tiers](#) dans le guide de l'utilisateur IAM.

- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez [Fournir un accès à des utilisateurs authentifiés en externe \(fédération d'identité\)](#) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

Utilisation de rôles liés à un service pour AWS Responsable de la sécurité réseau

AWS Network Security Manager utilise des rôles liés au [service](#) IAM. Un rôle lié à un service est un type unique de rôle IAM directement lié à AWS Network Security Manager. Service-linked les rôles sont prédéfinis par AWS Network Security Manager et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration de AWS Network Security Manager, car il n'est pas nécessaire d'ajouter manuellement les autorisations nécessaires. AWS Network Security Manager définit les autorisations associées à ses rôles liés aux services. Sauf indication contraire, seul le AWS Network Security Manager peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisations. Vous ne pouvez associer cette politique d'autorisation à aucune autre entité IAM.

Vous ne pouvez supprimer un rôle lié à un service qu'après avoir d'abord supprimé les ressources associées. Cela protège les ressources de votre AWS Network Security Manager, car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez la section [AWS Services qui fonctionnent avec IAM](#) et recherchez les services dont la valeur est Oui dans la Service-linked colonne des rôles. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Service-linked autorisations de rôle pour AWS Responsable de la sécurité réseau

AWS Network Security Manager utilise le rôle lié au service nommé.

`AWSServiceRoleForNetworkSecurityManager` Ce rôle lié au service fait confiance au principal du `network-security-manager.amazonaws.com` service pour assumer le rôle.

La politique d'autorisations de rôle nommée `NetworkSecurityManagerServiceRolePolicy` est une politique AWS gérée qui permet à AWS Network Security Manager d'effectuer des actions sur les ressources spécifiées.

La politique de confiance suivante permet au directeur du `network-security-manager.amazonaws.com` service d'assumer le rôle.

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

Note

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez les [autorisations relatives aux Service-linked rôles](#) dans le guide de l'utilisateur IAM.

Détails de l'autorisation

AWS Network Security Manager a besoin de chaque groupe d'autorisations pour protéger et découvrir les ressources de votre compte et de votre organisation. La politique `NetworkSecurityManagerServiceRolePolicy` gérée accorde les autorisations suivantes, regroupées par service :

- **wafv2**— Créez, lisez, mettez à jour et supprimez des ACL Web et des groupes de règles Firewall Manager. Associez et dissociez les ACL Web aux ressources protégées. Gérez les configurations de journalisation des ACL Web et les politiques d'autorisation des groupes de règles. Marquez et décochez les ressources. Validez les configurations de l'ACL et des règles Web de AWS Network Security Manager.

- `shield`— Créez, décrivez, listez et supprimez les protections AWS Shield Advanced. Créez et décrivez l'abonnement AWS Shield Advanced.
- `elasticloadbalancing`— Décrivez les équilibreurs de charge et les balises d'application. Créez, supprimez et définissez des associations ACL Web sur les équilibreurs de charge d'application.
- `cloudfront`— Obtenez et listez les CloudFront distributions, les configurations et les tags Amazon. Associez et dissociez les ACL Web de distribution. Lisez les origines du VPC.
- `apigateway`— Lisez les API REST, les étapes et les balises d'Amazon API Gateway. Définissez l'ACL Web sur une scène d'API.
- `ec2`— Lisez les ACL et les associations Web des instances Amazon EC2 Verified Access. Décrivez les adresses IP Elastic pour la protection AWS Shield Advanced.
- `cognito-idp`, `apprunner`, `appsync`, `amplify`, et `bedrock-agentcore` — Lisez les associations ACL Web pour les groupes d'utilisateurs Amazon Cognito, les AWS App Runner services, les API AWS AppSync GraphQL, AWS Amplify les applications et les AgentCore passerelles Amazon Bedrock afin que AWS Network Security Manager puisse découvrir les ressources protégées.
- `config`— Sélectionnez les configurations de ressources et gérez l'enregistreur de AWS Config configuration lié au service que AWS Network Security Manager utilise pour découvrir les ressources concernées.
- `organizations`— Lisez votre organisation, vos comptes, vos racines, vos unités organisationnelles et vos administrateurs délégués afin que AWS Network Security Manager puisse fonctionner dans l'ensemble de votre organisation.
- `logs`— Créez, lisez, mettez à jour, supprimez et listez les livraisons de journaux pour la journalisation des ACL Web.
- `s3`— Obtenez et placez des politiques de compartiment sur les compartiments Amazon S3 dont le nom commence par `aws-waf-logs-` afin que les journaux ACL Web puissent être envoyés.
- `iam`— Créez les rôles liés aux services requis par AWS Shield Advanced et AWS WAF AWS Config, dans le cadre de la clé de condition. `iam:AWSServiceName`

Le JSON suivant montre la politique `NetworkSecurityManagerServiceRolePolicy` d'autorisation complète.

```
{
  "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::*:vpccorigin/*"
},
{
  "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"
    }
  }
}
]
```

Création d'un rôle lié à un service pour AWS Responsable de la sécurité réseau

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous activez AWS Network Security Manager, AWS Network Security Manager crée le rôle lié au service pour vous. Il n'y a aucune étape manuelle à effectuer.

Si vous supprimez ce rôle lié à un service et que vous devez le créer à nouveau, AWS Network Security Manager le recréera la prochaine fois que vous utiliserez le service. Vous n'avez rien à faire.

Pour plus d'informations, consultez [Création d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Modification d'un rôle lié à un service pour AWS Responsable de la sécurité réseau

Vous ne pouvez pas modifier les autorisations du rôle

`AWSServiceRoleForNetworkSecurityManager` lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM.

Pour plus d'informations, consultez [Modification d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS Responsable de la sécurité réseau

Si vous n'avez plus besoin d'utiliser AWS Network Security Manager, nous vous recommandons de supprimer le rôle `AWSServiceRoleForNetworkSecurityManager` lié à un service.

Avant de supprimer le rôle lié à un service, nettoyez les ressources gérées par AWS Network Security Manager. Désactivez AWS Network Security Manager et supprimez les politiques et les champs d'application afin qu'aucune ressource gérée par AWS Network Security Manager ne reste dans votre compte. Vous pouvez ensuite supprimer le rôle manuellement.

Note

Si AWS Network Security Manager utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le panneau de navigation, choisissez Rôles.
3. Dans la zone de recherche `AWSServiceRoleForNetworkSecurityManager`, entrez, puis sélectionnez le rôle.
4. Sélectionnez Supprimer.
5. Pour confirmer la suppression, entrez le nom du rôle, puis choisissez Supprimer.

Pour plus d'informations, consultez la section [Suppression d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Régions prises en charge pour AWS Rôles liés au service Network Security Manager

AWS Network Security Manager prend en charge l'utilisation de rôles liés aux services dans toutes les AWS régions où AWS Network Security Manager est disponible.

Validation de conformité pour AWS Responsable de la sécurité réseau

Notre nouvelle expérience AWS d'inscription n'est pas conçue pour les charges de travail réglementées. Si vous utilisez notre nouvelle expérience d' AWS inscription, mais que vous souhaitez l'utiliser AWS pour des charges de travail réglementées, vous pouvez vous [inscrire à des fonctionnalités AWS \(avancées\)](#) ou [activer des fonctionnalités avancées](#) pour votre AWS environnement.

Pour savoir si un [programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité](#) spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de [AWS conformité Programmes AWS](#) de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir [Téléchargement de rapports dans AWS Artifact](#) .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. Pour plus d'informations sur votre responsabilité en matière de conformité lors de l'utilisation Services AWS, consultez [AWS la documentation de sécurité](#).

Résilience dans AWS Responsable de la sécurité réseau

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section [Infrastructure AWS globale](#).

Outre l'infrastructure AWS mondiale, AWS Network Security Manager propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données.

Sécurité de l'infrastructure dans AWS Responsable de la sécurité réseau

En tant que service géré, AWS Network Security Manager est protégé par les procédures de sécurité du réseau AWS mondial décrites dans le livre blanc [Amazon Web Services : présentation des processus de sécurité](#).

Vous utilisez des appels d'API AWS publiés pour accéder à AWS Network Security Manager via le réseau. Les clients doivent supporter le protocole TLS (Sécurité de la couche transport) 1.0 ou une version ultérieure. Nous vous recommandons le certificat TLS 1.2 ou une version ultérieure. Les clients doivent également prendre en charge les suites de chiffrement à parfaite confidentialité (PFS) telles que DHE (Ephemeral) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser [AWS Security Token Service](#) (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Bonnes pratiques en matière de sécurité pour AWS Responsable de la sécurité réseau

Les meilleures pratiques suivantes vous aident à maintenir une configuration sécurisée de AWS Network Security Manager.

Contrôles préventifs

- Utiliser le moindre privilège IAM : accordez uniquement les autorisations nécessaires à chaque utilisateur ou rôle pour effectuer ses tâches AWS Network Security Manager. Utilisez les clés de condition IAM pour restreindre l'accès à des ressources spécifiques lorsque cela est possible.
- Utiliser des rôles liés à un service : AWS Network Security Manager utilise des rôles liés à un service pour effectuer des actions en votre nom. Ces rôles sont dotés d'autorisations prédéfinies limitées à l'accès minimum requis.
- Configurez les étendues avec soin : définissez des configurations d'étendues qui ciblent uniquement les comptes et les types de ressources nécessitant une protection. Des champs d'application trop larges peuvent entraîner une application involontaire.

Contrôles de détection

- Activer la AWS CloudTrail journalisation : CloudTrail enregistre tous les appels d'API de AWS Network Security Manager. Consultez ces journaux pour savoir qui a modifié vos configurations de sécurité et à quel moment.
- Surveillez l'état de synchronisation : vérifiez régulièrement l'état de synchronisation de vos déploiements afin d'identifier les ressources qui ne sont pas synchronisées par rapport à la posture de sécurité que vous souhaitez adopter.

Contrôle AWS Responsable de la sécurité réseau

Le Monitoring AWS Network Security Manager vous aide à déterminer si vos ressources sont protégées comme prévu. AWS Network Security Manager fournit les fonctionnalités de surveillance suivantes :

- API d'état de synchronisation : interrogez l'état de protection des ressources individuelles dans l'ensemble de vos déploiements.
- AWS CloudTrail-- Enregistrez tous les appels d'API AWS Network Security Manager à des fins d'audit, de conformité et de résolution des problèmes opérationnels.

Surveillance de l'état de synchronisation

Le principal moyen de vérifier si vos ressources sont protégées consiste à utiliser les API d'état de synchronisation. AWS Network Security Manager évalue chaque ressource concernée et enregistre si la configuration réelle de son pare-feu correspond à la configuration prévue.

Opérations d'état de synchronisation

AWS Network Security Manager propose deux opérations pour demander l'état de synchronisation :

ListResourceSynchronizationStatuses

Renvoie le statut par ressource pour un déploiement spécifique. Nécessite un `deploymentIdentifier` paramètre. Filtrez éventuellement par `synchronizationStatus` (IN_SYNC, OUT_OF_SYNC ou NOT_APPLICABLE).

ListAggregateResourceSynchronizationStatuses

Renvoie le statut agrégé par ressource pour tous vos déploiements. Filtrez éventuellement par `synchronizationStatus`. Cette opération montre le résultat combiné de toutes les politiques qui s'appliquent à chaque ressource.

Les deux opérations prennent en charge la pagination avec `maxResults` (1 à 100) et `nextToken`.

Comprendre les valeurs d'état de synchronisation

SYNCHRONISÉ

La configuration réelle du pare-feu de la ressource correspond à la configuration effective calculée à partir de toutes les politiques applicables.

DÉSYNCHRONISÉ

La configuration réelle de la ressource est différente de la configuration effective. Le `outOfSyncReasons` champ fournit des détails par paramètre indiquant les valeurs attendues par rapport aux valeurs réelles.

NOT_APPLICABLE

Le compte et le type de ressource de la ressource sont concernés, mais la ressource elle-même ne correspond pas aux filtres de portée (par exemple, un filtre de balises l'exclut). Aucune action n'est nécessaire.

Si aucune ressource n'apparaît dans les résultats, le compte ou le type de ressource n'est pas concerné par le déploiement. Vérifiez la configuration de votre oscilloscope.

Comprendre les horodatages d'évaluation

Chaque entrée d'état de synchronisation inclut deux horodatages :

- `evaluatedAt`-- Date à laquelle AWS Network Security Manager a évalué la configuration de la ressource pour la dernière fois. Une `evaluatedAt` valeur périmée indique que l'évaluation des modifications récentes n'a pas encore été effectuée.
- `updatedAt`-- Date à laquelle l'enregistrement d'état de synchronisation lui-même a été modifié pour la dernière fois. S'`updatedAt` est plus ancien que `evaluatedAt`, le statut est stable depuis la dernière évaluation.

Cross-account visibilité

Lorsque plusieurs administrateurs protègent la même ressource, la visibilité de l'état de synchronisation agrégé dépend du `enableCrossAccountVisibility` paramètre de chaque déploiement.

- Si la visibilité entre comptes est activée pour tous les déploiements couvrant une ressource, tout administrateur peut consulter l'état global complet et les raisons de la désynchronisation.
- Si la visibilité entre comptes est désactivée pour un déploiement, les autres administrateurs voient un NOT_VISIBLE marqueur plutôt que des raisons détaillées. Cela indique qu'un autre administrateur protège également la ressource mais n'a pas partagé la visibilité.

Diagnostic des ressources désynchronisées

Lorsqu'une ressource indique OUT_OF_SYNC, le `outOfSyncReasons` champ identifie les différences de configuration spécifiques. La principale raison est l'une des suivantes :

- `missingFirewall`-- Aucune protection par pare-feu n'est associée à la ressource.
- `invalidFirewall`-- Un pare-feu existe mais sa configuration ne correspond pas aux attentes. Les différences spécifiques sont répertoriées dans des compartiments classés par catégories.

Si la correction est activée mais ne peut pas réparer la ressource, le `remediationIssues` champ fournit `correctiveAction` des instructions sur la manière de résoudre le problème manuellement. La correction est un paramètre de niveau politique qui est désactivé par défaut. Pour plus d'informations, consultez [the section called "Synchronisation et correction"](#).

Plusieurs déploiements avec différentes configurations peuvent cibler la même ressource. Dans ce cas, l'état de synchronisation par déploiement peut être OUT_OF_SYNC tandis que le statut de synchronisation agrégé est IN_SYNC. Il s'agit d'un comportement attendu et non d'un échec. Les paramètres d'une politique de priorité plus élevée étaient prioritaires lors de la fusion. Par conséquent, la ressource correspond à la configuration effective, même si elle ne correspond pas à la configuration du déploiement de priorité inférieure.

Logging AWS Appels d'API Network Security Manager avec AWS CloudTrail

AWS Network Security Manager est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service. CloudTrail capture tous les appels d'API pour AWS Network Security Manager en tant qu'événements de gestion. Les appels capturés incluent des appels provenant de la console AWS Network Security Manager et des appels programmatiques vers les opérations de l'API AWS Network Security Manager.

Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour AWS Network Security Manager. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. Pour plus d'informations, consultez le [Guide de l'utilisateur AWS CloudTrail](#).

AWS Informations relatives au Network Security Manager dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans AWS Network Security Manager, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section [Affichage des événements à l'aide de l'historique des CloudTrail événements](#).

Pour un enregistrement continu des événements survenus dans votre environnement Compte AWS, y compris ceux relatifs à AWS Network Security Manager, créez une trace. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition. Il fournit les fichiers journaux au compartiment Amazon S3 que vous spécifiez. Vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- [Présentation de la création d'un journal de suivi](#)
- [CloudTrail services et intégrations pris en charge](#)
- [Configuration des notifications Amazon SNS pour CloudTrail](#)

Toutes les opérations de AWS Network Security Manager sont enregistrées par CloudTrail. Les opérations publiques sont notamment les suivantes :

- Opérations de création, de lecture, de mise à jour et de suppression (CRUD) pour les règles, les modèles, les politiques, les étendues et les déploiements
- Opérations instantanées
- Opérations de balisage
- Opérations du compte administrateur
- Opérations d'état de synchronisation

- Opérations des associations de ressources
- Opérations de génération de règles

Chaque inscription à un événement inclut les informations suivantes :

- La source de l'événement : `network-security-manager.amazonaws.com`
- Le nom de l'événement, qui est le nom de l'opération d'API (par exemple, `CreatePolicy` ou `ListDeployments`)
- Les ressources concernées, identifiées par l'ARN et le type de ressource

Read-only les opérations (telles que `GetPolicyListRules`, `etListResourceSynchronizationStatuses`) sont enregistrées `readOnly: true` et n'incluent pas d'éléments de réponse. Les opérations de mutation incluent les paramètres de demande et les éléments de réponse.

Note

CloudTrail expédie les champs sensibles des enregistrements d'événements. Par exemple, CloudTrail expédie le prompt paramètre dans l'`GenerateRuleConfiguration` opération.

Exemple : CreatePolicy événement

L'exemple suivant montre une entrée de CloudTrail journal pour l'`CreatePolicy` opération.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROEXAMPLEID:my-session",
    "arn": "arn:aws:sts::123456789012:assumed-role/AdminRole/my-session",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEID",
        "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 Quotas du Network Security Manager

Vous Compte AWS disposez des quotas par défaut suivants pour AWS Network Security Manager. Sauf indication contraire, chaque quota est par compte, par région.

Quotas de ressources

Le tableau suivant répertorie le nombre maximum de ressources AWS Network Security Manager que vous pouvez créer par compte dans chaque région.

Ressource	Quota par défaut	Ajustable
Règles par compte	200	Non
Modèles par compte	100	Non
Stratégies par compte	100	Non
Étendue par compte	100	Non
Déploiements par compte	100	Non
Instantanés par ressource	10	Non

Quotas de composition des ressources

Le tableau suivant répertorie les quotas relatifs à la manière dont les ressources AWS Network Security Manager se réfèrent les unes les autres au sein de la hiérarchie des ressources.

Quota	Value
Règles par modèle	1 à 50
Modèles par politique AWS WAF	1 à 2
Règles et modèles combinés conformément à la AWS politique WAF	1 à 100

Quota	Value
Modèles ou règles conformes à la politique AWS Shield Advanced	0 (doit être vide)
Politiques par déploiement	1 à 2
Étendue par déploiement	1 (exactement un)

Quotas de configuration du périmètre

Le tableau suivant répertorie les quotas pour les expressions de configuration de portée.

Quota	Value
Étendue des types de ressources par étendue	20
Profondeur de l'expression Scope (niveaux imbriqués)	2
Étendue de l'expression du champ d'application (critères par niveau)	20

Quotas de comptes d'administrateur

Le tableau suivant répertorie les quotas pour les niveaux de priorité des comptes d'administrateur AWS Network Security Manager.

Quota	Value
Niveaux de priorité des administrateurs	1 à 10

Quotas de pagination des API

Le tableau suivant répertorie les limites de pagination pour les opérations de liste.

Quota	Value
Nombre maximum de résultats par page (<code>maxResults</code>)	100
Nombre minimal de résultats par page (<code>maxResults</code>)	1

Ajustement des quotas

Les quotas indiqués dans les sections précédentes sont fixes et ne peuvent pas être augmentés pour le moment.

Historique du document pour AWS Guide du développeur de Network Security Manager

Le tableau suivant décrit les versions de documentation relatives à AWS Network Security Manager.

Modification	Description	Date
Première version	Publication initiale du guide du développeur de AWS Network Security Manager.	1 août 2026

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.