IBM QRadar Risk Manager
Version 7.1.0 (MR1)

Guide d'utilisation

Remarque : Avant d'utiliser les présentes informations et le produit associé, prenez connaissance des informations dans les sections “Avis et Marques” et page 194.

CONTENU

C MENTIONS ET MARQUES

INDEX

A PROPOS DU PRÉSENT GUIDE

Le manuel *IBM Security QRadar Risk Manager - Guide d'utilisation* fournit des informations sur l'installation, la configuration et l'utilisation de QRadar Risk Manager.

Audience visée

Ce guide est conçu pour l'administrateur système chargé de la configuration de IBM Security QRadar Risk Manager dans votre réseau. Ce manuel suppose que vous disposiez d'un accès administrateur à IBM Security QRadar SIEM, d'un accès administrateur à vos périphériques réseau et vos pare-feux et d'une connaissance de votre réseau d'entreprise et des technologies réseau.

Conventions de la documentation

Les conventions suivantes s'appliquent dans ce manuel :

▶ Indique que la procédure contient une seule instruction.

REMARQUE

Indique que les informations fournies viennent compléter la fonction ou l'instruction associée.

MISE EN GARDE

Indique que les informations sont capitales. Une mise en garde vous avertit de l'éventuelle perte de données ou d'un éventuel endommagement de l'application, du système, du périphérique ou du réseau.

AVERTISSEMENT

Indique que les informations sont capitales. Un avertissement vous informe des éventuels dangers, des éventuelles menaces ou des risques de blessure. Lisez attentivement tout ou partie des messages d'avertissement avant de poursuivre.

Documentation technique	Pour des informations sur l'accès à une documentation plus technique, à des notes techniques et à des notes sur l'édition, voir la note technique ***Accès aux notes techniques et à la documentation d'IBM Security QRadar***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)
Contacter le service clients	Pour savoir comment contacter le service clients, voir la note technique ***Note technique de support et de téléchargement***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)

1 IBM SECURITY QRADAR RISK MANAGER

IBM Security QRadar Risk Manager est un dispositif installé séparément pour contrôler les configurations d'unité, afin de simuler les changements apportés à votre environnement réseau et de classer les risques et les vulnérabilités par ordre de priorité sur votre réseau. Les fonctions de QRadar Risk Manager sont gérées grâce à votre console, dans l'onglet **Risks** de votre tableau de bord.

QRadar Risk Manager optimise l'utilisation des données collectées par IBM Security QRadar SIEM, des données de configuration provenant des périphériques réseau et de sécurité (pare-feux, routeurs, commutateurs ou systèmes de prévention contre les intrusions (IPS)), des flux de vulnérabilité et des sources de sécurité tierces. Toutes ces sources de données permettent à QRadar Risk Manager d'identifier les risques liés à la sécurité, aux règles et à la conformité dans vos infrastructures de sécurité des réseaux et de déterminer la probabilité de voir ces risques utilisés.

QRadar Risk Manager vous alerte proactivement de la découverte de risques. Ces risques sont affichés comme des violations sous l'onglet Offenses. Ces données sont analysées et consignées dans le contexte de toutes les autres données que QRadar SIEM traite. QRadar Risk Manager vous permet d'évaluer et de gérer les risques à un niveau acceptable en fonction de la tolérance aux risques définie par votre entreprise.

Vous pouvez également utiliser QRadar Risk Manager pour interroger toutes les connexions réseau, afficher et comparer la configuration des périphériques, afficher le modèle topologique de votre réseau et y appliquer des filtres, ainsi que simuler et prévoir les éventuels effets qu'aurait un changement de la configuration d'un périphérique ou des règles.

QRadar Risk Manager vous permet de définir un ensemble de politiques (ou de questions) sur votre réseau et de surveiller les changements qui peuvent y être apportés. Par exemple, si vous souhaitez refuser des protocoles non chiffrés provenant d'Internet dans votre zone démilitarisée (DMZ), vous pouvez définir une question Policy Monitor pour détecter les protocoles non chiffrés. Le fait de soumettre la question permet de retourner une liste de protocoles non chiffrés communiquant entre Internet et votre zone DMZ et vous permet de déterminer quels protocoles non chiffrés présentent des risques de sécurité. Une fois le niveau de risque acceptable défini, des alertes sont générées pour les nouveaux risques détectés dans le réseau.

QRadar Risk Manager comprend les composants suivants :

- Connections
- Moniteur de configuration
- Topologie
- Policy Monitor
- Simulation
- QRadar Risk Manager : Rapports

Connections

Utilisez la page Connections pour surveiller les connexions réseau des systèmes hôtes locaux. Vous pouvez exécuter les requêtes et les rapports sur les connexions réseau des hôtes locaux en fonction de toutes les applications, tous les ports, les protocoles et les sites Web avec lesquels les hôtes locaux ont communiqué.

La page Connections vous permet d'effectuer les opérations suivantes :

- Rechercher les connexions
- Rechercher un sous-ensemble de connexions (sous-recherche)
- Afficher les informations de connexion regroupées par diverses options
- Exporter les connexions en format XML ou CSV
- Utiliser le graphique interactif pour afficher les connexions au sein de votre réseau

Pour plus d'informations sur les connexions, voir la section Etude des connexions

Moniteur de configuration

Utilisez le Moniteur de configuration pour étudier et comparer la configuration des périphériques, vous permettant d'appliquer des politiques de sécurité et de surveiller les modifications apportées aux périphériques de votre réseau.

Les configurations de périphérique peuvent concerner les commutateurs, les routeurs, les pare-feux et les périphériques IPS de votre réseau. Pour chaque périphérique, vous pouvez afficher l'historique de configuration de périphérique, les interfaces et les règles. Vous pouvez également comparer les configurations dans un périphérique et entre plusieurs périphériques.

Les informations de configuration de périphérique sont également utilisées pour créer la représentation d'entreprise de votre topologie de réseau, ce qui vous permet de déterminer l'activité autorisée et refusée au sein de votre réseau. La configuration de périphérique vous permet d'identifier les incohérences et les changements de configuration présentant un risque pour votre réseau.

Pour plus d'informations sur les configurations de périphérique, voir la section **Afficher les configuration d'appareil**.

Topologie

La topologie est une représentation graphique décrivant la couche réseau (couche 3 du modèle OSI (Open Systems Interconnection)) de votre réseau en fonction des périphériques provenant de Configuration Source Management.

L'utilisation du graphique interactif de la topologie vous permet d'afficher les connexions entre les périphériques, les périphériques virtuels de sécurité des réseaux disposant de plusieurs contextes, les actifs, les périphériques de conversion d'adresses réseau (NAT), les indicateurs NAT et les informations sur les mappages NAT. Vous pouvez rechercher des événements, des périphériques ou des chemins d'accès et enregistrer des dispositions du réseau.

La topologie vous permet d'interroger la couche transport (couche 4) et de filtrer les chemins d'accès réseau en fonction du port et du protocole. Les informations de graphique et de connexion sont créées à partir des informations de configuration détaillées provenant des périphériques réseau tels que les pare-feux, les routeurs et les systèmes IPS.

Pour plus d'informations sur l'utilisation de la topologie, voir la section **Utilisation de la topologie.**

Policy Monitor

Utilisez la fonction Policy Monitor afin de définir des questions spécifiques sur les risques encourus par votre réseau et de soumettre ces questions à QRadar Risk Manager.

QRadar Risk Manager évalue les paramètres que vous avez définis dans votre question et retourne les actifs de votre réseau afin de vous aider à évaluer les risques. Les questions sont basées sur une série de tests pouvant être combinés et configurés si nécessaire. QRadar Risk Manager dispose de nombreuses questions Policy Monitor prédéfinies. Il est toutefois possible de créer des questions personnalisées. Il est possible de créer des questions Policy Monitor pour les situations suivantes :

- Communications ayant été établies ou
- Communications possibles basées sur la configuration des pare-feux ou des routeurs
- Règles de pare-feu réelles (tests de périphérique)

Policy Monitor utilise les données provenant des données de configuration, des données d'activité de réseau, des événements de réseau et de sécurité et des données d'analyse des vulnérabilités pour déterminer la réponse adéquate. QRadar Risk Manager dispose de modèles de règle pour vous aider à identifier les risques liés à la multiplicité des mandats réglementaires tels que PCI, HIPPA et ISO 27001 et déterminer les meilleures pratiques en matière de sécurité des informations. Vous pouvez mettre à jour les modèles pour les adapter à votre politique de sécurité informatique d'entreprise. Une fois la réponse traitée, vous

pouvez accepter la réponse à la question et définir la façon dont vous souhaitez que le système réponde aux résultats non validés.

Policy Monitor permet de surveiller activement jusqu'à 10 questions. Lorsqu'une question est surveillée, QRadar Risk Manager évalue en continu la question en attente de résultats non approuvés. A la découverte de résultats non approuvés, QRadar Risk Manager peut envoyer des courriers électroniques, afficher des notifications, générer un événement syslog ou créer une violation dans QRadar SIEM.

Pour plus d'informations sur Policy Monitor, voir la section **Utilisation de Policy Monitor**.

Simulation

Utilisez la simulation pour définir, planifier et réaliser des simulations d'utilisation sur votre réseau.

Vous pouvez créer une attaque simulée sur votre topologie en vous basant sur une série de paramètres configurés de manière identique à Policy Monitor. Vous pouvez créer une attaque simulée sur votre topologie de réseau actuelle ou créer un modèle de topologie. Un modèle de topologie est une topologie virtuelle qui vous permet d'apporter des modifications à la topologie virtuelle et de simuler une attaque. Cela vous permet de simuler la façon dont les modifications apportées aux règles de réseau, aux ports, aux protocoles ou aux connexions autorisées ou refusées peuvent affecter votre réseau. La simulation est un outil performant permettant de déterminer l'impact des risques des changements à apporter à votre configuration de réseau avant que ces changements ne soient implémentés.

Une fois une simulation terminée, vous pouvez vérifier les résultats. Si vous souhaitez valider les résultats, vous pouvez configurer le mode simulation, ce qui permet de définir la façon dont vous souhaitez répondre aux résultats non validés.

QRadar Risk Manager autorise la surveillance active de 10 simulations maximum. Lorsqu'une simulation est surveillée, QRadar Risk Manager analyse en continu la topologie en attente de résultats non approuvés. A la découverte de résultats non approuvés, QRadar Risk Manager peut envoyer des courriers électroniques, afficher des notifications, générer un événement syslog ou créer une violation dans QRadar SIEM.

Pour plus d'informations sur les simulations, voir la section **Utilisation des simulations**.

QRadar Risk Manager : Rapports

Utilisez l'onglet Reports pour afficher des rapports spécifiques en fonction des données disponibles dans QRadar Risk Manager, comme les connexions, les règles des périphériques et les objets de périphérique non utilisés.

Les options de rapport suivantes sont spécifiques à QRadar Risk Manager :

- **Connections** - Un rapport des connexions affiche le schéma de connexions de vos périphériques réseau établies au cours de votre intervalle de temps spécifié.
- **Device rules** - Le rapport sur les règles des périphériques affiche les règles configurées sur le périphérique réseau pendant l'intervalle de temps que vous avez indiqué. Vous pouvez afficher les types de règles suivants pour un ou plusieurs périphériques réseau à l'aide de cette option de rapport :
  - Règles d'acceptation les plus utilisées
  - Règles de refus les plus utilisées
  - Règles d'acceptation les moins utilisées
  - Règles de refus les moins utilisées
  - Règles grisées
  - Règles d'objet inutilisées
- **Device unused objects** - Le rapport sur les objets inutilisés de périphérique génère une table contenant le nom, la configuration, la date et l'heure, ainsi qu'une définition des groupes de références des objets qui ne sont pas utilisés sur le périphérique. Un groupe de références d'objet est un terme générique utilisé pour décrire une collection d'adresses IP, d'adresses CIDR, de noms d'hôtes, de ports ou d'autres paramètres de périphérique regroupés et affectés aux règles du périphérique.

Pour plus d'informations sur les rapports, voir la section Gestion des rapports IBM Security QRadar Risk Manager.

Navigateurs Web pris en charge

Vous pouvez accéder à la console à partir d'un navigateur Web standard. Lorsque vous accédez au système, une invite s'affiche demandant un nom d'utilisateur et un mot de passe, configurés à l'avance par l'administrateur QRadar SIEM.

Table 1-1 Navigateurs Web pris en charge

Navigateur Web	Versions prises en charge
Mozilla Firefox	• 10.0 Compte tenu du cycle d'édition court de Mozilla, nous ne pouvons nous engager à effectuer des tests sur les toutes dernières versions du navigateur Mozilla Firefox. Cependant, nous pouvons tout à fait enquêter sur les différents problèmes signalés.
Microsoft Windows Internet Explorer, avec vue de compatibilité activée	• 8.0 • 9.0 Pour obtenir des instructions sur la façon d'activer l'affichage de compatibilité, voir la section Activation de l'affichage de compatibilité dans Microsoft Internet Explorer.

Activation de l'affichage de compatibilité dans Microsoft Internet Explorer

Pour activer l'affichage de compatibilité dans les navigateurs Web Microsoft Internet Explorer :

Etape 1 Appuyez sur la touche F12 pour ouvrir la fenêtre Developer Tools.

Etape 2 Dans la zone de liste **Browser Mode**, sélectionnez la version de votre navigateur Web.

Etape 3 Dans la zone de liste **Document Mode**, sélectionnez la version de votre navigateur Web.

Etape 4 Fermez la fenêtre Developer Tools.

Connexion à IBM Security QRadar Risk Manager

Pour vous connecter à QRadar Risk Manager :

Etape 1 Ouvrez votre navigateur Web.

Etape 2 Entrez l'adresse suivante dans la barre d'adresse :

`https://<IP Address>`

Où **`<IP Address>`** correspond à l'adresse IP du système QRadar SIEM. QRadar Risk Manager se gère à l'aide de l'onglet **Risks** dans QRadar SIEM.

Etape 3 Entrez le nom d'utilisateur et le mot de passe par défaut.

Nom d'utilisateur : **`admin`**

Mot de passe : **`<password>`**

Où **`<password>`** correspond au mot de passe qui vous est affecté par votre réseau ou votre administrateur système QRadar SIEM. Si vous vous connectez et que vous ne voyez pas s'afficher l'onglet **Risks**, vérifiez que l'option User Role for Risk Manager est activée pour votre compte. Pour plus d'informations, voir le manuel *IBM Security QRadar Risk Manager - Guide d'installation*.

Etape 4 Cliquez sur **Login To QRadar**.

REMARQUE

Si vous utilisez un navigateur Web Mozilla Firefox, alors vous devez y ajouter une exception afin de pouvoir vous connecter à QRadar SIEM. Pour plus d'informations, voir votre documentation Mozilla Firefox. Si vous utilisez un navigateur Microsoft Internet Explorer, un message à propos du certificat de sécurité du site Web s'affiche. Vous devez sélectionner l'option **Continue to this website** pour vous connecter à QRadar SIEM.

Fonctions de IBM Security QRadar Risk Manager non prises en charge

QRadar Risk Manager ne prend pas en charge les fonctions suivantes :

- High Availability (HA)
- Dynamic Routing
  - Border Gateway Protocol (BGP)
  - Open Shortest Path First (OSPF)
  - Routing Information Protocol (RIP)
  - Intermediate System to Intermediate System (IS-IS)
- IPv6
- Masques de réseau non contigus
- Store and Forward

  La fonction Store and Forward vous permet de gérer les planifications des commandes de début et d'arrêt de transfert des événements des collecteurs d'événements dédiés vers les processeurs d'événement de votre déploiement. Cette fonction n'est pas prise en charge dans QRadar Risk Manager.

2 INTERFACE UTILISATEUR

Les administrateurs système interagissent avec IBM Security QRadar Risk Manager en triant les résultats, en interrogeant les adresses IP et en redimensionnant les colonnes.

Utilisez les options de navigation pour naviguer dans IBM Security QRadar SIEM. N'utilisez jamais le bouton **Back** du navigateur.

Tri des résultats

Grâce aux pages Connections, Moniteur de configuration, Policy Monitor, Simulations et Modèle de topologie, vous pouvez trier les tables dans l'ordre croissant ou décroissant en cliquant sur un en-tête de colonne.

Une flèche au dessus de la colonne indique la direction du tri. Cliquez sur l'en-tête pour alterner entre le tri décroissant et croissant des résultats.

Par exemple, pour trier les connexions par la zone **Last Packet Time**, procédez comme suit :

Cliquez sur l'en-tête de colonne Last Packet Time. Une flèche s'affiche sur l'en-tête de la colonne pour indiquer que les résultats sont triés par ordre décroissant. Cliquez à nouveau sur l'en-tête de colonne Last Packet Time pour trier les informations dans l'ordre croissant.

Interrogation des adresses IP

Vous pouvez cliquer avec le bouton droit de la souris sur les adresses IP d'un périphérique pour filtrer davantage les résultats affichés ou accéder à des informations supplémentaires. Par exemple, le fait de cliquer avec le bouton droit de la souris sur une adresse IP de la zone **Device IP** de la page Moniteur de configuration permet d'afficher les options figurant dans la **Table 2-2**.

Tableau 2-1 Options d'adresse IP

Menu	Sous-menu	Sous-menu	Description
Filter on	Sans objet	Sans objet	Vous permet de filtrer la connexion sélectionnée en fonction du paramètre sélectionné.
View Connection Events	Sans objet	Sans objet	Vous permet d'afficher les connexions pour l'adresse IP sélectionnée.

Tableau 2-1 Options d'adresse IP (suite)

Menu	Sous-menu	Sous-menu	Description
Options supplémentaires	Navigate	View By Network	Affiche la fenêtre List of Networks qui affiche l'activité du réseau auquel l'adresse IP est associée.
		View Source Summary	Affichage la fenêtre de récapitulatif des sources qui affiche toutes les violations associées à la source sélectionnée.
		View Destination Summary	Affichage la fenêtre de récapitulatif des destinations qui affiche toutes les violations associées à la destination sélectionnée.
	Information	DNS Lookup	Recherche les entrées DNS en fonction de l'adresse IP.
		WHOIS Lookup	Recherche le propriétaire enregistré d'une adresse IP distante. Le serveur système par défaut est whois.crsnic.net.
		Port Scan	Effectue une analyse NMAP de l'adresse IP sélectionnée. Cette option est uniquement disponible si NMAP est installé sur votre système. Pour plus d'informations sur l'installation de NMAP, consultez la documentation de votre fournisseur.
		Asset Profile	Affiche les informations de profil d'actif. Cette option de menu est uniquement disponible lorsque les données de profil ont été acquises soit de manière active (via une analyse), soit de manière passive (via des sources de flux). Pour plus d'informations, voir le manuel *QRadar - Guide d'administration.*
		Search Events	Vous permet de rechercher les événements.
		Search Flows	Vous permet de rechercher les flux.
		Search Connections	Vous permet de rechercher les connexions. Pour plus d'informations, consultez **Etude des connexions.**
		Switch Port Lookup	Vous permet de déterminer le port de commutation d'un périphérique Cisco IOS pour l'adresse IP sélectionnée. Cette option s'applique uniquement aux commutateurs reconnus à l'aide de l'option Discover Devices de Configuration Source Management. Pour plus d'informations, voir la section **Découvrir les périphériques**.
		View Topology	Vous permet d'afficher la topologie. Pour plus d'informations, voir le chapitre **Utilisation de la topologie**.
	TNC Recommendations		Vous permet de restreindre ou de refuser l'accès réseau aux utilisateurs en se basant sur le nom d'utilisateur ou d'autres données d'identification.

Pour plus d'informations sur la personnalisation du menu contextuel consultez la *Note technique sur la personnalisation du menu contextuel*.

Redimensionnement des colonnes

Vous pouvez redimensionner la largeur de la plupart des colonnes de table dans QRadar Risk Manager. Placez votre souris sur la ligne qui sépare les colonnes et glissez l'arête de la colonne vers la largeur choisie.

Les colonnes peuvent également être redimensionnées automatiquement en cliquant deux fois sur la ligne de séparation de deux colonnes. Cela permet de redimensionner la colonne à gauche de la ligne à la largeur de la plus grande valeur de données de la table.

3 CONFIGURATION DES PARAMÈTRES D'IBM SECURITY QRADAR RISK MANAGER

Vous pouvez configurer les paramètres d'accès pour QRadar Risk Manager via une administration de système basée sur le Web à partir de l'onglet **Admin** de IBM Security QRadar SIEM.

Si vous disposez des droits adéquats, vous pouvez configurer plusieurs paramètres de dispositif pour IBM Security QRadar Risk Manager via une administration de système basée sur le Web.

Les administrateurs peuvent effectuer les tâches suivantes :

- Configurer les unités auxquelles QRadar Risk Manager peut accéder par le pare-feu local. Pour plus d'informations, voir la section **Configuration d'un accès au pare-feu**.
- Mettre à jour le serveur de messagerie de QRadar Risk Manager. Pour plus d'informations, voir la section **Mise à jour de votre configuration QRadar Risk Manager**.
- Configurer les rôles d'interface d'un hôte. Pour plus d'informations, voir la section **Configuration des rôles d'interface utilisateur**.
- Changer le mot de passe d'un hôte. Pour plus d'informations, voir la section **Changement des mots de passe**.
- Mettre à jour l'heure système. Pour plus d'informations, voir la section **Mise à jour de l'heure système**.

Les changements de configuration réalisés par l'intermédiaire de l'administration de système par le Web sont effectués dès que vous les enregistrez ou les appliquez.

Configuration d'un accès au pare-feu

Vous pouvez configurer l'accès au pare-feu local pour QRadar Risk Manager, ce qui vous permet d'activer ou de désactiver les communications entre QRadar Risk Manager et les adresses IP spécifiques, les protocoles et les ports.

Vous pouvez également définir une liste d'adresses IP autorisées pour accéder à l'administration de système basée sur le Web. Par défaut, ces zones restent vides, ce qui ne restreint pas la communication avec QRadar Risk Manager. Cependant, lorsque vous ajoutez une adresse IP, seule cette adresse peut accéder au système. Toutes les autres adresses IP sont bloquées.

REMARQUE

Vous devez inclure l'adresse IP du bureau de client que vous utilisez pour accéder à QRadar Risk Manager. Le non-respect de cette instruction risque d'affecter la connectivité.

Pour configurer un accès au pare-feu dans QRadar Risk Manager, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Cliquez sur l'icône **System Management.**

Etape 4 Connectez-vous pour accéder à l'administration de système basée sur le Web.

Nom d'utilisateur : **`root`**

Mot de passe : **`<password>`**

Les zones de nom d'utilisateur et de mot de passe sont sensibles à la casse.

Etape 5 Dans le menu, sélectionnez **Managed Host Config > Local Firewall**.

Etape 6 Dans la sous-fenêtre Device Access, configurez les adresses IP, les ports et les protocoles que vous souhaitez ajouter sous forme de règle de pare-feu locale dans QRadar Risk Manager.

Etape 7 Dans la zone **IP Address**, tapez les adresses IP des périphériques auxquels vous souhaitez accéder.

Etape 8 Dans la zone de liste déroulante **Protocol**, sélectionnez le protocole dont vous souhaitez activer l'accès pour l'adresse IP et le port spécifié(e) :

- **UDP** - Permet le trafic UDP.
- **TCP** - Permet le trafic TCP.
- **Any** - Permet tous les trafics.

Etape 9 Dans la zone **Port**, tapez le port sur lequel vous souhaitez activer les communications, puis cliquez sur **Allow**.

Etape 10 Tapez l'adresse IP de l'hôte géré que vous souhaitez autoriser à accéder à l'administration de système basée sur le Web, puis cliquez sur **Allow**.

Seules les adresses IP répertoriées ici ont accès à l'administration de système base sur le Web. Si vous laissez la zone vide, toutes les adresses IP ont accès à cette administration.

Etape 11 Cliquez sur **Apply Access Controls**.

Mise à jour de votre configuration QRadar Risk Manager

La configuration de QRadar Risk Manager vous permet de définir le serveur de messagerie utilisé pour les notifications de QRadar Risk Manager.

Pour configurer l'adresse du serveur de messagerie QRadar Risk Manager, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Cliquez sur l'icône **System Management.**

Etape 4 Connectez-vous à la page System Administration. La valeur par défaut est :

Nom d'utilisateur : **`root`**

Mot de passe : **`<password>`**

Le nom d'utilisateur et le mot de passe sont sensibles à la casse.

Etape 5 Dans le menu, sélectionnez **Managed Host Config > QRM Setup**.

Etape 6 Dans la zone **Mail Server**, tapez l'adresse IP ou le nom d'hôte du serveur de messagerie que vous souhaitez que QRadar Risk Manager utilise.

QRadar Risk Manager utilise ce serveur de messagerie pour répartir les alertes et les messages d'événement. Pour utiliser le serveur de messagerie fourni avec QRadar Risk Manager, tapez **localhost**.

Etape 7 Cliquez sur **Apply Configuration**.

Etape 8 Attendez l'actualisation de l'écran avant de tenter tout autre changement.

Configuration des rôles d'interface utilisateur

Si votre dispositif comprend plusieurs interfaces réseau, vous pouvez affecter des rôles spécifiques aux interfaces réseau de chaque système.

Pour obtenir de l'aide pour déterminer le rôle approprié à chaque interface, contactez le service clients.

Pour affecter des rôles à une interface réseau, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Cliquez sur l'icône **System Management.**

Etape 4 Connectez-vous à la fenêtre System Administration. La valeur par défaut est :

Nom d'utilisateur : **`root`**

Mot de passe : **`<password>`**

Le nom d'utilisateur et le mot de passe sont sensibles à la casse.

Etape 5 Dans le menu, sélectionnez **Managed Host Config > Network Interfaces.**

Etape 6 Pour chaque interface répertoriée, sélectionnez le rôle que vous souhaitez affecter à l'interface à l'aide de la zone de liste Role.

Dans la plupart des cas, la configuration en cours s'affiche et ne peut être éditée.

Etape 7 Cliquez sur **Save Configuration**.

Etape 8 Attendez l'actualisation de l'écran avant de tenter tout autre changement.

Changement des mots de passe

Pour changer le mot de passe root de QRadar Risk Manager, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Cliquez sur l'icône **System Management.**

Etape 4 Connectez-vous pour accéder aux paramètres d'administration de système.

Nom d'utilisateur : **`root`**

Mot de passe : **`<password>`**

Le nom d'utilisateur et le mot de passe sont sensibles à la casse.

Etape 5 Dans le menu, sélectionnez **Managed Host Config > Root Password**.

Etape 6 Dans la zone **New Root Password**, entrez le mot de passe root utilisé pour accéder à l'administration de système par le Web, puis entrez à nouveau ce mot de passe dans la zone **Confirm New Root Password.**

Etape 7 Cliquez sur **Update Password**.

Mise à jour de l'heure système

Vous devez contacter le service clients avant de mettre à jour l'heure système du dispositif QRadar Risk Manager.

Tous les changements apportés à l'heure système doivent être enregistrés sur la console. La console répartit ensuite les paramètres de temps mis à jour entre tous les hôtes gérés de votre déploiement.

Pour plus d'informations sur la configuration de l'heure système sur votre console, voir le manuel *IBM Security QRadar SIEM - Guide d'administration*.

Pour mettre à jour les paramètres de temps pour votre système, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Cliquez sur l'icône **System Management.**

Etape 4 Connectez-vous pour accéder aux paramètres d'administration de système.

Nom d'utilisateur : **`root`**

Mot de passe : **`<password>`**

Le nom d'utilisateur et le mot de passe sont sensibles à la casse.

Etape 5 Dans le menu, sélectionnez **Managed Host Config > System Time**.

MISE EN GARDE

*La fenêtre des paramètres de temps est composée de deux parties. Vous devez enregistrer chaque paramètre avant de poursuivre. Par exemple, lorsque vous configurez l'heure système, vous devez cliquer sur **Apply** dans la sous-fenêtre System Time avant de poursuivre.*

Etape 6 Cliquez sur **Set time**.

Etape 7 Dans la section **System Time**, sélectionnez la date et l'heure en cours que vous souhaitez affecter à l'hôte géré, puis cliquez sur **Apply**.

Etape 8 Dans la sous-fenêtre **Hardware Time**, sélectionnez la date et l'heure en cours que vous souhaitez affecter à l'hôte géré, puis cliquez sur **Save**.

4 GESTION DES SOURCES DE CONFIGURATION

Grâce à la fonction Configuration Source Management de l'onglet **Admin** de IBM Security QRadar SIEM, vous pouvez configurer les données d'identification, ajouter ou reconnaître des périphériques, afficher les configurations de périphérique et sauvegarder les configurations de périphérique dans QRadar Risk Manager. Les données provenant des périphériques de votre réseau permettent de renseigner la topologie. Vous devez disposer des privilèges d'administration pour accéder aux fonctions Configuration Source Management à partir de l'onglet **Admin** de QRadar SIEM.

Pour configurer vos sources de configuration, procédez comme suit :

1. Configurez les données d'identification de votre périphérique. Pour plus d'informations, voir la section Configuration des données d'identification.
2. Activez la reconnaissance ou l'importation des périphériques. Il existe deux façons d'ajouter des périphériques réseau à QRadar Risk Manager : activez la reconnaissance des périphériques à l'aide de la fonction Configuration Source Management ou importez une liste de périphériques à partir d'un fichier CSV à l'aide de l'option Device Import. Pour plus d'informations, voir les sections Reconnaissance des périphériques et Importation de périphériques.
3. Obtenez des informations de configuration de périphérique à partir de chacun de vos périphériques. Pour plus d'informations, voir la section Acquisition de la configuration d'un périphérique.
4. Vérifiez que toutes les mises à jour sur les configurations de périphérique sont capturées. Pour plus d'informations, voir la section Gestion des travaux de sauvegarde.
5. Configurez le planning de reconnaissance pour vérifier que les nouveaux périphériques sont automatiquement reconnus. Pour plus d'informations, voir la section Configuration de la planification du processus de reconnaissance.

La fonction Configuration Source Management vous permet également d'effectuer les actions suivantes :

- Ajouter, éditer, rechercher et supprimer les sources de configuration. Pour plus d'informations, voir la section Gestion des périphériques.
- Configurer ou gérer les protocoles de communication pour vos périphériques. Pour plus d'informations, voir la section Configuration de protocoles.

REMARQUE

Si vous utilisez le périphérique Juniper NSM, vous devez également obtenir des informations de configuration.

Pour des informations détaillées sur les adaptateurs utilisés pour communiquer avec les périphériques provenant de fabricants spécifiques, voir le manuel *IBM Security QRadar Risk Manager - Guide de configuration des adaptateurs*.

Configuration des données d'identification

Les administrateurs doivent configurer les données d'identification afin de permettre à QRadar Risk Manager de se connecter aux périphériques du réseau. Les données d'identification permettent à QRadar Risk Manager de télécharger et d'accéder à la configuration de périphériques tels que les pare-feux, les routeurs, les commutateurs ou les IPS.

La fonction Configuration Source Management permet à un administrateur d'entrer des données d'identification de périphérique d'entrée, ce qui permet au composant QRadar Risk Manager de pouvoir accéder à un périphérique spécifique. Il est possible d'enregistrer les données d'identification d'un périphérique réseau spécifique ou, si plusieurs périphériques réseau utilisent les mêmes données d'identification, de les affecter à un groupe de périphériques.

Par exemple, si tous les pare-feux d'une entreprise disposent des mêmes nom d'utilisateur et mot de passe, alors ces données d'identification sont associées aux ensembles d'adresses de tous les pare-feux. De plus, ils permettent de sauvegarder la configuration de tous les pare-feux de l'entreprise.

S'il n'est pas nécessaire d'avoir des données d'identification de réseau pour un périphérique spécifique, le paramètre peut rester vide dans Configuration Source Management. Pour obtenir une liste des données d'identification d'adaptateur obligatoires, voir le manuel *IBM Security QRadar Risk Manager - Guide de configuration des adaptateurs*.

Vous pouvez affecter plusieurs périphériques de votre réseau à des groupes du réseau, vous permettant ainsi d'unifier les données d'identification et les ensembles d'adresses de vos périphériques.

Un ensemble de données d'identification contient des valeurs telles que le nom d'utilisateur et le mot de passe d'un ensemble de périphériques.

Un ensemble d'adresses est une liste d'adresses IP définissant un groupe de périphériques qui partagent le même ensemble de données d'identification.

Chaque groupe du réseau peut posséder plusieurs ensembles de données d'identification et d'adresses. Vous pouvez également configurer votre composant QRadar Risk Manager pour définir les priorités d'évaluation de chaque groupe du réseau. Le groupe du réseau en haut de la liste possède la priorité la plus élevée. Le premier groupe du réseau correspondant à l'adresse IP configurée est intégré en tant que candidat lors de la sauvegarde d'un périphérique. Un maximum de

trois ensembles de données d'identification provenant d'un groupe du réseau est pris en compte.

Par exemple, si votre configuration comprend les deux groupes du réseau suivants :

- Network Group 1 comprend deux ensembles de données d'identification
- Network Group 2 comprend deux ensembles de données d'identification

QRadar Risk Manager tente de compiler une liste contenant au maximum trois ensembles de données d'identification. Le groupe Network Group 1 étant le premier dans la liste, les deux ensembles de données d'identification de Network Group 1 sont ajoutés à la liste de candidats. Etant donné que trois ensembles de données d'identification sont obligatoires, le premier ensemble de données d'identification du groupe Network Group 2 est ajouté à la liste.

Lorsqu'un ensemble de données d'identification parvient à accéder à un périphérique, QRadar Risk Manager utilise cet ensemble de données d'identification pour les prochaines tentatives d'accès au périphérique. Si les données d'identification de ce périphérique changent, l'authentification échoue lors de la tentative d'accès au périphérique. Ensuite, lors de la tentative suivante d'authentification, le composant QRadar Risk Manager synchronise à nouveau les données d'identification pour assurer le succès de l'opération.

Pour configurer les données d'identification du périphérique, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.

Etape 4 Dans le menu de navigation, cliquez sur **Credentials**.

Etape 5 Dans la sous-fenêtre **Network Groups**, cliquez sur l'icône **Add (+)**.

Etape 6 Entrez le nom d'un groupe du réseau, puis cliquez sur **OK**.

Etape 7 Déplacez en haut de la liste le groupe du réseau auquel vous souhaitez affecter la première priorité. Vous pouvez utiliser les icônes en forme de flèche **Move Up** et **Move Down** pour définir la priorité d'un groupe du réseau.

Etape 8 Dans la zone **Add Address**, entrez l'adresse IP ou la plage CIDR que vous souhaitez appliquer au groupe du réseau, puis cliquez sur l'icône **Add (+)**.

Vous pouvez entrer une plage d'adresses IP à l'aide d'un tiret ou indiquer une plage à l'aide du caractère générique (*****). Par exemple, 10.100.20.0-10.100.20.240 ou 1.1.1*. Si vous entrez 1.1.1.*, toutes les adresses IP répondant à cette exigence sont incluses.

Répétez cette procédure pour toutes les adresses IP à ajouter à l'ensemble d'adresses de ce groupe du réseau.

REMARQUE

Lorsque vous configurez l'ensemble d'adresses à l'aide de Juniper Networks NSM ou d'un adaptateur XML générique, vous devez entrer la plage d'adresses IP ou d'adresses CIDR pour tous les périphériques gérés par Juniper Networks NSM ou les fichiers des périphériques du référentiel.

Etape 9 Dans la sous-fenêtre **Credentials**, cliquez sur l'icône **Add (+)**.

Etape 10 Entrez le nom du nouvel ensemble de données d'identification, puis cliquez sur **OK**.

Etape 11 Entrez les valeurs pour les paramètres :

Tableau 4-1 Credential Parameters

Paramètre	Description
Username	Entrez le nom d'utilisateur de l'ensemble de données d'identification. ***Remarque :*** *Si vous utilisez Juniper Networks NSM ou un adaptateur générique XML, entrez un nom d'utilisateur disposant de droits d'accès au serveur Juniper NSM ou au référentiel de fichiers contenant vos fichiers SED.*
Password	Entrez le mot de passe de l'ensemble de données d'identification. ***Remarque :*** *Si vous utilisez Juniper Networks NSM ou un adaptateur générique XML, entrez le mot de passe du serveur Juniper NSM ou celui permettant de vous connecter au référentiel de fichiers contenant vos fichiers SED.*
Enable Username	Entrez le nom d'utilisateur de l'authentification de second niveau de l'ensemble de données d'identification.
Enable Password	Entrez le mot de passe de l'authentification de second niveau de l'ensemble de données d'identification.
SNMP Get Community	Entrez la communauté SNMP Get.
SNMPv3 Authentication Username	Entrez le nom d'utilisateur que vous souhaitez utiliser pour authentifier SNMPv3.
SNMPv3 Authentication Password	Entrez le mot de passe que vous souhaitez utiliser pour authentifier SNMPv3.
SNMPv3 Privacy Password	Entrez le protocole que vous souhaitez utiliser pour déchiffrer les alertes SNMPv3.

Etape 12 Déplacez en haut de la liste l'ensemble de données d'identification auquel vous souhaitez affecter la première priorité. Utilisez les icônes en forme de flèche **Move Up** et **Move Down** pour définir la priorité d'un ensemble de données d'identification.

Etape 13 Répétez la procédure pour chaque ensemble de données d'identification à ajouter.

Etape 14 Cliquez sur **OK**.

Reconnaissance des périphériques

Le processus de reconnaissance utilise le protocole SNMP et la ligne de commande (CLI) pour reconnaître les périphériques réseau. Une fois que vous avez configuré une adresse IP ou une plage CIDR, le moteur de reconnaissance effectue une analyse TCP en fonction de l'adresse IP afin de déterminer si le port 22, 23 ou 443 surveille les connexions. Si l'analyse TCP aboutit et que la requête SNMP est configurée pour déterminer le type de périphérique, la fonction SNMP Get Community String est utilisée en fonction de l'adresse IP.

QRadar Risk Manager utilise ces informations pour déterminer vers quel adaptateur le périphérique doit être mappé lors de l'ajout. QRadar Risk Manager se connecte au périphérique et collecte une liste d'interfaces et des informations voisines telles que des tables CDP, NDP ou ARP. Le périphérique est ensuite ajouté à l'inventaire.

L'adresse IP configurée utilisée pour lancer le processus de reconnaissance peut ne pas être l'adresse IP affectée pour le nouveau périphérique. QRadar Risk Manager ajoute un périphérique à l'aide de l'adresse IP pour l'interface portant le numéro le plus bas sur le périphérique (ou l'adresse de bouclage la plus basse le cas échéant).

De plus, si vous utilisez la case à cocher **Crawl the network from the addresses defined above**, l'adresse IP des voisins collectée à partir du périphérique est réintroduite dans le processus de reconnaissance et le processus se répète pour chaque adresse IP.

REMARQUE

Lors d'une reconnaissance de périphérique, tout périphérique non pris en charge, mais répondant au protocole SNMP est ajouté à l'adaptateur SNMP générique. Si vous souhaitez exécuter un filtrage de chemin dans le périphérique avec des routes simulées, vous devez supprimer manuellement le périphérique

Pour reconnaître les périphériques, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.

Etape 4 Dans le menu de navigation, cliquez sur **Discover Devices**.

Etape 5 Entrez une adresse IP ou une plage CIDR.

Cette adresse IP ou cette plage CIDR indique l'emplacement des périphériques à reconnaître.

Etape 6 Cliquez sur l'icône **Add (+).**

Etape 7 Si vous souhaitez également rechercher des périphériques dans le réseau à partir de l'adresse IP ou de la plage CIDR définie, cochez la case **Crawl the network from the addresses defined above**. Cette case est cochée par défaut.

Etape 8 Cliquez sur **Run**.

Importation de périphériques

Utilisez l'option Device Import pour ajouter en vrac une liste d'adaptateurs et de leurs adresses IP sur le réseau à Configuration Source Manager. La liste doit être au format.CSV. La liste d'importation de périphérique peut contenir jusqu'à 5 000 périphériques, mais cette liste doit contenir une seule ligne pour chaque adaptateur et son adresse IP associée dans le fichier d'importation.

Par exemple,

```
<Adapter::Name 1>,<IP Address>
<Adapter::Name 2>,<IP Address>
<Adapter::Name 3>,<IP Address>
```

Où :

<Adapter::Name> contient le nom du fabricant et du périphérique tel que Cisco::IOS.

<IP Address> contient l'adresse IP du périphérique telle que 191.168.1.1.

Tableau 4-2 Device Import Examples

Manufacturer	Name	Example <Adapter::Name>,<IP Address>
Check Point	SecurePlatform	CheckPoint::SecurePlatform,10.1.1.4
Cisco	IOS	Cisco::IOS,10.1.1.1
Cisco	Cisco Security Appliance	Cisco::SecurityAppliance,10.1.1.2
Cisco	CatOS	Cisco::CatOS, 10.1.1.3
Generic	SNMP	Generic::SNMP,10.1.1.8
Juniper Networks	Junos	Juniper::JUNOS,10.1.1.5

Importation d'un fichier CSV

Vous pouvez importer une liste maîtresse de périphériques à Configuration Source Management à l'aide d'un fichier au format CSV.

Si vous importez une liste de périphériques dans QRadar Risk Manager puis apportez un changement à une adresse IP dans le fichier CSV, vous risquez de dupliquer accidentellement un périphérique dans la liste Configuration Source Management. Pour cette raison, supprimez un périphérique dans Configuration Source Management avant de réimporter votre liste maîtresse de périphériques.

Pour importer une liste maîtresse de périphériques, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Dans la sous-fenêtre **Plug-Ins**, cliquez sur **Device Import**.

Etape 4 Cliquez sur **Browse**.

Etape 5 Localisez votre fichier CSV, puis cliquez sur **Open**.

Etape 6 Cliquez sur **Import Devices**.

Vous pouvez désormais gérer les périphériques que vous avez importés. Pour plus d'informations, voir la section Gestion des périphériques.

Si une erreur survient, alors vous devez réviser votre fichier CSV afin de corriger les erreurs puis réimporter le fichier. L'importation d'une liste de périphériques au format CSV peut échouer si elle ne dispose pas d'une structure correcte ou si elle contient des informations incorrectes. Par exemple, des points-virgules ou une commande peuvent manquer dans le fichier CSV, une ligne du fichier peut contenir plusieurs périphériques ou le nom d'un adaptateur peut contenir une erreur.

Si l'importation de périphérique est interrompue, aucun périphérique du fichier CSV n'est ajouté à la fonction Configuration Source Management.

Gestion des périphériques

L'onglet Devices de la fenêtre Configuration Source Management vous permet de gérer les périphériques de votre réseau. L'onglet Devices vous permet d'effectuer les opérations suivantes :

- Afficher tous les périphériques existants. Pour plus d'informations, voir la section Affichage des périphériques.
- Ajouter un périphérique. Pour plus d'informations, voir la section Ajout d'un périphérique.
- Editer un périphérique existant. Pour plus d'informations, voir la section Edition de périphériques.
- Supprimer un périphérique. Pour plus d'informations, voir la section Suppression d'un périphérique.
- Rechercher les périphériques existants. Pour plus d'informations, voir la section Filtrage de la liste de périphériques.
- Obtenir une configuration pour un périphérique. Pour plus d'informations, voir la section Acquisition de la configuration d'un périphérique.
- Collecter les données d'un périphérique. Pour plus d'informations, voir la section Collecte de données voisines.

Si vous souhaitez reconnaître tous les périphériques dans votre déploiement, voir la section Reconnaissance des périphériques.

Affichage des périphériques

L'onglet Devices affiche tous les périphériques dans votre déploiement. Pour afficher les périphériques, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.

Etape 4 Cliquez sur l'onglet **Devices**.

La table suivante décrit les paramètres de l'onglet **Devices** :

Tableau 4-3 Paramètres de périphériques

Paramètre	Description
Backup Status	Les icônes suivantes affichent le statut de la dernière tentative de sauvegarde d'un périphérique par QRadar Risk Manager: • **Point d'exclamation rouge** - Indique une erreur qui s'est produite au cours de la dernière tentative de sauvegarde du périphérique. • **Coche verte** - Indique que la sauvegarde du périphérique est terminée. • **Voyant d'avertissement jaune** - Indique qu'un avertissement ou une exception a été émis(e) au cours d'une sauvegarde de périphérique et a entraîné l'échec de cette dernière. L'incident le plus courant avec les voyants d'avertissement correspond à des données d'identification de périphérique non valides. Le message d'erreur peut être affiché en cliquant sur **View Error**. • **Point d'interrogation bleu** - Indique qu'il n'existe aucune archive de sauvegarde connue pour ce périphérique.
IP Address	Adresse IP de gestion du périphérique.
Hostname	Nom d'hôte du périphérique.
Adapter	Nom d'adaptateur du périphérique.
Model	Modèle du périphérique.

Etape 5 Pour afficher des informations détaillées pour une configuration de périphérique, sélectionnez le périphérique à afficher et cliquez sur **Open**.

La table suivante contient des informations sur la sous-fenêtre Properties :

Tableau 4-4 Paramètres des propriétés

Paramètre	Description
IP Address	Adresse IP du périphérique. Cette valeur est configurée lorsque le périphérique est ajouté à Configuration Source Management.
Adapter	Adaptateur utilisé pour le périphérique. Cette valeur est configurée lorsque le périphérique est ajouté à Configuration Source Management.
Hostname	Nom d'hôte du périphérique tel qu'il apparaît dans le périphérique. Cette valeur provient du périphérique au cours du processus de sauvegarde.
Make	Nom du fournisseur du périphérique. Cette valeur provient du périphérique au cours du processus de sauvegarde.
Model	Modèle du périphérique. Cette valeur provient du périphérique au cours du processus de sauvegarde.
Software Version	Version de logiciel actuellement en cours d'exécution pour le périphérique. Cette valeur provient du périphérique au cours du processus de sauvegarde.

Tableau 4-4 Paramètres des propriétés (suite)

Paramètre	Description
Serial Number	Numéro de série du périphérique. Cette valeur provient du périphérique au cours du processus de sauvegarde.
Device Type	Type de périphérique, par exemple, un routeur. Cette valeur provient du périphérique au cours du processus de sauvegarde.
Show historical configurations	Cochez cette case si vous voulez afficher toutes les révisions enregistrées. Une révision est uniquement recréée lorsque le contenu du fichier de configuration change. Décochez cette case si vous souhaitez uniquement afficher la révision la plus récente du fichier de configuration.

La table suivante contient des informations sur la sous-fenêtre Configurations :

Tableau 4-5 Paramètres des configurations

Paramètre	Description
Config	Nom du fichier de configuration tel qu'il apparaît dans le périphérique au cours du processus de sauvegarde. Cette liste peut contenir plusieurs entrées, ce qui comprend un historique de révision.
Date	Date à laquelle le fichier de configuration a été généré suite au processus de sauvegarde. Si le processus de sauvegarde n'a détecté aucun changement de configuration depuis le dernier processus de sauvegarde, la zone de date indique la date de la sauvegarde précédente. La date est uniquement mise à jour sur la toute dernière sauvegarde lorsque des changements de configuration sont détectés.

Ajout d'un périphérique

QRadar Risk Manager vous permet d'ajouter des périphériques réseau individuels et l'adaptateur à l'aide de la fonction Configuration Source Management. La section suivante vous informe sur l'ajout d'un périphérique individuel à la liste de périphériques de Configuration Source Management.

Pour des informations sur l'"ajout en vrac" de plusieurs périphériques à l'aide d'un fichier CSV, voir la section Importation de périphériques.

Pour ajouter un périphérique individuel, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.

Etape 4 Dans la sous-fenêtre de navigation, cliquez sur **Add Device**.

Etape 5 Configurez la valeur des paramètres ci-dessous :

- **IP Address** - Entrez l'adresse IP de gestion du périphérique.

- **Adapter** - Dans la zone de liste déroulante **Adapter**, sélectionnez l'adaptateur à affecter à ce périphérique.

Etape 6 Cliquez sur **Add**.

Le cas échéant, cliquez sur **Go** pour actualiser la liste des adaptateurs.

Edition de périphériques

Le fait d'éditer un périphérique vous permet de corriger l'adresse IP ou le type d'adaptateur en cas d'erreur ou si votre réseau a changé et que vous devez réaffecter une adresse IP.

Pour éditer un périphérique, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.

Etape 4 Sélectionnez le périphérique que vous souhaitez éditer.

Etape 5 Cliquez sur **Edit**.

Etape 6 Configurez la valeur des paramètres ci-dessous :

- **IP Address** - Entrez l'adresse IP à affecter à ce périphérique.
- **Adapter** - Dans la zone de liste déroulante **Adapter**, sélectionnez l'adaptateur à affecter à ce périphérique.

Etape 7 Cliquez sur **Save**.

Suppression d'un périphérique

Vous pouvez supprimer un périphérique de QRadar Risk Manager. Un périphérique supprimé l'est de Configuration Source Management, du Moniteur de configuration et et de la Topologie.

Une fois que vous avez supprimé un périphérique, le processus de suppression du périphérique de la topologie peut prendre quelques minutes.

Pour supprimer un périphérique de la topologie, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.

Etape 4 Cliquez sur l'onglet **Devices**.

Etape 5 Sélectionnez le périphérique que vous souhaitez supprimer.

Etape 6 Cliquez sur **Remove**.

Etape 7 Cliquez sur **Yes** pour supprimer le périphérique.

Filtrage de la liste de périphériques

QRadar Risk Manager peut gérer jusqu'à 5 000 périphériques réseau dans Configuration Source Management. Les grands nombres de périphériques réseau peuvent rendre l'exploration de la liste de périphériques extrêmement fastidieuse. Pour faciliter la recherche d'un périphérique dans la liste, un filtre est disponible à gauche de la liste de périphériques.

Pour réinitialiser un filtre, sélectionnez **Interface IP Address**, supprimez l'adresse **IP/CIDR**, puis cliquez sur **Go**.

Pour filtrer votre liste de périphériques :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Dans la sous-fenêtre Risk Manager, cliquez sur **Configuration Source Management**.

Etape 4 Cliquez sur l'onglet **Devices**.

Etape 5 Dans la zone de liste déroulante située à gauche de la liste de périphériques, sélectionnez un filtre :

Tableau 4-6 Filtres de périphérique

Option de recherche	Description
Interface IP Address	Filtres des périphériques possédant une interface correspondant soit à une adresse IP, soit à une plage CIDR. Entrez l'adresse IP ou la plage CIDR que vous souhaitez rechercher dans la zone **IP/CIDR**. Par exemple, si vous saisissez un critère de recherche 10.100.22.6, les résultats de la recherche retournent un périphérique présentant une adresse IP 10.100.22.6. Si vous entrez une plage CIDR 10.100.22.0/24, tous les périphériques de 10.100.22.* sont retournés.
Admin IP Address	Filtre la liste de périphériques en fonction de l'adresse IP de l'interface d'administration. Une adresse IP administrative est l'adresse IP qui identifie de manière unique un périphérique. Entrez l'adresse IP ou la plage CIDR que vous souhaitez rechercher dans la zone **IP/CIDR**.

Tableau 4-6 Filtres de périphérique (suite)

Option de recherche	Description
OS Version	Filtre la liste de périphériques en fonction de la version de système d'exploitation sur laquelle les périphériques sont exécutés. Sélectionnez les valeurs pour les paramètres suivants : • **Adapter** - Dans la zone de liste déroulante, sélectionnez le type d'adaptateur que vous souhaitez rechercher. • **Version** - Dans la zone de liste déroulante, sélectionnez les critères de recherche de la version. Par exemple, supérieure à, inférieure à, égale à la valeur spécifiée. Entrez le numéro de version dans la zone dans laquelle vous souhaitez effectuer la recherche. Si vous ne sélectionnez pas d'option de recherche pour la version, les résultats contiennent tous les périphériques configurés avec l'adaptateur sélectionné, quelle que soit la version.
Model	Filtre la liste de périphériques en fonction du fournisseur et du numéro de modèle. Configurez les valeurs des paramètres suivants : • **Vendor** - Dans la zone de liste déroulante, sélectionnez le fournisseur que vous souhaitez rechercher. • **Model** - Entrez le modèle que vous souhaitez rechercher.
Hostname	Filtre la liste de périphériques en fonction du nom d'hôte. Entrez le nom d'hôte sur lequel vous souhaitez effectuer une recherche dans la zone **Hostname**.

Etape 6 Cliquez sur **Go**.

Tous les résultats de la recherche correspondant à vos critères s'affichent dans la table.

Acquisition de la configuration d'un périphérique

Après avoir configuré les ensembles de données d'identification et les ensembles d'adresses pour accéder aux périphériques réseau, vous devez sauvegarder vos périphériques pour télécharger leur configuration. Ainsi, QRadar Risk Manager peut inclure les informations sur les périphériques dans la topologie. Le processus de sauvegarde d'un périphérique pour obtenir une configuration de périphérique peut être exécuté pour un périphérique unique dans la liste de périphériques. Vous pouvez également sauvegarder tous les périphériques à partir de l'onglet **Devices**.

Pour plus d'informations sur la planification des sauvegardes automatisées des configurations de périphériques à partir de l'onglet **Jobs**, voir la section Gestion des travaux de sauvegarde.

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.

Etape 4 Cliquez sur l'onglet **Devices**.

Etape 5 Sélectionnez l'une des options suivantes :

- **a** Si vous souhaitez connaître la configuration de tous les périphériques, cliquez sur **Backup All** dans la sous-fenêtre de navigation. Allez à l' Etape 7.
- **b** Si vous souhaitez connaître la configuration d'un périphérique spécifique, sélectionnez le périphérique individuel. Pour sélectionner plusieurs périphériques à sauvegarder, maintenez la touche CTRL enfoncée et sélectionnez tous les périphériques nécessaires. Allez à l' Etape 6.

Etape 6 Cliquez sur **Backup**.

Etape 7 Cliquez sur **Yes** pour poursuivre.

Etape 8 Le cas échéant, cliquez sur **View Error** pour afficher les détails d'une erreur. Après avoir corrigé l'erreur, cliquez sur **Backup All** dans la sous-fenêtre de navigation.

Pour plus d'informations sur l'affichage des détails des sauvegardes de périphériques réseau, voir la section **View device configurations**.

Collecte de données voisines

Utilisez le processus de reconnaissance pour obtenir les données voisines d'un périphérique à l'aide du protocole SNMP et d'une interface de ligne de commande (CLI). Les données voisines sont utilisées dans la topologie pour tirer les lignes de connexion afin d'afficher la mappe topologique graphique de vos périphériques réseau. Le bouton Discover vous permet de sélectionner un périphérique unique ou plusieurs périphériques et de mettre à jour les données voisines d'un périphérique. Ces informations permettent de mettre à jour les lignes de connexion pour un ou plusieurs périphériques de la topologie.

Pour obtenir des données voisines à partir d'un périphérique, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.

Etape 4 Cliquez sur l'onglet **Devices**.

Etape 5 Sélectionnez le périphérique pour lequel vous souhaitez obtenir des données. Pour sélectionner plusieurs périphériques, maintenez la touche CTRL enfoncée et sélectionnez tous les périphériques nécessaires.

Etape 6 Cliquez sur **Discover**.

Etape 7 Cliquez sur **Yes** pour poursuivre.

Si vous sélectionnez plusieurs périphériques, le processus de reconnaissance peut prendre plusieurs minutes.

Sélectionnez **Run in Background** pour utiliser un autre composant QRadar Risk Manager ou d'autres tâches QRadar SIEM.

Collecte de données à partir d'un référentiel de fichiers

Vous pouvez utiliser QRadar Risk Manager pour obtenir des fichiers XML SED de périphérique ou des fichiers d'entrée contenant une configuration de périphérique de base à partir d'un référentiel de fichiers réseau. Le référentiel de fichiers hébergeant les fichiers doit prendre en charge le protocole FTP ou SFTP. QRadar Risk Manager obtient des informations de périphérique de tous les fichiers XML SED situés dans le répertoire de fichier distant du référentiel de fichiers.

La fonction Configuration Collection Toolkit permet à un hôte de collecter des fichiers XML SED et de servir de référentiel de fichiers pour QRadar Risk Manager ou encore de créer un pont avec les périphériques déconnectés de votre réseau. Pour plus d'informations, voir la section Boite à outils de collecte de configuration.

Pour collecter des données à partir d'un référentiel de fichiers, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.

Etape 4 Cliquez sur l'onglet **Devices**.

Etape 5 Sélectionnez **Discover from Repository**.

Etape 6 Configurez les valeurs des paramètres suivants :

- **Protocol** - Dans la zone de liste déroulante **Protocol**, sélectionnez **FTP** ou **SFTP** comme protocole de communication pour accéder à votre référentiel de fichiers de configuration.
- **IP Address** - Saisissez l'adresse IP du référentiel de fichiers de configuration.
- **Remote Path** - Entrez le chemin d'accès de fichier distant au répertoire contenant vos fichiers XML SED. Le chemin d'accès par défaut des fichiers SED est le suivant : **`<install directory>/output`**.

  Où **`<install directory>`** correspond à l'emplacement du fichier extrait **`ziptie-adapter.<date>-<build>.zip`**.
- **Username** - Tapez le nom d'utilisateur requis pour accéder au système hébergeant le référentiel de fichiers de configuration.
- **Password** - Tapez le mot de passe requis pour accéder au système hébergeant le référentiel de fichiers de configuration.

Etape 7 Cliquez sur **OK** pour reconnaître un périphérique dans un référentiel.

Si l'opération aboutit, un message de journal s'affiche et détaille la connexion source et les fichiers XML SED reconnus.

Etape 8 Cliquez sur **Go** pour actualiser la liste de périphériques.

Gestion des travaux de sauvegarde

Un travail fait référence à un travail de sauvegarde, ce qui vous permet de sauvegarder automatiquement les informations de configuration de tous les périphériques de l'onglet **Devices** d'un planning. L'onglet **Jobs** de Configuration Source Management vous permet de créer des travaux de sauvegarde pour tous les périphériques ou des groupes individuels de périphériques dans Configuration Source Management.

Tout travail de sauvegarde que vous définissez sur la page Configuration Source Management n'affecte pas votre configuration de sauvegarde QRadar SIEM si vous utilisez l'icône **Backup and Recovery** de l'onglet **Admin**. La fonctionnalité Backup and Recovery permet d'obtenir des informations de configuration et des données pour QRadar SIEM. Le travail de sauvegarde de la page Configuration Source Management de QRadar Risk Manager permet seulement d'obtenir des informations pour les périphériques externes.

Affichage des travaux de sauvegarde

Les travaux créés dans QRadar Risk Manager s'affichent dans l'onglet **Jobs** avec des détails tels que le nom du travail, le groupe de périphériques affectés au travail, le type de travail et des commentaires supplémentaires ajoutés par l'utilisateur qui a créé le travail de sauvegarde.

Pour affichez les travaux de sauvegarde, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.

Etape 4 Cliquez sur l'onglet **Jobs**.

L'onglet **Jobs** s'affiche et présente tous les travaux de sauvegarde en cours ainsi que les paramètres associés.

Tableau 4-7 Paramètres des travaux de sauvegarde

Paramètre	Description
Job Type Icon	Indique l'icône représentant le type de travail.
Name	Indique le nom du travail de sauvegarde.
Group	Indique le groupe auquel ce travail de sauvegarde a été affecté.
Type	Indique le type de travail de sauvegarde. Il s'agit du travail de sauvegarde.
Comment	Indique tout commentaire fourni pour ce travail.

Etape 5 Cliquez deux fois sur un travail dont vous souhaitez afficher des détails supplémentaires.

La table suivante contient des informations sur les travaux :

Tableau 4-8 Paramètres des travaux

Paramètre	Description
Name	Indique le nom du travail de sauvegarde.
Group	Indique le groupe auquel le travail de sauvegarde est affecté.
Comment	Indique tous les commentaires associés à ce travail de sauvegarde.

Ajout d'un travail de sauvegarde

Pour ajouter un travail de sauvegarde, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.

Etape 4 Cliquez sur l'onglet **Jobs**.

Etape 5 Sélectionnez **New Job > Backup**.

Etape 6 Configurez les valeurs des paramètres suivants :

- **Job Name** - Entrez le nom à affecter à ce travail.
- **Group** - Dans la zone de liste déroulante **Group**, sélectionnez le groupe auquel vous souhaitez affecter ce travail.

  S'il n'apparaît aucun groupe dans la zone de liste déroulante, vous pouvez entrer un nom de groupe. Le fait d'affecter un travail à un groupe vous permet de trier les travaux.
- **Comment** - Facultatif. Entrez tous les commentaires à associer à ce travail de sauvegarde. Vous pouvez entrer jusqu'à 255 caractères dans votre description du travail de sauvegarde.

Etape 7 Cliquez sur **OK**.

Le travail s'affiche dans la liste de la sous-fenêtre Job Details.

Etape 8 Sélectionnez la méthode de recherche :

- **Static list** - Une liste statique vous permet de rechercher les périphériques à l'aide de plusieurs options. Grâce à cette option de liste statique, vous pouvez définir les périphériques spécifiques sur lesquels vous souhaitez exécuter le travail. Allez à l' Etape 9.
- **Search** - Entrez une adresse IP ou une plage CIDR à inclure dans le travail. Une fois que vous avez défini les critères de recherche, la recherche de périphériques est effectuée une fois le travail exécuté. Cela vous permet de vous assurer que tous les nouveaux périphériques sont inclus dans le travail. Allez à l' Etape 10.

Etape 9 Si vous sélectionnez Static List, définissez les critères de recherche :

a Cliquez sur l'onglet **Devices**.

b Dans la zone de liste déroulante de l'onglet **Devices**, sélectionnez les critères de recherche :

Tableau 4-9 Critères de recherche

Option de recherche	Description
Interface IP Address	Vous permet de rechercher les périphériques possédant une interface correspondant soit à une adresse IP, soit à une plage CIDR. Entrez l'adresse IP ou la plage CIDR que vous souhaitez rechercher dans la zone **IP/CIDR**. Par exemple, si vous saisissez un critère de recherche 10.100.22.6, les résultats de la recherche retournent un périphérique présentant une adresse IP 10.100.22.6. Si vous entrez une plage CIDR 10.100.22.0/24, tous les périphériques de 10.100.22.* sont retournés.
Admin IP Address	Vous permet de rechercher les périphériques possédant une adresse IP d'interface d'administration correspondant à la requête. Une adresse IP administrative est l'adresse IP qui identifie de manière unique un périphérique. Entrez l'adresse IP ou la plage CIDR que vous souhaitez rechercher dans la zone **IP/CIDR**.
OS Version	Vous permet de rechercher des périphériques en fonction de la version de système d'exploitation sur laquelle les périphériques sont exécutés. Sélectionnez les valeurs pour les paramètres suivants : • **Adapter** - Dans la zone de liste déroulante, sélectionnez le type d'adaptateur que vous souhaitez rechercher. • **Version** - Dans la zone de liste déroulante, sélectionnez les critères de recherche de la version. Par exemple, supérieure à, inférieure à, égale à la valeur spécifiée. Entrez le numéro de version dans la zone dans laquelle vous souhaitez effectuer la recherche. Si vous ne sélectionnez pas d'option de recherche pour la version, les résultats contiennent tous les périphériques configurés avec l'adaptateur sélectionné, quelle que soit la version.
Model	Vous permet de rechercher des périphériques en fonction du numéro de modèle. Configurez les valeurs des paramètres suivants : • **Vendor** - Dans la zone de liste déroulante, sélectionnez le fournisseur que vous souhaitez rechercher. • **Model** - Entrez le modèle que vous souhaitez rechercher.
Hostname	Vous permet de rechercher des périphériques en fonction du nom d'hôte. Entrez le nom d'hôte sur lequel vous souhaitez effectuer une recherche dans la zone **Hostname**.

c Cliquez sur **Go**.

Les résultats de la recherche s'affichent.

d Dans l'onglet **Devices**, sélectionnez les périphériques à inclure dans le travail.

e Dans la sous-fenêtre Job Details, cliquez sur **Add selected from device view search**.

Les périphériques sélectionnés apparaissent dans la sous-fenêtre Devices.

Etape 10 Si vous sélectionnez Search, définissez les critères suivants :

a Cliquez sur l'onglet **Devices**.

L'onglet Devices s'affiche.

b Dans la zone de liste déroulante de l'onglet **Devices**, sélectionnez les critères de recherche :

Tableau 4-10 Critères de recherche

Option de recherche	Description
Interface IP Address	Vous permet de rechercher les périphériques possédant une interface correspondant soit à une adresse IP, soit à une plage CIDR. Entrez l'adresse IP ou la plage CIDR que vous souhaitez rechercher dans la zone **IP/CIDR**. Par exemple, si vous saisissez un critère de recherche 10.100.22.6, les résultats de la recherche retournent un périphérique présentant une adresse IP 10.100.22.6. Si vous entrez une plage CIDR 10.100.22.0/24, tous les périphériques de la plage 10.100.22.* sont retournés.
Admin IP Address	Vous permet de rechercher les périphériques possédant une adresse IP d'interface d'administration correspondant à la requête. Une adresse IP administrative est l'adresse IP qui identifie de manière unique un périphérique. Entrez l'adresse IP ou la plage CIDR que vous souhaitez rechercher dans la zone **IP/CIDR**.
OS Version	Vous permet de rechercher des périphériques en fonction de la version de système d'exploitation sur laquelle les périphériques sont exécutés. Sélectionnez les valeurs pour les paramètres suivants : • **Adapter** - Dans la zone de liste déroulante, sélectionnez le type d'adaptateur que vous souhaitez rechercher. • **Version** - Dans la zone de liste déroulante, sélectionnez les critères de recherche de la version. Par exemple, supérieure à, inférieure à, égale à la valeur spécifiée. Entrez le numéro de version dans la zone dans laquelle vous souhaitez effectuer la recherche. Si vous ne sélectionnez pas d'option de recherche pour la version, les résultats contiennent tous les périphériques configurés avec l'adaptateur sélectionné, quelle que soit la version.

Tableau 4-10 Critères de recherche (suite)

Option de recherche	Description
Model	Vous permet de rechercher des périphériques en fonction du numéro de modèle. Sélectionnez les valeurs pour les paramètres suivants : • **Vendor** - Dans la zone de liste déroulante, sélectionnez le fournisseur que vous souhaitez rechercher. • **Model** - Entrez le modèle que vous souhaitez rechercher.
Hostname	Vous permet de rechercher des périphériques en fonction du nom d'hôte. Entrez le nom d'hôte sur lequel vous souhaitez effectuer une recherche dans la zone **Hostname**.

c Cliquez sur **Go**.

Le résultat de la recherche s'affiche.

d Dans la sous-fenêtre Job Details, cliquez sur **Use search from devices view**.

Les paramètres de recherche apparaissent dans la sous-fenêtre Devices. Ces critères de recherche permettent de déterminer les périphériques associés à ce travail.

Etape 11 Définissez la planification de travaux :

a Cliquez sur **Schedule**.

b Configurez les valeurs des paramètres suivants :

- **Name** - Entrez un nom pour la configuration de planification.
- **Start time** - Sélectionnez une heure et une date de départ du processus de sauvegarde. L'heure doit être indiquée en heure militaire.
- **Frequency** - Sélectionnez la fréquence à associer à cette planification. Les options sont :

  Once - Sélectionnez cette option pour exécuter ce travail une seule fois.

  Daily - Sélectionnez le nombre de jours écoulés entre les travaux. La valeur par défaut est 1.

  Weekly - Sélectionnez le jour de la semaine auquel vous souhaitez exécuter le travail.

  Monthly - Sélectionnez la fréquence et le jour du mois auxquels vous souhaitez exécuter le travail.

  Cron - Entrez une expression cron, interprétée en temps moyen de Greenwich (GMT). Pour obtenir de l'aide, contactez votre administrateur.
- **Specify End Date** - Facultatif. Sélectionnez une date de fin de la planification de travaux.

c Cliquez sur **Save** dans la sous-fenêtre Trigger.

La configuration de planification s'affiche dans la colonne Triggers. La colonne Triggers représente la planification d'un travail. Vous pouvez avoir plusieurs planifications configurées. Par exemple, vous pouvez configurer deux options de planification pour qu'un travail soit exécuté chaque lundi et le premier jour de chaque mois.

d Répétez les étapes a à c.

Etape 12 Si vous souhaitez exécuter le travail immédiatement, cliquez sur **Run Now**.

Etape 13 Cliquez sur **Yes** pour poursuivre.

Edition d'un travail de sauvegarde

Pour éditer un travail, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.

Etape 4 Cliquez sur l'onglet **Jobs**.

Etape 5 Cliquez deux fois sur le travail à éditer.

Etape 6 Les valeurs en cours du travail s'affichent :

- **Job Name** - Le nom affecté à ce travail s'affiche. Ce paramètre ne peut être modifié.
- **Group** - Le groupe affecté à ce travail s'affiche. Ce paramètre ne peut être modifié.
- **Comment** - Les commentaires associés à ce travail de sauvegarde s'affichent. Ce paramètre ne peut être modifié.

Etape 7 Sélectionnez les périphériques sur lesquels vous souhaitez exécuter le travail :

a Sélectionnez l'option de recherche dans le paramètre **Selection Type**.

- **Static List** - Vous permet de rechercher des périphériques spécifiques à l'aide de plusieurs options : allez sur l' Etape 9.
- **Search** - Entrez une adresse IP ou une plage CIDR à inclure dans le travail. Allez à l' Etape 10.

Les paramètres de recherche s'affichent.

Etape 8 Si vous sélectionnez Static List, définissez les critères de recherche :

a Cliquez sur l'onglet **Devices**.

b Dans la zone de liste déroulante de l'onglet **Devices**, sélectionnez les critères de recherche

Tableau 4-11 Critères de recherche

Option de recherche	Description
Interface IP Address	Vous permet de rechercher les périphériques possédant une interface correspondant soit à une adresse IP, soit à une plage CIDR. Entrez l'adresse IP ou la plage CIDR que vous souhaitez rechercher dans la zone **IP/CIDR**. Par exemple, si vous saisissez un critère de recherche 10.100.22.6, les résultats de la recherche retournent un périphérique présentant une adresse IP 10.100.22.6. Si vous entrez une plage CIDR 10.100.22.0/24, tous les périphériques de la plage 10.100.22.* sont retournés.
Admin IP Address	Vous permet de rechercher les périphériques possédant une adresse IP d'interface d'administration correspondant à la requête. Une adresse IP administrative est l'adresse IP qui identifie de manière unique un périphérique. Entrez l'adresse IP ou la plage CIDR que vous souhaitez rechercher dans la zone **IP/CIDR**.
OS Version	Vous permet de rechercher des périphériques en fonction de la version de système d'exploitation sur laquelle les périphériques sont exécutés. Sélectionnez les valeurs pour les paramètres suivants : • **Adapter** - Dans la zone de liste déroulante, sélectionnez le type d'adaptateur que vous souhaitez rechercher. • **Version** - Dans la zone de liste déroulante, sélectionnez les critères de recherche de la version. Par exemple, supérieure à, inférieure à, égale à la valeur spécifiée. Entrez le numéro de version dans la zone dans laquelle vous souhaitez effectuer la recherche. Si vous ne sélectionnez pas d'option de recherche pour la version, les résultats contiennent tous les périphériques configurés avec l'adaptateur sélectionné, quelle que soit la version.
Model	Vous permet de rechercher des périphériques en fonction du numéro de modèle. Configurez les valeurs des paramètres suivants : • **Vendor** - Dans la zone de liste déroulante, sélectionnez le fournisseur que vous souhaitez rechercher. • **Model** - Entrez le modèle que vous souhaitez rechercher.
Hostname	Vous permet de rechercher des périphériques en fonction du nom d'hôte. Entrez le nom d'hôte sur lequel vous souhaitez effectuer une recherche dans la zone **Hostname**.

c Cliquez sur **Go**.

d Dans l'onglet **Devices**, sélectionnez les périphériques à inclure dans le travail.

e Dans la sous-fenêtre **Job Details**, cliquez sur **Add selected from device view search**.

Etape 9 Si vous sélectionnez Search, définissez les critères suivants :

a Cliquez sur l'onglet **Devices**.

b Dans la zone de liste, sélectionnez les critères de recherche.

Tableau 4-12 Critères de recherche

Option de recherche	Description
Interface IP Address	Vous permet de rechercher les périphériques possédant une interface correspondant soit à une adresse IP, soit à une plage CIDR. Entrez l'adresse IP ou la plage CIDR que vous souhaitez rechercher dans la zone **IP/CIDR**. Par exemple, si vous saisissez un critère de recherche 10.100.22.6, les résultats de la recherche retournent un périphérique présentant une adresse IP 10.100.22.6. Si vous entrez une plage CIDR 10.100.22.0/24, tous les périphériques de la plage 10.100.22.* sont retournés.
Admin IP Address	Vous permet de rechercher les périphériques possédant une adresse IP d'interface d'administration correspondant à la requête. Une adresse IP administrative est l'adresse IP qui identifie de manière unique un périphérique. Entrez l'adresse IP ou la plage CIDR que vous souhaitez rechercher dans la zone **IP/CIDR**.
OS Version	Vous permet de rechercher des périphériques en fonction de la version de système d'exploitation sur laquelle les périphériques sont exécutés. Sélectionnez les valeurs pour les paramètres suivants : • **Adapter** - Dans la zone de liste déroulante, sélectionnez le type d'adaptateur que vous souhaitez rechercher. • **Version** - Dans la zone de liste déroulante, sélectionnez les critères de recherche de la version. Par exemple, supérieure à, inférieure à, égale à la valeur spécifiée. Entrez le numéro de version dans la zone dans laquelle vous souhaitez effectuer la recherche. Si vous ne sélectionnez pas d'option de recherche pour la version, les résultats contiennent tous les périphériques configurés avec l'adaptateur sélectionné, quelle que soit la version.
Model	Vous permet de rechercher des périphériques en fonction du numéro de modèle. Configurez les valeurs des paramètres suivants : • **Vendor** - Dans la zone de liste déroulante, sélectionnez le fournisseur que vous souhaitez rechercher. • **Model** - Entrez le modèle que vous souhaitez rechercher.

Tableau 4-12 Critères de recherche (suite)

Option de recherche	Description
Hostname	Vous permet de rechercher des périphériques en fonction du nom d'hôte. Entrez le nom d'hôte sur lequel vous souhaitez effectuer une recherche dans la zone **Hostname**.

c Cliquez sur **Go**.

d Dans la sous-fenêtre Job Details, cliquez sur **Use search from devices view**.

Les paramètres de recherche apparaissent dans la sous-fenêtre Devices. Ces critères de recherche permettent de déterminer les périphériques associés à ce travail.

Etape 10 Définissez la planification de travaux :

a Cliquez sur **Schedule**.

La sous-fenêtre Schedule s'affiche.

b Si vous souhaitez supprimer une option de planification, sélectionnez la planification. Cliquez sur **Remove**.

c Si vous souhaitez éditer une option de planification existante, sélectionnez la planification.

- **Name** - Entrez un nom pour la configuration de planification.
- **Start time** - Sélectionnez une heure et une date de départ du processus de sauvegarde. L'heure doit être indiquée en heure militaire.
- **Frequency** - Sélectionnez la fréquence à associer à cette planification. Les options sont :

  Once - Sélectionnez cette option pour exécuter cette planification une seule fois.

  Daily - Sélectionnez le nombre de jours écoulés entre les travaux. La valeur par défaut est 1.

  Weekly - Sélectionnez le jour de la semaine auquel vous souhaitez exécuter le travail.

  Monthly - Sélectionnez la fréquence et le jour du mois auxquels vous souhaitez exécuter le travail.

  Cron - Entrez le temps moyen de Greenwich (GMT) auquel vous souhaitez exécuter le travail. QRadar Risk Manager utilise Quarts 1.6.1 comme format d'expression.

- **Specify End Date** - Entrez une date de fin de la planification de travaux.

d Cliquez sur **Save**.

La configuration de planification s'affiche dans la colonne Triggers.

e Répétez les étapes a à c.

Etape 11 Cliquez sur **Run Now**.

Etape 12 Cliquez sur **Yes** pour poursuivre.

Renommage d'un travail de sauvegarde

Pour renommer un travail de sauvegarde, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.

Etape 4 Cliquez sur l'onglet **Jobs**.

Etape 5 Sélectionnez le travail de sauvegarde que vous souhaitez renommer.

Etape 6 Cliquez sur **Rename**.

La fenêtre Rename Job s'affiche.

Etape 7 Configurez les valeurs des paramètres suivants :

- **Job Name** - Entrez un nouveau nom pour le travail.
- **Group** - Dans la zone de liste déroulante **Group**, sélectionnez le groupe auquel vous souhaitez affecter ce travail. Vous pouvez également définir un nouveau nom de groupe.

Etape 8 Cliquez sur **OK**.

Suppression d'un travail de sauvegarde

Pour supprimer un travail de sauvegarde, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.

La fenêtre Configuration s'affiche.

Etape 4 Cliquez sur l'onglet **Jobs**.

Etape 5 Sélectionnez le travail de sauvegarde que vous souhaitez supprimer.

Etape 6 Cliquez sur **Delete**.

Configuration de protocoles

Pour que le composant QRadar Risk Manager communique avec les périphériques, vous devez définir la méthode de communication (protocole) requise pour la communication avec vos périphériques réseau. QRadar Risk Manager comprend la configuration de protocole par défaut pour votre système. Si vous devez définir les protocoles, vous pouvez les définir afin de permettre à QRadar Risk Manager d'obtenir une configuration de périphérique et de la mettre à jour. De nombreux environnements réseau possèdent différents protocoles de communication de différents types ou de différentes fonctions de périphérique. Par exemple, un routeur peut utiliser un protocole différent de celui des pare-feux dans

le réseau. Pour obtenir une liste des protocoles pris en charge par le fabricant de périphériques, voir le *Guide de configuration des adaptateurs*.

QRadar Risk Manager utilise des ensembles de protocoles pour définir des groupes de protocoles pour un ensemble de périphériques nécessitant un protocole de communication spécifique. Vous pouvez affecter des périphériques à des groupes du réseau. Cette opération vous permet d'unifier les ensembles de protocoles et les ensembles d'adresses de vos périphériques.

Les ensembles de protocoles disposent d'un nom et concernent les ensembles de périphériques nécessitant des données d'identification de protocole spécifiques.

Les ensembles d'adresses sont des adresses IP définissant un groupe du réseau.

Pour configurer les protocoles, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.

Etape 4 Dans le menu de navigation, cliquez sur **Protocols**.

Etape 5 Pour configurer un nouveau groupe du réseau, procédez comme suit :

a Dans la sous-fenêtre **Network Groups**, cliquez sur l'icône **Add (+)**.

b Entrez un nom pour un groupe du réseau.

c Cliquez sur **OK**.

Le groupe du réseau est ajouté et les paramètres d'ensembles d'adresses s'affichent.

d Utilisez les icônes **Move Up** et **Move Down** pour définir les priorités pour les groupes du réseau.

Déplacez en haut de la liste le groupe du réseau auquel vous souhaitez affecter la première priorité.

Etape 6 Pour configurer l'ensemble d'adresses, procédez comme suit :

a Dans la zone **Add Address**, entrez l'adresse IP ou la plage CIDR que vous souhaitez appliquer au groupe du réseau, puis cliquez sur l'icône **Add (+)**.

Par exemple, entrez une plage d'adresses IP en utilisant un tiret ou un caractère générique (*****) pour indiquer une plage, comme 10.100.20.0-10.100.20.240 ou 1.1.1*. Si vous entrez 1.1.1.*, toutes les adresses IP répondant à cette exigence sont incluses.

b Répétez cette procédure pour toutes les adresses IP à ajouter à l'ensemble d'adresses de ce groupe du réseau.

Etape 7 Pour configurer l'ensemble de protocoles, procédez comme suit :

a Dans la sous-fenêtre **Network Groups**, vérifiez que le groupe du réseau pour lequel vous souhaitez configurer des protocoles est sélectionné.

b Cochez une case pour appliquer un protocole à la plage d'adresses IP affectée au groupe du réseau créé.

Le fait de décocher la case désactive l'option de communication du protocole lors de la tentative de sauvegarde d'un périphérique réseau.

c Pour chaque protocole sélectionné, configurez les valeurs des paramètres suivants :

Tableau 4-13 Paramètres des protocoles

Protocole	Paramètre
SSH	Configurez les paramètres suivants : • **Port** - Entrez le port que vous souhaitez que le protocole SSH utilise lors de la communication avec les périphériques réseau et de leur sauvegarde. Le port de protocole SSH par défaut est 22. • **Version** - Sélectionnez la version de SSH que vous souhaitez que ce groupe du réseau utilise lors de la communication avec les périphériques réseau. Les options possibles sont les suivantes : **Auto** - Cette option détecte automatiquement la version SSH à utiliser lors de la communication avec les périphériques réseau. **1** - Utilisez SSH-1 lors de la communication avec les périphériques réseau. **2** - Utilisez SSH-2 lors de la communication avec les périphériques réseau.
Telnet	Entrez le numéro de port que vous souhaitez que le protocole Telnet utilise lors de la communication avec les périphériques réseau et de leur sauvegarde. Le port de protocole Telnet par défaut est 23.
HTTPS	Entrez le numéro de port que vous souhaitez que le protocole HTTPS utilise lors de la communication avec les périphériques réseau et de leur sauvegarde. Le port de protocole HTTPS par défaut est 443.
HTTP	Entrez le numéro de port que vous souhaitez que le protocole HTTP utilise lors de la communication avec les périphériques réseau et de leur sauvegarde. Le port de protocole HTTP par défaut est 80.
SCP	Entrez le numéro de port que vous souhaitez que le protocole SCP utilise lors de la communication avec les périphériques réseau et de leur sauvegarde. Le port de protocole SCP par défaut est 22.
SFTP	Entrez le numéro de port que vous souhaitez que le protocole SFTP utilise lors de la communication avec les périphériques réseau et de leur sauvegarde. Le port de protocole SFTP par défaut est 22.

Tableau 4-13 Paramètres des protocoles (suite)

Protocole	Paramètre
FTP	Entrez le numéro de port que vous souhaitez que le protocole FTP utilise lors de la communication avec les périphériques réseau et de leur sauvegarde. Le port de protocole SFTP par défaut est 22.
TFTP	Le protocole TFTP ne possède aucune option configurable.
SNMP	Configurez les paramètres suivants : • **Port** - Entrez le numéro de port que vous souhaitez que le protocole SNMP utilise lors de la communication avec les périphériques réseau et de leur sauvegarde. • **Timeout(ms)** - Sélectionnez la durée, en millisecondes, que vous souhaitez utiliser pour déterminer un délai d'attente de communication. • **Retries** - Sélectionnez le nombre de fois que vous souhaitez tenter de rétablir des communications avec un périphérique. • **Version** - Sélectionnez la version du protocole SNMP à utiliser pour les communications. Les options sont v1, v2 ou v3. • **V3 Authentication** - Sélectionnez l'algorithme à utiliser pour authentifier les alertes SNMP. • **V3 Encryption** - Sélectionnez le protocole à utiliser pour déchiffrer les alertes SNMP.

d Utilisez les icônes **Move Up** et **Move Down** pour définir les priorités pour les protocoles.

Déplacez en haut de la liste le protocole auquel vous souhaitez affecter la première priorité.

Etape 8 Cliquez sur **OK**.

Configuration de la planification du processus de reconnaissance

Vous pouvez configurer une planification des reconnaissances pour renseigner les tables ARP et MAC et les informations voisines pour vous périphériques. La planification des reconnaissances permet également d'ajouter automatiquement de nouveaux périphériques à l'inventaire.

Pour configurer la planification des reconnaissances, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de la navigation, cliquez sur **Plug-ins**.

Etape 3 Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.

Etape 4 Dans le menu de navigation, cliquez sur **Schedule Discovery.**

Etape 5 Cochez la case **Enable periodic discovery** pour activer la planification des reconnaissances.

Etape 6 Configurez les valeurs des paramètres suivants :

- **Start time** - Sélectionnez la date et l'heure de planification du processus de reconnaissance.
- **Schedule** - Sélectionnez la fréquence à laquelle vous souhaitez planifier le processus de reconnaissance. Les options sont :
  - **Once** - Sélectionnez cette option pour exécuter ce processus de reconnaissance une seule fois.
  - **Daily** - Sélectionnez le nombre de jours écoulés entre chaque processus de reconnaissance.
  - **Weekly** - Sélectionnez les jours de la semaine auxquels vous souhaitez planifier la reconnaissance.
  - **Monthly** - Sélectionnez la fréquence mensuelle et l'heure de planification du processus de reconnaissance.
  - **Cron** - Entrez l'expression requise (en temps GMT) pour utiliser cron dans le processus de planification.
- **Specify End Date** - Facultatif. Sélectionnez la date de fin planifiée du processus de reconnaissance.
- **Crawl and discover new devices** - Cochez cette case si vous souhaitez que le processus de reconnaissance reconnaisse de nouveaux périphériques. Décochez cette case si vous ne souhaitez pas ajouter de périphérique à l'inventaire.

Etape 7 Cliquez sur **OK**.

5 UTILISATION DE LA TOPOLOGIE

La page Topologie s'ouvre par défaut lorsque vous accédez à l'onglet **Risks**. Le modèle de topologie vous permet d'afficher, de filtrer et d'interagir avec un graphique représentant la connectivité physique de votre topologie de réseau de couche 3. Ce graphique est créé à partir des informations de configuration détaillées provenant des périphériques réseau tels que les pare-feux, les routeurs, les commutateurs et les systèmes IPS. Vous pouvez passer votre curseur au-dessus des lignes de connexion pour afficher les informations de connexion réseau. La fonction de recherche vous permet de filtrer la topologie pour les chemins d'accès d'attaques potentielles des protocoles, des ports ou des vulnérabilités agréés, d'afficher le flux de trafic entre les périphériques ou les sous-réseaux et les règles de périphérique.

La Topologie vous permet d'effectuer les actions suivantes :

- Visualiser les chemins réseau spécifiques et le sens du trafic pour une analyse avancée des menaces.
- Intégrer les mappes de sécurité IPS passives dans le graphique de topologie.
- Personnaliser le présentation de la topologie, y compris les groupes de réseaux définis par l'utilisateur.
- Créer des filtres de recherche pour votre topologie de réseau en fonction des protocoles, des ports ou des vulnérabilités.
- Afficher des informations de connexion détaillées entre les périphériques et les sous-réseaux.
- Afficher des règles de périphérique sur les connexions de topologie avec les ports et les protocoles agréés.
- Affichage des périphériques de conversion d'adresses réseau, des indicateurs NAT et des informations sur les mappages NAT.
- Affichage des périphériques virtuels de sécurité des réseaux disposant de plusieurs contextes.

Seuls les protocoles TCP, UDP et ICMP sont représentés dans le modèle de topologie lors de l'affichage des ports et protocoles agréés entre les périphériques.

Affichage de la topologie

Par défaut, la topologie s'affiche lors de l'application d'un regroupement à votre réseau. Si vous avez une présentation précédemment enregistrée et que vous retournez à la Topologie, la présentation enregistrée s'affiche.

Pour afficher la topologie, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Dans le menu de navigation, cliquez sur **Topology**.

La topologie représente les sous-réseaux, les périphériques et les pare-feux à l'aide des icônes suivantes :

Tableau 5-1 Icônes du graphique

Icône	Description
Cloud	L'icône de nuage représente un sous-réseau de votre réseau.
Brick Wall	L'icône de mur en briques représente le pare-feu et les périphériques IPS.
Router	L'icône Router représente les routeurs ou les périphériques non classifiés. Si une adresse de passerelle n'apparaît pas pour un périphérique, le graphique de la topologie affiche le texte Unclassified Device sous l'icône du routeur. Les périphériques non classifiés prennent en compte l'adresse IP de la passerelle et gèrent les sous-réseaux spécifiés dans les routes.
Circle	L'icône Circle représente un noeud du groupe réduit. Le numéro à l'intérieur du nom de groupe identifie le nombre de périphériques contenus dans le groupe.
Switch	L'icône Switch représente un commutateur de la topologie.
Périphérique à contextes multiples	L'icône du périphérique à contextes multiples représente un périphérique contenant plusieurs contextes.
Indicateur NAT	Le point vert représente un indicateur NAT qui s'affiche lorsque la recherche de topologie trouve un chemin qui contient des conversions source ou de destination.

Utilisation de la topologie

Si vous avez précédemment configuré et enregistré des critères de recherche par défaut, les résultats de cette recherche seront automatiquement affichés dans la topologie. Pour plus d'informations sur l'enregistrement des critères de recherche, voir la section Recherche dans la topologie.

Utilisation de la barre d'outils

Le graphique de la topologie contient plusieurs options de menu telles que :

Tableau 5-2 Options de la barre d'outils Topologie

Option de menu	Description
Search	Dans la zone de liste déroulante **Search**, sélectionnez une option pour effectuer des recherches avancées sur votre topologie. Les options sont les suivantes : • **New Search** - Sélectionnez cette option pour créer une nouvelle recherche d'événement. • **Edit Search**- Sélectionnez cette option pour sélectionner et modifier une recherche d'événement.
Quick Searches	Dans la zone de liste déroulante **Quick Searches**, vous pouvez exécuter les recherches précédemment sauvegardées. Les options s'affichent uniquement lorsque vous avez enregistré les critères de recherche et que vous cochez la case **Include in my Quick Searches**.
Save	Cliquez sur **Save** pour enregistrer votre topologie en cours en incluant la position des éléments, le filtre appliqué, l'échelle du zoom, la position du graphique et les extensions de groupes. La prochaine fois que vous vous connecterez à la Topologie, la présentation enregistrée s'affichera.
Reset Layout	Cliquez sur **Reset Layout** pour réinitialiser la présentation de la topologie à l'agencement précédemment enregistré. Cette option comprend les filtres précédemment enregistrés, les extensions de groupes et les positions de noeuds. Toutefois, l'option Reset Layout n'affecte pas les groupes de noeuds.
Undo	Cliquez sur **Undo** pour revenir à la dernière action de la topologie. Cette action comprend la réduction de la dernière extension de noeud, la création d'un groupe, la suppression d'un groupe, l'extension d'un groupe ou le déplacement d'un noeud. Si vous souhaitez annuler plusieurs actions, cliquez sur le bouton **Undo** pour chaque action à inverser.
Group Nodes	Cliquez sur **Group Nodes** pour regrouper les noeuds sélectionnés. Une fois les noeuds placés dans un groupe, vous pouvez développer et réduire la totalité du groupe. Pour plus d'informations, voir la section Noeuds de groupe.
Download	Cliquez sur **Download** pour enregistrer la topologie en cours sous un fichier image JPEG.

Utilisation du modèle de topologie

A l'aide du modèle de topologie, vous pouvez accéder aux fonctions graphiques suivantes :

Tableau 5-3 Fonctions graphiques du modèle de topologie

Si vous souhaitez	Alors
Afficher des détails supplémentaires concernant un sous-réseau	Placez le pointeur de votre souris sur le sous-réseau. Les informations de configuration s'affichent.

Tableau 5-3 Fonctions graphiques du modèle de topologie

Si vous souhaitez	Alors
Afficher des détails supplémentaires concernant un périphérique	Placez le pointeur de votre souris sur le périphérique. Les informations de configuration s'affichent.
Afficher des détails supplémentaires concernant une connexion	Placez le pointeur de votre souris sur une ligne de connexion entre un périphérique, un groupe ou un sous-réseau pour afficher des détails sur la connexion. Les multiples bords incurvés qui se trouvent entre un périphérique et un sous-réseau indiquent qu'un périphérique ou qu'un ensemble de contextes dispose de plusieurs interfaces sur le même sous-réseau.
Afficher des détails supplémentaires sur un périphérique à contextes multiples	Déplacez le pointeur de votre souris sur le périphérique à contextes multiples. Les informations de configuration s'affichent.
Répartir des noeuds	Pour répartir les noeuds, les groupes, les pare-feux ou les sous-réseaux sur le graphique, utilisez le pointeur de votre souris pour faire glisser le noeud vers l'emplacement préféré.
Effectuer un zoom avant ou arrière	Utilisez le curseur en haut à gauche du graphique pour changer l'échelle du graphique. ***Remarque :*** *Vous pouvez également utiliser la molette de votre souris pour mettre le graphique à l'échelle.*
Faire un panoramique gauche, droit, haut ou bas	Cliquez avec le bouton gauche de la souris sur l'espace vierge du modèle de topologie et faites glisser votre curseur pour faire un panoramique dans une direction. ***Remarque :*** *Vous pouvez également utiliser la boîte englobante en bas à droite pour faire un panoramique dans n'importe quelle direction du modèle de topologie.*

Utilisation des options du menu contextuel

Dans la topologie, vous pouvez cliquer avec le bouton droit de la souris sur un événement afin d'accéder à des informations supplémentaires de filtrage d'événements.

Tableau 5-4 Options du menu contextuel de topologie

Si vous souhaitez	Alors
Rechercher des connexions	Pour tout sous-réseau de la topologie, cliquez avec le bouton droit de la souris et sélectionnez **Search Connections**. Cela permet de créer une recherche dans laquelle la source ou la destination est l'adresse IP du sous-réseau sélectionné. Vous pouvez ajouter des paramètres de recherche supplémentaires et cliquer sur **Search** pour afficher les résultats.

Tableau 5-4 Options du menu contextuel de topologie (suite)

Si vous souhaitez	Alors
Afficher les informations de configuration d'un périphérique	Placez votre souris sur le périphérique, cliquez avec le bouton droit de la souris et sélectionnez **View Device Configuration**. Ces informations proviennent du périphérique. Pour plus d'informations sur les configurations de périphérique, voir le chapitre Afficher les configurations d'appareil.
Afficher les informations de configuration d'un périphérique à contextes multiples	Placez votre souris sur le périphérique, cliquez avec le bouton droit de la souris et sélectionnez **View Device Configuration**. Cette action affiche une liste des contextes qui appartiennent au périphérique à contextes multiples. Elle comprend des informations de base sur la configuration du périphérique. Vous pouvez afficher les informations détaillées de la configuration du périphérique pour un contexte en cliquant deux fois sur un contexte dans la liste.
Rechercher des événements	Placez le pointeur de votre souris sur un périphérique ou un sous-réseau de la topologie. Cliquez avec le bouton droit de la souris et sélectionnez **Search Events**. • Si vous recherchez des événements sur un sous-réseau, les paramètres de recherche sont renseignés avec l'adresse de source et de destination du fichier de recherche. • Si vous recherchez des événements sur un périphérique mappé vers une source de journal, une recherche d'événement est renseignée avec le nom de source de journal et l'adresse IP du filtre de recherche. Cela vous permet de rechercher des événements associés au périphérique dans la Topologie. Si un périphérique n'est pas mappé vers une source de journal, l'option **Search Events** n'est pas active. Pour plus d'informations, voir la section Mappage de source de journal.
Rechercher les flux associés à un sous-réseau	Placez le bouton de votre souris sur le sous-réseau. Cliquez avec le bouton droit de la souris et sélectionnez **Search Flows**. La fenêtre Flow Search s'affiche. Pour plus d'informations sur la recherche de flux, voir le manuel *IBM Security QRadar SIEM - Guide d'utilisation*.

Tableau 5-4 Options du menu contextuel de topologie (suite)

Si vous souhaitez	Alors
Afficher des informations de profil d'actif concernant un sous-réseau	Placez le pointeur de votre souris sur le sous-réseau, cliquez avec le bouton droit de la souris et sélectionnez **View Assets**. La fenêtre Assets List affiche la liste des actifs du sous-réseau. Pour plus d'informations sur les actifs, voir le manuel *IBM Security QRadar SIEM - Guide d'utilisation*.
Développer un noeud regroupé	Pour tout noeud regroupé à développer, cliquez avec le bouton droit de la souris sur le groupe et sélectionnez **Expand Group**. Vous pouvez également cliquer deux fois sur un groupe pour développer le noeud. Pour plus d'informations sur le regroupement de noeuds, voir la section Noeuds de groupe.
Réduire un noeud regroupé	Pour tout noeud regroupé à réduire, cliquez avec le bouton droit de la souris sur un périphérique faisant partie du groupe et sélectionnez **Collapse to Group**. Pour plus d'informations sur le regroupement de noeuds, voir la section Noeuds de groupe.
Supprimer un noeud regroupé	Pour tout noeud regroupé à réduire, cliquez avec le bouton droit de la souris sur un noeud faisant partie d'un groupe et sélectionnez **Remove Group**. Pour plus d'informations sur le regroupement de noeuds, voir la section Noeuds de groupe.
Ajouter une connexion IPS entre deux périphériques	Si votre topologie comprend un périphérique IPS, placez le pointeur de votre souris sur une ligne de connexion reliant un noeud de périphérique à un noeud de sous-réseau. Cliquez avec le bouton droit de la souris et sélectionnez **Add IPS**. Voir la section Ajout d'un système de prévention contre les intrusions (IPS).
Supprimer un système IPS	Placez le pointeur de votre souris sur la ligne de connexion reliant un noeud de périphérique à un noeud de sous-réseau comprenant le système IPS. Cliquez avec le bouton droit de la souris et sélectionnez **Remove IPS**. Ce menu s'affiche uniquement s'il existe un système IPS sur la connexion.

Recherche dans la topologie

Vous pouvez rechercher dans la topologie des périphériques par hôte, par réseau ou par chemin. Ces options de recherche peuvent ensuite être affinées par adresse IP, CIDR, protocole, adresses IP de source ou de destination ou ports de destination. Les résultats de la recherche consistent en une vue de topologie filtrée correspondant à vos critères de recherche.

Vous pouvez afficher une topologie existante ou charger une topologie précédemment enregistrée et rechercher la vue enregistrée. Une topologie filtrée

par une recherche affiche le nom du filtre de recherche en jaune, sous la barre de menus Current Topology.

Si un chemin est recherché, le sens du trafic, les protocoles agréés ou partiellement agréés et les règles de périphérique s'affichent. De plus, un indicateur NAT s'affiche dans le graphique de topologie si votre recherche trouve un chemin qui contient des conversions source ou de destination. Pour plus d'informations, voir la section Indicateurs NAT dans les résultats de recherche.

Pour effectuer une recherche dans la topologie :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Dans le menu de navigation, cliquez sur **Topology**.

Etape 3 Dans la zone de liste déroulante **Search**, sélectionnez **New Search**.

La fenêtre Saved Searches s'affiche.

Etape 4 Sélectionnez l'une des options de filtre suivantes :

- **None** - Supprime le filtre de recherche existant de la topologie.
- **Hosts** - Filtrez le modèle de topologie en fonction des hôtes, sélectionnez **Host** et indiquez l'adresse IP de l'hôte.

  Un filtre d'hôte retourne les résultats comprenant tous les périphériques environnants qui communiquent avec l'adresse IP de l'hôte. Les lignes de connexion entre les périphériques et les sous-réseaux affichent les informations d'interface de la connexion. Si l'hôte ne correspond pas à une interface d'un périphérique, mais est contenu dans le sous-réseau, le filtre retourne le sous-réseau et tous les périphériques connectés.
- **Network** - Pour filtrer le modèle de topologie en fonction des filtres spécifiques au réseau, sélectionnez l'option **Network Filter** et indiquez la plage d'adresse IP ou CIDR. Plusieurs adresses peuvent être saisies à l'aide d'une liste séparée par des virgules.

  Un filtre de réseau retourne les résultats qui contiennent tous les réseaux de la plage CIDR. Pour rechercher plusieurs adresses CIDR, séparez les adresses CIDR à l'aide d'une virgule.
- **Path** - Pour filtrer le modèle de topologie en fonction des filtres de chemin, sélectionnez l'option **Path Filter** et configurez les paramètres suivants :

  Un filtre de chemin comprend tous les sous-réseaux et périphériques se trouvant entre la source et la destination. Ils sont également autorisés à communiquer avec les protocoles et les ports spécifiés. Les détails de la connexion s'affichent en plaçant le curseur de votre souris sur les lignes de connexion, avec les flèches représentant le sens du trafic et les règles de périphérique le cas échéant. Un indicateur NAT s'affiche dans le graphique de topologie si votre recherche trouve un chemin qui contient des conversions source ou de destination.

  La table suivante affiche les options de filtre lorsque vous effectuez une recherche de chemin de topologie :

Tableau 5-5 Options de filtrage de chemin

Paramètre	Description
Source IP/CIDR	Entrez l'adresse IP ou la plage CIDR sur laquelle vous souhaitez filtrer le modèle de topologie. Séparez les entrées multiples en utilisant une liste séparée par des virgules.
Destination IP/CIDR	Entrez l'adresse IP ou la plage CIDR de destination sur laquelle vous souhaitez filtrer le modèle de topologie. Séparez les entrées multiples en utilisant une liste séparée par des virgules.
Protocol	Facultatif. Dans la zone de liste déroulante, sélectionnez le protocole que vous souhaitez utiliser pour filtrer le modèle de topologie. Les options sont : • Any Protocol (par défaut) • TCP • UDP • ICMP ***Remarque :*** *Seuls les protocoles TCP, UDP et ICMP sont représentés dans le modèle de topologie.*
Destination Port	Facultatif. Entrez le port de destination sur lequel vous souhaitez filtrer le modèle de topologie. Séparez les ports multiples en utilisant une liste séparée par des virgules.
Vulnerabilities	Ce paramètre ne s'affiche que si votre topologie comprend un système IPS. Pour filtrer à l'aide des vulnérabilités, procédez comme suit : **1** Cliquez sur **Vulnerabilities**. **2** Dans la zone de liste déroulante **Search By**, sélectionnez l'option de vulnérabilité sur laquelle vous souhaitez effectuer une recherche. Les options sont les suivantes : OSVDB Title, CVE ID, Bugtraq ID ou OSVDB ID. **3** Entrez ou sélectionnez un paramètre de recherche. **4** Cliquez sur **Search**. Les résultats de la recherche apparaissent dans la zone Search Results. **5** Pour tous les résultats dont vous souhaitez filtrer la topologie, sélectionnez la valeur dans la zone Search Results. Cliquez sur **Add**. **6** Répétez l'opération pour tous les résultats à filtrer. **7** Cliquez sur **Submit**.

Etape 5 Cliquez sur **Search**.

REMARQUE

Pour éditer un filtre de recherche existant, sélectionnez **Search > Edit Search** dans la barre d'outils Topologie.

Indicateurs NAT dans les résultats de recherche

Un indicateur NAT, représenté par un point vert fixe, s'affiche dans le graphique de topologie si votre recherche trouve un chemin qui contient des conversions source ou de destination.

Un indicateur NAT indique que l'adresse IP de destination spécifiée dans le filtre de chemin peut ne pas être la destination finale. Vous pouvez survoler l'indicateur avec votre curseur pour afficher les informations suivantes concernant les conversions.

Tableau 5-6 Informations disponibles dans l'indicateur NAT

Paramètre	Description
Source	IP ou CIDR source converti.
Port(s) source	Ports source convertis, le cas échéant.
Source convertie	Résultat de la conversion qui a été appliquée à la source.
Port(s) source converti(s)	Résultat de la conversion qui a été appliquée au(x) port(s) source, le cas échéant.
Destination	IP ou CIDR de destination converti.
Destination Port(s)	Ports de destination convertis, le cas échéant.
Destination convertie	Résultat de la conversion qui a été appliquée à la destination.
Port(s) de destination converti(s)	Résultat de la conversion qui a été appliquée au(x) port(s) de destination, le cas échéant.
Phase	Phase de routage lorsque la conversion a été appliquée. La conversion est appliquée avant ou après le routage.

Noeuds de groupe

Vous pouvez regrouper les noeuds en fonction des noeuds sélectionnés ou des critères de filtrage spécifiés. Cette section fournit des informations sur le regroupement des noeuds, comme :

- Regroupement des noeuds. Voir la section Regroupement des noeuds.
- Suppression d'un groupe de noeuds. Voir la section Suppression de noeuds de groupe.
- Développement d'un groupe de noeuds. Voir la section Développement de noeuds de groupe.

Regroupement des noeuds

Pour regrouper des noeuds, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Dans le menu de navigation, cliquez sur **Topology**.

Etape 3 Sélectionnez l'une des options suivantes :

a Si vous souhaitez regrouper les noeuds sélectionnés dans votre topologie, allez sur Etape 4.

b Si vous souhaitez regrouper des noeuds en fonction de critères de filtrage, allez à l' Etape 5.

Etape 4 Pour regrouper les noeuds sélectionnés, procédez comme suit :

a Appuyez sur la touche Ctrl et sélectionnez chaque noeud à inclure dans un groupe.

b Cliquez sur **Group Nodes.**

c Dans le paramètre Group Name, entrez le nom du groupe à créer.

d Sélectionnez l'option **Group Selected**.

e Cliquez sur **OK**.

Etape 5 Pour regrouper des noeuds en fonction d'un critère de filtrage, procédez comme suit :

a Cliquez sur **Group Nodes.**

b Dans le paramètre Group Name, entrez le nom du groupe à créer.

REMARQUE

Un nom de groupe est limité à un maximum de 50 caractères.

c Sélectionnez l'option **Group By Filter.**

d Configurez les valeurs des paramètres suivants :

- **IP/CIDR** - Entrez une adresse IP ou une plage CIDR pour les noeuds à regrouper.
- **Adapter Type** - Dans la zone de liste déroulante **Adapter Type**, sélectionnez l'adaptateur sur lequel vous souhaitez regrouper les noeuds.

e Cliquez sur **OK**.

Le groupe s'affiche dans la topologie en cours avec un cercle autour du centre de noeuds regroupés.

Suppression de noeuds de groupe

Pour supprimer un regroupement de noeud, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Topology**.

Etape 3 Dans Current Topology, sélectionnez le cercle indiquant le noeud de groupe à supprimer.

Etape 4 Cliquez avec le bouton droit de la souris et sélectionnez **Remove group**.

Les noeuds précédemment regroupés affichent les périphériques individuels dans la Topologie.

Développement de noeuds de groupe

Pour développer un regroupement de noeud, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Topology**.

Etape 3 Dans Current Topology, sélectionnez le cercle indiquant le noeud de groupe à développer.

Etape 4 Cliquez avec le bouton droit de la souris et sélectionnez **Expand group**.

Ajout d'un système de prévention contre les intrusions (IPS)

Si votre liste Configuration Source Management comprend un périphérique Intrusion Prevention System (IPS), vous pouvez ajouter un système IPS à une connexion reliant un noeud de périphérique à un noeud de sous-réseau. L'ajout d'une connexion IPS est utile pour déterminer l'emplacement du système IPS si le périphérique est passif.

Pour ajouter un système IPS, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Topology**.

Etape 3 Placez le pointeur de votre souris sur la ligne de connexion reliant un noeud de périphérique à un noeud de sous-réseau.

Etape 4 Cliquez avec le bouton droit de la souris sur la ligne de connexion, sélectionnez l'option **Add IPS**.

Etape 5 A l'aide des zones de liste déroulantes, sélectionnez le périphérique et les interfaces permettant d'ajouter la connexion IPS à votre topologie.

Etape 6 Cliquez sur **OK**.

La page la Topologie s'affiche avec le système IPS entre votre périphérique sélectionné et le sous-réseau.

Suppression d'un système de prévention contre les intrusions (IPS)

Pour supprimer une connexion IPS entre un périphérique et un sous-réseau, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Dans le menu de navigation, cliquez sur **Topology**.

Etape 3 Placez le pointeur de votre souris sur la ligne de connexion reliant un noeud de périphérique à un noeud de sous-réseau.

Etape 4 Cliquez avec le bouton droit de la souris sur la ligne de connexion, sélectionnez l'option **Remove IPS idp.**

Etape 5 Cliquez sur **OK**.

La page la Topologie s'actualise avec le périphérique IPS supprimé.

6 UTILISATION DE POLICY MONITOR

Policy Monitor permet à une organisation de définir les questions spécifiques aux risques à propos du réseau afin d'évaluer ou de contrôler le risque en fonction de l'analyse des indicateurs de risque. Les indicateurs de risque sont les suivants :

- Network activity - mesure le risque en se basant sur les communications de réseau établies dans le passé.
- Configuration/Topology - mesure le risque en fonction des communications possibles et des connexions réseau.
- Vulnerabilities - mesure le risque en fonction de votre configuration de réseau et des données d'analyse de la vulnérabilité collectées dans les actifs de réseau.
- Firewall rules - mesure le risque en fonction de la mise en application ou de l'absence de règles de pare-feu appliquées au réseau.

Policy Monitor permet aux utilisateurs de définir des tests en fonction des indicateurs de risque, puis de restreindre les résultats de test pour filtrer la requête afin d'obtenir des résultats ou des violations spécifiques. Des questions peuvent être créées pour les actifs ou les périphériques/règles afin d'exposer les professionnels de sécurité à des risques dans leurs réseaux. Une fois qu'une question à propos d'un actif ou d'un(e) périphérique/règle est soumise au composant Policy Monitor, QRadar Risk Manager retourne les résultats spécifiés par le niveau de risque. Policy Monitor vous permet d'approuver les résultats retournés à partir des actifs ou de définir la façon dont vous souhaitez que le système réponde aux résultats non validés.

Les résultats permettent aux utilisateurs d'évaluer les risques pour de nombreux scénarios de sécurité, par exemple :

- Evaluation si les utilisateurs ont communiqué en utilisant des protocoles interdits.
- Evaluation si les utilisateurs des réseaux spécifiques peuvent communiquer avec des réseaux ou des actifs interdits.
- Evaluation si les règles de pare-feu respectent la politique de l'entreprise.
- Définition des priorités des vulnérabilités en évaluant quels systèmes peuvent être compromis en raison de la configuration de réseau.

Pour configurer vos questions de moniteur de règles, vous devez :

Etape 1 Définir des politiques en créant des questions. Voir la section Création d'une question.

Etape 2 Evaluer le respect d'une politique. Voir la section Soumission d'une question.

Etape 3 Accepter les risques spécifiques. Voir la section Validation des résultats d'une question.

Etape 4 Contrôler les nouveaux risques. Voir la section Surveillance des questions.

Utilisation de Policy Monitor

A l'aide de la barre d'outils principale de Policy Monitor, vous pouvez accéder aux options suivantes.

Tableau 6-1 Options de la barre d'outils

Option	Description
Group	Vous permet d'afficher les questions basées sur un groupe. Dans la zone de liste déroulante **Group**, sélectionne le groupe pour les questions à afficher.
Groups	Vous permet de configurer les groupes pour les questions. Voir la section Regroupement des questions.
Monitor	Vous permet de contrôler une question, ce qui vous permet de vérifier qu'un événement est généré suite à un changement de question. Voir la section Surveillance des questions.
Events	Vous permet d'afficher les événements générés suite à la question sélectionnée. Cette option est uniquement active si la question sélectionnée est posée en mode moniteur. Pour plus d'informations sur les événements, voir le manuel *QRadar - Guide d'utilisation.*
Offenses	Vous permet d'afficher la violation générée suite à la question sélectionnée. Cette option est uniquement active si la question sélectionnée est posée en mode moniteur et que les résultats sont en corrélation avec la question. Pour plus d'informations sur les violations, voir le manuel *IBM Security QRadar SIEM - Guide d'utilisation.*
Actions	La zone de liste déroulante **Actions** vous permet d'exécuter les actions suivantes : • **New** - Vous permet de créer une nouvelle question. Voir la section Création d'une question. • **Duplicate** - Vous permet de copier une question. Voir la section Copie d'une question. • **Edit** - Vous permet d'éditer une question. Voir la section Edition d'une question. • **Delete** - Vous permet de supprimer une question. Voir la section Suppression d'une question. • **Assign Groups** - Vous permet d'affecter une question à un groupe. Voir la section Affectation d'un élément à un groupe.

Affichage des questions

Policy Monitor fournit une liste de modèles de questions par défaut permettant d'évaluer et de contrôler le risque de votre réseau.

Pour afficher les questions par défaut, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Dans le menu de navigation, cliquez sur **Policy Monitor**.

Etape 3 Dans la zone de liste déroulante **Groups**, sélectionnez le groupe de questions à afficher.

Le groupe de questions sélectionné s'affiche dans la table Questions en fournissant les informations suivantes :

Tableau 6-2 Paramètres des questions

Paramètre	Description
Name	Nom associé à cette question.
Group	Groupe ou groupes associé(s) à cette question.
Return Type	Type de question. Les options sont : • Assets • Devices/Rules
Facteur d'importance	Niveau d'importance affecté à cette question. La plage est comprise entre 1 et 10, 10 correspondant au niveau le plus important.
Monitored	Indique si la question est posée en mode moniteur.
Created By	Utilisateur qui a créé la question.
Modified By	Dernier utilisateur à modifier la question.

Etape 4 Sélectionnez la question que vous souhaitez afficher.

La description de la question s'affiche dans la zone Description.

Gestion des questions

Policy Monitor permet de créer, de soumettre, d'approuver, d'éditer, de copier et de supprimer des questions. Cette section fournit des informations sur l'étape suivante :

Création d'une question

Pour créer une question, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Dans le menu de navigation, cliquez sur **Policy Monitor**.

Etape 3 Dans la zone de liste déroulante **Actions**, sélectionnez **New**.

Etape 4 Dans la zone **What do you want to name this question?**, saisissez un nom pour la question.

Etape 5 Dans la zone de liste déroulante **What type of data do you want to return?**, sélectionnez le type de données à retourner.

Lorsqu'une question est soumise, le système recherche la topologie en fonction du type de données que vous sélectionnez. Les options sont :

- **Assets** - Identifie les actifs du réseau qui violent une politique définie ou qui ont induit un risque dans l'environnement. Allez à l'Etape 6.
- **Devices/Rules** - Identifie les règles d'un périphérique qui violent une politique définie ou qui induisent un risque dans l'environnement. Allez à l'Etape 7.

Etape 6 Si vous avez sélectionné **Assets** comme type de données à retourner, utilisez la zone de liste déroulante **Evaluate On** pour indiquer le type de communications que vous souhaitez que cette question prenne en considération. Les options sont les suivantes :

- **Actual Communication** - Comprend tous les actifs sur lesquels les communications ont été détectées à l'aide des connexions.
- **Possible Communication** - Comprend tous les actifs sur lesquels les communications sont autorisées dans votre topologie de réseau, comme les pare-feux. Les questions de communication possible vous permettent de voir si des communications spécifiques sont possibles sur les actifs, qu'une communication ait été ou non détectée.

Etape 7 Dans la zone de liste déroulante **Importance Factor**, sélectionnez le niveau d'importance à associer à cette question.

Ce facteur d'importance permet de calculer l'indice de risque et de définir le nombre de résultats renvoyés pour une question. Le plage est comprise entre 1 (faible importance) et 10 (haute importance). La valeur par défaut est 5.

Tableau 6-3 Matrice de résultats du facteur d'importance

Importance Factor	Résultats renvoyés pour les tests d'actifs	Résultats renvoyés pour les tests des périphériques/règles
1 (faible importance)	10 000	1 000
10 (haute importance)	1	1

Par exemple, une question de politique stipulant **have accepted communication from the internet and include only the following networks (DMZ)** requiert un facteur d'importance élevé de 10, car aucun résultat de la question n'est acceptable en raison de la nature de risque élevé de la question. Cependant, une question de politique stipulant “have accepted communication from the internet and include only the following inbound applications(P2P)” peut nécessiter un facteur d'importance moindre, étant donné que les résultats de la question n'indiquent pas de risque élevé. Vous pouvez donc surveiller cette communication à titre informatif.

Etape 8 Pour déterminer l'intervalle de temps de la question, sélectionnez l'une des options suivantes :

a Pour déterminer un intervalle, sélectionnez l'option **Interval**, puis, à l'aide de la zone de liste déroulante, sélectionnez l'intervalle de temps de la question.

Les options sont les suivantes : Last Hour, Last 24 hrs, Last 7 days et Last 30 days.

b Pour déterminer un intervalle de temps fixe, sélectionnez **Fixed**, puis utilisez les options de date et heure pour appliquer un intervalle de temps à la question.

Etape 9 Dans la zone **Which tests do you want to include in your question?** , sélectionnez le signe **+** à côté des tests à inclure. Les tests d'actif sont divisés dans les deux catégories suivantes :

- **Contributing tests** - Un test de contribution utilise les paramètres de la question pour examiner les indicateurs de risque spécifiés dans la question et génère les résultats des données de risque qui peuvent encore être filtrés à l'aide d'un test de restriction. Les règles suivantes s'appliquent aux tests de contribution :
  - Les tests de contribution s'affichent par défaut dans la fenêtre **Which tests do you want to include in your question?**.
  - Les tests de contribution retournent des données basées sur les actifs détectés correspondant à la question de test.
- **Restrictive tests** - Un test de restriction permet d'affiner les résultats retournés par une question de test de contribution. Les règles suivantes s'appliquent aux tests de restriction :
  - Les tests de restriction s'affichent uniquement dans la fenêtre **Which tests do you want to include in your question?** une fois qu'un test de contribution a été ajouté.
  - Les tests de restriction peuvent uniquement être ajoutés une fois un test de contribution inclus dans la question.
  - La fenêtre Question Editor ne permet pas d'enregistrer un test de restriction si vous retirez ou supprimez la question du test de contribution.

Pour plus d'informations sur les tests de contribution et de restriction, voir la section Soumission d'une question.

REMARQUE

Les questions de périphériques/règles recherchent les violations de règles et de politique et ne comptent pas de composant de test de restriction.

Etape 10 Configurez les paramètres de vos tests.

Les paramètres configurables apparaissent en gras et soulignés. Cliquez sur chaque paramètre pour afficher les options actives de votre question.

REMARQUE

Les questions du moniteur de règles créées pour les actifs ou les périphériques/règles effectuent une évaluation du haut vers le bas. Lors de la création de vos questions de moniteur de règles, l'ordre de la question peut avoir un impact sur les résultats.

Etape 11 Dans la zone Groups, cochez les cases permettant d'affecter cette question à un groupe.

Pour plus d'informations sur le regroupement des questions, voir la section Regroupement des questions.

Etape 12 Cliquez sur **Save Question**.

Pour soumettre la question, voir la section Soumission d'une question.

Soumission d'une question

Une fois que vous avez créé une question, vous pouvez la soumettre pour déterminer le risque associé à cette question. Pour soumettre une question, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Policy Monitor**.

Etape 3 Sélectionnez la question que vous souhaitez soumettre.

Etape 4 Cliquez sur **Submit Question**.

Les résultats s'affichent. Les informations qui s'affichent dépendent de la configuration de la question :

- **Devices** - Pour plus d'informations, voir la table Résulats périphériques/règles.
- **Assets** - Pour plus d'informations, voir la table Asset Results.

Si vous soumettez une question et que vous effectuez ensuite des changements affectant les tests associés à la question, ces changements peuvent prendre jusqu'à une heure pour s'afficher.

La table suivante contient des résultats de périphérique :

Tableau 6-4 Résulats périphériques/règles

Paramètre	Description
Risk Score	Niveau de risque associé à cette question. L'indice de risque est calculé en fonction du nombre de résultats et du facteur d'importance affectés à cette question. Le calcul est basé sur les valeurs suivantes : • Pondération des actifs/périphériques retournée dans les résultats d'une question. Pour plus d'informations sur les actifs, voir le manuel *IBM Security QRadar SIEM - Guide d'utilisation.* • Facteur d'importance de la question. Pour plus d'informations sur le facteur d'importance, voir la section Création d'une question. • Nombre de résultats retournés suite à la question.
Device IP	Adresse IP du périphérique.
Device Name	Nom du périphérique tel qu'il apparaît dans le Moniteur de configuration.

Tableau 6-4 Résulats périphériques/règles (suite)

Paramètre	Description
Device Type	Type de périphérique tel qu'il apparaît dans le profil d'actif. Pour plus d'informations sur les profils d'actif, voir le manuel *IBM Security QRadar SIEM - Guide d'utilisation.*
List	Nom de la règle provenant du périphérique.
Entry	Numéro d'entrée de la règle.
Action	Action associée à la règle correspondant du périphérique. Les options sont les suivantes : permit, deny ou NA.
Source Service(s)	Ports source et comparaison associés à la règle correspondante du périphérique au format suivant : **<comparison>:<port>** Où **<comparison>** peut contenir l'une des options suivantes : • eq - Equal • ne - Not equal • lt - Less than • gt - Greater than Par exemple, si le paramètre indique ne:80, tous les ports autres que 80 s'appliquent à ce service source. Si le paramètre indique lt:80, la plage de ports applicables est comprise entre 0 et 80. Ce paramètre affiche le port source de la règle de périphérique. S'il n'existe aucun port pour cette règle de périphérique, le terme NA s'affiche.
Destination Service(s)	Ports de destination et comparaison associés à la règle correspondante du périphérique au format suivant : **<comparison>:<port>** Où **<comparison>** peut contenir l'une des options suivantes : • eq - Equal • ne - Not equal • lt - Less than • gt - Greater than Par exemple, si le paramètre indique ne:80, tous les ports autres que 80 s'appliquent à ce service de destination. Si le paramètre indique lt:80, la plage de ports applicables est comprise entre 0 et 80. Ce paramètre affiche le port de destination de la règle de périphérique. S'il n'existe aucun port pour cette règle de périphérique, le terme NA s'affiche.
Source(s)	Réseau source associé à cet actif.
Destination(s)	Réseau de destination associé à la règle correspondante du périphérique.

Tableau 6-4 Résulats périphériques/règles (suite)

Paramètre	Description
Protocol(s)	Protocole ou groupe de protocoles associé à la règle correspondant du périphérique.
Signature(s)	Signature de ce périphérique uniquement affichée pour une règle de périphérique IP.

La table suivante contient des résultats d'actif :

Tableau 6-5 Asset Results

Paramètre	Description
Risk Score	L'indice de risque est calculé en fonction du nombre de résultats et de l'élément Importance Factor affectés à cette question. Le niveau de risque indique le niveau de risque associé à cette question. Pour plus d'informations sur l'élément Importance Factor, voir la section Création d'une question.
IP	Adresse IP de l'actif.
Name	Nom de l'actif tel qu'il apparaît dans le profil d'actif. Pour plus d'informations sur les profils d'actif, voir le manuel *QRadar - Guide d'utilisation.*
Weight	Pondération de l'actif telle qu'elle apparaît dans le profil d'actif. Pour plus d'informations sur les profils d'actif, voir le manuel *QRadar - Guide d'utilisation.*
Destination Port(s)	Liste des ports de destination associée à cet actif dans le cadre des tests de question. S'il existe plusieurs ports associés à cet actif et à cette question, cette zone indique Multiple et le nombre. La liste des ports est obtenue en filtrant les connexions associées à cette question afin d'obtenir tous les ports uniques dans lesquels l'actif était la source, la destination ou la connexion. Cliquez sur **Multiple (N)** pour afficher les connexions. Cet écran comprend les connexions agrégées par port, filtrées par l'adresse IP d'actif et basées sur l'intervalle de temps spécifié dans la question.
Protocol(s)	Liste des protocoles associée à cet actif dans le cadre des tests de question. S'il existe plusieurs protocoles associés à cet actif et à cette question, cette zone indique Multiple et le nombre. La liste des protocoles est obtenue en filtrant les connexions associées à cette question afin d'obtenir tous les protocoles uniques dans lesquels l'actif était la source, la destination ou la connexion. Cliquez sur **Multiple (N)** pour afficher les connexions. Cet écran comprend les connexions agrégées par protocole, filtrées par l'adresse IP d'actif et basées sur l'intervalle de temps spécifié dans la question.

Tableau 6-5 Asset Results (suite)

Paramètre	Description
Flow App(s)	Liste des applications associée à cet actif dans le cadre des tests de question. S'il existe plusieurs applications associées à cet actif et à cette question, cette zone indique Multiple et le nombre. La liste des applications est obtenue en filtrant les connexions associées à cette question afin d'obtenir toutes les applications uniques dans lesquelles l'actif était la source, la destination ou la connexion. Cliquez sur **Multiple (N)** pour afficher les connexions. Cet écran comprend les connexions agrégées par applications, filtrées par l'adresse IP d'actif et basées sur l'intervalle de temps spécifié dans la question.
Vuln(s)	Liste des vulnérabilités associée à cet actif dans le cadre des tests de question. S'il existe plusieurs vulnérabilités associées à cet actif et à cette question, cette zone indique Multiple et le nombre. La liste des vulnérabilités est obtenue en utilisant une liste de toutes les vulnérabilités compilées à partir des tests associés et en utilisant cette liste pour filtrer les vulnérabilités détectées sur cet actif. Si aucune vulnérabilité n'est spécifiée pour cette question, toutes les vulnérabilités de l'actif sont utilisées pour compiler cette liste. Cliquez sur **Multiple (N)** pour afficher les actifs. Cet écran comprend les connexions agrégées par vulnérabilité, filtrées par l'adresse IP d'actif et basées sur l'intervalle de temps spécifié dans la question.
Flow Count	Nombre total de flux associé à cet actif dans le cadre des tests de question. Le nombre de flux est déterminé en filtrant les connexions associées à cette question afin d'obtenir le nombre total de flux dans lesquels l'actif était la source, la destination ou la connexion.
Source(s)	Liste des adresses IP source associées à cet actif dans le cadre des tests de question. S'il existe plusieurs adresses IP source associées à cet actif et à cette question, cette zone indique Multiple et le nombre. La liste des adresses IP source est obtenue en filtrant les connexions associées à cette question afin d'obtenir tous les adresses IP source uniques dans lesquelles l'actif est la destination de la connexion. Cliquez sur **Multiple (N)** pour afficher les connexions. Cet écran comprend les connexions agrégées par adresse IP source, filtrées par l'adresse IP d'actif basée sur l'intervalle de temps spécifié dans la question.

Tableau 6-5 Asset Results (suite)

Paramètre	Description
Destination(s)	Liste des adresses IP de destination associées à cet actif dans le cadre des tests de question. S'il existe plusieurs adresses IP de destination associées à cet actif et à cette question, cette zone indique Multiple et le nombre. La liste des adresses IP de destination est obtenue en filtrant les connexions associées à cette question afin d'obtenir tous les adresses IP de destination uniques dans lesquelles l'actif est la source de la connexion. Cliquez sur **Multiple (N)** pour afficher les connexions. Cet écran comprend les connexions agrégées par adresses IP de destination, filtrées par l'adresse IP d'actif basée sur l'intervalle de temps spécifié dans la question.
Flow Source Bytes	Nombre total d'octets source associé à cet actif dans le cadre des tests de question. Le nombre d'octets source est déterminé en filtrant les connexions associées à cette question afin d'obtenir le nombre total d'octets source dans lequel l'actif est la source de la connexion.
Flow Destination Bytes	Nombre total d'octets de destination associé à cet actif dans le cadre des tests de question. Le nombre d'octets de destination est déterminé en filtrant les connexions associées à cette question afin d'obtenir le nombre total d'octets de destination dans lequel l'actif est la destination de la connexion.

Validation des résultats d'une question

Les résultats retournés suite à la soumission d'une question de Policy Monitor permettent à un utilisateur d'évaluer la liste d'actifs ou de règles de périphérique retournée afin de déterminer le niveau de risque impliqué. La validation d'un résultat de question revient à adapter votre système pour informer QRadar Risk Manager que l'actif associé au résultat de la question est sécurisé ou peut être ignoré à l'avenir. Lorsqu'un utilisateur valide un résultat d'actif, le composant Policy Monitor voit ce résultat d'actif comme validé et lorsque la question du Policy Monitor sera soumise ou contrôlée à l'avenir, l'actif ne sera pas répertorié dans les résultats de la question. L'actif validé n'apparaît pas dans la liste de résultats de la question à moins que la validation ne soit révoquée. Policy Monitor enregistre l'utilisateur et l'adresse IP du périphérique, le motif de l'approbation, le périphérique ou les règles applicables, ainsi que la date et l'heure pour les administrateurs de la sécurité de votre entreprise. Pour approuver les résultats d'une question :

Etape 1 Dans la table de résultats, cochez la case en regard des résultats à valider.

Pour plus d'informations sur la soumission d'une question pour obtenir des résultats, voir la section Soumission d'une question

Etape 2 Sélectionnez l'une des options suivantes :

a Si vous souhaitez valider tous les résultats, cliquez sur **Approve All**.

Un message de confirmation s'affiche. Vous devez confirmer vos sélections avant de poursuivre.

b Si vous souhaitez valider des résultats spécifiques, cochez la case en regard des résultats à accepter, puis cliquez sur **Approve Selected**.

La fenêtre Approval Note s'affiche.

Etape 3 Entrez le motif de la validation.

Etape 4 Cliquez sur **OK**.

Une fenêtre de confirmation s'affiche.

Etape 5 Cliquez sur **OK**.

Etape 6 Pour afficher les résultats validés de la question, cliquez sur **View Approved**.

La fenêtre Approved Question Results contient les informations suivantes :

Tableau 6-6 Paramètres Approved Question Results

Paramètre	Description
Device/Rule	Pour un résultat de question de périphérique ou de règle, cette option indique le périphérique associé à ce résultat.
IP	Pour un résultat de question d'actif, cette option indique l'adresse IP associée à l'actif.
Approved By	Utilisateur qui a validé les résultats.
Approved On	Date et l'heure de validation des résultats.
Remarques	Affiche le texte des notes associées à ce résultat, comme indiqué dans Etape 3.

REMARQUE

Si vous souhaitez supprimer les validations d'un résultat, cochez la case de chaque résultat dont vous souhaitez supprimer la validation et cliquez sur **Revoke Selected**. Pour supprimer toutes les validations, cliquez sur **Revoke All**.

Edition d'une question

Pour éditer une question, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Policy Monitor**.

Etape 3 Sélectionnez la question à éditer.

Etape 4 Dans la zone de liste déroulante **Actions**, sélectionnez **Edit**.

Etape 5 Mettez à jour les paramètres, au besoin.

Pour plus d'informations sur les paramètres Question Editor, voir la section Création d'une question.

Etape 6 Cliquez sur **Save Question**.

Copie d'une question

Pour copier une question, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Policy Monitor**.

Etape 3 Sélectionnez la question que vous souhaitez copier.

Etape 4 Dans la zone de liste déroulante **Actions**, sélectionnez **Duplicate**.

Etape 5 Tapez un nom que vous souhaitez attribuer à la question copiée.

Etape 6 Cliquez sur **OK**.

Etape 7 Editez la question si nécessaire.

Pour plus d'informations sur l'édition d'une question, consultez Edition d'une question.

Suppression d'une question

Pour supprimer une question, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Policy Monitor**.

Etape 3 Sélectionnez la question que vous souhaitez supprimer.

Etape 4 Dans la zone de liste déroulante **Actions**, sélectionnez **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 5 Cliquez sur **OK**.

Surveillance des questions

Si vous souhaitez générer un événement lorsque les résultats d'une question changent, vous pouvez configurer une question à contrôler. Lorsque vous sélectionnez une question à contrôler, QRadar Risk Manager analyse en continu la question pour déterminer si les résultats d'une question changent. Si QRadar Risk Manager détecte un changement de résultats, une violation peut être générée pour vous avertir d'un changement dans votre politique définie. QRadar Risk Manager peut contrôler les résultats de 10 questions en mode moniteur.

Une question en mode moniteur correspond par défaut à un intervalle de temps d'1 heure. Cette valeur écrase la valeur temporelle définie lors de la création de la question. Pour plus d'informations sur la création d'une question, voir la section Création d'une question.

Pour configurer une question à contrôler, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Policy Monitor**.

Etape 3 Sélectionnez la question que vous souhaitez contrôler.

Etape 4 Cliquez sur **Monitor**.

Etape 5 Configurez la valeur des paramètres ci-dessous :

Tableau 6-7 Paramètres Monitor Question Results

Paramètre	Description
Event Name	Entrez le nom de l'événement que vous souhaitez afficher dans les onglets **Log Activity** et **Offenses**.
Event Description	Entrez une description de l'événement. La description est affichée dans le panneau Annotations des détails de l'événement.
Event Details	Configurez les options suivantes : • **High-Level Category** - Dans la zone de liste déroulante, sélectionnez les catégories d'événements de haut niveau dont vous avez besoin lors du traitement des événements. • **Low-Level Category** - Dans la zone de liste déroulante, sélectionnez les catégories d'événements de bas niveau dont vous avez besoin lors du traitement des événements. Pour plus d'informations sur les catégories d'événements, consultez *QRadar - Guide d'utilisation*. • **Ensure the dispatched event is part of an offense (Correlate By:)** - Cochez cette case si vous voulez, qu'à la suite de cette question contrôlée, les événements soient transmis au composant magistrate. Si aucune violation n'a été créée, une nouvelle violation est créée. Si une violation existe, cet événement est ajouté. Si vous cochez cette case, l'option suivante s'affiche : **Question/Simulation** - Tous les événements d'une question sont associés à une violation unique. **Asset** - Une violation unique est créée (ou mise à jour) pour chaque actif unique. • **Dispatch question passed events** - Cochez cette case pour transférer les événements passant par la question du moniteur de règles vers le composant Magistrate.

Tableau 6-7 Paramètres Monitor Question Results (suite)

Paramètre	Description
Additional Actions	Cochez ces cases pour indiquer les actions supplémentaires à entreprendre lorsqu'un événement est enregistré. Les options sont les suivantes : • **Email** - Cochez cette case et entrez l'adresse électronique pour envoyer une notification si l'événement est généré. Séparez par virgule plusieurs adresses électroniques. • **Send to Syslog** - Cochez cette case si vous souhaitez consigner l'événement. Par défaut, la case est décochée. Par exemple, la sortie syslog peut ressembler à : `Sep 28 12:39:01 localhost.localdomain ECS: Rule 'Name of Rule' Fired: 172.16.60.219:12642 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID: 1000398, Category: 1011, Notes: Event description` • **Notify** - Cochez cette case si vous voulez que les événements qui se génèrent à la suite de cette question contrôlée s'affichent dans l'élément System Notifications du tableau de bord. Pour plus d'informations sur l'onglet **Log Activity** et le tableau de bord QRadar SIEM, voir le manuel *IBM Security QRadar SIEM - Guide d'utilisation.*
Enable Monitor	Cochez cette case si vous voulez surveiller la question. Cette case est cochée par défaut. Si vous ne souhaitez pas surveiller une question, décochez cette case.

Etape 6 Cliquez sur **Save Monitor**.

Regroupement des questions

Vous pouvez regrouper et afficher vos questions en fonction de vos critères choisis. Le classement de vos questions vous permet d'afficher et de suivre efficacement vos questions. Par exemple, vous pouvez afficher toutes les questions relatives à la conformité.

Lorsque vous créez de nouvelles questions, vous pouvez affecter la question à un groupe existant. Pour plus d'informations sur l'affectation d'un groupe, consultez Gestion des questions.

Viewing Groups

Pour afficher les questions à l'aide des groupes, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Policy Monitor**.

Etape 3 Dans la zone de liste déroulante **Group**, sélectionnez le groupe à afficher.

La liste des éléments affectés à ce groupe s'affiche.

Création d'un groupe Pour créer un groupe :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Policy Monitor**.

Etape 3 Cliquez sur **Groups**.

Etape 4 Dans l'arborescence du menu, sélectionnez le groupe dans lequel vous souhaitez créer un nouveau groupe.

Etape 5 Cliquez sur **New**.

Etape 6 Configurez les valeurs des paramètres suivants :

- **Name** - Entrez le nom à affecter au nouveau groupe. Le nom peut contenir jusqu'à 225 caractères.
- **Description** - Entrez une description à affecter à ce groupe. La description peut contenir plus de 255 caractères.

Etape 7 Cliquez sur **OK**.

Etape 8 Pour changer l'emplacement du nouveau groupe, cliquez sur le nouveau groupe et faites glisser le dossier vers l'emplacement choisi dans votre arborescence de menus.

Etape 9 Fermez la fenêtre Groups.

Edition d'un groupe Pour modifier un groupe :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Policy Monitor**.

Etape 3 Cliquez sur **Groups**.

Etape 4 Dans l'arborescence de menu, sélectionnez le groupe que vous souhaitez éditer.

Etape 5 Cliquez sur **Edit**.

Etape 6 Mettez les valeurs des paramètres à jour, si nécessaire :

- **Name** - Entrez le nom à affecter au nouveau groupe. Le nom peut contenir jusqu'à 225 caractères.
- **Description** - Entrez une description à affecter au nouveau groupe. La description peut contenir plus de 255 caractères.

Etape 7 Cliquez sur **OK**.

Etape 8 Pour changer l'emplacement du groupe, sélectionnez le groupe et faites glisser le dossier vers l'emplacement favori dans l'arborescence de menus.

Etape 9 Fermez la fenêtre Groups.

Copie d'un élément dans un autre groupe

En utilisant la fonctionnalité Question Groups, vous pouvez copier une question vers un ou plusieurs groupes.

Pour copier une question, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Policy Monitor**.

Etape 3 Cliquez sur **Groups**.

Etape 4 Dans l'arborescence de menu, sélectionnez la question que vous souhaitez copier dans un autre groupe.

Etape 5 Cliquez sur **Copy**.

Etape 6 Cochez la case pour le groupe dans lequel vous souhaitez copier la question.

Etape 7 Cliquez sur **Assign Groups**.

Etape 8 Fermez la fenêtre Groups.

Suppression d'un élément d'un groupe

Pour supprimer une question d'un groupe, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Policy Monitor**.

Etape 3 Cliquez sur **Groups**.

Etape 4 Dans l'arborescence de menus, sélectionnez le groupe de niveau supérieur.

Etape 5 Dans la liste des groupes, sélectionnez le groupe que vous souhaitez supprimer.

Etape 6 Cliquez sur **Remove**.

Etape 7 Cliquez sur **OK**.

Etape 8 Si vous souhaitez modifier l'emplacement du nouveau groupe, cliquez sur le nouveau groupe en question et déplacez le dossier vers l'emplacement désiré dans l'arborescence du menu.

Etape 9 Fermez la fenêtre Groups.

Affectation d'un élément à un groupe

Pour affecter une question à un groupe, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Policy Monitor**.

Etape 3 Sélectionnez la question à affecter à un groupe.

Etape 4 Dans la zone de liste déroulante **Actions**, sélectionnez **Assign Groups**.

Etape 5 Sélectionnez le groupe auquel vous souhaitez affecter la question.

Etape 6 Cliquez sur **Assign Groups**.

Cas d'utilisation de Policy Monitor

Policy Monitor propose de nombreuses options lors de la création de questions pour analyser les risques encourus par votre réseau. Les exemples de composant Policy Monitor ci-dessous présentent des cas d'utilisation courant que vous pouvez utilisez dans votre environnement de réseau. Les questions de cas d'utilisation suivantes sont présentées :

- Test d'actif pour les communications réelles des protocoles restreints DMZ. Voir la section Communication réelle des protocoles agréés DMZ.
- Test d'actif pour les communications possibles sur le serveur indispensable à la mission. Voir la section Test d'actifs en vue d'une éventuelle communication avec des actifs protégés.
- Test de périphérique pour détecter le moment où une règle de pare-feu permet d'accéder à un protocole dangereux. Voir la section Communication test de périphérique/règle par un accès Internet.

Communication réelle des protocoles agréés DMZ

Dans la plupart des organisations, le trafic réseau à travers DMZ est limité aux protocoles bien connus et sécurisés, tels que HTTP ou HTTPS sur des ports spécifiés. En cas de risque, il est important de contrôler en continu le trafic dans le DMZ afin de s'assurer que seuls des protocoles sécurisés sont présents. QRadar Risk Manager effectue cette opération en créant une question du moniteur de règles basée sur le test d'actif pour les communications réelles.

Il existe plusieurs façons de générer une question de moniteur de règles pour ce cas d'utilisation. Etant donné que nous savons que la politique de réseau autorise uniquement quelques protocoles sécurisés, nous sélectionnons une option pour créer notre question de moniteur de règles en fonction de la liste connue de protocoles sécurisés pour DMZ.

Pour créer une question de moniteur de règles pour DMZ, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Policy Monitor**.

Etape 3 Dans la zone de liste déroulante **Actions**, sélectionnez **New**.

Etape 4 Configurez les valeurs suivantes :

a **What do you want to name this question?** - Saisissez un nom pour la question du composant Policy Monitor.

b **What type of data do you want to return?** - Sélectionnez **Assets**.

c **Evaluate On** - Sélectionnez **Actual Communication**.

d **Importance Factor** - Indiquez un niveau d'importance à associer à votre question de composant Policy Monitor.

e **Time Range** - Indiquez l'intervalle de temps de la question.

Etape 5 A l'aide de la zone **Which tests do you want to include in your question?** , sélectionnez le signe **+** à côté des tests suivants :

a Sélectionnez le test de contribution **have accepted communication to destination networks**.

Une fois le test affiché dans la fenêtre **Find Assets that**, les paramètres configurables apparaissent en gras et soulignés. Dès que vous avez ajouté un test de contribution, les tests de restriction s'affichent et peuvent à leur tour être ajoutés.

b Cliquez sur **destination networks** pour continuer à configurer ce test et spécifier votre DMZ comme réseau de destination.

c Sélectionnez le test de restriction **and exclude the following inbound ports**.

d Cliquez sur **ports**.

La fenêtre Specify Parameter s'affiche.

e Tapez **80**, puis cliquez sur **Add**.

f Tapez **443**, puis cliquez sur **Add**.

Etape 6 Cliquez sur **Save Question**.

Etape 7 Sélectionnez la question DMZ du composant Policy Monitor que vous avez créée.

Etape 8 Cliquez sur **Submit Question**.

Etape 9 Examinez les résultats pour voir si des protocoles autres que le port 80 et le port 443 communiquent sur le réseau.

Etape 10 Facultatif. Une fois les résultats correctement ajustés, vous pouvez contrôler votre question DMZ en mettant la question en mode moniteur

Pour plus d'informations, voir la section Surveillance des questions.

Test d'actifs en vue d'une éventuelle communication avec des actifs protégés

Toutes les organisations possèdent des réseaux qui contiennent des serveurs critiques dans lesquels le trafic est contrôlé et est uniquement accessible par les employés dignes de confiance. En cas de risque, il est important de savoir quels utilisateurs de votre organisation peuvent communiquer avec les actifs de réseau critiques. QRadar Risk Manager effectue cette tâche en créant une question du moniteur de règles basée sur le test d'actif pour les communications possibles.

Il existe plusieurs façons de générer une question de moniteur de règles pour ce cas d'utilisation. Vous pouvez consulter toutes les connexions au serveur critique dans le temps, mais vous ne devez pas oublier que les employés régionaux n'accèdent pas à ces serveurs critiques. Pour ce faire, vous pouvez créer une question de moniteur de règles concernant la topologie du réseau par adresse IP.

Pour créer une question de moniteur de règles par adresse IP, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Policy Monitor**.

Etape 3 Dans la zone de liste déroulante **Actions**, sélectionnez **New**.

Etape 4 Configurez les valeurs suivantes :

a **What do you want to name this question?** - Saisissez un nom pour la question du composant Policy Monitor.

b **What type of data do you want to return?** - Sélectionnez **Assets**.

c **Evaluate On** - Sélectionnez **Possible Communication**.

d **Importance Factor** - Indiquez un niveau d'importance à associer à votre question de composant Policy Monitor.

e **Time Range** - Indiquez l'intervalle de temps de la question.

Etape 5 Dans la fenêtre **Which tests do you want to include in your question?** , sélectionnez le signe **+** en regard des tests suivants :

a Sélectionnez le test de contribution **have accepted communication to destination asset building blocks**.

Une fois le test de contribution affiché dans la zone **Find Assets that**, les paramètres configurables apparaissent en gras et soulignés. Dès que vous avez ajouté un test de contribution, les tests de restriction sont disponibles.

b Cliquez sur **asset building blocks** pour continuer à configurer ce test et spécifier **Protected Assets**.

REMARQUE

Pour définir vos actifs distant de réseau, vous devez avoir précédemment défini vos éléments structurants d'actifs distants.

c Sélectionnez le test de restriction **et intégrez uniquement l'adresse IP suivante**.

d Cliquez sur **IP Address**.

La fenêtre Specify Parameter s'affiche.

e Indiquez la plage d'adresse IP ou d'adresse CIDR de votre réseau distant.

Etape 6 Cliquez sur **Save Question**.

Etape 7 Sélectionnez la question du composant Policy Monitor que vous avez créée pour les actifs protégés.

Etape 8 Cliquez sur **Submit Question**.

Les résultats s'affichent.

Etape 9 Examinez les résultats pour voir si un actif protégé a accepté la communication à partir d'une adresse IP ou d'une plage CIDR inconnue.

Etape 10 Facultatif. Une fois les résultats correctement ajustés, vous pouvez contrôler vos actifs protégés en mettant la question en mode moniteur Si un actif protégé se connecte à une adresse IP non reconnue, alors QRadar Risk Manager peut générer une alerte.

Pour plus d'informations, voir la section Surveillance des questions.

Communication test de périphérique/règle par un accès Internet

Les tests de périphériques identifient les règles d'un périphérique qui violent une politique définie ou des changements, introduisant des risques dans l'environnement. Côté réseau, il est important de savoir quelles règles de périphérique peuvent avoir changé et de vous en avertir afin de les corriger. Une situation très courante est lorsqu'un serveur qui ne disposait auparavant pas d'un accès Internet s'en voit accorder un suite à un changement de pare-feu sur le réseau. QRadar Risk Manager peut surveiller les changements de règles des périphériques réseau en créant une question du moniteur de règles basée sur les règles de périphérique.

Il existe plusieurs façons de générer une question de moniteur de règles pour ce cas d'utilisation. Dans cet exemple, vous créez une question de moniteur de règles permettant de savoir quels périphériques ont accès à Internet.

Pour créer une question de moniteur de règles par adresse IP, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Policy Monitor**.

Etape 3 Dans la zone de liste déroulante **Actions**, sélectionnez **New**.

Etape 4 Configurez les valeurs suivantes :

- **a** **What do you want to name this question?** - Saisissez un nom pour la question du composant Policy Monitor.
- **b** **What type of data do you want to return?** - Sélectionnez **Device/Rules**.
- **c** **Importance Factor** - Indiquez un niveau d'importance à associer à votre question de composant Policy Monitor.

Etape 5 Dans la fenêtre **Which tests do you want to include in your question?** , sélectionnez le signe **+** et ajoutez les tests suivants : **allow connection to the internet**.

REMARQUE

Les questions de périphériques/règles recherchent les violations de règles et de politique et ne comptent pas de composant de test de restriction.

Les paramètres configurables apparaissent en gras et soulignés.

Etape 6 Cliquez sur **Save Question**.

Etape 7 Sélectionnez la question du composant Policy Monitor que vous avez créée pour surveiller les règles de périphérique.

Etape 8 Cliquez sur **Submit Question**.

Etape 9 Examinez les résultats pour voir si des règles autorisent l'accès à Internet.

Etape 10 Facultatif. Une fois les résultats correctement ajustés, vous pouvez contrôler vos actifs protégés en mettant la question en mode moniteur

Pour plus d'informations, voir la section Surveillance des questions.

7 ANALYSE DES CONNEXIONS

Une connexion est un enregistrement d'une communication (comprenant les communications refusées) entre deux adresses IP uniques via un port de destination spécifique, tel qu'il est détecté sur un intervalle de temps spécifique (par défaut 1 heure). Si deux adresses IP communiquent plusieurs fois sur le même intervalle sur un port, une seule communication est enregistrée, mais les octets communiqués et le nombre de flux sont cumulés avec la connexion. A la fin de l'intervalle, les informations de connexion sont cumulées sur l'intervalle et sont stockées dans la base de données.

Les connexions vous permettent de surveiller et d'analyser les connexions du périphérique réseau ou d'effectuer des recherches avancées. Vous pouvez utiliser les connexions pour :

- Rechercher les connexions
- Rechercher un sous-ensemble de connexions (sous-recherche)
- Afficher les informations de connexion regroupées par diverses options
- Exporter les connexions au format XML ou CSV

Utilisation de la barre d'outils Connections

A l'aide de la barre d'outils, vous pouvez accéder aux options suivantes :

Tableau 7-1 Options de la barre d'outils

Option	Description
Search	Dans la zone de liste déroulante **Search**, sélectionnez une option pour effectuer des recherches avancées sur vos connexions. Les options comprennent : • **New Search** - Vous permet de créer une nouvelle recherche. • **Edit Search** - Vous permet de sélectionner et d'éditer une recherche. • **Manage Search Results** - Vous permet d'afficher et de gérer les résultats de la recherche. Voir la section Gérer les résultats de recherche. Pour plus d'informations sur la fonction de recherche, voir la section Utilisation de la fonction de recherche.

Tableau 7-1 Options de la barre d'outils (suite)

Option	Description
Quick Searches	Dans la zone de liste déroulante **Quick Searches**, vous pouvez exécuter les recherches précédemment sauvegardées. Les options s'affichent uniquement lorsque vous créez une recherche et que vous cochez la case **Include in my Quick Searches**.
Add Filter	Cliquez sur **Add Filter** afin d'ajouter un filtre aux résultats de la recherche en cours.
Save Criteria	Cliquez sur **Save Criteria** afin de sauvegarder le critère de recherche suivant.
Save Results	Cliquez sur **Save Results** afin de sauvegarder les résultats de la recherche en cours. Cette option s'affiche uniquement une fois qu'une recherche est terminée.
Cancel	Cliquez sur **Cancel** pour annuler une recherche en cours.
False Positive	Cliquez sur **False Positive** pour marquer un résultat de la recherche comme étant un faux positif. Vous pouvez utiliser la fonction False Positive Tuning pour différencier les événements de faux positif des violations créées.
Actions	La zone de liste déroulante **Actions** vous permet d'exécuter les actions suivantes : • **Show All** - Permet de supprimer tous les filtres sur les critères de recherche et d'afficher toutes les connexions. • **Print** - Vous permet d'imprimer les connexions affichées dans la fenêtre. • **Export to XML** - Vous permet d'exporter les connexions au format XML. Voir la section Exportation de connexions. • **Export to CSV** - Vous permet d'exporter les connexions au format CSV. Voir la section Exportation de connexions. • **Delete** - Vous permet de supprimer un résultat de la recherche. Voir la section Suppression d'une recherche. • **Notify** - Vous permet d'indiquer que vous souhaitez un courrier électronique de notification à la fin des recherches sélectionnées. Cette option est uniquement activée pour les recherches en cours.

Affichage des connexions

Pour afficher les connexions, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Dans le menu de navigation, cliquez sur **Connections**.

Si vous avez enregistré précédemment une recherche par défaut, les résultats enregistrés pour cette recherche sont affichés. Par défaut, la fenêtre Connections affiche les graphiques suivants :

- Le graphique des enregistrements comparés dans le temps fournit des informations de série temporelle indiquant le nombre de connexions basées sur le temps.
- Graphique des connexions fournissant une représentation visuelle des connexions récupérées.

Pour plus d'informations sur les graphiques, voir la section Utilisation des graphiques. Pour plus d'informations sur l'enregistrement des critères de recherche, voir la section Enregistrement critères de recherche.

Etape 3 Dans la zone de liste déroulante **View**, sélectionnez l'intervalle de temps à afficher.

La fenêtre Connections affiche les informations suivantes :

Tableau 7-2 Fenêtre Connections - Valeurs par défaut

Paramètre	Description
Current Filters	En haut de la table s'affichent les détails du filtre appliqué au résultat de la recherche. Pour effacer les valeurs de filtre, cliquez sur **Clear Filter.** ***Remarque :*** *Ce paramètre s'affiche uniquement après avoir appliqué un filtre.*
View	Vous permet d'indiquer l'intervalle de temps que vous souhaitez filtrer. Dans la zone de liste déroulante, sélectionnez l'intervalle de temps que vous souhaitez filtrer.
Current Statistics	Les statistiques actuelles sont les suivantes : • **Total Results** - Nombre total de résultats correspondant à vos critères de recherche. • **Data Files Searched** - Nombre total de fichiers de données recherchés pendant l'intervalle de temps spécifié. • **Compressed Data Files Searched** - Nombre total de fichiers de données compressées recherchées au cours de l'intervalle de temps spécifié. • **Index File Count** - Nombre total de fichiers d'indexation recherchés pendant l'intervalle de temps spécifié. • **Duration** - Durée de la recherche. ***Remarque :*** *Les statistiques en cours sont utiles pour l'identification et la résolution des problèmes. Lorsque vous contactez le service clients pour identifier et résoudre un problème, on pourrait vous demander de fournir des informations statistiques actuelles. Cliquez sur la flèche à côté de Current statistics pour afficher ou masquer les statistiques.*
Charts	Affiche les graphiques représentant les enregistrements correspondants par intervalle de temps et/ou option de regroupement. Cliquez sur **Hide Charts** si vous souhaitez supprimer les graphiques de votre affichage. Pour plus d'informations sur la configuration des graphiques, voir la section Utilisation des graphiques. ***Remarque :*** *Si vous utilisez Mozilla Firefox en tant que navigateur et qu'une extension de navigateur Adblock Plus est installée, les graphiques ne s'affichent pas. Pour que les graphiques s'affichent, vous devez supprimer l'extension de navigateur Adblock Plus. Pour plus d'informations, consultez la documentation du navigateur.*
Last Packet Time	Last Packet Time indique la date et l'heure du dernier paquet traité pour cette connexion.
Source Type	Source Type est le type de source de cette connexion. Les options sont les suivantes : Host ou Remote.

Tableau 7-2 Fenêtre Connections - Valeurs par défaut (suite)

Paramètre	Description
Source	Source de cette connexion. Les options sont : • **IP address** - Adresse IP de la source de cette connexion. L'adresse IP s'affiche si le type de source est Host. • **Country** - Pays source (avec le drapeau du pays) de cette connexion. Le drapeau du pays s'affiche si le type de source est remote.
Destination Type	Type de destination de cette connexion. Les options sont les suivantes : Host ou Remote.
Destination	Adresse IP du type d'hôte comprenant le drapeau du pays. Les options sont : • **IP address** - Adresse IP de la destination de cette connexion. L'adresse IP s'affiche si le type de destination est Host. • **Country** - Pays destination (avec le drapeau du pays) de cette connexion. Le drapeau du pays s'affiche uniquement si le type de destination est remote.
Protocole	Protocole utilisé pour cette connexion.
Destination Port	Port de destination de cette connexion.
Flow Application	Application de flux ayant généré la connexion.
Flow Source	Source de flux associée à cette connexion. Ce paramètre s'applique uniquement aux connexions validées.
Flow Count	Nombre total de flux associés à cette connexion.
Flow Source Bytes	Nombre total d'octets de source de flux associés à cette connexion.
Flow Destination Bytes	Nombre total d'octets de destination associés à cette connexion.
Log Source	Source des événements ayant contribué à cette connexion.
Event Count	Nombre total d'événements détectés pour la connexion.
Connection Type	Type de connexion. Les options sont : • **Allow** - Permet d'établir la connexion. • **Deny** - Permet de refuser la connexion.

Utilisation des graphiques

La fenêtre Connections vous permet d'afficher les données de connexion à l'aide de différentes options de graphique. Par défaut, vous pouvez afficher les données à l'aide des types de graphiques suivants :

- **Records matched over time** - Indique le nombre de connexions basées sur le temps. Voir la section Utilisation du graphique de série temporelle.
- **Connection graph** - Fournit une représentation visuelle des connexions récupérées. Si vous souhaitez continuer à analyser les connexions à l'aide du graphique des connexions, voir la section Utilisation du graphique de connexions.

Les options de graphique suivantes sont disponibles pour les connexions regroupées sous forme de résultat d'une recherche. Pour plus d'informations sur la recherche des connexions, voir la section Utilisation de la fonction de recherche.

- **Table** - Affiche les données dans une table.
- **Bar** - Affiche les données dans un graphique à barres.
- **Pie** - Affiche les données dans un graphique circulaire.

MISE EN GARDE

Si vous utilisez Mozilla Firefox en tant que navigateur et qu'une extension de navigateur Adblock Plus est installée, les graphiques risquent de ne pas s'afficher correctement. Pour que les graphiques s'affichent, vous devez supprimer l'extension de navigateur Adblock Plus s'il est installé. Pour plus d'informations sur la suppression des ajouts, consultez la documentation de votre navigateur.

Utilisation du graphique de série temporelle

Les graphiques de série temporelle sont des représentations graphiques de vos connexions au fil du temps, les pics et creux qui s'affichent représentent l'activité haute et basse des connexions. Les graphiques de série temporelle sont utiles pour l'analyse des tendances de données à court et à long terme. À l'aide des graphiques de série temporelle, vous pouvez accéder, naviguer et analyser les connexions de divers points de vue et perspectives.

Pour configurer des graphiques de série temporelle, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Dans le menu de navigation, cliquez sur **Connections**.

La fenêtre Connections s'affiche.

Si vous avez déjà sauvegardé une recherche en tant que recherche par défaut, les résultats de cette recherche s'affichent. Si la recherche comprend les options Group By sélectionnées dans la zone Advanced View Definitions, le graphique de série temporelle n'est pas disponible. Vous devez supprimer les critères de recherche avant de poursuivre. Pour plus d'informations sur l'enregistrement des critères de recherche, voir la section Enregistrement critères de recherche.

Etape 3 Dans la sous-fenêtre Charts, cliquez sur l'icône **Configuration**.

La zone de liste déroulante **Chart Type** s'affiche.

Etape 4 Dans la zone de liste déroulante **Chart Type**, sélectionnez **Time Series**.

Le graphique de série temporelle est affiché.

Etape 5 A l'aide des graphiques de série temporelle interactifs, vous pouvez parcourir une ligne temporelle pour analyser les connexions.

La table suivante fournit les fonctions que vous pouvez utiliser pour afficher les graphiques de série temporelle comme :

Tableau 7-3 Fonctions de graphiques de séries temporelles

Si vous souhaitez	Alors
Afficher les connexions plus en détail	Le fait d'augmenter les données d'un graphique de série temporelle vous permet d'analyser des segments temporels plus petits des connexions. Vous pouvez agrandir le graphique de séries temporelles à l'aide des options suivantes : • Appuyez sur le bouton Shift et cliquez sur le temps que vous souhaitez étudier dans le graphique. • Appuyez sur les boutons Maj et Ctrl lorsque vous cliquez et vous glissez le pointeur de la souris sur l'intervalle que vous souhaitez afficher. • Placez le pointeur de votre souris sur le graphique, puis appuyez sur la flèche vers le bas de votre clavier. • Placez le pointeur de votre souris sur le graphique et ensuite utilisez la molette de votre souris pour effectuer un zoom avant (roulez la molette de la souris vers le haut). Une fois que vous avez agrandi un graphique de série temporelle, le graphique s'actualise pour afficher un plus petit segment de temps.
Afficher une plus grande intervalle de temps des connexions	Le fait d'intégrer des intervalles de temps supplémentaires dans le graphique des séries temporelles vous permet d'étudier les plus grands segments temporels ou de revenir à la plage horaire maximale. Vous pouvez afficher un intervalle de temps en utilisant l'une des options suivantes : • Cliquez sur **Max** à gauche du graphique ou appuyez sur la touche Home pour retourner à l'intervalle de temps maximal. • Placez le pointeur de votre souris sur le graphique, puis appuyez sur la flèche vers le bas sur votre clavier. • Placez le pointeur de votre souris sur le graphique du tracé et ensuite utilisez la molette de votre souris pour effectuer un zoom arrière (roulez la molette de la souris vers le bas).

Tableau 7-3 Fonctions de graphiques de séries temporelles (suite)

Si vous souhaitez	Alors
Analyser le graphique	Pour afficher le graphique afin de déterminer les informations sur chaque point de données, procédez comme suit : • Cliquez et faites glisser le graphique pour analyser la ligne de temps. • Appuyez sue le bouton Page Up pour que la ligne de temps supprime une page complète vers la gauche. • Appuyez sur la touche de déplacement vers la gauche pour déplacer la page de la moitié de ligne de temps vers la gauche. • Appuyez sur le bouton Page Down pour que la ligne de temps déplace toute la page vers la droite. • Appuyez sur la touche de déplacement vers la droite pour déplacer la page de la moitié de ligne de temps vers la droite

Etape 6 Pour actualiser les informations dans le graphique, cliquez sur **Update Details**.

Utilisation du graphique de connexions

Le graphique des connexions fournit une représentation visuelle des connexions dans votre réseau. Le graphique qui ne s'affiche pas dans la fenêtre Connections n'est pas interactif. Toutefois, si vous cliquez sur le graphique, la fenêtre Radial Data Viewer s'affiche. La fenêtre Radial Data Viewer vous permet de manipuler le graphique si nécessaire.

Par défaut, le graphique affiche vos connexions réseau comme suit :

- Seules les connexions autorisées s'affichent.
- Toutes les adresses IP locales sont réduites pour afficher uniquement les réseaux en feuilles.
- Tous les noeuds de pays sont réduits en un noeud appelé Remote Countries.
- Tous les noeuds distants sont réduits en un noeud appelé Remote Networks.
- La prévisualisation de la vue miniature du graphique affiche une partie du graphique principal. Cette option est utile pour les graphiques de grande taille.

Radial Data Viewer comprend plusieurs options de menu, comme :

Tableau 7-4 Options du menu Radial Data Viewer

Option de menu	Description
Connection Type	Par défaut, le graphique radial affiche les connexions validées. Si vous souhaitez afficher les connexions refusées, sélectionnez **Deny** dans la zone de liste déroulante **Connection Type**.

Tableau 7-4 Options du menu Radial Data Viewer (suite)

Option de menu	Description
Undo	Permet de réduire le développement du dernier noeud. Si vous souhaitez annuler plusieurs développements, cliquez sur le bouton **Undo** pour chaque développement.
Download	Vous permet d'enregistrer le graphique sous forme d'image JPEG.

La table suivante contient des fonctions supplémentaires pour afficher les connexions, comme :

Tableau 7-5 Fonctions Radial Data Viewer

Si vous souhaitez...	Alors...
Effectuer un zoom avant ou arrière	Utilisez le curseur en haut à droite du graphique pour changer l'échelle. ***Remarque :*** *Vous pouvez également utiliser la molette de votre souris pour mettre le graphique à l'échelle.*
Répartir les noeuds sur le graphique pour afficher plus de détails	Pour répartir les noeuds sur le graphique, utilisez votre souris pour faire glisser le noeud vers l'emplacement préféré.
Développer un noeud réseau	Pour tout noeud réseau que vous souhaitez développer pour afficher ses actifs, cliquez deux fois sur le noeud. Le noeud se développe pour inclure les actifs spécifiques avec lesquels ce noeud communiquait. Par défaut, ce développement est limité aux 100 premiers actifs du réseau.
Afficher des détails supplémentaires concernant une connexion	Placez le pointeur de votre souris sur la ligne de connexion pour afficher des détails supplémentaires. Si la connexion est établie entre un noeud réseau et un réseau distant ou un pays distant, cliquez sur le bouton droit de la souris pour afficher le menu suivant : • **Source** - Pour obtenir des informations concernant le menu Source, voir la section Utilisation de la barre d'outils Connections. • **View Flows** - Sélectionnez cette option pour filtrer l'affichage. La fenêtre Search s'affiche. Pour plus d'informations, voir *IBM Security QRadar SIEM - Guide d'utilisation*. Si la connexion est établie entre deux adresses IP, les informations de source, de destination et de port s'affichent lorsque vous cliquez sur la ligne de connexion.
Déterminer le nombre de données impliquées dans la connexion	L'épaisseur de la ligne du graphique détermine le nombre de données impliquées dans la connexion. Une ligne plus épaisse indique un nombre de données plus important. Ces informations sont basées sur le nombre d'octets impliqués dans la communication

Tableau 7-5 Fonctions Radial Data Viewer (suite)

Si vous souhaitez...	Alors...
Sélectionner un chemin de connexion	Placez le pointeur de votre souris sur la ligne de connexion. Si la connexion est autorisée, le chemin est surligné en vert. Si la connexion est refusée, le chemin est surligné en rouge.
Déterminer le chemin de connexion pour un noeud particulier	Placez le pointeur de votre souris sur le noeud. Si le noeud est autorisé, le chemin d'accès au noeud et le noeud sont surlignés en vert. Si le noeud est refusé, le chemin d'accès au noeud et le noeud sont surlignés en rouge.
Changer la vue graphique	A l'aide de la miniature de prévisualisation, placez la miniature sur la partie de graphique que vous souhaitez afficher.

Utilisation des graphiques circulaires, à barres et tabulaires

Pour afficher les données de connexion dans un graphique circulaire, à barres ou tabulaire, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Dans le menu de navigation, cliquez sur **Connections**.

Si vous avez déjà sauvegardé une recherche en tant que recherche par défaut, les résultats de cette recherche s'affichent. Pour plus d'informations sur l'enregistrement des critères de recherche, voir la section Enregistrement critères de recherche.

Etape 3 Effectuez une recherche.

Pour plus d'informations sur la recherche, voir la section Utilisation de la fonction de recherche.

REMARQUE

Les options des graphiques circulaires, à barres et tabulaires s'affichent uniquement si la recherche a les options Group By sélectionnées dans Advanced View Definition. Pour plus d'informations, voir la section Utilisation de la fonction de recherche.

Etape 4 Dans la sous-fenêtre Charts, cliquez sur l'icône **Configuration**.

Les options de configuration s'affichent.

Etape 5 Configurez les paramètres suivants :

Tableau 7-6 Options du menu Chart

Paramètres	Description
Value to Graph	Dans la zone de liste déroulante **Value to Graph**, sélectionnez le type d'objet que vous souhaiter faire apparaître sur le graphique. Les options comprennent tous les paramètres du flux normalisés et personnalisés inclus dans vos paramètres de recherche.
Chart Type	Dans la zone de liste déroulante **Chart Type**, sélectionnez le type de graphique à afficher. Les options comprennent : • **Table** - Affiche les données dans une table. • **Bar** - Affiche les données dans un graphique à barres. • **Pie** - Affiche les données dans un graphique circulaire.

Etape 6 Cliquez sur **Save**.

Le graphique est actualisé et s'affiche en fonction de vos changements de configuration. Les données ne s'actualisent pas automatiquement, sauf si vos critères de recherche s'affichent pour afficher automatiquement les détails. Voir la section Utilisation de la fonction de recherche.

Etape 7 Pour actualiser les données, cliquez sur **Update Details**.

Utilisation de la fonction de recherche

La fonction de recherche vous permet de rechercher des connexions en utilisant des critères spécifiques et d'afficher des connexions qui correspondent aux critères de recherche dans une liste de résultats. Vous pouvez créer une nouvelle recherche ou charger un ensemble de critères de recherche précédemment enregistré.

Recherche de connexions

Pour rechercher les connexions, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Dans le menu de navigation, cliquez sur **Connections**.

La fenêtre Connections s'affiche. Si vous avez déjà sauvegardé une recherche en tant que recherche par défaut, les résultats de cette recherche s'affichent.

Etape 3 Dans la zone de liste déroulante **Search**, sélectionnez **New Search**.

La fenêtre Search s'affiche.

Etape 4 Si vous souhaitez charger une recherche précédemment sauvegardée, utilisez l'une des options suivantes :

a Dans la zone de liste déroulante **Group**, sélectionnez le groupe auquel la recherche sauvegardée est associée.

b A partir de la liste Available Saved Searches sélectionner la recherche enregistrée que vous voulez charger.

c Dans le champ **Type Saved Search ou Select from List** , saisissez le nom de la recherche que vous voulez charger. A partir de la liste Available Saved Searches, sélectionnez la recherche enregistrée que vous voulez charger.

d Cliquez sur **Load**.

Après avoir chargé la recherche sauvegardée, le volet Edit Search s'affiche.

e Dans le volet Edit Search, sélectionnez les options souhaitées pour cette recherche :

Tableau 7-7 Options Edit Search

Paramètre	Description
Include in my Quick Searches	Cochez cette case si vous souhaitez inclure cette recherche dans vos éléments de recherche rapide.
Include in my Dashboard	Cochez cette case si vous voulez inclure les données de votre recherche enregistrée dans votre tableau de bord. Ce paramètre ne s'affiche que si la recherche est regroupée. ***Remarque :*** *Pour plus d'informations sur le tableau de bord QRadar SIEM, voir le manuel IBM Security QRadar SIEM - Guide d'utilisation.*
Set as Default	Cochez cette case si vous souhaitez définir cette recherche en tant que votre recherche par défaut.
Share with Everyone	Cochez cette case si vous souhaitez partager ces critères de recherche avec tous les autres utilisateurs QRadar Risk Manager.

Etape 5 Dans la sous-fenêtre Time Range, sélectionnez une option pour l'intervalle que vous voulez capturer pour cette recherche :

a Sélectionnez l'une des options suivantes.

Tableau 7-8 Options Edit Search

Paramètre	Description
Recent	Dans la zone de liste déroulante, indiquez l'intervalle de temps que vous souhaitez filtrer.
Specific Interval	A l'aide de l'agenda, indiquez la plage de dates et heures que vous souhaitez filtrer.

b Si vous avez fini de configurer la recherche et que vous souhaitez afficher les résultats, cliquez sur **Search**.

Etape 6 Dans la sous-fenêtre Search Parameters, définissez vos critères de recherche spécifiques :

a Dans la première zone de liste déroulante, sélectionnez un attribut de recherche. Par exemple, Connection Type, Source Network ou Direction.

b Dans la deuxième zone de liste, sélectionnez le modificateur que vous souhaitez utiliser pour la recherche. La liste des modificateurs qui s'affichent dépend de l'attribut sélectionné dans la première liste.

c Dans la zone de texte, entrez les informations spécifiques associées à votre recherche.

d Dans la zone Value, sélectionnez le modificateur que vous souhaitez utiliser pour la recherche. La liste des modificateurs qui s'affichent dépend de l'attribut sélectionné dans la zone de liste déroulante Type.

e Cliquez sur **Add Filter**.

f Répéter les étapes dea à e pour chaque filtre que vous souhaitez ajouter aux critères de recherche.

g Si vous avez fini de configurer la recherche et que vous souhaitez afficher les résultats, cliquez sur **Search**. Sinon, passez à l'étape suivante.

Le filtre s'affiche dans la zone de texte Current Filters.

Etape 7 Si vous souhaitez enregistrer automatiquement les résultats de recherche lorsque la recherche est terminée, cochez la case **Save results when search is complete** et entrez un nom.

Etape 8 Si vous avez fini de configurer la recherche et que vous souhaitez afficher les résultats, cliquez sur **Search**. Sinon, passez à l'étape suivante.

Etape 9 A l'aide du volet Column Definition, définissez les colonnes et l'agencement de colonne que vous souhaitez utiliser pour afficher les résultats :

a Dans la zone de liste **Display**, sélectionnez la vue que vous souhaitez associer à cette recherche.

b Cliquez sur la flèche à côté de Advanced View Definition afin d'afficher les paramètres de recherche avancée. Cliquez à nouveau sur la flèche pour masquer les paramètres.

c Personnaliser les colonnes à afficher dans les résultats de recherche :

Tableau 7-9 Options de définition d'affichage avancées

Paramètre	Description
Type Column or Select from List	Filtre les colonnes dans la liste Available Columns. Saisissez le nom de la colonne que vous souhaitez localiser ou saisissez un mot-clé pour afficher une liste de noms de colonnes qui incluent ce mot-clé. Par exemple, saisissez **Source** pour afficher la liste des colonnes qui comprend Source dans le nom de la colonne.
Available Columns	Répertorie les colonnes disponibles associées à la vue sélectionnée. Les colonnes qui sont actuellement en usage pour cette recherche enregistrée sont soulignées et affichées dans la liste **Columns**.

Tableau 7-9 Options de définition d'affichage avancées (suite)

Paramètre	Description
Add and remove column buttons (top set)	Le premier ensemble de boutons vous permet de personnaliser la liste **Group By**. • **Add Column** - Sélectionnez une ou plusieurs colonnes dans la liste **Available Columns** et cliquez sur le bouton **Add Column**. • **Remove Column** - Sélectionnez une ou plusieurs colonnes dans la liste **Group By** et cliquez sur le bouton **Remove Column**.
Add and remove column buttons (bottom set)	Le dernier ensemble de boutons vous permet de personnaliser la liste **Columns**. • **Add Column** - Sélectionnez une ou plusieurs colonnes dans la liste **Available Columns** et cliquez sur le bouton **Add Column**. • **Remove Column** - Sélectionnez une ou plusieurs colonnes dans la liste **Columns** et cliquez sur le bouton **Remove Column**.
Group By	Indique les colonnes dans lesquelles la recherche enregistrée regroupe les résultats. Vous pouvez personnaliser davantage la liste **Group By** en utilisant les options suivantes : • **Move Up** - Sélectionnez une colonne et déplacez-le vers la liste prioritaire en utilisant l'icône **Move Up**. • **Move Down** - Sélectionnez une colonne et déplacez-le vers le bas liste prioritaire en utilisant l'icône **Move Down**. La liste de priorité indique l'ordre dans lequel les résultats sont regroupés. Les résultats de la recherche se regrouperont selon la première colonne de la liste **Group By**, puis selon la colonne suivante sur la liste.
Columns	Indique les colonnes choisies pour la recherche. Les colonnes sont chargées depuis une recherche enregistrée. Vous pouvez personnaliser la liste **Columns** en sélectionnant des colonnes à partir de la liste **Available Columns.** Vous pouvez personnaliser davantage la liste **Columns** en utilisant les options suivantes : • **Move Up** - Sélectionnez une colonne et déplacez-la vers la liste prioritaire en utilisant le bouton de déplacement vers le haut. • **Move Down** - Sélectionnez une colonne et déplacez-la vers la liste prioritaire en utilisant le bouton de déplacement vers le bas. Si le type de colonne est numérique ou temporel *et* qu'il existe une entrée dans la liste **Group By**, la colonne contient une zone de liste déroulante qui vous permet de choisir la façon dont vous souhaitez regrouper la colonne.

Tableau 7-9 Options de définition d'affichage avancées (suite)

Paramètre	Description
Order By	A partir de la première zone de liste, indiquez la colonne par laquelle vous voulez trier les résultats de la recherche. Puis, à partir de la deuxième zone de liste, indiquez la commande que vous souhaitez afficher pour les résultats de la recherche : **Descending** ou **Ascending**.

Etape 10 Cliquez sur **Search**.

Les résultats de la recherche sont affichés.

Enregistrement critères de recherche

Pour enregistrer les critères de recherche spécifiés pour une utilisation ultérieure :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Dans le menu de navigation, cliquez sur **Connections.**

La fenêtre Connections s'affiche.

Etape 3 Effectuez une recherche. Voir la section Recherche de connexions.

Les résultats de la recherche s'affichent.

Etape 4 Cliquez sur **Save Criteria**

La fenêtre Save Search s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 7-10 Paramètres Save Search

Paramètre	Description
Search Name	Tapez un nom que vous souhaitez attribuer à ces critères de recherche.
Assign Search to Group(s)	Cochez la case pour le groupe auquel vous souhaitez affecter cette recherche enregistrée. Si vous ne sélectionnez pas un groupe, cette recherche enregistrée est attribuée à l'autre groupe par défaut.
Timespan options	Sélectionnez l'une des options suivantes : • **Recent** - Dans la zone de liste déroulante, indiquez l'intervalle de temps que vous souhaitez filtrer. • **Specific Interval** - A l'aide de l'agenda, indiquez la plage de dates et heures que vous souhaitez filtrer.
Include in my Quick Searches	Cochez cette case si vous souhaitez inclure cette recherche dans vos éléments Quick Search disponibles dans la zone de liste déroulante **Search**.

Tableau 7-10 Paramètres Save Search (suite)

Paramètre	Description
Include in my Dashboard	Cochez cette case si vous voulez inclure les données de votre recherche enregistrée dans votre tableau de bord. Pour plus d'informations sur le tableau de bord, voir le manuel *IBM Security QRadar SIEM - Guide d'utilisation*. ***Remarque :*** *Ce paramètre ne s'affiche que si la recherche est regroupée.*
Set as Default	Cochez cette case si vous souhaitez définir cette recherche en tant que votre recherche par défaut.
Share with Everyone	Cochez cette case si vous souhaitez partager ces critères de recherche avec tous les autres utilisateurs QRadar Risk Manager.

Etape 6 Cliquez sur **OK**.

Effectuer une sous-recherche

Chaque fois que vous effectuez une recherche, QRadar SIEM recherche dans la base de données entière des connexions correspondant à vos critères. Ce processus peut prendre une longue période de temps selon la taille de la base de données.

La fonction de sous-recherche vous permet d'effectuer des recherches dans un ensemble de résultats de recherche réalisée. La fonction de sous-recherche vous permet d'affiner vos résultats de recherche sans avoir besoin de rechercher à nouveau dans la base de données. Cette fonction n'est pas disponible pour les recherches regroupées ou les recherches en cours.

Pour effectuer une sous-recherche, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Dans le menu de navigation, cliquez sur **Connections.**

La fenêtre Connections s'affiche.

Etape 3 Effectuez une recherche.

Pour plus d'informations, voir la section Recherche de connexions.

Etape 4 Attendez la fin de la recherche.

Les résultats de la recherche sont affichés. Les recherches supplémentaires utilisent le jeu de données provenant de la recherche précédente lorsque des sous-recherches sont effectuées.

Etape 5 Pour ajouter un filtre, procédez comme suit :

a Cliquez sur **Add Filter**.

La fenêtre Add Filter s'affiche.

b Dans la première zone de liste déroulante, sélectionnez un attribut de recherche.

c Dans la deuxième zone de liste, sélectionnez le modificateur que vous souhaitez utiliser pour la recherche. La liste des modificateurs qui s'affichent dépend de l'attribut sélectionné dans la première liste.

d Dans la zone de texte, entrez les informations spécifiques associées à votre recherche.

e Cliquez sur **Add Filter**.

Vous pouvez également cliquer avec le bouton droit de la souris sur une connexion pour sélectionner une option Filter on.

REMARQUE

Si la recherche est toujours en cours, les résultats partiels sont affichés.

La sous-fenêtre Original Filter indique le filtre sur lequel la recherche d'origine est basée. La sous-fenêtre Current Filter indique le filtre appliqué à la sous-recherche.

REMARQUE

Vous pouvez effacer les filtres de sous-recherche sans avoir à redémarrer la recherche d'origine. Cliquez sur le lien Clear Filter à côté du filtre que vous souhaitez effacer. Si vous désactivez un filtre dans le volet Original Filter, la recherche initiale est relancée.

Etape 6 Cliquez sur **Save Criteria** pour enregistrer la sous-recherche.

Pour plus d'informations, voir la section Enregistrement critères de recherche.

REMARQUE

Si vous supprimez la recherche d'origine, vous pouvez accéder à la sous-recherche enregistrée. Si vous ajoutez un filtre, la sous-recherche recherche dans la base de données entière puisque la fonction de recherche ne fonde plus sa recherche sur un ensemble de données précédemment recherchées.

Gérer les résultats de recherche

Vous pouvez effectuer des plusieurs recherches de connexion tout en naviguant sur d'autres interfaces. Vous pouvez configurer la fonction de recherche pour vous envoyer une notification par courrier électronique lorsqu'une recherche est terminée. A tout moment pendant qu'une recherche est en cours, vous pouvez consulter les résultats partiels d'une recherche en cours.

Affichage de Managed Search Results

Pour gérer les résultats de la recherche, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Dans le menu de navigation, cliquez sur **Connections**.

La fenêtre Connections s'affiche.

Etape 3 Dans le menu, sélectionnez **Search > Manage Search Results**.

La fenêtre des résultats de la recherche affiche les paramètres suivants :

Tableau 7-11 Fenêtre Manage Search Results

Paramètre	Description
Flags	Indique qu'une notification par courrier électronique est en attente pour la fin de la recherche.
User	Nom de l'utilisateur ayant lancé la recherche.
Name	Nom de la recherche, si la recherche a été enregistrée. Pour plus d'informations sur la sauvegarde d'une recherche, voir la section Enregistrement des résultats de recherche.
Started On	Date et l'heure de lancement de la recherche.
Ended On	Date et l'heure de la fin de la recherche.
Duration	Durée d'exécution qu'il a fallu pour la recherche. Si la recherche est actuellement en cours, l'option Duration indique la durée du traitement de la recherche à ce jour. Si la recherche a été annulée, le paramètre Duration indique la durée du traitement de la recherche avant l'annulation.
Expires On	Date et l'heure d'expiration d'un résultat de la recherche non enregistrée. Une recherche sauvegardée n'expire pas.
Status	Statut de la recherche. Les options sont : • **Queued** - Indique que la recherche est placée dans une file d'attente pour démarrer. • **<percent>% Complete** - Etat d'avancement de la recherche en termes de pourcentage de travail effectué. Vous pouvez cliquer sur le lien pour afficher des résultats partiels. • **Sorting** - Indique que la recherche a fini de collecter des résultats et les prépare actuellement pour l'affichage. • **Canceled** - Indique que la recherche a été annulée. Vous pouvez cliquer sur le lien pour voir les résultats collectés avant l'annulation. • **Completed** - Indique que la recherche est terminée. Vous pouvez cliquer sur le lien pour afficher les résultats. Voir la section Affichage des connexions.
Size	Taille du fichier de l'ensemble des résultats de la recherche.

La barre d'outils des résultats de la recherche fournit les options suivantes :

Tableau 7-12 Barre d'outils de gestion des résultats de recherche

Paramètre	Description
New Search	Cliquez sur **New Search** afin créer une recherche. Lorsque vous cliquez sur ce bouton, la fenêtre de recherche s'affiche. Pour plus d'informations, voir la section Recherche de connexions.

Tableau 7-12 Barre d'outils de gestion des résultats de recherche (suite)

Paramètre	Description
Save Results	Click **Save Results** afin de sauvegarder les résultats de recherche. Pour plus d'informations, voir la section Enregistrement des résultats de recherche. ***Remarque :*** *Cette option est activée uniquement lorsque vous avez sélectionné une ligne dans la liste Manage Search Results.*
Cancel	Cliquez sur **Cancel** afin d'annuler les recherches qui sont en cours ou qui sont en attente pour démarrer. Pour plus d'informations, voir la section Annulation d'une recherche.
Delete	Cliquez sur **Delete** afin de supprimer un résultat de recherche. Pour plus d'informations, voir la section Suppression d'une recherche.
Notify	Sélectionnez le ou les recherches pour lesquelles vous souhaitez recevoir de notification, puis cliquez sur **Notify** pour activer la notification par courriel lorsque la recherche est terminée.
View	Dans la zone de liste déroulante, indiquez les résultats de la recherche que vous voulez lister dans la fenêtre correspondante. Les options sont : • Saved Search Results • All Search Results • Canceled/Erroneous Searches • Searches in Progress

Enregistrement des résultats de recherche

Pour enregistrer les résultats de la recherche sauvegardée, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Dans le menu de navigation, cliquez sur **Connections.**

La fenêtre Connections s'affiche.

Etape 3 Effectuez une recherche ou une sous-recherche de connexion. Pour plus d'informations sur la façon d'effectuer une recherche de connexion, voir la section Recherche de connexions.

Pour plus d'informations sur la façon d'effectuer une sous-recherche, voir la section Effectuer une sous-recherche.

Etape 4 Dans la fenêtre Search Results, sélectionnez **Search > Manage Search Results** et sélectionnez un résultat de la recherche.

Etape 5 Cliquez sur **Save Results**.

REMARQUE

Le bouton Save Results est activé uniquement lorsque la recherche est terminée ou si la recherche a été annulée en cours d'exécution.

La fenêtre Save Search Result s'affiche.

Etape 6 Saisissez un nom pour les résultats de la recherche.

Etape 7 Cliquez sur **OK**.

Les résultats de recherche enregistrés affichent le nom de la colonne **Name** de la fenêtre Manage Search Results.

Annulation d'une recherche

Pour annuler une recherche, procédez comme suit :

Etape 1 A partir de la fenêtre Manage Search Results, sélectionnez les résultats de recherche en attente ou en cours que vous souhaitez annuler.

REMARQUE

Vous pouvez également annuler une recherche de la recherche de résultats partiels à l'aide du bouton Cancel Search.

Etape 2 Cliquez sur **Cancel Search**.

REMARQUE

Vous pouvez sélectionner plusieurs recherches pour annuler.

Une fenêtre de confirmation s'affiche.

Etape 3 Cliquez sur **Oui**.

Si la recherche était en cours lors de l'annulation, les résultats qui ont été accumulés jusqu'à l'annulation sont maintenus.

Suppression d'une recherche

Pour supprimer une recherche, procédez comme suit :

Etape 1 A partir de la fenêtre Manage Search Results page, sélectionnez les résultats de recherche que vous souhaitez supprimer.

Etape 2 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 3 Cliquez sur **Oui**.

La recherche est supprimée de la fenêtre des résultats de la recherche.

Exportation de connexions

Vous pouvez exporter des connexions au format XML ou CSV.

Pour exporter les connexions, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Dans le menu de navigation, cliquez sur **Connections.**

La fenêtre Connections s'affiche.

a Si vous souhaitez exporter la connexion au format XML, sélectionnez **Actions > Export to XML**.

b Si vous souhaitez exporter la connexion au format CSV, sélectionnez **Actions > Export to CSV**.

La fenêtre d'état s'affiche.

Etape 3 Si vous souhaitez reprendre vos activités, cliquez sur **Notify When Done**.

Lorsque l'exportation est terminée, vous recevez une notification vous informant que l'exportation est terminée. Si vous n'avez pas sélectionné l'option **Notify When Done**, la fenêtre d'état disparaît une fois l'exportation terminée.

8 AFFICHAGE DES CONFIGURATIONS DE PÉRIPHÉRIQUES

Vous pouvez afficher les informations sur la configuration des périphériques de votre réseau dans la page Moniteur de configuration.

Utilisez cette page pour comparer les configurations des périphériques réseau et afficher les règles existantes, le nombre de déclenchements des règles et un historique des règles des périphériques dans votre topologie.

REMARQUE

Il est important pour la recherche des règles et les nombres d'événements que les périphériques de QRadar Risk Manager soient correctement mappés vers les sources de journal des périphériques. Pour plus d'informations sur le mappage des sources de journal, voir la section Mappage de sources de journal.

Configurations de périphérique

Dans la topologie, vous pouvez afficher les informations sur les périphériques tels que les routeurs, les pare-feux et les commutateurs.

Vous pouvez également rechercher des périphériques et créer ou éditer un mappage de sources de journal. Pour plus d'informations, voir la section Création d'un mappage de sources de journal.

Il existe deux niveaux d'informations s'affichant dans la page Moniteur de configuration : le niveau de base et le niveau détaillé.

Les informations de base sur les périphériques contiennent une liste de tous les périphériques inclus dans le Moniteur de configuration et des détails de base sur le périphérique, comme son adresse IP, ses contextes, les informations sur l'adaptateur et l'heure de la dernière sauvegarde de la configuration. Chaque contexte d'un périphérique à contextes multiples s'affiche dans des lignes distinctes dans la liste. S'y trouve également une ligne représentant le contexte Admin du périphérique à contextes multiples.

Les informations de périphérique détaillées contiennent des informations de configuration détaillées pour un périphérique précis, telles que les informations sur les règles de périphérique, les interfaces, les informations sur l'adaptateur et les recherches spécialisées sur votre périphérique à partir de la barre d'outils.

Affichage de base des configurations des périphériques

Utilisez la configuration par défaut pour afficher une liste des périphériques et leurs informations d'identification de base.

Pour afficher une configuration de périphérique de base, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Configuration Monitor**.

La liste des périphériques configurés s'affiche et contient les informations de configuration suivantes.

Tableau 8-1 Paramètres du Moniteur de configuration

Paramètre	Description
Device IP	Adresse IP de gestion du périphérique.
Contexte	Nom du contexte du périphérique.
Hostname	Nom d'hôte du périphérique.
Adapter	Nom d'adaptateur associé à ce périphérique.
Type	Type de périphérique. Par exemple pare-feu, routeur ou système IPS.
Vendor	Fournisseur du périphérique.
Model	Numéro de modèle du périphérique.
Log Source(s)	Si une source de journal est configurée dans QRadar SIEM, les informations suivantes sont fournies : • Sources de journal mappées sur le périphérique en cours. • Nom d'utilisateur entre parenthèses de l'utilisateur qui a mappé la source de journal sur un périphérique. Si le périphérique a été automatiquement mappé, il s'affiche.
Config Obtained On	Date et heure d'obtention de la configuration pour ce périphérique.

Affichage détaillé des configurations des périphériques

Vous pouvez cliquer deux fois sur un périphérique dans la liste du Moniteur de configuration pour afficher les informations détaillées d'un périphérique réseau spécifique. Les informations détaillées du périphérique contiennent des informations de configuration, telles que les règles configurées, les interface, les nombres d'événements, l'historique de configuration et une recherche de règles avancée.

Dans la topologie, vous pouvez filtrer les connexions de périphériques par événements, violations ou historique. Vous pouvez également les afficher.

Pour afficher la configuration de périphérique détaillée, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Configuration Monitor**.

Etape 3 Cliquez deux fois sur un périphérique pour afficher les informations de configuration détaillées.

Etape 4 La barre d'outils du périphérique fournit les fonctions suivantes :

Tableau 8-2 Fonctionnalité de la barre d'outils de périphérique

Bouton	Fonction
Interfaces	Vous permet d'afficher une liste d'interfaces pour ce périphérique. Ces informations proviennent de la configuration de périphérique.
Rules	Vous permet d'afficher une liste de règles provenant de la configuration de périphérique. La sous-fenêtre Rules comprend une fonction de recherche qui permet de rechercher des règles de périphérique spécifiques. Pour plus d'informations, voir la section Recherche de règles.
NAT	Vous permet d'afficher une liste des règles NAT du périphérique.
History	Vous permet d'afficher un historique des informations de sauvegarde de configuration de la fonction Configuration Source Management et propose une comparaison des configurations de périphérique en cours et précédentes.
Events	Vous permet d'afficher tous les événements associés à ce périphérique. Pour plus d'informations sur l'onglet **Log Activity**, voir le manuel *IBM Security QRadar SIEM - Guide d'utilisation*.
Offenses	Vous permet d'afficher toutes les violations associées à ce périphérique. Pour plus d'informations sur l'onglet **Offenses**, voir le manuel *IBM Security QRadar SIEM - Guide d'utilisation*.
Topology	Vous permet d'afficher la topologie avec un filtre affichant les périphériques et les sous-réseaux communiquant avec votre périphérique dans le modèle de topologie. Pour plus d'informations sur le modèle de topologie, voir le chapitre **Utilisation de la topologie**.
Print	Vous permet d'imprimer les détails du périphérique.

La table du périphérique contient un récapitulatif détaillé des informations de votre périphérique :

Tableau 8-3 Informations détaillées du Moniteur de configuration

Paramètre	Description
IP/Contexte	La première entrée fournit l'adresse de gestion du périphérique. Si un périphérique à contextes multiples existe, la deuxième entrée fournit le nom du contexte du périphérique. Dans le cas contraire, N/A s'affiche.

Tableau 8-3 Informations détaillées du Moniteur de configuration

Paramètre	Description
Current Interfaces	Nombre d'interfaces réseau du périphérique. Des informations d'interface détaillées peuvent s'afficher à l'aide de l'une des méthodes suivantes : • Pour afficher des informations d'interface avancées, sélectionnez **Interfaces** dans la barre d'outils du périphérique. • Pour afficher des informations d'interface avancées, dans la zone **Current Interfaces**, cliquez sur le nombre d'interfaces affichées.
Current Rules	Nombre de règles configurées sur le périphérique. Des informations de règle détaillées peuvent s'afficher à l'aide de l'une des deux méthodes suivantes : • Pour afficher des informations de règle, sélectionnez **Rules** dans la barre d'outils du périphérique. • Pour afficher des informations de règle dans la zone **Current Rules**, clique sur le nombre de règles affichées.
Règles NAT en cours	Nombre de règles NAT configurées sur le périphérique. Des informations de règle détaillées peuvent s'afficher à l'aide de l'une des deux méthodes suivantes : • Pour afficher les informations sur les règles, sélectionnez **NAT** dans la barre d'outils Device. • Pour afficher les informations d'une règle de la zone **Current NAT**, cliquez sur le numéro de la règle qui s'affiche.
Config Obtained On	Date et heure d'obtention de la configuration pour ce périphérique.
Current Log Source(s)	Si une source de journal est configurée dans QRadar SIEM, les informations suivantes sont fournies : • Nom des sources de journal mappées sur le périphérique en cours. • Nom d'utilisateur entre parenthèses de l'utilisateur qui a mappé la source de journal sur un périphérique. Si le périphérique a été automatiquement mappé, il s'affiche. Pour plus d'informations sur le mappage de la source de journal, voir la section Mappage de sources de journal.
Hostname	Nom d'hôte du périphérique.
Adapter	Nom d'adaptateur associé à ce périphérique.
Type	Type de périphérique. Par exemple pare-feu, routeur, commutateur ou système IPS/IDP.
Vendor	Fournisseur du périphérique.
Model	Numéro de modèle du périphérique.

Etape 5 Cliquez sur **Interfaces** pour afficher une liste détaillée des informations d'interface pour votre périphérique.

Tableau 8-4 Paramètres d'interface

Paramètre	Description
Name	Nom de l'interface tel qu'il apparaît sur le périphérique.
IF Index	La valeur IFIndex est associée à l'interface.
Status	Statut en cours de l'interface. Les options sont : • **Up** - L'interface de périphérique fonctionne correctement. • **Down** - L'interface de périphérique est désactivée ou ne fonctionne pas correctement.
Type	Type d'interface, par exemple Ethernet ou Software Loopback.
CIDR	Plage CIDR de l'interface.
MAC	Adresse MAC associée à l'interface.
Speed (bps)	Vitesse de l'interface, en bits par seconde (bps).
MTU	Unité de transmission maximale de l'interface.

La table suivante contient des fonctions supplémentaires disponibles dans la table d'interface.

Tableau 8-5 Fonctions de table d'interface

Fonction	Description
Search	Entrez une adresse IP ou une plage CIDR pour filtrer la table d'interface. • Si vous indiquez une adresse IP unique, toutes les interfaces comprenant une adresse IP d'hôte correspondante s'affichent. • Si vous indiquez une plage CIDR, toutes les interfaces comprenant une plage CIDR correspondante ou contenant le routage CIDR de filtre s'affichent.

Etape 6 Cliquez sur **Rules** pour afficher la liste des règles de ce périphérique.

Tableau 8-6 Paramètres de règle

Paramètre	Description
Status	Statut des règles du périphérique. Les règles possédant des messages de statut s'affichent dans cette colonne, comme les règles grisées ou supprimées. Si une icône apparaît dans la colonne **Status**, des informations supplémentaires sont disponibles si vous passez la souris au-dessus de l'icône de statut.

Tableau 8-6 Paramètres de règle (suite)

Paramètre	Description
Config Date/Time	Date et heure d'obtention de la configuration pour ce périphérique. ***Remarque :*** *Si une règle contient plusieurs configurations, la zone affiche Multiple(n), où n représente le nombre de configurations ayant subi une coalescence. Placez votre curseur au-dessus de la valeur Multiple(n) pour afficher toutes les règles ayant subi ensemble une coalescence.*
List	Nom de la liste de contrôle d'accès (ACL), tel qu'il est défini dans le périphérique. Une liste ACL est une collecte de règles individuelles.
Entry	Numéro d'ordre de la règle sur laquelle vous effectuez une recherche.
Action	Action associée à cette règle. Les options sont : • **Accept** - Le périphérique accepte le paquet. • **Deny** - Le périphérique refuse le paquet. • **Forward** - Le paquet a été transféré par le périphérique. • **Next** - La règle est évaluée par rapport à la liste ACL suivante. • **None** - La règle est évaluée par rapport à la liste ACL suivante.
Source(s)	Source de la règle, par exemple adresse IP, groupe ou nom d'hôte.
Source Service(s)	Service source de la règle. Ce paramètre comprend une collecte de plages de ports, comme 100-200, ou des expressions de port, comme 80(TCP). Si le port est annulé, les informations associées contiennent également un point d'exclamation et peuvent être mises entre parenthèses, par exemple !(100-200) ou !80(TCP).
Destination(s)	Destination de la règle, par exemple adresse IP, groupe ou nom d'hôte.
Destination Service(s)	Service de destination de la règle. Ce paramètre comprend une collecte de plages de ports, comme 100-200, ou des expressions de port, comme 80(TCP). Si le port est annulé, les informations associées contiennent également un point d'exclamation et peuvent être mises entre parenthèses, par exemple !(100-200) ou !80(TCP).
Protocol(s)	Protocole ou groupe de protocoles associé à cette règle.
Signature(s)	Informations sur les vulnérabilités associées à cette règle comme défini par le périphérique IPS.
Event Count	Le nombre d'événements déclenchés par la règle s'affiche.

Etape 7 Cliquez sur **NAT** pour afficher la liste des règles NAT correspondant à un périphérique.

Tableau 8-7 Paramètres NAT

Paramètre	Description
List	Nom de la liste à laquelle appartient la règle NAT.
Entry	Numéro d'ordre de la règle sur laquelle vous effectuez une recherche.
Phase	Indique le moment de déclenchement de la règle NAT. Par exemple, avant ou après le routage.
Type	Indique la façon dont les conversions s'appliquent à la règle NAT. Elle peut être statique ou dynamique.
Source(s)	Source à l'origine du déclenchement de la règle. Par exemple, une adresse IP, un groupe ou un nom d'hôte.
Source Service(s)	Service source à l'origine du déclenchement de la règle.
Destination(s)	Destination à l'origine du déclenchement de la règle. Par exemple, une adresse IP, un groupe ou un nom d'hôte.
Destination Service(s)	Service de destination à l'origine du déclenchement de la règle.
Protocol(s)	Protocole ou groupe de protocoles associé à cette règle.
Conversion(s) source	Conversions pouvant être appliquées à la ou aux sources.
Conversion(s) des ports source	Conversions pouvant être appliquées au(x) port(s) source.
Conversion(s) de destination	Conversions pouvant être appliquées à la ou aux destination(s).
Conversion(s) des ports de destination	Conversions pouvant être appliquées au(x) port(s) de destination.
Config Date/Time	Date et heure de sauvegarde de la règle.

Affichage de l'historique des configurations de périphériques

Lorsque QRadar Risk Manager sauvegarde des périphériques dans le temps, les configurations sont conservées, ce qui vous permet d'afficher les changements d'historique apportés au périphérique. Les configurations de périphérique historiques peuvent être utilisées pour comparer les changements entre les sauvegardes d'un périphérique unique ou pour comparer les configurations entre les périphériques. Le fait de comparer les configurations de périphérique vous permet d'afficher les règles de périphérique dans une vue de comparaison normalisée ou d'afficher la configuration de périphérique brute. La fonction Normalized Device Configuration est une vue de comparaison graphique fournissant les règles ajoutées, supprimées ou modifiées entre les périphériques. La fonction Raw Device Configuration est une vue de langage XML ou de texte brut du fichier de périphérique.

Affichage de l'historique d'un seul périphérique

Pour afficher l'historique de configuration d'un périphérique réseau unique, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Configuration Monitor**.

Etape 3 Cliquez deux fois sur une configuration pour afficher les informations de périphérique détaillées.

Etape 4 Cliquez sur **History**.

Tableau 8-8 Paramètres de Device Backup History

Paramètre	Description
Configuration	La configuration indique le type de fichiers stockés dans QRadar Risk Manager pour votre périphérique réseau. Les types de configuration courants peuvent être les suivants : • **Standard-Element-Document** - Les fichiers SED sont des fichiers de données XML qui contiennent des informations sur votre périphérique réseau. Les fichiers SED individuels s'affichent dans leur format XML brut. Si un fichier SED est comparé à un autre fichier SED, la vue est normalisée pour afficher les différences de règles. • **Config** - Les fichiers de configuration sont fournis par certains périphériques réseau, suivant le fabricant de périphériques. Un fichier de configuration peut s'afficher en cliquant deux fois sur le fichier de configuration. ***Remarque :*** *Suivant les informations que l'adaptateur collecte pour votre périphérique, plusieurs autres types de configuration peuvent s'afficher. Ces fichiers s'affichent en texte brut lorsque vous cliquez deux fois dessus.* ***Remarque :*** *La vue de texte brut prend en charge les options find (Ctrl +f), paste (Ctrl+v) et copy (Ctrl+C) à partir de la fenêtre de navigateur.*
Date Obtained	Date de la dernière sauvegarde de la configuration de périphérique à partir de Configuration Source Management.

Etape 5 Dans la sous-fenêtre History, sélectionnez une configuration.

Etape 6 Cliquez sur **View Selected**.

Comparaison de configurations

Les configurations de périphérique peuvent être comparées les unes aux autres en comparant plusieurs sauvegardes sur un périphérique unique ou en comparant un périphérique réseau à un autre.

Pour comparer les configurations de périphérique, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks**.

Etape 2 Dans le menu de navigation, cliquez sur **Configuration Monitor**.

Etape 3 Cliquez deux fois sur un périphérique pour afficher les informations de configuration détaillées.

Etape 4 Cliquez sur **History** pour afficher l'historique de ce périphérique.

Etape 5 Sélectionnez votre type de comparaison à partir de la table ci-dessous :

Tableau 8-9 Comparaisons de périphériques

Si vous souhaitez	Alors
Comparer deux configurations sur un périphérique unique	Pour comparer deux configurations sur un périphérique unique, procédez comme suit : **1** Sélectionnez une configuration primaire. **2** Appuyez sur la touche Ctrl et sélectionnez une seconde configuration pour la comparaison. **3** Dans la sous-fenêtre History, cliquez sur **Compare Selected**. Si les fichiers de comparaison sont des fichiers SED, la fenêtre Normalized Device Configuration Comparison s'affiche avec une table présentant les différences de règles entre les sauvegardes. Lors de la comparaison des configurations normalisées, la couleur du texte indique les éléments suivants : • **Green Dotted Outline** - Indique une règle ou une configuration ajoutée au périphérique. • **Red Dashed Outline** - Indique une règle ou une configuration supprimée du périphérique. • **Yellow Solid Outline** - Indique une règle ou une configuration modifiée sur le périphérique. **4** Facultatif. Pour afficher les différences brutes de configuration, cliquez sur **View Raw Comparison**. ***Remarque :*** *Si la comparaison est un fichier de configuration ou un autre type de sauvegarde, la comparaison brute s'affiche.*

Tableau 8-9 Comparaisons de périphériques (suite)

Si vous souhaitez	Alors
Comparer deux configurations sur différents périphériques	Pour comparer deux configurations sur des périphériques distincts, vous devez marquer une configuration pour une comparaison sur un seul périphérique, puis comparer une sauvegarde de périphérique à la configuration marquée. Pour comparer des configurations de périphérique, procédez comme suit : **1** Sélectionnez une configuration primaire dans un périphérique. **2** Cliquez sur **Mark for Comparison**. **3** Dans le menu de navigation, sélectionnez **All Devices** pour retourner à la liste de périphériques. **4** Cliquez deux fois sur le périphérique pour comparer et cliquez sur **History**. **5** Sélectionnez une configuration à comparer à la configuration marquée. **6** Cliquez sur **Compare with Marked**. Si les fichiers de comparaison sont des fichiers SED, la fenêtre Normalized Device Configuration Comparison s'affiche avec une table présentant les différences de règles entre les sauvegardes. Lors de la comparaison des configurations normalisées, la couleur du texte indique les éléments suivants : • **Green Dotted Outline** - Indique une règle ou une configuration ajoutée au périphérique. • **Red Dashed Outline** - Indique une règle ou une configuration supprimée du périphérique. • **Yellow Solid Outline** - Indique une règle ou une configuration modifiée sur le périphérique. **7** Facultatif. Pour afficher les différences brutes de configuration, cliquez sur **View Raw Comparison**. ***Remarque :*** *Si la comparaison est un fichier de configuration ou un autre type de sauvegarde, la comparaison brute s'affiche.*

Recherche des périphériques

Le Moniteur de configuration propose une fonction de recherche afin de localiser les périphériques que vous avez ajoutés à l'aide de Configuration Source Management. La recherche de configuration de périphérique permet de rechercher des périphériques à l'aide d'un intervalle de temps spécifié, puis de filtrer les résultats par adresse IP/CIDR, contexte, nom d'hôte, adaptateur, fournisseur, type ou modèle.

Pour rechercher dans le périphérique des informations de règle détaillées, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Configuration Monitor**.

Etape 3 Dans la zone de liste **Search**, sélectionnez une option de recherche :

Tableau 8-10 Options de recherche

Paramètre	Description
New Search	Démarrez une nouvelle recherche de périphérique.
Edit Search	Editez une recherche de périphérique existante. Cette option vous permet de modifier une recherche afin d'ajouter ou de supprimer des paramètres. Des paramètres de recherche supplémentaires sont contenus comme des filtres de recherche en cours dans les résultats.

Etape 4 Configurez les valeurs de votre recherche de périphérique :

Tableau 8-11 Critères de recherche de périphérique

Paramètre	Description
Config Obtained Date/Time Range	Sélectionnez un intervalle de temps de recherche des périphériques. La recherche est basée sur l'horodatage de la dernière sauvegarde de configuration de périphérique dans Configuration Source Management. Les options suivantes s'affichent : • **Current** - Recherchez les périphériques depuis la dernière sauvegarde de configuration de périphérique. • **Interval** - Recherchez les périphériques utilisant un intervalle de temps prédéfini. Les périphériques possédant des sauvegardes de configuration dans l'intervalle spécifié sont compris dans les résultats et filtrés par toutes les options de recherche supplémentaires. L'intervalle comprend un intervalle de temps minimal de la dernière heure jusqu'à un intervalle de temps maximal des 30 derniers jours. • **Specific** - Recherchez les périphériques utilisant une configuration dans une plage de dates et heures spécifique. Les périphériques possédant des sauvegardes de configuration dans l'intervalle spécifié sont compris dans les résultats et filtrés par toutes les options de recherche supplémentaires.
IP/CIDR	Entrez l'adresse IP/CIDR du périphérique que vous recherchez dans la liste de périphériques.
Hostname	Entrez le nom d'hôte du périphérique que vous recherchez dans la liste de périphériques. Ce paramètre prend en charge des caractères alphanumériques, des tirets (-) ou des points (.).

Tableau 8-11 Critères de recherche de périphérique (suite)

Paramètre	Description
Type	Sélectionnez le type de périphérique que vous recherchez dans la liste de périphériques. Les types de recherche sont les suivants : • Router • Firewall • Switch • IPS/IDS
Contexte	Entrez le nom du contexte.
Adapter	Sélectionnez le type d'adaptateur que vous recherchez dans la liste. Les options sont les suivantes : • Check Point SecurePlatform • Cisco IOS • Cisco Security Appliance • Generic XML • Juniper JunOS • Juniper NSM • Juniper Screen OS
Vendor	Entrez le nom du fournisseur du périphérique que vous recherchez dans la liste de périphériques. Ce paramètre prend en charge des caractères alphanumériques, des tirets (-) ou des points (.).
Model	Entrez le modèle du périphérique que vous recherchez dans la liste de périphériques. Ce paramètre prend en charge des caractères alphanumériques, des tirets (-) ou des points (.).

Etape 5 Cliquez sur **Search**.

Recherche de règles

Le Moniteur de configuration propose une fonction de recherche pour localiser les règles modifiées sur les périphériques de votre topologie. La recherche de règles peut uniquement être effectuée dans la sous-fenêtre Rules située dans la vue détaillée des périphériques du Moniteur de configuration. La recherche de règle offre une méthode de reconnaissance des changements de règle se produisant entre chaque sauvegarde de configuration de périphérique.

REMARQUE

Les résultats retournés pour une recherche de règle sont basés sur la sauvegarde Configuration Source Management de périphérique. Nous vous conseillons de planifier les sauvegardes de périphérique à l'aide de votre fenêtre de mise à jour de la politique de pare-feu. Cela permet au composant QRadar Risk Manager de

disposer des dernières informations de règle lorsque des recherches règle sont effectuées.

Pour rechercher dans un périphérique des informations de règle détaillées, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Configuration Monitor**.

Etape 3 Cliquez deux fois sur un périphérique dans le Moniteur de configuration.

Etape 4 Cliquez sur **Rules**.

Etape 5 Dans la sous-fenêtre Rules, cochez la case **Search** et sélectionnez une option de recherche :

Tableau 8-12 Options de recherche

Paramètre	Description
New Search	Démarrez une nouvelle recherche de règle.
Edit Search	Editez une recherche de règle existante. Cette option vous permet de modifier une recherche afin d'ajouter ou de supprimer des paramètres. Des paramètres de recherche supplémentaires sont contenus comme des filtres de recherche en cours dans les résultats.

Etape 6 Configurez les valeurs de votre recherche de règle :

Tableau 8-13 Paramètres de critères de recherche

Paramètre	Description
Config Obtained Date/Time Range	Sélectionnez un intervalle de temps ou une plage de recherche des périphériques basée sur l'intervalle de temps ou sur la dernière fois qu'une configuration de périphérique a été modifiée ou sur la spécification du périphérique (modèle, fournisseur etc.). Les options suivantes s'affichent : • **Current** - Recherchez les périphériques depuis la dernière sauvegarde de configuration de périphérique. • **Interval** - Recherchez les règles utilisant une configuration à partir d'un intervalle de temps prédéfini. L'intervalle comprend un intervalle de temps minimal de la dernière heure jusqu'à un intervalle de temps maximal des 30 derniers jours. • **Specific** - Recherchez les règles utilisant une configuration dans une plage de dates et heures spécifique.

Tableau 8-13 Paramètres de critères de recherche (suite)

Paramètre	Description
Status	Cochez une case pour le statut de la règle à inclure dans la recherche de règle. Les options sont les suivantes : • **Shadowed** - Une règle grisée est une règle qui ne peut jamais s'appliquer. Dans la plupart des cas, les règles grisées sont dues à une liste ACL existant auparavant dans la liste de règles pour le périphérique couvrant le même trafic réseau. • **Deleted** - Une règle supprimée est une règle qui a été supprimée dans l'intervalle de temps de votre recherche. • **Other** - Les règles portant la marque other comprennent les règles ne présentant aucun statut ou les règles constituant un sous-ensemble de règle grisée ou supprimée.
List	Entrez le nom de la liste de contrôle d'accès (ACL), tel qu'il est défini dans le périphérique. Une liste ACL est une collecte de règles individuelles.
Entry	Entrez le numéro d'ordre de l'entrée de règle du périphérique. Seules des valeurs numériques peuvent être saisies dans la zone **Entry**. La liste ACL du périphérique est analysée pour rechercher l'ordre des règles spécifié.
Action	Action associée à cette règle. Les options sont : • **Accept** - Le périphérique accepte le paquet. • **Deny** - Le périphérique refuse le paquet. • **Forward** - Le paquet a été transféré par le périphérique. • **Next** - La règle est évaluée par rapport à la liste ACL suivante. • **None** - La règle est évaluée par rapport à la liste ACL suivante.
Protocol	Protocole ou groupe de protocoles associé à cette règle. ***Remarque :*** *Seuls les protocoles TCP, UDP et ICMP retournent des nombres d'événements lors de la recherche de règles dans QRadar Risk Manager. Les autres protocoles retournent les règles de correspondance lorsqu'elles sont recherchées, mais pas les nombres d'événements.*

Tableau 8-13 Paramètres de critères de recherche (suite)

Paramètre	Description
Source/Destination	Entrez une adresse IP, une adresse CIDR, un nom d'hôte ou une référence de groupe d'objets pour la source ou la destination de la règle. • Si vous entrez un nom d'hôte ou un nom de référence de groupe d'objets, une recherche de texte est effectuée pour la source ou la destination de la règle. Les résultats de la recherche contiennent des règles correspondant au texte que vous avez saisi. • Si vous entrez une adresse CIDR dans votre recherche de règle, les résultats retournés sont des règles contenant une correspondance d'adresse CIDR exacte ou des règles dans lesquelles l'adresse CIDR fait partie d'un groupe d'adresses CIDR plus grand.
Service	Entrez une valeur pour rechercher la règle sur le service. Le service peut comprendre des ports ou des références de groupes d'objets. Par exemple, le service peut comprendre une collecte de plages de ports, comme 100-200, ou des expressions de port, comme 80(TCP). Si le port est annulé, les informations associées contiennent également un point d'exclamation et peuvent être mises entre parenthèses, par exemple !(100-200) ou !80(TCP).
Signature(s)	Informations sur les vulnérabilités associées à cette règle comme défini par le périphérique IPS.
Event Count	Sélectionnez un opérateur et entrez une valeur numérique pour rechercher un nombre d'événements correspondant dans l'intervalle de temps de la recherche de configuration. ***Remarque :*** *Le fait de sélectionner un protocole autre que TCP, UDP ou ICMP risque de ne pas retourner de nombre d'événements.*
Order By	Sélectionnez l'ordre des résultats de la recherche. Les options sont les suivantes : • **Device Rule Order** - Triez les résultats de la recherche par ordre numérique de l'entrée de règle de la liste ACL. • **Event Count** - Trie les résultats de la recherche par nombre d'événements.
Asc	Les résultats de la recherche sont triés de manière croissante, par exemple de 1 à 5.
Desc	Les résultats de la recherche sont triés de manière décroissante, par exemple de 5 à 1.

Etape 7 Cliquez sur **Search**.

Mappage de sources de journal

QRadar Risk Manager identifie et mappe automatiquement les périphériques vers la source de journal en fournissant des événements dans QRadar SIEM. Cela

permet à un administrateur de vérifier que tous les périphériques configurés dans QRadar Risk Manager sont mappés vers la source de journal correcte. Un maximum de 255 périphériques peuvent être mappés vers une source de journal dans QRadar Risk Manager, mais les périphériques peuvent posséder plusieurs sources de journal.

La fonction Log Source Mapping fournit aux administrateurs les éléments suivants :

- La colonne Log Source(s) contient des informations sur la source de journal mappée vers un périphérique particulier.
- Fonction permettant d'afficher les périphériques mappés vers plusieurs sources de journal.
- Identifie si une mappe de source de journal est annulée, ajoutée ou modifiée par un administrateur ou si le composant QRadar Risk Manager a automatiquement mappé la source de journal vers un périphérique.
- Active l'option contextuelle **Search Events** de Topologie.
- Fournit des informations sur les nombres d'événements lorsque les règles sont recherchées sur des périphériques spécifiques.

Le Moniteur de configuration affiche les informations suivantes dans la colonne Log Source(s) :

- **Auto-Mapped** - Ce terme (Auto-mapped) s'affiche dans la colonne Log Source(s) lorsque QRadar Risk Manager a identifié la source de journal et l'a automatiquement mappée vers le périphérique.
- **Username** - Si un administrateur a ajouté ou modifié manuellement une source de journal, QRadar Risk Manager identifie cet administrateur par un nom d'utilisateur entre parenthèses.
- **Blank** - Si QRadar Risk Manager ne peut pas identifier une source de journal pour le périphérique, la colonne Log Source(s) n'affiche aucune valeur.

Création d'un mappage de sources de journal

Pour créer un mappage de source de journal dans QRadar Risk Manager, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Configuration Monitor**.

Etape 3 Sélectionnez le périphérique sans source de journal.

Etape 4 Cliquez sur **Create/Edit Mapping**.

La fenêtre Create/Edit Mapping s'affiche.

Etape 5 Dans la zone de liste déroulante **Log Source**, sélectionnez un groupe.

Etape 6 Sélectionnez une source de journal.

Etape 7 Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

Edition d'un mappage de sources de journal incorrect

Le fait d'éditer une source de journal n'empêche pas le composant QRadar Risk Manager d'effectuer un nouveau mappage d'une source de journal. Si vous souhaitez éviter une source de journal incorrecte d'être automatiquement remappée, vous devez supprimer le mappage de la source de journal et cocher la case **Do not allow this mapping to be auto-mapped again.**

Pour plus d'informations sur la suppression d'un mappage de sources de journal, voir la section Suppression d'un mappage de source de journal.

Pour éditer un mappage de sources de journal incorrect dans QRadar Risk Manager, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Configuration Monitor**.

Etape 3 Sélectionnez le périphérique avec un mappage de source de journal incorrect.

Etape 4 Cliquez sur **Create/Edit Mapping**.

Etape 5 Dans la fenêtre **Mapping Log Sources**, sélectionnez la source de journal mappée de manière incorrecte.

Etape 6 Cliquez sur **Remove Selected**.

Etape 7 Dans la zone de liste déroulante **Log Source**, sélectionnez un groupe.

Etape 8 Sélectionnez la source de journal correcte à mapper.

Etape 9 Cliquez sur **Add**.

Etape 10 Cliquez sur **Save**.

Suppression d'un mappage de source de journal

Pour supprimer un mappage de source de journal d'un périphérique, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks**.

Etape 2 Dans le menu de navigation, cliquez sur **Configuration Monitor**.

Etape 3 Sélectionnez le périphérique avec un mappage de source de journal incorrect.

Etape 4 Cliquez sur **Delete Mapping**.

Dans la fenêtre Delete Mapping, la case à cocher **Do not allow this mapping to be auto-mapped again** est active.

- Cochez la case **Do not allow this mapping to be auto-mapped again** pour empêcher que le composant QRadar Risk Manager ne tente d'effectuer un mappage de la source de journal vers un périphérique à l'avenir.
- Si vous décochez la case **Do not allow this mapping to be auto-mapped again**, alors QRadar Risk Manager essaie par la suite de remapper la source de journal à un périphérique.

Etape 5 Cliquez sur **Delete** pour confirmer.

Impression d'une configuration de périphérique

Pour imprimer une configuration de périphérique, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Dans le menu de navigation, cliquez sur **Configuration Monitor**.

Etape 3 Cliquez deux fois sur un périphérique dans le Moniteur de configuration.

Etape 4 Dans la sous-fenêtre Device, cliquez sur **Print**.

9 GESTION DES RAPPORTS IBM SECURITY QRADAR RISK MANAGER

Vous pouvez générer, éditer, distribuer et gérer des rapports concernant vos périphériques réseau à l'aide d'IBM Security QRadar Risk Manager. Des rapports détaillés sur les règles de pare-feu et les connexions entre les périphériques sont souvent nécessaires pour satisfaire les diverses normes de réglementation, telles que la conformité PCI.

QRadar Risk Manager fournit les options de rapport supplémentaires suivantes :

- Rapports détaillés sur les connexions entre vos périphériques.
- Rapports détaillés sur les règles de pare-feu de votre périphérique.
- Rapports détaillés sur les objets inutilisés de votre périphérique.

Génération de rapports QRadar Risk Manager

Vous pouvez utiliser Report Wizard pour générer un rapport. Le Report Wizard fournit un guide étape par étape sur la conception, la planification et la génération des rapports. L'assistant utilise les éléments clés suivants pour vous aider à générer un rapport :

- **Layout** - La position et la taille de chaque conteneur
- **Container** - Marque de réservation et emplacement du contenu de votre rapport
- **Content** - Définit les données de rapport que QRadar Risk Manager contient dans le graphique du conteneur

Lorsque vous sélectionnez l'agencement d'un rapport, considérez le type de rapport que vous souhaitez générer. Par exemple, ne choisissez pas un petit conteneur de graphique pour un contenu graphique qui affiche un grand nombre d'objets. chaque graphique comprend une légende et une liste de réseaux dont le contenu est dérivé, choisissez un conteneur assez grand pour contenir les données.

Le délai planifié des rapports générés toutes les semaines ou tous les mois doit s'écouler avant que ces derniers ne renvoient des résultats. Pour un rapport planifié, vous devez attendre l'heure planifiée pour la construction des résultats.

Par exemple, une recherche hebdomadaire nécessite 7 jours pour construire les données. Cette recherche renvoie des résultats après un délai de 7 jours.

Tableau 9-1 Intervalle de rapport QRadar Risk Manager

Intervalle de rapport	Description
Manuel	Génère un unique rapport sans planification de reproduction.
Hourly	Planifie le rapport pour le générer toutes les heures. Si vous sélectionnez l'option **Hourly**, une configuration supplémentaire est nécessaire. Dans les zones de liste, sélectionnez un cadre temporel de début et de fin du cycle de production. Un rapport est généré à chaque heure dans ce cet intervalle de temps. L'heure est disponible par incréments de 30 minutes. Le rapport horaire par défaut est planifié pour une exécution à 1h00.
Daily	Planifie le rapport pour le générer quotidiennement. Pour chaque graphique sur un rapport, vous pouvez sélectionner les 24 dernières heures de la journée, ou sélectionner un cadre temporel précis de la journée précédente. Si vous sélectionnez l'option **Daily**, une configuration supplémentaire est nécessaire. Cochez la case à côté de chaque jour où vous souhaitez générer un rapport. En outre, vous pouvez utiliser la zone de liste pour sélectionner une heure de début du cycle de génération de rapports. Les rapports quotidiens peuvent être planifiés par incréments de 30 minutes. Le rapport quotidien par défaut est planifié pour une exécution à 1h00.
Weekly	Planifie le rapport pour le générer de manière hebdomadaire. si vous sélectionnez l'option **Weekly**, une configuration supplémentaire est nécessaire. Sélectionnez le jour où vous souhaitez générer le rapport. La valeur configurée par défaut est le lundi. Dans la zone de liste, sélectionnez l'heure de début du cycle de génération de rapports. Les rapports hebdomadaires peuvent être planifiés par incréments de 30 minutes. Le rapport hebdomadaire par défaut est planifié pour une exécution à 1h00.

Tableau 9-1 Intervalle de rapport QRadar Risk Manager

Intervalle de rapport	Description
Monthly	Planifie le rapport pour le générer mensuellement. Si vous sélectionnez l'option **Monthly**, une configuration supplémentaire est nécessaire. A partir de la zone de liste, sélectionnez la date où vous souhaitez générer le rapport. La valeur configurée par défaut est le premier jour du mois. Vous pouvez également utiliser la zone de liste pour sélectionner un temps de commencement pour le cycle de génération de rapports. Les rapports mensuels peuvent être planifiés par incréments de 30 minutes. Le rapport mensuel par défaut est planifié pour une exécution à 1h00.

Les types de graphique suivants sont disponibles pour QRadar Risk Manager.

Tableau 9-2 Types de graphiques QRadar Risk Manager

Type de rapport	Description
Connections	Un rapport des connexions affiche le schéma de connexions de vos périphériques réseau établies au cours de votre intervalle de temps spécifié.
Device rules	Un rapport des règles de périphérique affiche les règles configurées sur votre périphérique réseau au cours de votre intervalle de temps spécifié.
Device unused objects	Un rapport sur les objets inutilisés du périphérique affiche une table contenant le nom, la date/heure de configuration et une définition des groupes de références d'objet non utilisés sur le périphérique. Un groupe de références d'objet est un terme générique utilisé pour décrire une collection d'adresses IP, d'adresses CIDR, de noms d'hôtes, de ports ou d'autres paramètres de périphérique regroupés et affectés aux règles du périphérique.

Des objets inutilisés de périphérique se présentent comme suit. Les périphériques Check Point prennent en charge le regroupement d'adresses IP dans des objets réseau. Les objets réseau peuvent ensuite être affectés aux règles du périphérique Check Point. Si un changement est apporté à l'objet réseau, il est implémenté sur toutes les règles faisant référence à l'objet réseau. Lorsque la configuration de périphérique d'un périphérique Check Point est normalisée par QRadar Risk Manager, les objets réseau sont convertis en groupes de références d'objet. Tous les périphériques ne prennent pas en charge la notion de groupe de références d'objet.

Création d'un rapport

Vous pouvez générer des rapports correspondant à un intervalle spécifique et choisir un type de graphique. Un rapport est composé de plusieurs données élémentaires. Il peut représenter les données réseau et les données de sécurité

sous plusieurs formes, telles qu'une table, un graphique à courbes, un graphique circulaire et un graphique à barres.

Pour générer un rapport :

Etape 1 Cliquez sur l'onglet **Reports**.

Etape 2 Dans la zone de liste **Actions**, sélectionnez **Create**.

Etape 3 Cliquez sur **Next** afin de se déplacer à la page suivante du Report Wizard.

Etape 4 Sélectionnez la fréquence pour le planning de génération de rapports.

Etape 5 Dans la sous-fenêtre Allow this report to generate manually, sélectionnez **Yes** pour activer ou **No** pour désactiver la génération manuelle du rapport.

Etape 6 Cliquez sur **Next**.

Etape 7 Configurez la présentation de votre rapport :

a Dans la zone de liste **Orientation**, sélectionnez le sens de la page.

b Sélectionnez une option de présentation pour votre rapport QRadar Risk Manager.

c Cliquez sur **Next**.

Etape 8 Indiquez des valeurs pour les paramètres suivants :

- **Report Title** - Entrez un titre de rapport. Le titre peut comporter jusqu'à 100 caractères de longueur. N'utilisez pas des caractères spéciaux.
- **Logo** - Dans la zone de liste, sélectionnez un logo. Le logoQRadar est le logo configuré par défaut. Pour plus d'informations sur l'image de marque de votre rapport, voir le manuel *IBM Security QRadar SIEM - Guide d'administration*.

Etape 9 Pour configurer chaque conteneur dans le rapport :

a Dans la zone de liste **Chart Type** , sélectionnez l'un des rapports spécifiques à QRadar Risk Manager.

b Configurez les données de rapport pour votre graphique.

Pour avoir des informations détaillées sur la configuration de votre graphique, voir la section Configuration de graphiques.

c Cliquez sur **Save Container Details**.

d Si nécessaire, répétez les étapes a à c pour tous les conteneurs de votre présentation de rapport.

e Cliquez sur **Next**.

Les graphiques affichés sur la page d'aperçu n'affichent pas les données réelles. Il ne s'agit que d'une représentation graphique de l'agencement que vous avez configuré.

Etape 10 Cliquez sur **Next** afin de se déplacer à la page suivante du Report Wizard.

Etape 11 Cochez les cases pour les formats de rapport. Vous pouvez sélectionner plusieurs options.

Les rapports Device Rules et Unused Object Rules ne peuvent être générés qu'aux formats PDF, HTML et RTF.

Etape 12 Cliquez sur **Next**.

Etape 13 Sélectionnez les canaux de distribution que vous souhaitez pour votre rapport.

Tableau 9-3 Options de distribution des rapports générés

Options	Description
Report Console	Cochez cette case pour envoyer le rapport généré à l'onglet **Reports**. Il s'agit du canal de distribution par défaut.
Sélectionnez les utilisateurs qui devraient être en mesure d'afficher le rapport généré.	Cette option s'affiche uniquement une fois que vous avez coché la case **Report Console**. Dans la liste des utilisateurs, sélectionnez les utilisateurs QRadar Risk Manager auxquels vous souhaitez accorder le droit d'afficher les rapports générés. ***Remarque :*** *Vous devez disposer des autorisations réseau appropriées pour partager les rapports générés avec d'autres utilisateurs. Pour plus d'informations à propos des autorisations, voir le manuel IBM Security QRadar SIEM - Guide d'administration.*
Select all users	Cette option s'affiche uniquement une fois que vous avez coché la case **Report Console**. Cochez cette case si vous voulez accorder le droit à tous les utilisateurs QRadar Risk Manager d'afficher les rapports générés. ***Remarque :*** *Vous devez disposer des autorisations réseau appropriées pour partager les rapports générés avec d'autres utilisateurs. Pour plus d'informations à propos des autorisations, voir le manuel IBM Security QRadar SIEM - Guide d'administration.*
E-mail	Cochez cette case si vous voulez distribuer les rapports générés par e-mail.
Entrez le(s) adresse(s) e-mail de distribution de rapport	Cette option s'affiche uniquement une fois que vous avez coché la case **E-mail**. Entrez l'adresse e-mail de chaque destinataire des rapports générés; séparez la liste des adresses e-mail avec des virgules. Le nombre maximum de caractères pour ce paramètre est 255. ***Remarque :*** *Les destinataires reçoivent cet e-mail de no_reply_reports@qradar.*
Include Report as attachment (non-HTML only)	Cette option s'affiche uniquement une fois que vous avez coché la case **E-mail**. Cochez cette case pour envoyer le rapport généré en tant que pièce jointe.

Tableau 9-3 Options de distribution des rapports générés (suite)

Options	Description
Include link to Report Console	Cette option s'affiche uniquement une fois que vous avez coché la case **E-mail**. Cochez cette case pour inclure un lien vers Report Console dans l'e-mail.

Etape 14 Cliquez sur **Next**.

Etape 15 Configurez les valeurs des paramètres suivants :

Tableau 9-4 Paramètres de finalisation

Paramètre	Description
Report Description	Entrez une description pour ce rapport. La description est affichée dans la page Report Summary et dans l'e-mail de distribution des rapports générés.
Groups	Sélectionnez les groupes auxquels vous voulez affecter ce rapport. Pour plus d'informations sur les groupes, voir la section Managing Reports (Gestion des rapports) dans le manuel*IBM Security QRadar SIEM Guide d'administration*.
Would you like to run the report now?	Cochez cette case si vous souhaitez générer le rapport lorsque l'assistant est terminé. Par défaut, la case est cochée.

Etape 16 Cliquez sur **Next** afin d'afficher le rapport récapitulatif.

vous pouvez sélectionner les onglets disponibles sur le rapport récapitulatif afin de prévisualiser les sélections du rapport.

Etape 17 Cliquez sur **Finish**.

Le rapport génère immédiatement. Si vous décochez la case **Would you like to run the report now** sur la dernière page de l'assistant, le rapport est enregistré et généré comme planifié.

Le titre du rapport est le titre par défaut pour le rapport généré. Si vous reconfigurez un rapport afin d'entrer un nouveau titre de rapport, le rapport est enregistré comme nouveau rapport avec le nouveau nom, mais l'original rapport reste le même.

Configuration de graphiques

Le type de graphique détermine les données configurées et affichées dans le graphique. Vous pouvez créer plusieurs graphiques pour les données spécifiques collectées par les périphériques dans QRadar Risk Manager.

Les types de graphiques suivants sont spécifiques à QRadar Risk Manager :

- Connections
- Device Rules
- Device Unused Objects

Connections

Vous pouvez utiliser le graphique Connections pour afficher les informations de connexion réseau. Vous pouvez baser vos graphiques sur des données provenant des recherches enregistrées à partir de l'onglet Risks. Ceci vous permet de personnaliser les données que vous souhaitez afficher dans le rapport généré. Vous pouvez configurer le graphique pour tracer des données sur une période de temps configurable. Cette fonctionnalité vous aide à détecter les tendances des connexions.

▶ Pour configurer un conteneur Connections Chart, configurez les valeurs des paramètres suivants :

Tableau 9-5 Paramètres des graphiques Connections

Paramètre	Description
Détails du conteneur - Connections	
Chart Title	Entrez un titre de graphique ne dépassant pas les 100 caractères.
Chart Sub-Title	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas les 100 caractères.
Graph Type	Dans la zone de liste, sélectionnez le type de graphique à afficher dans le rapport généré. Les options incluent : • **Bar** - Affiche les données dans un graphique à barres. Il s'agit du type de graphique par défaut. Ce type de graphique nécessite que la recherche enregistrée corresponde à une recherche groupée. • **Line** - Affiche les données dans un graphique à courbes. • **Pie** - Affiche les données dans un graphique circulaire. Ce type de graphique nécessite que la recherche enregistrée corresponde à une recherche groupée. • **Stacked Bar** - Affiche les données dans un graphique à barres empilées. • **Stacked Line** - Affiche les données dans un graphique à courbes empilées. • **Table** - Affiche les données sous la forme d'une table. L'option **Table** est uniquement disponible pour le conteneur de largeur pleine page seulement.
Graph	Dans la zone de liste, sélectionnez le nombre de connexions à afficher dans le rapport généré.

Tableau 9-5 Paramètres des graphiques Connections (suite)

Paramètre	Description
Manual Scheduling	Le panneau Manual Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Manually** dans le Report Wizard. Pour créer une planification manuelle : **1** Dans la zone de liste **From**, entrez la date de début que vous souhaitez pour le rapport ou sélectionnez la date en utilisant l'icône **Calendar**. La valeur configurée par défaut est la date actuelle. **2** Dans les zones de liste, sélectionnez l'heure de début que vous souhaitez pour le rapport. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00. **3** Dans la zone de liste **To** entrez la date de fin que vous souhaitez pour le rapport ou sélectionnez la date en utilisant l'icône **Calendar**. La valeur configurée par défaut est la date actuelle. **4** Dans les zones de liste, sélectionnez l'heure de fin que vous souhaitez pour le rapport. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00.
Hourly Scheduling	Le panneau Hourly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Hourly** dans le Report Wizard. La planification horaire place automatiquement dans des graphiques toutes les données de l'heure précédente.
Daily Scheduling	La sous-fenêtre Daily Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Daily** dans le Report Wizard. Sélectionnez l'une des options suivantes : • **All data from previous day (24 hours)** • **Data of previous day from** - Dans les zones de liste, sélectionnez la période de temps que vous souhaitez pour le rapport généré. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00.
Weekly Scheduling	Le panneau Weekly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Weekly** dans le Report Wizard. Sélectionnez l'une des options suivantes : • **All data from previous week** • **All Data from previous week from** - Dans les zones de liste, sélectionnez la période de temps que vous souhaitez pour le rapport généré. La valeur configurée par défaut est le dimanche.

Tableau 9-5 Paramètres des graphiques Connections (suite)

Paramètre	Description
Monthly Scheduling	La sous-fenêtre Monthly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Monthly** dans le Report Wizard. Sélectionnez l'une des options suivantes : • **All data from previous month** • **Data from previous month from the** - Dans les zones de liste, sélectionnez la période de temps que vous souhaitez pour le rapport généré. La valeur configurée par défaut s'étend du 1er au 31.
Graph Content	
Group	Dans la zone de liste, sélectionnez une recherche enregistrée pour afficher les recherches enregistrées appartenant à ce groupe dans la zone de liste **Available Saved Searches**.
Type Saved Search or Select from List	Pour affiner la liste **Available Saved Searches**, entrez le nom de la recherche que vous souhaitez localiser dans la zone **Type Saved Search or Select from List**. Vous pouvez également entrer un mot-clé pour afficher la liste des recherches incluant ce mot clé. Par exemple, entrez **`DMZ`** afin d'afficher une liste de toutes les recherches qui incluent DMZ dans le nom de la recherche.
Available Saved Searches	Fournit une liste des recherches enregistrées disponibles. Toutes les recherches enregistrées disponibles s'affichent par défaut, Cependant, vous pouvez filtrer la liste en sélectionnant un groupe dans la zone de liste **Group** ou en entrant le nom d'une recherche enregistrée connue dans la zone **Type Saved Search or Select from List**.
Create New Connection Search	Cliquez sur **Create New Connection Search** afin de créer une nouvelle recherche.

Device Rules

Vous pouvez utiliser le graphique Device Rules pour afficher les règles de pare-feu et le nombre d'événements de règles de pare-feu déclenchés dans votre réseau. Les rapports Device Rule vous permettent de générer un rapport pour les règles de pare-feu suivantes :

- Règles de périphérique d'acceptation les plus actives
- Règles de périphérique de refus les plus actives
- Règles de périphérique d'acceptation les moins actives
- Règles de périphérique de refus les moins actives
- Règles de périphérique inutilisées
- Règles de périphérique grisées

Les rapports que vous générez vous permettent de comprendre quelles règles sont acceptées, refusées, inutilisées ou appliquées dans un périphérique unique, dans un adaptateur spécifique ou dans plusieurs périphériques. Les rapports permettent à QRadar Risk Manager d'automatiser la génération de rapports sur l'état des règles de vos périphériques et d'afficher les rapports dans la console QRadar SIEM.

Cette fonctionnalité vous permet d'identifier la façon dont les règles sont utilisées sur vos périphériques réseau.

▶ Pour créer un conteneur Device Rules Chart, configurez les valeurs des paramètres suivants :

Tableau 9-6 Paramètres des graphiques Device Rules

Paramètre	Description
Détails du conteneur - Device Rules	
Limit Rules to Top	Dans la zone de liste, sélectionnez le nombre de règles à afficher dans le rapport généré. Par exemple, si vous limitez votre rapport aux 10 premières règles, créez un rapport pour les règles d'acceptation les plus utilisées dans tous les périphériques. Le rapport retourne 10 résultats. Les résultats contiennent une liste des 10 règles d'acceptation les plus utilisées en fonction du nombre d'événements parmi tous les périphériques visibles dans QRadar Risk Manager.

Tableau 9-6 Paramètres des graphiques Device Rules (suite)

Paramètre	Description
Type	Sélectionnez le type de règles de périphérique à afficher dans le rapport. Les options incluent : • **Most Used Accept Rules** - Affiche les règles d'acceptation les plus utilisées par le nombre d'événements pour un périphérique unique ou un groupe de périphériques. Ce rapport répertorie les règles présentant le plus grand nombre d'événements acceptés, dans l'ordre décroissant, pour l'intervalle de temps spécifié dans le rapport. • **Most Used Deny Rules** - Affiche les règles de refus les plus utilisées par le nombre d'événements pour un périphérique unique ou un groupe de périphériques. Ce rapport répertorie les règles présentant le plus grand nombre d'événements refusés, dans l'ordre décroissant, pour l'intervalle de temps spécifié dans le rapport. • **Unused Rules** - Affiche toutes les règles d'un périphérique unique ou d'un groupe de périphériques inutilisées. Les règles inutilisées ne présentent aucun événement pour l'intervalle de temps spécifié pour le rapport. • **Least Used Accept Rules** - Affiche les règles d'acceptation les moins utilisées pour un périphérique unique ou un groupe de périphériques. Ce rapport répertorie les règles présentant le plus petit nombre d'événements acceptés, dans l'ordre croissant, pour l'intervalle de temps spécifié dans le rapport. • **Least Used Deny Rules** - Affiche les règles de refus les moins utilisées pour un périphérique unique ou un groupe de périphériques. Ce rapport répertorie les règles présentant le plus petit nombre d'événements refusés, dans l'ordre croissant, pour l'intervalle de temps spécifié dans le rapport. • **Shadowed Rules** - Affiche toutes les règles d'un périphérique unique ne pouvant s'appliquer car la règle est verrouillée par une règle en cours d'application. Les résultats s'affichent dans une table des règles à l'origine de la désactivation et de toutes les règles ne pouvant s'appliquer sur votre périphérique, car elles sont désactivées par une règle en cours d'application sur le périphérique. ***Remarque :*** *Les rapports de règles grisées peuvent uniquement être exécutés par un périphérique unique. Ces règles ne présentent aucun événement pour l'intervalle de temps spécifié.*

Tableau 9-6 Paramètres des graphiques Device Rules (suite)

Paramètre	Description
Plage de dates/heures	Sélectionnez l'intervalle de temps de votre rapport. Les options sont les suivantes : • **Current Configuration** - Les résultats du rapport Device Rules sont basés sur les règles existant dans la configuration actuelle du périphérique. Ce rapport affiche les règles et les nombres d'événements pour la configuration de périphérique existante. La configuration actuelle d'un périphérique est basée sur la dernière fois que le composant Configuration Source Management a sauvegardé votre périphérique réseau. • **Interval** - Les résultats du rapport Device Rules sont basés sur les règles existant dans l'intervalle de temps de l'intervalle. Ce rapport affiche les règles et les nombres d'événements pour l'intervalle spécifié compris entre la dernière heure et 30 jours. • **Specific Range** - Les résultats du rapport Device Rules sont basés sur les règles existant entre l'heure de début et l'heure de fin de l'intervalle. Ce rapport affiche les règles et les nombres d'événements pour l'intervalle de temps spécifié.
Timezone	Sélectionnez le fuseau horaire que vous souhaitez utiliser comme base de votre rapport. Le fuseau horaire par défaut est basé sur la configuration de votre console QRadar SIEM. Lors de la configuration du paramètre Timezone pour votre rapport, prenez en compte l'emplacement des périphériques associés aux données de rapport. Si le rapport utilise des données couvrant plusieurs fuseaux horaires, les données utilisées pour le rapport sont basées sur l'intervalle de temps spécifique du fuseau horaire. Par exemple, si votre console QRadar SIEM est configurée pour l'heure standard EST, que vous planifiez un rapport quotidien entre 13h00 et 15h00 et que vous paramétrez le fuseau horaire sur l'heure standard CST, les résultats du rapport contiennent des informations entre 14h00 et 16h00 EST.

Tableau 9-6 Paramètres des graphiques Device Rules (suite)

Paramètre	Description
Targeted Data Selection	Targeted Data Selection permet de filtrer la plage de dates/heures pour obtenir une valeur plus précise. Grâce aux options Targeted Data Selection, vous pouvez générer un rapport pour afficher vos règles de périphérique sur une période de temps personnalisée définie, avec la possibilité d'inclure uniquement les données des heures et des jours que vous sélectionnez. Par exemple, vous pouvez programmer un rapport pour qu'il soit exécuté du 1er au 31 Octobre et afficher vos règles les plus actives, les moins actives ou inutilisées ainsi que leurs nombres de règles générées pendant vos heures de travail, telles que du lundi au vendredi, de 8 heures à 21 heures. ***Remarque :*** *Les détails de filtre s'affichent uniquement lorsque vous cochez la case* ***Targeted Data Selection*** *dans Report Wizard.*
Format	Sélectionnez le format de votre rapport de règles de périphérique. Les options sont les suivantes : • **One aggregate report for specified devices** - Ce format de rapport cumule les données de rapport dans plusieurs périphériques. Par exemple, si vous créez un rapport pour afficher les dix règles les plus souvent refusées, un rapport de cumul affiche les dix règles les plus souvent refusées dans tous les périphériques sélectionnés pour le rapport. Ce rapport retourne 10 résultats au total pour le rapport. • **One report per device** - Ce format de rapport affiche les données de rapport pour un seul périphérique. Par exemple, si vous créez un rapport pour afficher les dix règles les plus souvent refusées, un rapport de cumul affiche les dix règles les plus souvent refusées pour chaque périphérique sélectionné pour le rapport. Ce rapport retourne les 10 meilleurs résultats pour chaque périphérique sélectionné pour le rapport. Si vous avez sélectionné 5 périphériques, le rapport retourne 50 résultats. ***Remarque :*** *Les rapports de règles grisées peuvent afficher uniquement un rapport par périphérique.*

Tableau 9-6 Paramètres des graphiques Device Rules (suite)

Paramètre	Description
Devices	Sélectionnez les périphériques contenus dans le rapport. Les options sont les suivantes : • **All Devices** - Sélectionnez cette option pour intégrer tous les périphériques de QRadar Risk Manager dans votre rapport. • **Adapter** - Dans la zone de liste, sélectionnez un type d'adaptateur à intégrer à votre rapport. Un seul type d'adaptateur peut être sélectionné dans la zone de liste d'un rapport. • **Specific Devices** - Sélectionnez cette option pour intégrer uniquement des périphériques spécifiques dans votre rapport. La fenêtre Device Selection vous permet de sélectionner et d'ajouter des périphériques à votre rapport. Pour ajouter des périphériques individuels à votre rapport, procédez comme suit : **1** Cliquez sur **Browse** pour afficher la fenêtre Device Selection. **2** Sélectionnez tous les périphériques et cliquez sur **Add Selected**. Pour ajouter tous les périphériques à votre rapport, procédez comme suit : **1** Cliquez sur **Browse** pour afficher la fenêtre Device Selection. **2** Cliquez sur **Add All**. Pour rechercher des périphériques à intégrer à votre rapport, procédez comme suit : **1** Cliquez sur **Browse** pour afficher la fenêtre Device Selection. **2** Cliquez sur **Search**. **3** Sélectionnez les options de recherche pour filtrer la liste complète de périphériques par configuration obtenue, adresse IP ou CIDR, nom d'hôte, type, adaptateur, fournisseur ou modèle. **4** Cliquez sur **Search**. **5** Sélectionnez tous les périphériques et cliquez sur **Add Selected**.

Device Unused Objects

Un rapport sur les objets inutilisés du périphérique affiche les groupes de référence d'objet non utilisés par votre périphérique réseau. Ce rapport affiche les références d'objet telles qu'une collection d'adresses IP, de plages d'adresses CIDR ou de noms d'hôtes non utilisés par votre périphérique réseau.

▶ Pour configurer un conteneur d'objets inutilisés de périphérique, configurez les valeurs des paramètres suivants :

Tableau 9-7 Paramètres des rapports Device Unused Objects

Paramètre	Description
Détails du conteneur - Device Unused Objects	
Limit Objects to Top	Dans la zone de liste, sélectionnez le nombre de règles à afficher dans le rapport généré.
Devices	Sélectionnez les périphériques contenus dans le rapport. Les options sont les suivantes : • **All Devices** - Sélectionnez cette option pour intégrer tous les périphériques de QRadar Risk Manager dans votre rapport. • **Adapter** - Dans la zone de liste, sélectionnez un type d'adaptateur à intégrer à votre rapport. Un seul type d'adaptateur peut être sélectionné dans la zone de liste d'un rapport. • **Specific Devices** - Sélectionnez cette option pour intégrer uniquement des périphériques spécifiques dans votre rapport. La fenêtre Device Selection vous permet de sélectionner et d'ajouter des périphériques à votre rapport. Pour ajouter des périphériques individuels à votre rapport, procédez comme suit : **1** Cliquez sur **Browse** pour afficher la fenêtre Device Selection. **2** Sélectionnez tous les périphériques et cliquez sur **Add Selected**. Pour ajouter tous les périphériques à votre rapport, procédez comme suit : **1** Cliquez sur **Browse** pour afficher la fenêtre Device Selection. **2** Cliquez sur **Add All**. Pour rechercher des périphériques à intégrer à votre rapport, procédez comme suit : **1** Cliquez sur **Browse** pour afficher la fenêtre Device Selection. **2** Cliquez sur **Search**. **3** Sélectionnez les options de recherche pour filtrer la liste complète de périphériques par configuration obtenue, adresse IP ou CIDR, nom d'hôte, type, adaptateur, fournisseur ou modèle. **4** Cliquez sur **Search**. **5** Sélectionnez tous les périphériques et cliquez sur **Add Selected**.

Génération manuelle d'un rapport

Les rapports peuvent être générés manuellement au lieu d'attendre que QRadar Risk Manager ne génère un rapport basé sur une planification. Si vous générez plusieurs rapports manuellement, ces derniers sont ajoutés à une file d'attente et portent le libellé de leur position dans la file d'attente. Le fait de générer manuellement un rapport ne réinitialise pas le planning de rapport existant. Par exemple, si vous générez un rapport hebdomadaire pour les refus de pare-feu les plus actifs, générez manuellement le rapport. Le rapport hebdomadaire continuera à être généré selon le planning initialement configuré.

Pour générer manuellement un rapport :

Etape 1 Cliquez sur l'onglet **Reports**.

Etape 2 Sélectionnez le rapport que vous souhaitez générer.

Etape 3 Cliquez sur **Run Report**.

Le rapport génère. Alors que le rapport génère, la colonne **Next Run Time** affiche l'un des trois messages suivants :

- **Generating** - Le rapport est en cours de génération.
- **Queued (*position in the queue*)** - Le rapport est mis en attente pour la génération. Le message indique la position du rapport en file d'attente. Par exemple, 1 de 3.
- **(*x* hour(s) *x* min(s) *y* sec(s))** - Le rapport est planifié pour s'exécuter. Le message est un compte à rebours qui indique quand le rapport suivant sera exécuté.

REMARQUE

Vous pouvez sélectionner l'icône **Refresh** pour actualiser l'affichage, y compris les informations dans la colonne**Next Run Time**.

Après la génération d'un rapport, vous pouvez afficher le rapport généré dans la colonne**Generated Reports**.

Edition d'un rapport

L'édition d'un rapport vous permet d'ajuster sa planification, sa présentation, sa configuration, son titre, son format et son mode de diffusion. Vous pouvez éditer les rapports existants ou éditer un rapport par défaut.

Pour éditer un rapport existant, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Reports**.

Etape 2 Sélectionnez le rapport que vous souhaitez éditer.

Etape 3 A partir de la zone de liste **Actions**, sélectionnez **Edit**.

REMARQUE

Le fait de cliquer deux fois sur un rapport ouvre également Report Wizard, ce qui vous permet d'éditer un rapport existant.

Etape 4 Sélectionnez la fréquence pour le nouveau planning de génération de rapports.

- **Manually** - Génère un rapport une seule fois sans planning se reproduisant.
- **Hourly** - Planifie le rapport pour générer, à la fin de chaque heure en utilisant les données de la précédente heure.
- **Daily** - Planifie le rapport pour générer quotidiennement en utilisant les données de la journée précédente. Pour chaque graphique sur un rapport, vous pouvez sélectionner les 24 dernières heures de la journée, ou sélectionner un cadre temporel précis de la journée précédente.
- **Weekly** - Planifie le rapport pour générer hebdomadairement en utilisant les données de la semaine précédente.
- **Monthly** - Planifie le rapport pour générer mensuellement en utilisant les données du mois précédent.

Etape 5 Pour autoriser ce rapport à générer un panneau manuel, sélectionnez l'une des options suivantes :

- **Yes** - Active la génération manuelle de ce rapport.
- **No** - Désactive la génération manuelle de ce rapport.

Etape 6 Cliquez sur **Next** afin de se déplacer à la page suivante du Report Wizard.

Etape 7 Configurez la présentation de votre rapport :

a Dans la zone de liste **Orientation**, sélectionnez le sens de la page.

b Sélectionnez une option de présentation pour votre rapport QRadar Risk Manager.

c Cliquez sur **Next**.

Etape 8 Indiquez des valeurs pour les paramètres suivants :

- **Report Title** - Entrez un titre de rapport. Le titre peut comporter jusqu'à 100 caractères de longueur. N'utilisez pas des caractères spéciaux.
- **Logo** - Dans la zone de liste, sélectionnez un logo. Le logoQRadar est le logo configuré par défaut. Pour plus d'informations sur l'image de marque de votre rapport, voir le manuel *IBM Security QRadar SIEM - Guide d'administration*.

Etape 9 Configurez le conteneur pour vos données de rapport :

a Cliquez sur **Define**.

b Configurez les données de rapport pour votre graphique.

Pour plus d'informations sur la configuration de votre conteneur de graphique, voir la section Configuration de graphiques.

c Cliquez sur **Save Container Details**.

L'assistant revient à la page précédente, vous permettant d'indiquer plus de contenus pour votre rapport.

d Si nécessaire, répétez les étapes a à c pour éditer tous les conteneurs supplémentaires.

e Cliquez sur **Next** afin de se déplacer à la page suivante du Report Wizard.

Etape 10 Cliquez sur **Next** afin de se déplacer à la page suivante du Report Wizard.

Etape 11 Cochez les cases pour les formats de rapport. Vous pouvez sélectionner plus d'une option. Les options sont les suivantes :

- Portable Document Format (PDF) - Il s'agit du format de rapport configuré par défaut.
- Hypertext Markup Language (HTML)
- Rich Text Format (RTF)
- Extended Markup Language (XML)
- Excel Spreadsheet (XLS)

REMARQUE

Les rapports spécifiques à QRadar Risk Manager tels que Device Rule et Device Unused Object ne peuvent être produits qu'aux formats PDF, HTML et RTF.

Etape 12 Cliquez sur **Next** afin de se déplacer à la page suivante du Report Wizard.

Etape 13 Sélectionnez les canaux de distribution pour votre rapport.

Etape 14 Cliquez sur **Next** afin de se déplacer à la page suivante du Report Wizard.

Etape 15 Configurez les valeurs des paramètres suivants :

Tableau 9-8 Paramètres de finalisation

Paramètre	Description
Report Description	Entrez une description pour ce rapport. Cette description est affichée dans la page Report Summary et dans l'e-mail de distribution des rapports générés.
Groups	Sélectionnez les groupes auxquels vous voulez affecter ce rapport. Pour plus d'informations sur les groupes, voir la section Managing Reports (Gestion des rapports) dans le manuel *IBM Security QRadar SIEM - Guide d'administration*.
Would you like to run the report now?	Cochez cette case si vous souhaitez générer le rapport lorsque l'assistant est terminé. Par défaut, la case est cochée.

Etape 16 Cliquez sur **Next** afin d'afficher le rapport récapitulatif.

La page du rapport récapitulatif s'affiche, fournissant des détails pour le rapport. vous pouvez sélectionner les onglets disponibles sur le rapport récapitulatif afin de prévisualiser les sélections du rapport.

Etape 17 Cliquez sur **Finish**.

Le rapport est mis à jour avec vos changements.

Duplication d'un Rapport

Pour dupliquer un rapport :

Etape 1 Cliquez sur l'onglet **Reports**.

Etape 2 Sélectionnez le rapport que vous souhaitez dupliquer.

Etape 3 Dans la zone de liste **Actions**, cliquez sur **Duplicate**.

Etape 4 Entrez un nouveau nom, sans espaces, pour le rapport.

Partage d'un rapport

Vous pouvez partager des rapports avec d'autres utilisateurs. Lorsque vous partager un rapport, vous devez fournir une copie du rapport sélectionné à un autre utilisateur pour modifier ou planifier. Toutes les mises à jour effectuées par l'utilisateur sur un rapport partagé n'affecte pas la version originale du rapport.

REMARQUE

Vous devez disposer de privilèges administratifs afin de partager des rapports. En outre, pour qu'un nouvel utilisateur puisse afficher et accéder aux rapports, un administrateur doit partager tous les rapports nécessaires avec le nouvel utilisateur.

Pour partager un rapport :

Etape 1 Cliquez sur l'onglet **Reports**.

Etape 2 Sélectionnez le rapport que vous souhaitez partager.

Etape 3 Dans la zone de liste **Actions**, cliquez sur **Share**.

Etape 4 Dans la liste des utilisateurs, sélectionnez les utilisateurs avec lesquels vous souhaitez partager ce rapport.

Si aucun utilisateur ayant un accès approprié n'est disponible, un message s'affiche.

Etape 5 Cliquez sur **Share**.

Pour plus d'informations sur les rapports, voir le manuel *IBM Security QRadar SIEM - Guide d'utilisation*.

10 UTILISATION DES SIMULATIONS

La fonction Simulations vous permet de définir, planifier et effectuer des simulations d'utilisation sur votre réseau. Vous pouvez créer des simulations en vous basant sur une série de règles pouvant être combinées et configurées. La simulation peut être planifiée pour être exécutée de manière périodique ou manuellement. Une fois la simulation terminée, vous pouvez vérifier les résultats de la simulation et approuver tous les résultats acceptables ou de faible risque en fonction de votre politique réseau. Cela vous permet de valider les actions ou le trafic acceptable(s) provenant de vos résultats. Après avoir réglé votre simulation, vous pouvez la configurer afin de surveiller les résultats. Le fait de surveiller une simulation vous permet de définir la façon dont vous souhaitez que le système réponde lorsque des résultats non validés sont retournés. Cette réponse peut être un e-mail, la création d'un événement ou l'envoi de la réponse à syslog.

Utilisation des simulations

A l'aide de la barre d'outils principale de la page Simulations, vous pouvez accéder aux options suivantes:

Tableau 10-1 Options de la barre d'outils

Option	Description
Group	Vous permet d'afficher les simulations basées sur un groupe. Dans la zone de liste déroulante **Group**, sélectionne le groupe pour les simulations à afficher.
Groups	Vous permet de configurer les groupes pour les simulations. Voir la section Regroupement de simulations.
Monitor	Vous permet de contrôler une simulation, ce qui vous permet de vérifier qu'un événement est généré lorsque de nouveaux résultats apparaissent. Voir la section Surveillance des simulations.

Tableau 10-1 Options de la barre d'outils (suite)

Option	Description
Actions	La zone de liste déroulante **Actions** vous permet d'exécuter les actions suivantes : • **New** - Vous permet de créer une nouvelle simulation. Voir la section Création d'une simulation. • **Edit** - Vous permet d'afficher ou d'éditer la configuration d'une simulation existante. Voir la section Edition d'une simulation. • **Duplicate** - Vous permet de copier une simulation. Voir la section Duplication d'une simulation. • **Delete** - Vous permet de supprimer une simulation. Voir la section Suppression d'une simulation. • **Assign Groups** - Vous permet d'affecter une simulation à un groupe. Voir la section Affectation d'un élément à un groupe. • **Toggle Scheduling** - Bascule entre active/inactive pour la simulation sélectionnée. • **Run Simulation** - Vous permet d'exécuter manuellement une simulation. Voir la section Exécution manuelle d'une simulation.
Print	Vous permet d'imprimer l'affichage en cours.

Affichage des simulations

Les simulations créées par les utilisateurs et les résultats de simulation peuvent s'afficher sur la page Simulations.

Pour afficher les simulations existantes, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Sur le menu de navigation, sélectionnez **Simulation > Simulations**.

La fenêtre Simulations affiche les informations suivantes :

Tableau 10-2 Paramètres des définitions de simulations

Paramètre	Description
Simulation Name	Nom de la simulation tel qu'il a été défini par le créateur de la simulation.
Model	Type de modèle. Les simulations peuvent être modélisées en dehors de votre modèle Current Topology ou Topology. Les options sont : • Current Topology • Nom du modèle de topologie. Pour plus d'informations sur les modèles de topologie, voir le **Chapitre 11** Utilisation de modèles de topologie.
Groups	Groupes avec lesquels la simulation est associée.
Created By	Utilisateur qui a créé la simulation.
Creation Date	Date et heure de création de la simulation.

Tableau 10-2 Paramètres des définitions de simulations (suite)

Paramètre	Description
Last Modified	Date et heure de la dernière modification de la simulation.
Schedule	Fréquence d'exécution planifiée de la simulation. Les options sont les suivantes : • **Manual** - La simulation fonctionne lorsqu'elle est manuellement exécutée. • **Once** - Indiquez la date et heure d'exécution planifiée de la simulation. • **Daily** - Indiquez l'heure d'exécution planifiée de la simulation. • **Weekly** - Indiquez le jour de la semaine et l'heure d'exécution planifiée de la simulation. • **Monthly** - Indiquez le jour du mois et l'heure d'exécution planifiée de la simulation.
Last Run	Date et heure de la dernière exécution de la simulation.
Next Run	Date et heure de la prochaine exécution de la simulation.
Results	Si la simulation a été exécutée, ce paramètre comprend une zone de liste déroulante qui contient une liste des dates renfermant les résultats de votre simulation. Si la simulation n'a pas été exécutée, la colonne Results affiche la valeur No Results. Pour plus d'informations, voir la section Affichage des résultats de simulation.

Gestion des simulations

Vous pouvez créer, afficher, éditer, dupliquer et supprimer des simulations. T

Création d'une simulation

Vous pouvez créer des simulations dans l'onglet **Risks.**

Pour créer une simulation, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Sur le menu de navigation, sélectionnez **Simulation > Simulations**.

Etape 3 Dans la zone de liste déroulante **Actions**, sélectionnez **New**.

Etape 4 Entrez un nom pour la simulation dans le paramètre **What do you want to name this simulation?**.

Le nom s'affiche dans la fenêtre principale Simulation.

Etape 5 Dans la zone de liste déroulante **Which model do you want to base this on?** , sélectionnez le type de données à retourner. Les options sont :

- **Current Topology** - Vous permet d'exécuter une simulation selon le modèle de topologie en cours.

- **<Topology Model>** - Vous permet d'afficher les modèles de topologie existants. Si aucun modèle de topologie n'a été créé, seule l'option Current Topology s'affiche.

Etape 6 Sélectionnez l'une des options suivantes :

a Si vous souhaitez baser la simulation sur les données de connexion et de topologie, cochez la case **Use Connection Data**.

b Si vous souhaitez baser la simulation uniquement sur les données de topologie, décochez la case **Use Connection Data**.

Si votre modèle de topologie ne contient aucune donnée et que vous décochez la case **Use Connection Data**, la simulation ne renvoie aucun résultat.

Etape 7 Dans la zone de liste déroulante **Importance Factor**, sélectionnez le niveau d'importance à associer à cette simulation.

L'option Importance Factor permet de calculer le niveau de risque. Le plage est comprise entre 1 (faible importance) et 10 (haute importance). La valeur par défaut est 5.

Etape 8 Dans la zone de liste déroulante **Where do you want the simulation to begin?**, sélectionnez une origine pour la simulation.

La valeur sélectionnée détermine le point de départ de la simulation. Par exemple, l'attaque provient d'un réseau spécifique.

Les paramètres de simulation sélectionnés s'affichent dans la fenêtre **Generate a simulation where**.

Etape 9 Ajoutez les cibles de l'attaque de simulation au test de simulation.

Lorsque les cibles de test sont ajoutées à la fenêtre **Generate a simulation where** , les paramètres configurables s'affichent soulignés.

Tableau 10-3 Tests de simulation

Intitulé du test	Description	Paramètres
Attack originates from one of the following **IP addresses**	Vous permet de simuler les attaques provenant des adresses IP ou plages CIDR spécifiques.	Configurez le paramètre **IP addresses** pour définir la ou les adresses IP ou plages CIDR d'où vous souhaitez faire partir cette simulation.
Attack originates from one of the following **networks**	Vous permet de simuler les attaques provenant des actifs membres de l'un ou de plusieurs des emplacements de réseau définis.	Configurez le paramètre **networks** pour définir les réseaux d'où vous souhaitez faire partir cette simulation.
Attack originates from the Internet	Vous permet de simuler les attaques provenant d'Internet.	Aucun.
Attack originates from one of the following **asset building blocks**	Vous permet de simuler les attaques provenant d'un ou de plusieurs groupes d'éléments structurants d'actifs définis.	Configurez le paramètre **asset building blocks** pour définir les éléments structurants d'actifs d'où vous souhaitez faire partir cette simulation.

Tableau 10-3 Tests de simulation (suite)

Intitulé du test	Description	Paramètres
Attack originates from one of the following **geographic network locations**	Vous permet de simuler les attaques provenant d'un ou de plusieurs emplacements géographiques de réseau hostiles.	Configurez le paramètre **geographic network locations** pour définir l'emplacement d'où vous souhaitez faire partir cette simulation.
Attack originates from somebody that has visited one of the following **geographic network locations** over the last **1** days	Vous permet de simuler un actif qui a pu visité un serveur hébergé dans un ou plusieurs emplacements géographiques hostiles dans un intervalle de temps récent, ce qui peut indiquer des vulnérabilités côté client.	Configurez les paramètres suivants : • **geographic network locations -** Indiquez l'emplacement d'où vous souhaitez faire partir cette simulation. • **1** - Indiquez le nombre de jours que vous souhaitez que ce simulation considère. La valeur par défaut est 1.
Attack originates from one of the following **remote network locations**	Vous permet de simuler une attaque provenant d'un ou de plusieurs réseaux distants hostiles.	Configurez le paramètre **remote network locations** pour définir l'emplacement distant d'où vous souhaitez faire partir cette simulation.
Attack originates from somebody that has visited one of the following **remote network locations** over the last **1** days.	Vous permet de simuler un actif qui a pu visité un ou plusieurs réseaux distants hostiles dans un intervalle de temps récent, ce qui peut indiquer des vulnérabilités côté client.	Configurez les paramètres suivants : • **remote network locations -** Indiquez l'emplacement d'où vous souhaitez faire partir cette simulation. • **1** - Indiquez le nombre de jours que vous souhaitez que ce simulation considère. La valeur par défaut est 1.

Etape 10 Dans la zone **Which simulations do you want to include in the attack?** , sélectionnez le signe **+** côté de la simulation à inclure.

Les options de simulation s'affichent dans la fenêtre **Generate a simulation where**.

Etape 11 Dans la fenêtre **Generate a simulation where**, cliquez sur les paramètres soulignés pour continuer à configurer les paramètres de simulation.

Tableau 10-4 Tests de simulation

Intitulé du test	Description	Paramètres
Attack targets one of the following IP addresses	Vous permet de simuler les attaques contre des adresses IP ou plages CIDR spécifiques.	Configurez le paramètre **IP addresses** pour définir la ou les adresses IP ou plages CIDR auxquelles vous souhaitez que cette simulation s'applique.
Attack targets one of the following networks	Vous permet de simuler les attaques visant des réseaux membres de l'un ou de plusieurs des emplacements de réseau définis.	Configurez le paramètre **networks** pour définir les réseaux auxquels vous souhaitez que cette simulation s'applique.

Tableau 10-4 Tests de simulation (suite)

Intitulé du test	Description	Paramètres
Attack targets one of the following **asset building blocks**	Vous permet de simuler les attaques visant un ou de plusieurs éléments structurants d'actifs définis.	Configurez le paramètre **asset building blocks** pour définir les éléments structurants d'actifs auxquels vous souhaitez que cette simulation s'applique.
Attack targets a vulnerability on one of the following ports using protocols	Vous permet de simuler les attaques visant une vulnérabilité d'un ou de plusieurs ports définis.	Configurez les paramètres suivants : • **Ports** - Indiquez les ports que vous souhaitez que cette simulation considère. • **Protocols** - Indiquez le protocole que vous souhaitez que cette simulation considère.
Attack targets a vulnerability on one of the following **operating systems**	Vous permet de simuler les attaques visant une vulnérabilité d'un ou de plusieurs systèmes d'exploitation définis.	Configurez le paramètre des systèmes d'exploitation pour identifier les **systèmes d'exploitation** que vous souhaitez que cette simulation considère. Seuls les systèmes d'exploitation connus pour les actifs de votre déploiement apparaissent dans la liste.
Remarque : *Le test de simulation de l'option* ***attack targets a vulnerability on one of the following operating systems*** *a été masqué dans Simulation Editor. Si vous utilisez actuellement cette simulation, l'option reste visible, mais a été remplacée par un test de simulation qui recherche dans les actifs des vulnérabilités par entrées de texte ou expressions régulières.*		
Attack targets assets susceptible to one of the following vulnerabilities	Vous permet de simuler les attaques visant des actifs sensibles à une ou plusieurs vulnérabilités définies.	Configurez le paramètre **vulnerabilities** pour identifier les vulnérabilités que vous souhaitez que ce test applique. Vous pouvez rechercher les vulnérabilités à l'aide des options OSVDB ID, Bugtraq ID, CVE ID ou title.
Attack targets assets susceptible to vulnerabilities with one of the following **classifications**	Vous permet de simuler les attaques visant un actif sensible à des vulnérabilités pour une ou plusieurs classifications définies.	Configurez le paramètre **classifications** pour identifier les classifications de vulnérabilité. Par exemple, une classification de vulnérabilité peut être Input Manipulation ou Denial of Service.
Attack targets assets susceptible to vulnerabilities with CVSS score greater than 5	Une valeur CVSS (Common Vulnerability Scoring System) est une norme de l'industrie permettant d'évaluer la gravité des vulnérabilités. Cette simulation filtre les actifs de votre réseau qui comprennent la valeur CVSS configurée. Vous permet de simuler les attaques visant un actif sensible à des vulnérabilités d'un niveau CVSS supérieur à 5.	Configurez les paramètres suivants : • **greater than** - Indiquez si vous souhaitez que la valeur du risque CVSS soit supérieure à, supérieure ou égale à, inférieure à, inférieure ou égale à, égale à ou différente de la valeur configurée. La valeur par défaut est greater than. • **5** - Indiquez la valeur de risque CVSS vous souhaitez que ce test considère. La valeur par défaut est 5.
Attack targets assets susceptible to vulnerabilities from one of the following **vendors**	Vous permet de simuler les attaques visant un actif sensible à des vulnérabilités provenant des fournisseurs définis.	Configurez le paramètre **vendor** pour identifier les fournisseurs de vulnérabilités que vous souhaitez que cette simulation considère.

Tableau 10-4 Tests de simulation (suite)

Intitulé du test	Description	Paramètres
Remarque : *Le test de simulation de l'option* **attack targets assets susceptible to vulnerabilities from one of the following vendors** *a été masqué dans Simulation Editor. Si vous utilisez actuellement ce test de simulation, l'option reste visible, mais a été remplacée par un test de simulation qui recherche dans les actifs des vulnérabilités par entrées de texte ou expressions régulières.*		
Attack targets assets susceptible to vulnerabilities from one of the following **products**	Vous permet de simuler les attaques visant un actif sensible à des vulnérabilités provenant des produits définis.	Configurez le paramètre **products** pour identifier les produits de vulnérabilités que vous souhaitez que cette simulation considère.
Remarque : *Le test de simulation de l'option* **attack targets assets susceptible to vulnerabilities from one of the following products** *a été masqué dans Simulation Editor. Si vous utilisez actuellement ce test de simulation, l'option reste visible, mais a été remplacée par un test de simulation qui recherche dans les actifs des vulnérabilités par entrées de texte ou expressions régulières.*		
Attack targets assets susceptible to vulnerabilities disclosed after this date	Vous permet de simuler les attaques visant un actif sensible à des vulnérabilités reconnues avant, après ou à la date configurée.	Configurez les paramètres suivants : • **before | after | on** - Indiquez si vous souhaitez que la simulation considère les vulnérabilités divulguées comme se trouvant après, avant ou à la date configurée sur les actifs. La valeur par défaut est before. • **this date** - Indiquez la date que vous souhaitez que cette simulation considère.
Attack targets assets susceptible to vulnerabilities where the name, vendor, version or service contains one of the following **text entries**	Vous permet de simuler les attaques visant un actif sensible à des vulnérabilités comparant le nom d'actif, le fournisseur, la version ou le service à une ou plusieurs entrées de texte.	Configurez le paramètre **text entries** pour identifier le nom d'actif, le fournisseur, la version ou le service que vous souhaitez que cette simulation considère.
Attack targets assets susceptible to vulnerabilities where the name, vendor, version or service contains one of the following **regular expressions**	Vous permet de simuler les attaques visant un actif sensible à des vulnérabilités comparant le nom d'actif, le fournisseur, la version ou le service à une ou plusieurs expressions régulières.	Configurez le paramètre **regular expressions** pour identifier le nom d'actif, le fournisseur, la version ou le service que vous souhaitez que cette simulation considère.

Etape 12 Dans la zone de liste déroulante **Run this simulation for**, sélectionnez le nombre d'étapes à utiliser pour exécuter cette simulation (de 1 à 5) ainsi que le planning d'exécution de la simulation. Les options sont :

- **Manual** - La simulation fonctionne lorsqu'elle est manuellement exécutée.
- **Once** - Indiquez la date et heure d'exécution planifiée de la simulation.
- **Daily** - Indiquez l'heure d'exécution planifiée de la simulation.
- **Weekly** - Indiquez le jour de la semaine et l'heure d'exécution planifiée de la simulation.
- **Monthly** - Indiquez le jour du mois et l'heure d'exécution planifiée de la simulation.

Etape 13 Dans la zone de groupes, cochez la case pour tout groupe à affecter à cette simulation. Pour plus d'informations sur le regroupement des simulations, voir la section Regroupement de simulations.

Etape 14 Cliquez sur **Save Simulation**.

Edition d'une simulation

Vous pouvez éditer des simulations dans l'onglet **Risks**.

Pour éditer une simulation, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Sur le menu de navigation, sélectionnez **Simulation > Simulations**.

Etape 3 Sélectionnez la définition de simulation à éditer.

Etape 4 Dans la zone de liste déroulante **Actions**, sélectionnez **Edit**.

Etape 5 Mettez à jour les paramètres, au besoin.

Pour plus d'informations sur les paramètres Simulation, voir la section Création d'une simulation.

Etape 6 Cliquez sur **Save Simulation**.

Duplication d'une simulation

Vous pouvez dupliquer des simulations dans l'onglet **Risks**.

Pour dupliquer une simulation, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Sur le menu de navigation, sélectionnez **Simulation > Simulations**.

Etape 3 Sélectionnez la simulation que vous souhaitez dupliquer.

Etape 4 Dans la zone de liste déroulante **Actions**, sélectionnez **Duplicate**.

Etape 5 Entrez le nom de la simulation.

Etape 6 Cliquez sur **OK**.

Suppression d'une simulation

Vous pouvez supprimer des simulations dans l'onglet **Risks**.

Pour supprimer une simulation, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Sur le menu de navigation, sélectionnez **Simulation > Simulations**.

Etape 3 Sélectionnez la simulation que vous souhaitez supprimer.

Etape 4 Dans la zone de liste déroulante **Actions**, sélectionnez **Delete**.

Etape 5 Cliquez sur **OK**.

Exécution manuelle d'une simulation

A l'aide de Simulation Editor, vous pouvez planifier une simulation à exécuter. Vous pouvez également exécuter manuellement une simulation à l'aide du

processus ci-dessous. Pour plus d'informations sur la planification d'une simulation, voir la section Création d'une simulation.

Pour exécuter manuellement une simulation, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Sur le menu de navigation, sélectionnez **Simulation > Simulations**.

Etape 3 Dans la zone de liste déroulante **Actions**, sélectionnez **Run Simulation**.

Etape 4 Cliquez sur **OK**.

Le processus de simulation peut prendre un certain temps. Lors de l'exécution de la simulation, la colonne Next Run indique le pourcentage de tâche réalisée. Une fois le processus terminé, la colonne Results affiche la date et heure de la simulation. Pour afficher les résultats, voir la section Affichage des résultats de simulation.

Si vous exécutez une simulation et que vous effectuez ensuite des changements affectant les tests associés à la simulation, ces changements peuvent prendre jusqu'à une heure pour s'afficher.

Gestion des résultats de simulations

Une fois une simulation exécutée, la colonne Results affiche la zone de liste déroulante contenant une liste des dates de génération de la simulation. Tous les résultats de la simulation sont conservés pendant 30 jours.

Affichage des résultats de simulation

Pour affichez les résultats de la simulation, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Sur le menu de navigation, sélectionnez **Simulation > Simulations**.

Etape 3 Dans la colonne Results, sélectionnez la date et l'heure de la simulation à afficher à l'aide de la zone de liste déroulante.

REMARQUE

La zone de liste déroulante s'affiche uniquement dans la colonne Results si la simulation a été exécutée. Si aucune simulation n'est exécutée, cette zone indique la valeur No Results.

Etape 4 Cliquez sur **View Result**.

Les résultats de la simulation apparaissent en fournissent des informations sur chaque étape de la simulation.

Par exemple, la première étape fournit une liste des actifs directement connectés concernés par la simulation. La seconde étape répertorie les actifs de votre réseau qui peuvent communiquer avec les actifs de premier niveau de votre simulation.

La fenêtre Simulation Results contient les informations suivantes :

Tableau 10-5 Paramètres des résultats de simulation

Paramètre	Description
Simulation Definition	Description de la simulation.
Using Model	Nom du modèle sur lequel la simulation a été exécutée.
Simulation Result	Date d'exécution de la simulation.
Step Results	Nombre d'étapes du résultat comprenant l'étape actuellement affichée.
Assets Compromised	Nombre total d'actifs impliqués dans cette étape et dans toutes les étapes de simulation. Si le modèle de topologie contient des données d'une plage IP de /32 définies comme pouvant être atteintes, QRadar Risk Manager ne valide pas ces actifs par rapport à la base de données. C'est la raison pour laquelle ces actifs ne sont pas pris en considération dans le total Asset Compromised. QRadar Risk Manager valide uniquement les actifs des plages IP supérieures, telles que /24, pour déterminer quels actifs existent.
Risk Score	L'indice de risque est calculé en fonction du nombre de résultats, des étapes, du nombre d'actifs impliqués et de l'élément Importance Factor affectés à la simulation. Cette valeur indique le niveau de gravité associé à la simulation pour l'étape affichée.

Etape 5 Affichez les informations de progression pour afficher la progression de la simulation :

a Placez le pointeur de votre souris sur une connexion pour déterminer la liste des actifs concernés par cette simulation.

Les 10 premiers actifs s'affichent lorsque vous placez le pointeur de votre souris sur la connexion. La table située sous le graphique affiche la liste complète d'actifs.

b Placez le pointeur de votre souris sur la connexion pour sélectionner le chemin via le réseau tel qu'il est défini par le sous-réseau.

Etape 6 Affichez la table des résultats de cette étape pour déterminer les actifs concernés :

La table des résultats de cette étape contient les informations suivantes :

Tableau 10-6 Paramètres des résultats

Paramètre	Description
Approve	Vous permet de valider les résultats de la simulation. Voir la section Approbation des résultats de simulations.
Parent	Adresse IP d'origine de l'étape affichée de la simulation.
IP	Adresse IP de l'actif concerné.
Network	Réseau des adresses IP cible telles qu'elles sont définies dans la hiérarchie de réseau.
Asset Name	Nom de l'actif concerné tel qu'il est défini dans le profil d'actif.

Tableau 10-6 Paramètres des résultats (suite)

Paramètre	Description
Asset Weight	Pondération de l'actif concerné telle qu'elle est définie dans le profil d'actif.

Etape 7 Pour afficher l'étape suivante des résultats de la simulation, cliquez sur **Next Step**.

Approbation des résultats de simulations

Les résultats de la simulation vous permettent de valider le trafic réseau correspondant à un faible risque ou à une communication normale sur l'actif. La validation des résultats vous permet de filtrer la liste de résultats de telle sorte que les simulations à venir ignorent les communications normales ou validées.

Pour valider les résultats de la simulation, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Sur le menu de navigation, sélectionnez **Simulation > Simulations**.

Etape 3 Dans la colonne Results, sélectionnez la date et l'heure de la simulation à afficher à l'aide de la zone de liste déroulante.

La zone de liste déroulante s'affiche uniquement dans la colonne Results si la simulation est exécutée. Si aucune simulation n'est exécutée, cette zone indique la valeur No Results.

Etape 4 Cliquez sur **View Result**.

Etape 5 Dans la table des résultats de cette étape, utilisez l'une des méthodes suivantes pour valider les actifs :

a Cochez une case pour chaque actif à valider, puis cliquez sur **Approve Selected**.

b Cliquez sur **Approve All**.

Etape 6 Cliquez sur **View Approved** pour afficher tous les actifs validés.

Révocation des approbations de simulations

La révocation des validations vous permet de sélectionner une connexion ou une communication validée dans la liste validée. Une fois un résultat de simulation validé supprimé, les simulations à venir affichent les communications non validées dans les résultats de la simulation.

Pour révoquer la validation des résultats de la simulation, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Sur le menu de navigation, sélectionnez **Simulation > Simulations**.

Etape 3 Dans la colonne Results, sélectionnez la date et l'heure de la simulation à afficher à l'aide de la zone de liste déroulante.

La zone de liste déroulante s'affiche uniquement dans la colonne Results si la simulation a été exécutée. Si aucune simulation n'a été exécutée, cette zone indique la valeur No Results.

Etape 4 Cliquez sur **View Result**.

Etape 5 Cliquez sur **View Approved** pour afficher tous les actifs validés.

Etape 6 Sélectionnez l'une des options suivantes :

a Cochez la case pour chaque résultat dont vous souhaitez révoquer la validation, puis cliquez sur **Revoke Selected**.

b Pour révoquer toutes les validations de résultats, cliquez sur **Revoke All**.

Surveillance des simulations

Si vous souhaitez générer un événement lorsque de nouveaux résultats de simulation apparaissent, vous pouvez configurer la simulation à contrôler. Lorsque vous configurez une simulation à contrôler, QRadar Risk Manager analyse la simulation pour déterminer si ses résultats ont changé. Vous pouvez configurer un maximum de 10 simulations en mode moniteur.

REMARQUE

Une simulation en mode moniteur correspond par défaut à un intervalle de temps d'1 heure. Cette valeur écrase la valeur temporelle configurée lors de la création de la simulation. Pour plus d'informations sur la création d'une simulation, voir la section Création d'une simulation.

Pour configurer une simulation à contrôler, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Sur le menu de navigation, sélectionnez **Simulation > Simulations**.

Etape 3 Sélectionnez la simulation que vous souhaitez contrôler.

Etape 4 Cliquez sur **Monitor**.

Etape 5 Entrez les valeurs pour les paramètres :

Tableau 10-7 Paramètres des résultats de la surveillance des simulations

Paramètre	Description
Event Name	Entrez le nom de l'événement que vous souhaitez afficher dans les onglets **Log Activity** et **Offenses**.
Event Description	Entrez une description de l'événement. La description est affichée dans le panneau Annotations des détails de l'événement.

Tableau 10-7 Paramètres des résultats de la surveillance des simulations (suite)

Paramètre	Description
Event Details	Sélectionnez une des options suivantes : • **High-Level Category** - Dans la zone de liste déroulante, sélectionnez la catégorie d'événement de haut niveau que vous souhaitez que cette simulation utilise lors du traitement des événements. Par défaut, la catégorie est Risk. • **Low-Level Category** - Dans la zone de liste déroulante, sélectionnez la catégorie d'événement de bas niveau que vous souhaitez que cette simulation utilise lors du traitement des événements. Par défaut, la catégorie est Compliance Violation. • **Ensure the dispatched event is part of an offense (Correlate By:)** - Cochez cette case si vous voulez, qu'à la suite de cette simulation contrôlée, les événements soient transmis au composant Magistrate. Si aucune violation n'a été créée sur l'onglet **Offenses**, une nouvelle violation est créée. Si une violation existe, cet événement est ajouté à la violation existante. Si vous cochez cette case, l'option suivante s'affiche : • **Question/Simulation** - Tous les événements d'une question sont associés à une violation unique. • **Asset** - Une violation unique est créée (ou mise à jour) pour chaque actif unique. ***Remarque :*** *Pour plus d'informations sur les catégories d'événements, voir le manuel QRadar - Guide d'utilisation.*

Tableau 10-7 Paramètres des résultats de la surveillance des simulations (suite)

Paramètre	Description
Additional Actions	Cochez la ou les cases à cocher pour indiquer les méthodes supplémentaires à utiliser sur un événement. Les options sont les suivantes : • **Email** - Cochez cette case et entrez la ou les adresses électroniques pour envoyer des notifications si l'événement est généré. Séparez par virgule plusieurs adresses électroniques. • **Send to Syslog** - Cochez cette case si vous souhaitez consigner l'événement. Par défaut, la case est décochée. Par exemple, la sortie syslog peut ressembler à : `Sep 28 12:39:01 localhost.localdomain ECS: Rule 'Name of Rule' Fired: 172.16.60.219:12642 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID: 1000398, Category: 1011, Notes: Event description` • **Notify** - Cochez cette case si vous voulez que les événements qui se génèrent à la suite de cette question contrôlée s'affichent dans l'élément System Notifications du tableau de bord. Pour plus d'informations sur l'onglet **Log Activity** et le tableau de bord QRadar SIEM, voir le manuel *IBM Security QRadar SIEM - Guide d'utilisation.*
Enable Monitor	Cochez cette case si vous voulez surveiller la simulation.

Etape 6 Cliquez sur **Save Monitor**.

Regroupement de simulations

Vous pouvez regrouper et afficher vos simulations en fonction de vos critères choisis. Le classement de vos simulations vous permet d'afficher et de suivre efficacement vos simulations. Par exemple, vous pouvez afficher toutes les simulations relatives à la conformité.

Lorsque vous créez des nouvelles simulations, vous pouvez assigner les simulations à un groupe existant. Pour plus d'informations sur l'affectation d'un groupe, consultez Gestion des simulations.

Affichage des groupes

Pour afficher les simulations à l'aide des groupes, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Sur le menu de navigation, sélectionnez **Simulation > Simulations**.

La fenêtre Simulations s'affiche.

Etape 3 Dans la zone de liste déroulante **Group**, sélectionnez le groupe à afficher.

La liste des éléments affectés à ce groupe s'affiche.

Création d'un groupe Pour créer un groupe :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Sur le menu de navigation, sélectionnez **Simulation > Simulations**.

Etape 3 Cliquez sur **Groups**.

Etape 4 Dans l'arborescence du menu, sélectionnez le groupe dans lequel vous souhaitez créer un nouveau groupe.

REMARQUE

Une fois un groupe créé, vous pouvez glisser-déplacer les groupes de l'arborescence des menus pour changer l'organisation.

Etape 5 Cliquez sur **New**.

Etape 6 Entrez les valeurs pour les paramètres :

- **Name** - Entrez le nom à affecter au nouveau groupe. Le nom peut contenir jusqu'à 225 caractères.
- **Description** - Entrez une description à affecter au nouveau groupe. La description peut contenir plus de 255 caractères.

Etape 7 Cliquez sur **OK**.

Etape 8 Pour changer l'emplacement du nouveau groupe, cliquez sur le nouveau groupe et faites glisser le dossier vers l'emplacement favori dans votre arborescence de menus.

Etape 9 Fermez la fenêtre Groups.

Edition d'un groupe Pour modifier un groupe :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Sur le menu de navigation, sélectionnez **Simulation > Simulations**.

Etape 3 Cliquez sur **Groups**.

Etape 4 Dans l'arborescence de menu, sélectionnez le groupe que vous souhaitez éditer.

Etape 5 Cliquez sur **Edit**.

Etape 6 Mettez les valeurs des paramètres à jour, si nécessaire :

- **Name** - Entrez le nom à affecter au nouveau groupe. Le nom peut contenir jusqu'à 225 caractères.
- **Description** - Entrez une description à affecter au nouveau groupe. La description peut contenir plus de 255 caractères.

Etape 7 Cliquez sur **OK**.

Etape 8 Pour changer l'emplacement du groupe, sélectionnez un groupe et faites glisser le dossier vers l'emplacement favori dans votre arborescence de menus.

Etape 9 Fermez la fenêtre Groups.

Copie d'un élément dans un autre groupe

En utilisant la fonctionnalité des groupes, vous pouvez copier une simulation vers un ou plusieurs groupes. Pour copier une simulation, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Sur le menu de navigation, sélectionnez **Simulation > Simulations**.

Etape 3 Cliquez sur **Groups**.

Etape 4 Dans l'arborescence de menu, sélectionnez la question que vous souhaitez copier dans un autre groupe.

Etape 5 Cliquez sur **Copy**.

Etape 6 Cochez la case pour le groupe dans lequel vous souhaitez copier la simulation.

Etape 7 Cliquez sur **Copy**.

Etape 8 Fermez la fenêtre Groups.

Suppression d'un élément d'un groupe

Pour supprimer une question d'un groupe, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Sur le menu de navigation, sélectionnez **Simulation > Simulations**.

Etape 3 Cliquez sur **Groups**.

Etape 4 Dans l'arborescence de menus, sélectionnez le groupe de niveau supérieur.

Etape 5 Dans la liste des groupes, sélectionnez l'élément ou le groupe que vous souhaitez supprimer.

Etape 6 Cliquez sur **Remove**.

Etape 7 Cliquez sur **OK**.

Etape 8 Fermez la fenêtre Groups.

Affectation d'un élément à un groupe

Pour affecter une simulation à un groupe, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks .**

Etape 2 Sur le menu de navigation, sélectionnez **Simulation > Simulations**.

La fenêtre Simulations s'affiche.

Etape 3 Sélectionnez la simulation à affecter à un groupe.

Etape 4 Dans la zone de liste déroulante **Actions**, sélectionnez **Assign Groups**.

La fenêtre Choose Group s'affiche.

Etape 5 Sélectionnez le groupe auquel vous souhaitez affecter la question.

Etape 6 Cliquez sur **Assign Groups**.

11 UTILISATION DE MODÈLES DE TOPOLOGIE

L'option Topology Model du menu de navigation Simulation vous permet de définir les modèles de réseau virtuel basés sur votre réseau existant. Vous pouvez créer un modèle de réseau en vous basant sur une série de modifications pouvant être combinées et configurées. Cela vous permet de déterminer l'effet des changements de configuration sur votre réseau à l'aide de la fonctionnalité Simulation. Pour plus d'informations sur les simulations, consultez **Utilisation des simulations**.

Affichage de modèles de topologie

Pour afficher les modèles de topologie :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Sur le menu de navigation, sélectionnez **Simulations > Topology Models**.

La page Topology Models fournit les informations suivantes :

Tableau 11-1 Paramètres des définitions des modèles

Paramètre	Description
Model Name	Nom du modèle de topologie tel qu'il a été défini par l'utilisateur lors de sa création.
Group(s)	Groupes auxquels cette topologie est associée.
Created By	Utilisateur qui a créé la définition de modèle.
Created On	Date et heure de création de la définition de modèle.
Last Modified	Nombre de jours écoulés depuis la création de la définition de modèle.

Création d'un modèle de topologie

Pour créer un modèle de topologie, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Sur le menu de navigation, sélectionnez **Simulations > Topology Models**.

La fenêtre Topology Models s'affiche.

Etape 3 Dans le menu déroulant **Actions**, sélectionnez **New**.

La fenêtre Model Editor s'affiche.

Etape 4 Dans la zone **What do you want to name is model?**, saisissez un nom pour la définition de modèle.

Etape 5 Dans la sous-fenêtre **Which modifications do you want to apply to your model?**, sélectionnez les modifications à appliquer à la topologie pour créer votre modèle.

Les tests sélectionnés sont affichés dans la sous-fenêtre Configure model as follows.

Etape 6 Configurez les tests ajoutés à la sous-fenêtre **Configure model as follows**.

Une fois le test affiché dans la sous-fenêtre, les paramètres configurables apparaissent soulignés. Cliquez sur chaque paramètre pour poursuivre la configuration de cette modification pour votre modèle.

Tableau 11-2 Tests sur la topologie

Intitulé du test	Paramètres
Une règle est ajoutée aux périphériques sélectionnés et permet d'établir des connexions entre les CIDR source et les CIDR cible sur les protocoles, les ports	Configurez les paramètres suivants : • **devices** - Indiquez les périphériques que vous souhaitez ajouter à cette règle. Dans la fenêtre Customize Parameter, cochez la case **All** pour inclure tous les périphériques. Vous pouvez également rechercher les périphériques à l'aide de l'un des critères de recherche suivants : I**P/CIDR** - Sélectionnez l'option IP/CIDR et indiquez l'adresse IP ou le routage CIDR que vous souhaitez ajouter à cette règle. **Hostname** - Sélectionnez l'option Hostname et indiquez le nom d'hôte que vous souhaitez filtrer. Pour rechercher plusieurs noms d'hôtes, utilisez un caractère générique (*) au début ou à la fin de la chaîne. **Adapter** - Sélectionnez l'option Adapter et utilisez la zone de liste déroulante pour filtrer la liste de périphériques par adaptateur. **Vendor** - Sélectionnez l'option Vendor et utilisez la zone de liste déroulante pour filtrer la liste de périphériques par fournisseur. Vous pouvez également définir un modèle pour le fournisseur. Pour rechercher plusieurs modèles, utilisez un caractère générique (*) au début ou à la fin de la chaîne. • **allows | denies** - Sélectionnez l'état (accept ou denied) des connexions que vous souhaitez que ce test applique. • **CIDRs** - Sélectionnez toutes les adresses IP source ou plages CIDR que vous souhaitez ajouter à cette règle. • **CIDRs** - Sélectionnez toutes les adresses IP cible ou plages CIDR que vous souhaitez ajouter à cette règle. • **protocols** - Indiquez les protocoles que vous souhaitez ajouter à cette règle. Pour insérer tous les protocoles, cochez la case **All**. • **ports** - Indiquez les ports que vous souhaitez ajouter à cette règle. Pour insérer tous les ports, cochez la case **All**.

Tableau 11-2 Tests sur la topologie (suite)

Intitulé du test	Paramètres
Une règle est ajoutée aux périphériques IPS sélectionnés et permet d'établir des connexions entre les CIDR source et les CIDR cible présentant certaines vulnérabilités	Configurez les paramètres suivants : • **IPS devices** - Indiquez les périphériques IPS que vous souhaitez intégrer à ce modèle de topologie. Pour insérer tous les périphériques IPS, cochez la case **All**. • **allows | denies** - Indiquez l'état (accept ou denied) des connexions que vous souhaitez que ce test applique. • **CIDRs** - Indiquez toutes les adresses IP source ou plages CIDR que vous souhaitez intégrer à ce modèle de topologie. • **CIDRs** - Indiquez toutes les adresses IP cible ou plages CIDR que vous souhaitez intégrer à ce modèle de topologie. • **vulnerabilities** - Indiquez les vulnérabilités que vous souhaitez appliquer à ce modèle de topologie. Vous pouvez rechercher les vulnérabilités à l'aide des options Bugtraq ID, OSVDB ID, CVE ID ou du titre.
Les actifs suivants permettent d'établir des connexions avec les ports sélectionnés	Configurez les paramètres suivants : • **assets** - Indiquez les actifs que vous souhaitez intégrer à ce modèle de topologie. • **allow | deny** - Indiquez l'état (allow ou deny) des connexions que vous souhaitez que ce modèle de topologie applique. La valeur configurée par défaut est allow. • **ports** - Indiquez les ports que vous souhaitez intégrer à ce modèle de topologie. Pour insérer tous les ports, cochez la case **All**.
Les actifs des **blocs de construction d'actifs suivants permettent** d'établir des connexions avec les **ports**	Configurez les paramètres suivants : • **assets building blocks** - Indiquez les blocs de construction que vous souhaitez intégrer à ce modèle de topologie. • **allow | deny** - Indiquez l'état (allow ou deny) que vous souhaitez que ce modèle de topologie applique. La valeur configurée par défaut est allow. • **ports** - Indiquez les ports que vous souhaitez intégrer à ce modèle de topologie. Pour insérer tous les ports, cochez la case **All**.

Etape 7 Dans la zone Groups, cochez la case permettant d'affecter des groupes à cette question. Pour plus d'informations sur le regroupement de questions, consultez Regroupement de modèles de topologie.

Etape 8 Cliquez sur **Save Model**.

Edition d'un modèle de topologie

Pour éditer un modèle de topologie, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Sur le menu de navigation, sélectionnez **Simulations > Topology Models**.

La fenêtre Topology Models s'affiche.

Etape 3 Sélectionnez la définition de modèle à éditer.

Etape 4 Dans le menu déroulant **Actions**, sélectionnez **Edit**.

La fenêtre Model Editor s'affiche.

Etape 5 Mettez à jour les paramètres, au besoin.

Pour plus d'informations sur les paramètres Model Editor, consultez Création d'un modèle de topologie.

Etape 6 Cliquez sur **Save Model**.

Duplication d'un modèle de topologie

Pour dupliquer un modèle de topologie, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Sur le menu de navigation, sélectionnez **Simulations > Topology Models**.

La fenêtre Topology Models s'affiche.

Etape 3 Sélectionnez la définition de modèle à dupliquer.

Etape 4 Dans le menu déroulant **Actions**, sélectionnez **Duplicate**.

La fenêtre Name s'affiche.

Etape 5 Tapez un nom que vous souhaitez attribuer au modèle de topologie copié.

Etape 6 Cliquez sur **OK**.

Etape 7 Editez le modèle comme vous le souhaitez.

Pour plus d'informations sur l'édition d'une question, consultez Edition d'un modèle de topologie.

Suppression d'un modèle de topologie

Pour supprimer un modèle de topologie, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Sur le menu de navigation, sélectionnez **Simulations > Topology Models**.

La fenêtre Topology Models s'affiche.

Etape 3 Sélectionnez la définition de modèle à supprimer.

Etape 4 Dans le menu déroulant **Actions**, sélectionnez **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 5 Cliquez sur **OK**.

Regroupement de modèles de topologie

Vous pouvez regrouper et afficher vos modèles de topologie en fonction de vos critères choisis. Le classement de votre modèle de topologie vous permet d'afficher et de suivre efficacement vos modèles. Par exemple, vous pouvez afficher tous les modèles de topologie relatifs à la conformité.

Lorsque vous créez de nouveaux modèles de topologie, vous pouvez les affecter au groupe existant. Pour plus d'informations sur l'affectation d'un groupe, consultez Création d'un modèle de topologie.

Viewing Groups

Pour afficher les modèles de topologie à l'aide des groupes, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Sur le menu de navigation, sélectionnez **Simulations > Topology Models**.

La fenêtre Topology Models s'affiche.

Etape 3 Dans la zone de liste déroulante **Group**, sélectionnez le groupe à afficher.

La liste des modèles de topologie affectés à ce groupe s'affiche.

Création d'un groupe

Pour créer un groupe :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Sur le menu de navigation, sélectionnez **Simulations > Topology Models**.

La fenêtre Topology Model s'affiche.

Etape 3 Cliquez sur **Groups**.

La fenêtre Group s'affiche.

Etape 4 Dans l'arborescence du menu, sélectionnez le groupe dans lequel vous souhaitez créer un nouveau groupe.

Une fois le groupe créé, vous pouvez glisser-déplacer les groupes des éléments de l'arborescence des menus pour changer l'organisation.

Etape 5 Cliquez sur **New**.

La fenêtre Group Properties s'affiche.

Etape 6 Entrez les valeurs pour les paramètres :

- **Name** - Entrez le nom à affecter au nouveau groupe. Le nom peut contenir jusqu'à 225 caractères.
- **Description** - Entrez une description à affecter à ce groupe. La description peut contenir plus de 255 caractères.

Etape 7 Cliquez sur **OK**.

Etape 8 Pour changer l'emplacement du nouveau groupe, cliquez sur le nouveau groupe et faites glisser le dossier vers un emplacement dans votre arborescence de menus.

Etape 9 Fermez la fenêtre Groups.

Edition d'un groupe

Pour modifier un groupe :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Sur le menu de navigation, sélectionnez **Simulations > Topology Models**.

La fenêtre Topology Models s'affiche.

Etape 3 Cliquez sur **Groups**.

La fenêtre Group s'affiche.

Etape 4 Dans l'arborescence de menu, sélectionnez le groupe que vous souhaitez éditer.

Etape 5 Cliquez sur **Edit**.

La fenêtre Group Properties s'affiche.

Etape 6 Mettez les valeurs des paramètres à jour, si nécessaire :

- **Name** - Entrez le nom à affecter au nouveau groupe. Le nom peut contenir jusqu'à 225 caractères.
- **Description** - Entrez une description à affecter à ce groupe. La description peut contenir plus de 255 caractères.

Etape 7 Cliquez sur **OK**.

Etape 8 Pour changer l'emplacement du groupe, cliquez sur le nouveau groupe et faites glisser le dossier vers un emplacement dans votre arborescence de menus.

Etape 9 Fermez la fenêtre Groups.

Copie d'un élément dans un autre groupe

En utilisant la fonctionnalité des groupes, vous pouvez copier un modèle de topologie vers un ou plusieurs groupes.

Pour copier un modèle de topologie, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Sur le menu de navigation, sélectionnez **Simulations > Topology Models**.

La fenêtre Topology Models s'affiche.

Etape 3 Cliquez sur **Groups**.

La fenêtre Group s'affiche.

Etape 4 Dans l'arborescence de menu, sélectionnez la question que vous souhaitez copier dans un autre groupe.

Etape 5 Cliquez sur **Copier**.

La fenêtre Choose Group s'affiche.

Etape 6 Cochez la case pour le groupe dans lequel vous souhaitez copier la simulation.

Etape 7 Cliquez sur **Copy**.

Etape 8 Fermez la fenêtre Groups.

Suppression d'un élément d'un groupe

Pour supprimer un modèle de topologie d'un groupe, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Sur le menu de navigation, sélectionnez **Simulations > Topology Models**.

Etape 3 Cliquez sur **Groups**.

Etape 4 Dans l'arborescence de menus, sélectionnez le groupe de niveau supérieur.

Etape 5 Dans la liste des groupes, sélectionnez le groupe que vous souhaitez supprimer.

Etape 6 Cliquez sur **Remove**.

Etape 7 Cliquez sur **OK**.

Etape 8 Pour changer l'emplacement du nouveau groupe, cliquez sur le nouveau groupe et faites glisser le dossier vers un emplacement dans votre arborescence de menus.

Etape 9 Fermez la fenêtre Groups.

Affectation d'une topologie à un groupe

Pour affecter un modèle de topologie à un groupe, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Risks.**

Etape 2 Sur le menu de navigation, sélectionnez **Simulations > Topology Models**.

Etape 3 Sélectionnez le modèle de topologie à affecter à un groupe.

Etape 4 Dans le menu déroulant **Actions**, sélectionnez **Assign Group**.

Etape 5 Sélectionnez le groupe auquel vous souhaitez affecter la question.

Etape 6 Cliquez sur **Assign Groups**.

A QUESTIONS POLICY MONITOR

Policy Monitor permet aux utilisateurs de définir des questions de test pour identifier les risques dans des périphériques réseau ou dans les règles qu'ils contiennent. Cette annexe inclut les paramètres détaillés des questions correspondant aux tests Policy Monitor.

Cette section fournit des informations sur l'étape suivante :

- **Asset Questions** - Identifie les actifs du réseau qui violent une règle définie ou qui introduisent des risques dans l'environnement. Pour une liste détaillée des questions sur les actifs, voir la section Questions de test sur les actifs.
- **Devices/Rules** - Identifie les règles dans un périphérique qui violent une règle définie qui peut introduire un risque dans l'environnement. Pour une liste détaillée des questions sur les règles des périphériques, voir la section Tests périphériques ou règles.

Questions de test sur les actifs

Les questions de test sur les actifs sont classées par type de communication : réel ou éventuel.

- **Communication réelle** - Inclut tous les actifs sur lesquels des communications ont été détectées à l'aide de connexions.
  - **Test de contribution** - Une question de test de contribution est une question de test de base qui définit le type de communication réelle que vous essayez de tester. Pour plus d'informations, voir la section Tests d'actifs - Communication réelle (contribution).
  - **Test de restriction** - Une question de test de restriction restreint les résultats d'un test de contribution afin de filtrer davantage les violations caractéristiques dans une communication réelle. Pour plus d'informations, voir la section Tests d'actifs - Communication réelle (restriction).
- **Communication éventuelle** - Les questions sur les communications éventuelles vous permettent de vérifier si des communications caractéristiques sont possibles sur des actifs, qu'une communication ait été détectée ou non.
  - **Test de contribution** - Une question de test de contribution est une question de test de base qui définit le type de communication réelle que vous tentez de tester. Pour plus d'informations, voir la section Tests d'actifs - Communication réelle (contribution).

- **Test de restriction** - Une question de test de restriction restreint les résultats d'un test de contribution afin de filtrer davantage les violations caractéristiques dans une communication éventuelle. Pour plus d'informations, voir la section Tests d'actifs - Communication éventuelle (restriction).Les tests de communication réelle pour les actifs incluent les paramètres de questions de restriction suivants :

Tests d'actifs - Communication réelle (contribution)

Les tests de communication réelle pour les actifs incluent les paramètres de questions de contribution suivants :

Tableau A-1 Communication réelle - Tests de contribution

Intitulé du test	Description	Paramètres
have accepted communication **to any destination**	Détecte les actifs disposant de communications vers ou depuis un réseau configuré. Ce test vous permet de définir un point de départ ou d'arrivée pour votre question. Par exemple, pour identifier les actifs qui ont accepté une communication en provenance d'une zone démilitarisée (DMZ), configurez le test comme suit : have accepted communication from any source <networks> Vous pouvez utiliser ce test pour détecter les communications non conformes aux règles.	Configurez les paramètres suivants : • **accepted | rejected** - Indique si vous souhaitez que le test prenne en compte les communications acceptées ou rejetées. L'option par défaut est accepted. • **to any destination | from any source** - Indique si vous souhaitez que le test prenne en compte le réseau source ou celui de destination. L'option par défaut est to any destination.

Tableau A-1 Communication réelle - Tests de contribution (suite)

Intitulé du test	Description	Paramètres
have accepted communication **to destination networks**	Détecte les actifs disposant de communications vers ou depuis le réseau configuré. Ce test vous permet de définir un point de départ ou d'arrivée pour votre question. Par exemple, pour identifier les actifs qui communiquent avec une DMZ, configurez le test comme suit : have accepted communication from source <networks> Vous pouvez utiliser ce test pour détecter les communications non conformes aux règles.	Configurez les paramètres suivants : • **have | have not** - Indique la condition que vous souhaitez que le test applique. Les options sont have ou have not. L'option par défaut est have. Lorsque vous appliquez la condition have not à ce test, la condition not s'applique au paramètre networks. Par exemple, si vous le configurez avec la condition **have not accepted communication to destination networks**, le test détecte les actifs qui ont accepté des communications vers des réseaux autres que celui configuré. • **accepted | rejected** - Indique si vous souhaitez que le test prenne en compte les communications acceptées ou rejetées. L'option par défaut est accepted. • **to destination | from source** - Indique si vous souhaitez que le test prenne en compte le réseau source ou celui de destination. L'option par défaut est to destination. • **networks** - Indique la zone des réseaux à laquelle vous souhaitez appliquer le test.
have accepted communication **to destination IP addresses**	Détecte les actifs disposant de communications vers ou depuis l'adresse IP configurée. Ce test vous permet d'indiquer une adresse IP ou CIDR. Par exemple, si vous souhaitez identifier tous les actifs qui ont communiqué avec un serveur de conformité spécifique, configurez le test comme suit : have accepted communications to destination <compliance server IP address>	Configurez les paramètres suivants : • **have | have not** - Indique la condition que vous souhaitez que le test applique. Les options sont have ou have not. L'option par défaut est have. Lorsque vous appliquez la condition have not à ce test, la condition not s'applique au paramètre IP addresses. Par exemple, si vous le configurez avec la condition **have not accepted communication to destination IP addresses**, le test détecte les actifs qui ont accepté des communications vers des adresses IP autres que celles configurées. • **accepted | rejected** - Indique si vous souhaitez que le test prenne en compte les communications acceptées ou rejetées. L'option par défaut est accepted. • **to destination | from source** - Indique si vous souhaitez que le test prenne en compte les adresses IP source ou celles de destination. L'option par défaut est to destination. • **IP addresses** - Indique la liste d'adresses IP sur laquelle vous souhaitez appliquer le test.

Tableau A-1 Communication réelle - Tests de contribution (suite)

Intitulé du test	Description	Paramètres
have accepted communication **to destination asset building blocks**	Détecte les actifs disposant de communications vers ou depuis les éléments structurants d'actifs configurés. Ce test vous permet de réutiliser dans votre requête les éléments structurants définis dans QRadar Rules Wizard. Pour plus d'informations sur les règles, les actifs et les éléments structurants, voir le manuel *QRadar - Guide d'administration*.	Configurez les paramètres suivants : • **have | have not** - Indique la condition que vous souhaitez que le test applique. Les options sont have ou have not. L'option par défaut est have. Lorsque vous appliquez la condition have not à ce test, la condition not s'applique au paramètre asset building blocks. Par exemple, si vous le configurez avec la condition **have not accepted communication to destination asset building blocks**, le test détecte les actifs qui ont accepté des communications vers des éléments structurants d'actifs autres que ceux configurés. • **accepted | rejected** - Indique si vous souhaitez que le test prenne en compte les communications acceptées ou rejetées. L'option par défaut est accepted. • **to destination | from source** - Indique si vous souhaitez que le test prenne en compte les éléments structurants d'actifs source ou ceux de destination. L'option par défaut est to destination. • **asset building blocks** - Indique les éléments structurants d'actifs auxquels vous souhaitez appliquer le test.
have accepted communication **to destination remote network locations**	Détecte les actifs qui ont communiqué avec des réseaux définis comme distants. Par exemple, ce test peut identifier les hôtes qui ont communiqué avec des botnets ou des espaces adresse Internet suspects.	Configurez les paramètres suivants : • **have | have not** - Indique la condition que vous souhaitez que le test applique. Les options sont have ou have not. L'option par défaut est have. Lorsque vous appliquez la condition have not à ce test, la condition not s'applique au paramètre remote network locations. Par exemple, si vous le configurez avec la condition **have not accepted communication to destination remote network locations**, le test détecte les actifs qui ont accepté des communications vers des emplacements réseau distant autres que ceux configurés. • **accepted | rejected** - Indique si vous souhaitez que le test prenne en compte les communications acceptées ou rejetées. L'option par défaut est accepted. • **to destination | from source** - Indique si vous souhaitez que le test prenne en compte les emplacements réseau source ou ceux de destination. L'option par défaut est to destination. • **remote network locations** - Indique les réseaux distants auxquels vous souhaitez appliquer ce test.

Tableau A-1 Communication réelle - Tests de contribution (suite)

Intitulé du test	Description	Paramètres
have accepted communication **to destination geographic network locations**	Détecte les actifs qui ont communiqué avec des réseaux définis comme géographiques. Par exemple, ce test peut détecter les actifs qui ont tenté de communiquer avec des pays où vous n'avez aucune opération métier.	Configurez les paramètres suivants : • **have | have not** - Indique la condition que vous souhaitez que le test applique. Les options sont have ou have not. L'option par défaut est have. Lorsque vous appliquez la condition have not à ce test, la condition not s'applique au paramètre geographic network locations. Par exemple, si vous le configurez avec la condition **have not accepted communication to destination geographic network locations**, le test détecte les actifs qui ont accepté des communications vers des emplacements réseau géographiques autres que ceux configurés. • **accepted | rejected** - Indique si vous souhaitez que le test prenne en compte les communications acceptées ou rejetées. L'option par défaut est accepted. • **to destination | from source** - Indique si vous souhaitez que le test prenne en compte les emplacements réseau source ou ceux de destination. L'option par défaut est to destination. • **geographic network locations** - Indique les réseaux géographiques auxquels vous souhaitez appliquer le test.
have accepted communication **to** the Internet	Détecte les communications source ou de destination vers ou depuis Internet.	Configurez les paramètres suivants : • **have | have not** - Indique la condition que vous souhaitez que le test applique. Les options sont have ou have not. L'option par défaut est have. Lorsque vous appliquez la condition have not à ce test, la condition not s'applique à la portion Internet du test. Par exemple, si vous le configurez avec la condition **have not accepted communication to the Internet**, le test détecte les actifs qui ont accepté des communications depuis ou vers des zones autres qu'Internet. • **accepted | rejected** - Indique si vous souhaitez que le test prenne en compte les communications acceptées ou rejetées. L'option par défaut est accepted. • **to | from -** Indique si vous souhaitez que le test prenne en compte le trafic de communication vers ou depuis Internet. L'option par défaut est to.

Tableau A-1 Communication réelle - Tests de contribution (suite)

Intitulé du test	Description	Paramètres
are susceptible to one of the following **vulnerabilities**	Détecte les vulnérabilités spécifiques. Si vous souhaitez détecter les vulnérabilités d'un type en particulier, utilisez le test “are susceptible to vulnerabilities with one of the following classifications”.	Configurez les paramètres suivants : • **are | are not** - Indique la condition (are ou are not) que vous souhaitez que le test applique. L'option par défaut est are. • **vulnerabilities** - Indique les vulnérabilités auxquelles vous souhaitez appliquer le test. Vous pouvez rechercher les vulnérabilités à l'aide de leur ID OSVDB, de leur ID CVE, de leur ID Bugtraq ou de leur titre. Pour plus d'informations sur OSVDB, voir le site à l'adresse http://osvdb.org.
are susceptible to vulnerabilities with one of the following **classifications**	Une vulnérabilité peut être associée à au moins une classification de vulnérabilité. Ce test filtre tous les actifs qui comprennent des vulnérabilités correspondant aux classifications spécifiées.	Configure le paramètre **classifications** afin d'identifier les classifications de vulnérabilité que vous souhaitez que le test applique. Par exemple, une classification de vulnérabilité peut être Input Manipulation ou Denial of Service.
are susceptible to vulnerabilities with CVSS score **greater than 5**	Une valeur CVSS (Common Vulnerability Scoring System) est une norme de l'industrie permettant d'évaluer la gravité des vulnérabilités. La valeur CVSS est composée de trois groupes d'indicateurs : de base, temporels et environnementaux. Ces indicateurs permettent à CVSS de définir et de communiquer les caractéristiques fondamentales d'une vulnérabilité. Ce test filtre les actifs de votre réseau ayant des vulnérabilités dont l'indice CVSS correspond à celui spécifié.	Configurez les paramètres suivants : • **greater than | less than | equal to** - Indique si l'indice Common Vulnerability Scoring System (CVSS) doit être supérieur à, inférieur à ou égal à la valeur configurée, respectivement. La valeur par défaut est greater than. • **5** - Indiquez la valeur de risque CVSS vous souhaitez que le test considère. La valeur par défaut est 5.
are susceptible to vulnerabilities from the following **vendors**		Configure le paramètre **vendors** afin d'identifier les vulnérabilités qui ont pu avoir été introduites dans des actifs et provenant de fournisseurs spécifiques.

Remarque : *Le test de contribution des actifs sujets aux vulnérabilités provenant des fournisseurs suivants a été masqué dans Policy Monitor. Si vous utilisez actuellement ce test de contribution, il est toujours visible parmi les tests. Toutefois, il a été remplacé par un test de contribution qui recherche les vulnérabilités des actifs grâce à des saisies ou à des expressions régulières.*

Tableau A-1 Communication réelle - Tests de contribution (suite)

Intitulé du test	Description	Paramètres
are susceptible to vulnerabilities with the following **services**		Configure le paramètre **services** afin d'identifier les vulnérabilités qui ont pu avoir été introduites dans des actifs et provenant de services spécifiques.
Remarque : *Le test de contribution des actifs sujets aux vulnérabilités provenant des services suivants a été masqué dans Policy Monitor. Si vous utilisez actuellement ce test de contribution, il est toujours visible parmi les tests. Toutefois, il a été remplacé par un test de contribution qui recherche les vulnérabilités des actifs grâce à des saisies ou à des expressions régulières.*		
are susceptible to vulnerabilities disclosed **after specified date**	Détecte les actifs de votre réseau ayant une vulnérabilité divulguée après, avant ou à la date configurée.	Configurez les paramètres suivants : • **after | on | before** - Indique si vous souhaitez que le test considère que la date de divulgation des vulnérabilités soit après ou avant, ou encore corresponde à la date configurée, respectivement. L'option par défaut est after. • **specified date** - Indique la date à laquelle vous souhaitez que le test soit effectif.
are susceptible to vulnerabilities on one of the following **ports**	Détecte les actifs de votre réseau ayant une vulnérabilité associée aux ports configurés.	Configure le paramètre **ports** afin d'identifier les ports que vous souhaitez que le test prenne en compte.
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following **text entries**	Détecte les actifs de votre réseau ayant une vulnérabilité qui correspond à au moins une saisie concernant le nom de l'actif, le fournisseur, la version ou le service.	Configure le paramètre **text entries** afin d'identifier le nom d'actif, le fournisseur, la version ou le service que vous souhaitez que le test prenne en compte.
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following **regular expressions**	Détecte les actifs de votre réseau ayant une vulnérabilité qui correspond à au moins une expression régulière concernant le nom de l'actif, le fournisseur, la version ou le service.	Configure le paramètre **regular expressions** afin d'identifier le nom d'actif, le fournisseur, la version ou le service que vous souhaitez que le test prenne en compte.

Tests d'actifs - Communication réelle (restriction)

Les tests de communication réelle pour les actifs incluent les paramètres de questions de restriction suivants :

Tableau A-2 Communication réelle - Tests de restriction

Intitulé du test	Description	Paramètres
include only the following **protocols**	Filtre les actifs du test de contribution qui incluent ou excluent les protocoles spécifiés. Ce test ne peut être sélectionné que lorsqu'un test de contribution concernant un actif est ajouté à la question.	Configurez les paramètres suivants : • **include only | exclude** - Indique la condition (include only ou exclude) que vous souhaitez que le test applique. Lorsque vous appliquez la condition exclude à ce test, la condition not s'applique au paramètre protocols. Par exemple, si vous le configurez avec la condition **exclude the following protocols**, le test exclut tous les résultats d'actifs renvoyés qui excluent les protocoles spécifiés autres que ceux configurés. • **protocols** - Indique la liste de protocoles à laquelle vous souhaitez appliquer le test.
include only the following **inbound ports**	Filtre les actifs du test de contribution qui incluent uniquement ou excluent les ports spécifiés. Ce test ne peut être sélectionné que lorsqu'un test de contribution concernant un actif est ajouté à la question.	Configurez les paramètres suivants : • **include only | exclude** - Indique la condition (include only ou exclude) que vous souhaitez que le test applique. Lorsque vous appliquez la condition exclude à ce test, la condition not s'applique au paramètre ports. Par exemple, si vous le configurez avec la condition **exclude the following inbound ports**, le test exclut tous les résultats d'actifs renvoyés qui excluent les ports spécifiés venant vers l'actif autres que le port configuré. • **inbound | outbound** - Indique si vous souhaitez que le test prenne en compte les communications entrantes ou sortantes. L'option par défaut est inbound. • **ports** - Indique les ports auxquels vous souhaitez appliquer le test.

Remarque : *Inbound fait référence à un test qui filtre les connexions pour lesquelles l'actif en question est une destination. Outbound, quant à elle, fait référence à un test qui filtre les connexions pour lesquelles l'actif en question est une source.*

Remarque : *Lors de leur utilisation, il est recommandé d'appliquer aux tests de restriction la même direction que celle des tests de contribution. Il est possible d'utiliser des tests de restriction mélangeant les directions entrantes et sortantes lorsque vous essayez de localiser des actifs entre deux points, tels que deux réseaux ou deux adresses IP.*

Tableau A-2 Communication réelle - Tests de restriction (suite)

Intitulé du test	Description	Paramètres
include only the following **inbound applications**	Filtre les actifs de la question du test de contribution qui incluent uniquement ou excluent des applications entrantes ou sortantes. Ce test ne filtre que les connexions qui incluent des données de flux.	Configurez les paramètres suivants : • **include only | exclude** - Indique la condition (include only ou exclude) que vous souhaitez que le test applique. Lorsque vous appliquez la condition exclude à ce test, la condition not s'applique au paramètre application. Par exemple, si vous le configurez avec la condition **exclude the following inbound applications**, le test exclut tous les résultats d'actifs renvoyés qui excluent les applications entrantes spécifiées vers l'actif. • **inbound | outbound** - Indique si vous souhaitez que le test prenne en compte les communications entrantes ou sortantes. L'option par défaut est inbound. • **applications** - Indique les applications auxquelles vous souhaitez appliquer le test. Ces informations ne sont disponibles que lorsque les flux de niveau d'application sont fournis.

Remarque : *Inbound fait référence à un test qui filtre les connexions pour lesquelles l'actif en question est une destination. Outbound, quant à elle, fait référence à un test qui filtre les connexions pour lesquelles l'actif en question est une source.*

Remarque : *Lors de leur utilisation, il est recommandé d'appliquer aux tests de restriction la même direction que celle des tests de contribution. Il est possible d'utiliser des tests de restriction mélangeant les directions entrantes et sortantes lorsque vous essayez de localiser des actifs entre deux points, tels que deux réseaux ou deux adresses IP.*

Tableau A-2 Communication réelle - Tests de restriction (suite)

Intitulé du test	Description	Paramètres
include only if the **source inbound** and **destination outbound** bytes have a percentage difference **less than 10**	Filtre les actifs de la question du test de contribution en fonction des communications disposant d'un rapport spécifique de communications entrantes sur sortantes (ou sortantes sur entrantes) en octets. Ce test est pratique pour détecter les hôtes qui peuvent présenter un comportement de type proxy (communications entrantes = communications sortantes).	Configurez les paramètres suivants : • **source | destination** - Indique si vous souhaitez que le test prenne en compte les communications source ou de destination. L'option par défaut est source. • **inbound | outbound** - Indique si vous souhaitez que le test prenne en compte les communications entrantes ou sortantes. L'option par défaut est inbound. • **destination | source** - Indique si vous souhaitez que le test prenne en compte les communications source ou de destination. L'option par défaut est destination. • **outbound | inbound** - Indique si vous souhaitez que le test prenne en compte les communications entrantes ou sortantes. L'option par défaut est outbound. • **less than | greater than | equal to** - Indique si vous souhaitez que le test prenne en compte les valeurs supérieures à, inférieures à ou égales à la valeur configurée. L'option par défaut est less than. • **10** - Indique le nombre que vous souhaitez que le test prenne en compte.
include only if the inbound and outbound **flow count** has a percentage difference **less than 10**	Filtre les actifs de la question du test de contribution en fonction des communications disposant d'un rapport spécifique de flux de communications entrantes sur sortantes (ou sortantes sur entrantes). Ce test ne filtre que les connexions qui incluent des données de flux lorsque le comptage des flux est sélectionné.	Configurez les paramètres suivants : • **flow count | host count -** Indique si vous souhaitez que le test prenne en compte le comptage des flux ou celui des hôtes. L'option par défaut est host count. • **less than | greater than | equal to** - Indique si vous souhaitez que le test prenne en compte les valeurs supérieures à, inférieures à ou égales à la valeur configurée. L'option par défaut est less than. • **10** - Indique le nombre que vous souhaitez que le test prenne en compte.

Remarque : *Ce test de restriction requiert deux tests de contribution qui indiquent une source et une destination. Le test suivant présente un ensemble de questions essayant de déterminer quels actifs entre deux points disposent d'un pourcentage de différence entre communications entrantes et sortantes supérieur à 40 %. Par exemple,*

- **Test de contribution** - have accepted communication to the internet.
- **Test de contribution** - and have accepted communication from the internet.
- **Test de restriction** - and include only if the inbound and outbound flow count has a percentage difference greater than 40.

Tableau A-2 Communication réelle - Tests de restriction (suite)

Intitulé du test	Description	Paramètres
include only if the time is between **start time** and **end time** inclusive	Filtre les communications au sein de votre réseau qui ont eu lieu dans un intervalle spécifique. Cela vous permet de détecter les communications non conformes aux règles. Par exemple, si vos règles d'entreprise autorisent les communications FTP entre 1h00 et 3h00 du matin, ce test peut détecter les tentatives de communication avec le FTP en dehors de cet intervalle.	Configurez les paramètres suivants : • **include only | exclude** - Indique la condition (include only ou exclude) que vous souhaitez que le test applique. Lorsque vous appliquez la condition exclude à ce test, la condition not s'applique à la fenêtre de temps spécifiée. Par exemple, si vous le configurez avec la condition **exclude if the time is between start time and end time inclusive**, le test exclut tous les résultats d'actifs renvoyés qui sont compris entre les heures de début et de fin spécifiées. • **start time** - Indique l'heure de début que vous souhaitez que le test prenne en compte. • **end time** - Indique l'heure de fin que vous souhaitez que le test prenne en compte.
include only if the day of week is between **start day** and **end day** inclusive	Filtre les actifs de la question du test de contribution en fonction des communications réseau qui ont eu lieu dans l'intervalle caractéristique. Cela vous permet de détecter les communications non conformes aux règles.	Configurez les paramètres suivants : • **include only | exclude** - Indique la condition (include only ou exclude) que vous souhaitez que le test applique. Lorsque vous appliquez la condition exclude à ce test, la condition not s'applique à la fenêtre de temps spécifiée. Par exemple, si vous le configurez avec la condition **exclude if the day of the week is between start day and end day inclusive**, le test exclut tous les résultats d'actifs renvoyés qui sont compris entre les heures de début et de fin spécifiées. • **start day** - Indique le jour de la semaine que vous souhaitez que le test prenne en compte. • **end day** - Indique le jour de la semaine que vous souhaitez que le test prenne en compte.
include only if susceptible to vulnerabilities that are exploitable.	Filtre les actifs provenant d'une question de test de contribution recherchant des vulnérabilités caractéristiques et restreint les résultats aux actifs exploitables.	Ce test de restriction ne contient pas de paramètre configurable. Cependant, il est utilisé conjointement avec le test de contribution **are susceptible to one of the following vulnerabilities**. La règle de contribution contenant le paramètre vulnerabilities est obligatoire.

Tableau A-2 Communication réelle - Tests de restriction (suite)

Intitulé du test	Description	Paramètres
include only the following **networks**	Filtre les actifs provenant d'une question de test de contribution qui inclut ou exclut les réseaux configurés.	Configurez les paramètres suivants : • **include only | exclude** - Indique la condition (include only ou exclude) que vous souhaitez que le test applique. Lorsque vous appliquez la condition exclude à ce test, la condition not s'applique au réseau spécifié. Par exemple, si vous le configurez avec la condition **exclude the following network**, le test exclut tous les résultats d'actifs renvoyés qui n'incluent pas le réseau spécifié. • **networks** - Indique la zone de réseaux à laquelle vous souhaitez appliquer le test.
include only the following **asset building blocks**	Filtre les actifs provenant d'une question de test de contribution qui sont ou ne sont pas associés aux éléments structurants d'actifs configurés.	Configurez les paramètres suivants : • **include only | exclude** - Indique la condition (include only ou exclude) que vous souhaitez que le test applique. Lorsque vous appliquez la condition exclude à ce test, la condition not s'applique au réseau spécifié. Par exemple, si vous le configurez avec la condition **exclude the following asset building blocks**, le test exclut tous les résultats d'actifs renvoyés qui ne contiennent pas les éléments structurants spécifiés. • **asset building blocks** - Indique les actifs auxquels vous souhaitez appliquer le test.
include only the following **IP addresses**	Filtre les actifs qui sont ou ne sont pas associés aux adresses IP configurées.	Configurez les paramètres suivants : • **include only | exclude** - Indique la condition (include only ou exclude) que vous souhaitez que le test applique. Lorsque vous appliquez la condition exclude à ce test, la condition not s'applique au réseau spécifié. Par exemple, si vous le configurez avec la condition **exclude the following IP addresses**, le test exclut tous les résultats d'actifs renvoyés qui n'incluent pas les adresses IP spécifiées. • **IP addresses** - Indique l'adresse ou les adresses IP auxquelles vous souhaitez appliquer le test.

Tests d'actifs - Communication réelle (contribution)

Les tests de communication éventuelle pour les actifs incluent les paramètres de questions de contribution suivants :

Tableau A-3 Communication éventuelle - Tests de contribution

Intitulé du test	Description	Paramètres
have accepted communication **to any destination**	Détecte les actifs disposant de communications éventuelles vers ou depuis n'importe quelle source ou destination spécifiée. Par exemple, pour déterminer si un serveur critique peut éventuellement recevoir des communications depuis n'importe quelle source, configurez le test comme suit : have accepted communication from any source. Vous pouvez ensuite appliquer un test de restriction à renvoyer si le serveur critique en question a reçu des communications sur le port 21. Cela vous permet de détecter les communications non conformes aux règles pour le serveur critique en question.	Configurez les paramètres suivants : • **to any destination | from any source** - Indique si vous souhaitez que le test prenne en compte le réseau source ou celui de destination. L'option par défaut est to any destination. • **networks** - Indique la zone des réseaux à laquelle vous souhaitez appliquer le test.
have accepted communication **to destination networks**	Détecte les actifs disposant de communications éventuelles vers ou depuis le réseau configuré. Ce test vous permet de définir un point de départ ou d'arrivée pour votre question. Par exemple, pour identifier les actifs qui disposent d'une possibilité de communication avec la DMZ, configurez le test comme suit : have accepted communication from source <networks> Vous pouvez utiliser ce test pour détecter les communications non conformes aux règles.	Configurez les paramètres suivants : • **to destination | from source** - Indique si vous souhaitez que le test prenne en compte le réseau source ou celui de destination. L'option par défaut est to destination. • **networks** - Indique la zone des réseaux à laquelle vous souhaitez appliquer le test.

Tableau A-3 Communication éventuelle - Tests de contribution (suite)

Intitulé du test	Description	Paramètres
have accepted communication **to destination IP addresses**	Détecte les actifs disposant de communications éventuelles vers ou depuis l'adresse IP configurée. Ce test vous permet d'indiquer une seule adresse IP et de vous en servir comme point central pour des communications éventuelles. Par exemple, si vous souhaitez identifier tous les actifs qui peuvent communiquer avec un serveur de conformité spécifique, configurez le test comme suit : have accepted communications to destination <compliance server IP address>	Configurez les paramètres suivants : • **to destination | from source** - Indique si vous souhaitez que le test prenne en compte les adresses IP source ou celles de destination. L'option par défaut est to destination. • **IP addresses** - Indique la liste d'adresses IP sur laquelle vous souhaitez appliquer le test.
have accepted communication **to destination asset building blocks**	Détecte les actifs disposant de communications éventuelles vers ou depuis l'actif configuré à l'aide d'éléments structurants. Ce test vous permet de réutiliser dans votre requête les éléments structurants définis dans QRadar Rules Wizard.Par exemple, si vous souhaitez identifier tous les actifs qui peuvent communiquer avec un élément Protected Assets, configurez le test comme suit : have accepted communications to destination <BB:HostDefinition:Protected Assets> Pour plus d'informations sur les règles et les éléments structurants, voir le manuel *QRadar - Guide d'administration*.	Configurez les paramètres suivants : • **to destination | from source** - Indique si vous souhaitez que le test prenne en compte les éléments structurants d'actifs source ou ceux de destination. L'option par défaut est to destination. • **asset building blocks** - Indique les actifs auxquels vous souhaitez appliquer le test.

Tableau A-3 Communication éventuelle - Tests de contribution (suite)

Intitulé du test	Description	Paramètres
have accepted communication **to** the Internet	Détecte si les communications source ou de destination sont possible vers ou depuis Internet.	Configure le paramètre **to | from**, lequel vous permet d'indiquer si vous souhaitez que le test prenne en compte le trafic de communication à direction ou en provenance d'Internet. L'option par défaut est to.
are susceptible to one of the following **vulnerabilities**	Détecte les vulnérabilités spécifiques éventuelles. Si vous souhaitez détecter les vulnérabilités d'un type en particulier, utilisez le test “are susceptible to vulnerabilities with one of the following classifications”.	Configure le paramètre **vulnerabilities**, lequel vous permet d'indiquer les vulnérabilités auxquelles vous souhaitez appliquer le test. Vous pouvez rechercher les vulnérabilités à l'aide de leur ID OSVDB, de leur ID CVE, de leur ID Bugtraq ou de leur titre. Pour plus d'informations sur OSVDB, voir le site à l'adresse http://osvdb.org.
are susceptible to vulnerabilities with one of the following **classifications**	Une vulnérabilité peut être associée à au moins une classification de vulnérabilité. Ce test filtre tous les actifs ayant des vulnérabilités éventuelles à l'aide d'un indice Common Vulnerability Scoring System (CVSS) spécifié.	Configure le paramètre **classifications** afin d'identifier les classifications de vulnérabilité que vous souhaitez que le test applique.
are susceptible to vulnerabilities with CVSS score **greater than 5**	Une valeur CVSS (Common Vulnerability Scoring System) est une norme de l'industrie permettant d'évaluer la gravité des vulnérabilités éventuelles. La valeur CVSS est composée de trois groupes d'indicateurs : de base, temporels et environnementaux. Ces indicateurs permettent à CVSS de définir et de communiquer les caractéristiques fondamentales d'une vulnérabilité. Ce test filtre les actifs de votre réseau qui comprennent la valeur CVSS configurée.	Configurez les paramètres suivants : • **greater than | less than | equal to** - Indique si l'indice Common Vulnerability Scoring System (CVSS) doit être supérieur à, inférieur à ou égal à la valeur configurée, respectivement. La valeur par défaut est greater than. • **5**- Indiquez la valeur de risque CVSS vous souhaitez que le test considère. La valeur par défaut est 5.
are susceptible to vulnerabilities from the following **vendors**		Configure le paramètre **vendors** afin d'identifier les vulnérabilités éventuelles qui ont pu avoir été introduites dans des actifs et provenant de fournisseurs spécifiques.

Tableau A-3 Communication éventuelle - Tests de contribution (suite)

Intitulé du test	Description	Paramètres
Remarque : *Le test de contribution des actifs sujets aux vulnérabilités provenant des fournisseurs suivants a été masqué dans Policy Monitor. Si vous utilisez actuellement ce test de contribution, il est toujours visible parmi les tests. Toutefois, il a été remplacé par un test de contribution qui recherche les vulnérabilités des actifs grâce à des saisies ou à des expressions régulières.*		
are susceptible to vulnerabilities with the following **services**		Configure le paramètre **services** afin d'identifier les vulnérabilités éventuelles qui ont pu avoir été introduites dans des actifs et provenant de services spécifiques.
Remarque : *Le test de contribution des actifs sujets aux vulnérabilités provenant des services suivants a été masqué dans Policy Monitor. Si vous utilisez actuellement ce test de contribution, il est toujours visible parmi les tests. Toutefois, il a été remplacé par un test de contribution qui recherche les vulnérabilités des actifs grâce à des saisies ou à des expressions régulières.*		
are susceptible to vulnerabilities disclosed **after specified date**	Filtre les actifs de votre réseau ayant une éventuelle vulnérabilité divulguée après, avant ou à la date configurée.	Configurez les paramètres suivants : • **after | on | before** - Indique si vous souhaitez que le test considère que la date de divulgation des vulnérabilités soit après ou avant, ou encore corresponde à la date configurée, respectivement. L'option par défaut est after. • **specified date** - Indique la date à laquelle vous souhaitez que le test soit effectif.
are susceptible to vulnerabilities on one of the following **ports**	Filtre les actifs de votre réseau ayant une éventuelle vulnérabilité associée aux ports configurés.	Configure le paramètre **ports** pour identifier les actifs ayant d'éventuelles vulnérabilités en fonction du numéro de port spécifié.
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following **text entries**	Détecte les actifs de votre réseau ayant une vulnérabilité qui correspond à au moins une saisie concernant le nom de l'actif, le fournisseur, la version ou le service.	Configure le paramètre **text entries** afin d'identifier le nom d'actif, le fournisseur, la version ou le service que vous souhaitez que le test prenne en compte.
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following **regular expressions**	Détecte les actifs de votre réseau ayant une vulnérabilité qui correspond à au moins une expression régulière concernant le nom de l'actif, le fournisseur, la version ou le service.	Configure le paramètre **regular expressions** afin d'identifier le nom d'actif, le fournisseur, la version ou le service que vous souhaitez que le test prenne en compte.

Tests d'actifs - Communication éventuelle (restriction)

Les tests de communication éventuelle pour les actifs incluent les paramètres de questions de restriction suivants :

Tableau A-4 Communication éventuelle - Tests de restriction

Intitulé du test	Description	Paramètres
include only the following **protocols**	Filtre les actifs qui ont éventuellement communiqué ou non avec les protocoles configurés, conjointement avec les autres tests ajoutés à la question.	Configure le paramètre **protocols**, lequel vous permet d'indiquer la liste des protocoles à laquelle vous souhaitez appliquer le test.
include only the following inbound **ports**	Filtre les actifs qui ont éventuellement communiqué ou non avec les ports configurés, conjointement avec les autres tests ajoutés à la question.	Configure le paramètre **ports**, lequel vous permet d'indiquer les ports auxquels vous souhaitez appliquer le test.
include only ports other than the following **inbound ports**	Filtre les actifs provenant d'une question de test de contribution qui ont éventuellement communiqué ou non avec des ports autres que ceux configurés, conjointement avec les autres tests ajoutés à la question.	Configurez les paramètres suivants : • **inbound | outbound** - Indique si vous souhaitez que le test prenne en compte les communications entrantes ou sortantes. L'option par défaut est inbound. • **ports** - Indique les ports auxquels vous souhaitez appliquer le test.

Remarque : *Inbound fait référence à un test qui filtre les connexions pour lesquelles l'actif en question est une destination. Outbound, quant à elle, fait référence à un test qui filtre les connexions pour lesquelles l'actif en question est une source.*

Remarque : *Lors de leur utilisation, il est recommandé d'appliquer aux tests de restriction la même direction que celle des tests de contribution. Il est possible d'utiliser des tests de restriction mélangeant les directions entrantes et sortantes lorsque vous essayez de localiser des actifs entre deux points, tels que deux réseaux ou deux adresses IP.*

include only if susceptible to vulnerabilities that are exploitable.	Filtre les actifs provenant d'une question de test de contribution recherchant d'éventuelles vulnérabilités caractéristiques et restreint les résultats aux actifs exploitables.	Ce test de restriction ne contient pas de paramètre configurable. Cependant, il est utilisé conjointement avec le test de contribution **are susceptible to one of the following vulnerabilities**. La règle de contribution contenant le paramètre vulnerabilities est obligatoire.
include only the following **networks**	Filtre les actifs provenant d'une question de test de contribution qui inclut uniquement ou exclut les réseaux configurés.	Configurez les paramètres suivants : • **include only | exclude** - Indique la condition (include only ou exclude) que vous souhaitez que le test applique. • **networks** - Indique la zone de réseaux à laquelle vous souhaitez appliquer le test.

Tableau A-4 Communication éventuelle - Tests de restriction (suite)

Intitulé du test	Description	Paramètres
include only the following **asset building blocks**	Filtre les actifs provenant d'une question de test de contribution qui inclut uniquement ou exclut les éléments structurants d'actifs configurés.	Configurez les paramètres suivants : • **include only | exclude** - Indique la condition (include only ou exclude) que vous souhaitez que le test applique. • **asset building blocks** - Indique les actifs auxquels vous souhaitez appliquer le test.
include only the following **IP addresses**	Filtre les actifs provenant d'une question de test de contribution qui inclut uniquement ou exclut les adresses IP configurées.	Configurez les paramètres suivants : • **include only | exclude** - Indique la condition (include only ou exclude) que vous souhaitez que le test applique. • **IP addresses** - Indique l'adresse ou les adresses IP auxquelles vous souhaitez appliquer le test.

Tests périphériques ou règles

Les tests périphériques ou règles incluent :

Tableau A-5 Tests périphérique/règles

Intitulé du test	Description	Paramètres
allow connections **to** the following **networks**	Filtre les règles et les connexions de périphérique vers ou depuis les réseaux configurés. Par exemple, si vous configurez le test d'autorisation des communications vers un réseau, le test filtre toutes les règles et connexions qui autorisent des connexions au réseau configuré.	Configurez les paramètres suivants : • **allow | deny** - Indique la condition (allow ou do not allow) que vous souhaitez que le test applique. L'option par défaut est allow. • **to | from** - Indique si vous souhaitez que le test prenne en compte le trafic de communication vers ou depuis les réseaux spécifiés. L'option par défaut est to. • **networks** - Indique la zone de réseaux à laquelle vous souhaitez appliquer le test.
allow connections **to** the following **IP addresses**	Filtre les règles et les connexions des périphériques vers ou depuis les adresses IP configurées. Par exemple, si vous configurez le test d'autorisation des communications vers une adresse IP, ce dernier filtre toutes les règles et connexions qui autorisent des connexions vers l'adresse IP configurée.	Configurez les paramètres suivants : • **allow | deny** - Indique la condition (allow ou do not allow) que vous souhaitez que le test applique. L'option par défaut est allow. • **to | from** - Indique si vous souhaitez que le test prenne en compte le trafic de communication vers ou depuis les adresses IP spécifiées. L'option par défaut est to. • **IP addresses** - Indique l'adresse ou les adresses IP auxquelles vous souhaitez appliquer le test.

Tableau A-5 Tests périphérique/règles (suite)

Intitulé du test	Description	Paramètres
allow connections **to** the following **asset building blocks**	Filtre les règles et les connexions des périphériques vers ou depuis les éléments structurants d'actifs configurés.	Configurez les paramètres suivants : • **allow | deny** - Indique la condition (allow ou do not allow) que vous souhaitez que le test applique. L'option par défaut est allow. • **to | from** - Indique si vous souhaitez que le test prenne en compte le trafic de communication vers ou depuis les éléments structurants d'actifs configurés. L'option par défaut est to. • **asset building blocks** - Indique les actifs auxquels vous souhaitez appliquer le test.
allow connections using the following **destination ports and protocols**	Filtre les règles et les connexions des périphériques vers ou depuis les ports et les protocoles configurés.	Configurez les paramètres suivants : • **allow | deny** - Indique la condition (allow ou do not allow) que vous souhaitez que le test applique. L'option par défaut est allow. • **destination | source** - Indique si vous souhaitez que le test prenne en compte le port source ou de destination. L'option par défaut est destination. • **ports** - Indique les ports de destination auxquels vous souhaitez appliquer le test. • **protocols** - Indique la liste de protocoles à laquelle vous souhaitez appliquer le test.
allow connections using the following **protocols**	Filtre les règles et les connexions des périphériques vers ou depuis les protocoles configurés.	Configurez les paramètres suivants : • **allow | deny** - Indique la condition (allow ou do not allow) que vous souhaitez que le test applique. La valeur configurée par défaut est allow. • **protocols** - Indique la liste de protocoles à laquelle vous souhaitez appliquer le test.
allow connections **to** the Internet	Filtre les règles et les connexions des périphériques vers ou depuis Internet.	**Configurez les paramètres suivants :** • **allow | deny** - Indique la condition (allow ou do not allow) que vous souhaitez que le test applique. L'option par défaut est allow. • **to | from** - Indique si vous souhaitez que le test prenne en compte le trafic de communication vers ou depuis Internet. L'option par défaut est to.

Tableau A-5 Tests périphérique/règles (suite)

Intitulé du test	Description	Paramètres
are one of the following **devices**	Filtre tous les périphériques réseau sur les périphériques configurés. Ce test peut filtrer en fonction des périphériques qui sont ou ne sont pas dans la liste configurée.	Configurez les paramètres suivants : • **are | are not** - Indique la condition (are ou are not) que vous souhaitez que le test applique. L'option par défaut est are. • **devices** - Indique les périphériques que vous souhaitez que le test prenne en compte.

B AFFICHAGE DES JOURNAUX D'AUDIT

Les changements apportés par les utilisateurs IBM Security QRadar Risk Manager sont enregistrés sous l'onglet **Log Activity** d'IBM Security QRadar SIEM. Tous les journaux apparaissent dans la catégorie Risk Manager Audit. Pour plus d'informations sur l'utilisation de l'onglet **Log Activity** dans QRadar SIEM, voir le manuel *IBM Security QRadar SIEM - Guide d'utilisation.*

Actions consignées

QRadar Risk Manager consigne les catégories suivantes d'actions :

Tableau B-1 Actions consignées

Categorie	Action
Policy Monitor	Création d'une question.
	Edition d'une question.
	Suppression d'une question.
	Soumission manuelle d'une question.
	Soumission automatiqu d'une question.
	Validation des résultats.
	Révocation de la validation des résultats.
Modèle de topologie	Création d'un modèle de topologie.
	Edition d'un modèle de topologie.
	Suppression d'un modèle de topologie.
Topologie	Enregistrement de la disposition.
	Création d'une recherche sauvegardée de Topologie.
	Edition d'une recherche sauvegardée de topologie.
	Suppression d'une recherche sauvegardée de topologie.
	Mise en place d'un système de prévention contre les intrusions.
Moniteur de configuration	Création d'un mappage de source de journal
	Edition d'un mappage de source de journal
	Suppression d'un mappage de source de journal

Tableau B-1 Actions consignées (suite)

Categorie	Action
Simulations	Création d'une simulation.
	Edition d'une simulation.
	Suppression d'une simulation.
	Exécution manuelle d'une simulation.
	Exécution automatique d'une simulation.
	Validation des résultats de la simulation.
	Révocation des résultats de la simulation.

Tableau B-1 Actions consignées (suite)

Categorie	Action
Gestion de la source de configuration	Authentifiez-vous pour la première fois auprès d'une session avec succès.
	Ajout d'un périphérique.
	Suppression d'un périphérique.
	Edition de l'adresse IP ou de l'adaptateur pour un périphérique.
	Enregistrement d'une configuration de données d'identification.
	Suppression d'une configuration de données d'identification.
	Enregistrement d'une configuration de protocole.
	Suppression d'une configuration de protocole.
	Création d'une planification pour un travail de sauvegarde.
	Suppression d'une planification pour un travail de sauvegarde.
	Edition d'un travail de sauvegarde.
	Ajout d'un travail de sauvegarde.
	Suppression d'un travail de sauvegarde.
	Exécution d'un travail de sauvegarde planifié.
	Exécution d'un travail planifié, qu'il ait abouti ou échoué.
	Une fois le traitement d'un travail de sauvegarde terminé et la configuration conservée, aucun changement n'est constaté.
	Une fois le traitement d'un travail de sauvegarde terminé et la configuration conservée, des changements ont été constatés.
	Une fois le traitement d'un travail de sauvegarde terminé et la configuration conservée, des changements non définitifs ont été constatés.
	Le traitement d'un travail de sauvegarde est terminé et la configuration auparavant conservée a disparu du périphérique.
	Début d'une tentative de mise en fonctionnement de l'adaptateur comprenant des protocoles et des données d'identification.
	Une tentative de mise en fonctionnement de l'adaptateur comprenant des protocoles et des données d'identification a abouti.

Affichage de l'activité des utilisateurs QRadar Risk Manager dans QRadar Risk Manager

Pour afficher l'activité des utilisateurs QRadar Risk Manager dans QRadar SIEM, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Log Activity**.

La page Log Activity s'affiche. Si vous avez déjà sauvegardé une recherche en tant que recherche par défaut, les résultats de cette recherche sauvegardée s'affichent.

Etape 2 Cliquez sur **Search** > **New Search** pour créer une recherche.

Etape 3 Dans la sous-fenêtre **Time Range**, sélectionnez une option pour l'intervalle à capturer pour cette recherche.

Etape 4 Dans la sous-fenêtre **Search Parameters**, définissez vos critères de recherche :

a Dans la zone de liste déroulante, sélectionnez **Category**.

b Dans la zone de liste déroulante **High Level Category**, sélectionnez **Risk Manager Audit**.

c Facultatif. Dans la zone de liste déroulante **Low Level Category**, sélectionnez une catégorie pour affiner votre recherche.

Etape 5 Cliquez sur **Add Filter**.

L'option Current Filters permet de mettre à jour votre filtre de recherche.

Etape 6 Cliquez sur **Filter** pour rechercher les événements QRadar Risk Manager.

Affichage du fichier journal

Tous les journaux d'audit sont stockés au format texte brut et sont archivés et compressés lorsque le fichier suivi responsable atteint la taille de 200 Mo. Le fichier journal en cours est appelé **`audit.log`**. Si le fichier suivi responsable atteint à nouveau la taille de 200 Mo, il est compressé et l'ancien journal d'audit est renommé **`audit.1.gz, audit.2.gz`**, etc. Le numéro de fichier s'incrémente chaque fois qu'un fichier journal est archivé. QRadar Risk Manager peut stocker jusqu'à 50 fichiers journaux archivés.

Pour afficher un journal d'audit dans QRadar Risk Manager, procédez comme suit :

Etape 1 A l'aide de SSH, connectez-vous à votre console QRadar SIEM en tant que superutilisateur.

Nom d'utilisateur : **`root`**

Mot de passe : **`<Password>`**

Etape 2 Grâce à SSH de la console QRadar SIEM, connectez-vous au dispositif QRadar Risk Manager en tant que superutilisateur.

Nom d'utilisateur : **`root`**

Mot de passe : **<Password>**

Etape 3 Accédez au répertoire suivant :

/var/log/audit

Etape 4 Ouvrez votre fichier suivi responsable.

Chaque entrée du fichier journal s'affiche au format suivant :

REMARQUE

La taille maximale d'un message d'audit (si l'on exclut la date, l'heure et le nom d'hôte) est de 1 024 caractères.

<date_time> <host name> <user>@<IP address> (thread ID) [<category>] [<sub-category>] [<action>] <payload>

Où :

<date_time> correspond à la date et heure de l'activité au format : Mois Date HH:MM:SS.

<host name> correspond au nom d'hôte de la console dans laquelle cette activité a été consignée.

<user> correspond au nom de l'utilisateur qui a exécuté l'action.

<IP address> correspond à l'adresse IP de l'utilisateur qui a exécuté l'action.

(thread ID) correspond à l'identificateur de l'unité d'exécution Java™ qui a consigné cette activité.

<category> correspond à la catégorie de haut niveau de cette activité.

<sub-category> correspond à la catégorie de bas niveau de cette activité.

<action> correspond à l'activité qui s'est déroulée.

<payload> correspond à la totalité de l'enregistrement changé le cas échéant.

C AVIS ET MARQUES

Contenu de la présente annexe :

La présente section contient les mentions importantes, les marques et les informations de conformité.

Mentions

Les présentes informations ont été élaborées pour des produits et des services proposés aux Etats-Unis.

IBM peut ne pas proposer les produits, services et fonctions abordés dans le présent document dans d'autres pays. Renseignez-vous auprès de votre interlocuteur IBM local habituel sur les produits et les services actuellement disponibles dans votre région. Toute référence à un produit, programme ou service IBM n'affirme ou n'implique aucunement que seul ledit produit, programme ou service IBM puisse être utilisé. Tout produit, programme ou service présentant un fonctionnement similaire et n'enfreignant aucun droit de propriété intellectuelle d'IBM peut être utilisé en lieu et place. Cependant, l'utilisateur est tenu de vérifier et d'évaluer le fonctionnement du produit, programme ou service non IBM.

IBM peut disposer de brevets ou de demandes de brevets en instance protégeant le domaine abordé dans le présent document. La remise du présent document ne vous accorde aucun droit sur ces brevets. Vous pouvez envoyer vos demandes au sujet des licences par écrit à :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 Etats-Unis

Pour des demandes au sujet des licences concernant les informations sur le jeu de caractères codé sur deux octets (DBCS), contactez le service de la Propriété intellectuelle d'IBM de votre pays ou envoyez vos demandes par écrit à :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.

19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japon

Le paragraphe suivant ne s'applique pas au Royaume-Uni ni aux pays où ces dispositions sont incompatibles avec la loi en vigueur : INTERNATIONAL BUSINESS MACHINES CORPORATION FOURNIT LA PRESENTE PUBLICATION "DANS L'ETAT" SANS GARANTIE D'AUCUNE SORTE, EXPLICITE OU IMPLICITE, INCLUANT SANS S'Y LIMITER LES GARANTIES IMPLICITES DE NON-CONTREFACON, DE VALEUR MARCHANDE OU D'ADAPTATION A UN USAGE PARTICULIER. Certains pays n'autorisent pas les clauses de non-responsabilité des garanties explicites ou implicites dans certaines transactions. En conséquence, le présent énoncé peut ne pas s'appliquer à vous.

Les présentes informations peuvent contenir des imprécisions techniques ou des erreurs typographiques. Des changements sont régulièrement apportés aux informations contenues. Ils sont incorporés dans les nouvelles éditions de cette publication. IBM peut apporter des améliorations et/ou des changements au(x) produit(s) et/ou au(x) programme(s) décrits dans la présente publication à tout moment et sans préavis.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, Etats-Unis

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans le présent document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions du Contrat sur les produits et services IBM, des Conditions Internationales d'Utilisation de Logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans le présent document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats réels peuvent donc varier. Il incombe aux

utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs desdits produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Tous les tarifs indiqués sont des prix de vente actuels conseillés par IBM et sont susceptibles d'être modifiés sans préavis. Les prix appliqués par les distributeurs peuvent varier.

Les présentes informations peuvent contenir des exemples de données et de rapports utilisés dans les activités quotidiennes de l'entreprise. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

Si vous visualisez les présentes informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp., enregistrés dans de nombreux pays à travers le monde. Il se peut que d'autres produits et services soient des marques d'IBM ou d'autres sociétés. Une liste actualisée des marques d'IBM est disponible sur le site Web dans la rubrique “Droits d'auteur et marques de commerce (US)” à l'adresse *www.ibm.com/legal/copytrade.shtml*.

Les noms suivants sont des marques ou des marques déposées d'autres sociétés :

Java et toutes les marques et tous les logos Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

INDEX

T