IBM Security QRadar
Version 7.1.0 (MR1)

Guide de configuration de l'évaluation de la vulnérabilité

Remarque : Avant d'utiliser le présent document et le produit associé, lisez les informations disponibles dans “Avis et Marques” à page 140.

© Copyright IBM Corp. 2012, 2013 Tous droits réservés. US Government Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

TABLE DES MATIERES

A PROPOS DE CE GUIDE

Le guide de configuration de l'évaluation de la vulnérabilité *IBM Security QRadar SIEM* vous fournit des informations sur la gestion des scanners de vulnérabilité et la configuration des plannings d'analyse pour travailler avec QRadar SIEM.

Public cible

Ce guide est destiné à l'administrateur système chargé de configurer QRadar SIEM dans votre réseau. Ce guide suppose que vous disposez d'un accès administrateur à QRadar SIEM et des connaissances sur votre réseau d'entreprise et vos technologies réseau.

Conventions

Les conventions suivantes s'appliquent dans ce guide :

▶ Indique que la procédure contient une seule instruction.

REMARQUE

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

ATTENTION

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 plus d'informations sur la façon d'accéder à la documentation plus technique, aux notes techniques et aux notes sur l'édition, voir la note de documentation technique **Accès à IBM Security QRadar SIEM.** (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)
Contacter le service client	Pour savoir comment contacter le service client, voir la note technique **Support et Téléchargement** (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)

1 PRÉSENTATION

L'intégration d'évaluation de la vulnérabilité permet à QRadar SIEM de générer des profils d'évaluation de vulnérabilité. Les profils d'évaluation de la vulnérabilité utilisent des données d'événement corrélées, une activité réseau, ainsi que des changements du comportement pour supprimer des faux positifs afin de déterminer le niveau de menace pour les éléments métier essentiels.

L'intégration de QRadar SIEM aux outils d'évaluation des vulnérabilités vous permet de planifier des analyses pour garder vos données d'évaluation des vulnérabilités à jour.

REMARQUE

Vous devez disposer d'autorisations appropriées pour accéder aux réseaux contenant des adresses CIDR que vous planifiez pour les analyses d'évaluation de vulnérabilité.

REMARQUE

Les informations trouvées dans cette documentation relatives à la configuration des scanners sont basées sur les fichiers RPM les plus récents du site Web Qmmunity, à l'adresse*https://qmmunity.q1labs.com/*.

Cette section fournit des informations sur les éléments suivants :

- **Configuration de l'évaluation de la vulnérabilité**
- **Installation des Scanners**
- **Affichage des Scanners**

Configuration de l'évaluation de la vulnérabilité

Pour configurer une évaluation de vulnérabilité, procédez comme suit :

1. Installez le scanner RPM, si nécessaire.

   Pour plus d'informations, voir **Installation des Scanners**.
2. Configurez votre scanner à l'aide de la liste suivante des scanners pris en charge :
   - **Managing IBM Security AppScan Enterprise Scanners**
   - **Managing nCircle IP360 Scanners**

- **Managing Nessus Scanners**
- **Managing Nmap Scanners**
- **Managing Qualys Scanners**
- **Managing FoundScan Scanners**
- **Managing Juniper Networks NSM Profiler Scanners**
- **Managing Rapid7 NeXpose Scanners**
- **Managing netVigilance SecureScout Scanners**
- **Managing eEye Scanners**
- **Managing PatchLink Scanners**
- **Managing McAfee Vulnerability Manager Scanners**
- **Managing SAINT Scanners**
- **Managing AXIS Scanners**
- **Managing Tenable SecurityCenter**

Le scanner détermine les essais réalisés lors de l'analyse de l'hôte. Le scanner choisi remplit vos données de profil, y compris les informations sur l'hôte, les ports et les vulnérabilités potentielles.

REMARQUE

Si vous ajoutez, modifiez ou supprimez un scanner, vous devez cliquer sur **Deploy Changes** sur l'onglet **Admin** afin que les modifications soient mises à jour sur la console QRadar. Les modifications de configuration ne peuvent interrompre les analyses en cours, car les modifications sont appliquées une fois l'analyse terminée.

3 Planifiez une analyse de vulnérabilité afin d'importer les données vers QRadar SIEM. Pour plus d'informations, voir **Gestion des plannings d'analyse**.

Les résultats d'analyse fournissent un système d'exploitation sûr et une version de chaque CIDR, serveur et version de chaque port. L'analyse fournit également des vulnérabilités connues sur des ports découverts et sur des services.

Installation des scanners

Pour mettre à jour ou installer un nouveau scanner, vous devez soit configurerQRadar SIEM afin qu'il télécharge automatiquement et installe les fichiers rpm du scanner à l'aide de l'icône de mise à jour automatique sur l'onglet **Admin**, soit installer les fichiers rpm manuellement. Si vous choisissez le processus d'installation manuelle, les fichiers d'installation de votre scanner sont disponibles sur le site Web Qmmunity.

Pour installer un scanner manuellement :

Etape 1 Téléchargez les fichiers rpm du scanner à partir du site Web Qmmunity :

https://qmmunity.q1labs.com/

Etape 2 Copiez les fichiers sur votre QRadar SIEM.

Etape 3 A l'aide de SSH, connectez-vous à votre QRadar SIEM en tant que superutilisateur.

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

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

Etape 4 Accédez au répertoire contenant les fichiers téléchargés.

Etape 5 Entrez la commande suivante :

`rpm -Uvh <filename>`

Où **`<filename>`** est le nom du fichier téléchargé.

Par exemple : **`rpm -Uvh VIS-nCircleIP360 -7.0-148178.rpm`**

Etape 6 Connectez-vous à QRadar SIEM.

`https://<IP Address>`

Où <IP Address> est l'adresse IP de QRadar SIEM.

Etape 7 Cliquez sur l'onglet **Admin**.

L'onglet Administration s'affiche.

Etape 8 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Affichage des scanners

Pour afficher les scanners configurés, procédez comme suit :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners fournit les détails suivants pour chaque scanner :

Tableau 1-1 Paramètres du scanner

Paramètre	Description
Name	Affiche le nom du scanner.
Type	Affiche le type de scanner, par exemple, Nessus Scan Results Importer (Importateur de résultats de d'analyse Nesssus).
Host	Affiche le nom d'adresse IP ou le nom d'hôte sur lequel le scanner fonctionne.
Approved CIDR ranges	Affiche le routage CIDR que le scanner doit prendre en compte. Plusieurs routages CIDR sont affichés à l'aide d'une liste séparée par une virgule.
Description	Affiche une description de ce scanner.

Tableau 1-1 Paramètres du scanner (suite)

Paramètre	Description
Status	Affiche l'état de planification du scanner. ***Note:*** *Lorsque l'état d'une analyse planifiée change, la zone d'état située dans la liste des scanners installés se met à jour, consultez* **Tableau 17-1** *pour en savoir plus sur l'état d'analyse.*

2 GESTION DES SCANNERS IBM SECURITY APPSCAN ENTERPRISE

QRadar SIEM peut importer des résultats d'analyse à partir des données du rapport IBM Security AppScan® Enterprise, ce qui vous offre un environnement de sécurité centralisé pour une numérisation d'application avancée et une création de rapports de conformité de sécurité. L'importation des résultats d'analyse IBM Security AppScan Enterprise vous permet de collecter les informations de vulnérabilité pour le logiciel malveillant, l'application Web et les services Web dans votre déploiement. QRadar SIEM récupère les rapports AppScan Enterprise à l'aide du service Web Representational State Transfer (REST) pour importer les données de vulnérabilité et générer les offenses dans votre équipe de sécurité QRadar SIEM.

Pour intégrer AppScan Enterprise avec QRadar SIEM, vous devez :

1. Générer des rapports d'analyse dans AppScan Enterprise. Pour en savoir plus sur la génération de rapports d'analyse, voir la documentation du fournisseur AppScan Enterprise.
2. Configurez AppScan Enterprise pour accorder l'accès QRadar SIEM aux données de rapport. Pour plus d'informations, voir **Configuration d'AppScan Enterprise pour autoriser l'accès à QRadar SIEM.**
3. Configurez votre scanner AppScan Enterprise dans QRadar SIEM. Pour plus d'informations, voir **Configuration d'AppScan Enterprise dans QRadar SIEM**.
4. Créer une planification dans QRadar SIEM pour importer les résultats AppScan Enterprise. Pour plus d'informations, voir **Gestion des plannings d'analyse**.

Configuration d'AppScan Enterprise pour autoriser l'accès à QRadar SIEM.

Un membre de l'équipe de sécurité ou votre administrateur AppScan Enterprise doit déterminer l'AppScan Enterprise sur lequel les utilisateurs peuvent publier des rapports vers QRadar SIEM. Après avoir configuré les utilisateurs AppScan Enterprise, les rapports générés par AppScan Enterprise peuvent être publiés sur QRadar SIEM, les rendant disponibles pour téléchargement.

Pour configurer AppScan Enterprise afin d'accorder l'accès QRadar SIEM aux données de rapport :

1. Créez un type d'utilisateur personnalisé. Voir **Création de types d'utilisateurs personnalisés**.
2. Activez AppScan Enterprise et l'intégration QRadar SIEM. Voir. **Activation de QRadar Integration**.
3. Créez une Application Deployment Map. Voir **Création d'une Application Deployment Map**.
4. Publiez vos résultats d'analyse sur QRadar SIEM. Voir **Publication de rapports sur QRadar SIEM**.

Création de types d'utilisateurs personnalisés

Les types d'utilisateurs personnalisés permettent aux administrateurs d'effectuer des tâches administratives spécifiques limitées. Un type d'utilisateur personnalisé doit être créé avant de pouvoir affecter des autorisations.

Pour créer un type d'utilisateur personnalisé :

Etape 1 Connectez-vous à IBM Security AppScan Enterprise.

Etape 2 Cliquez sur l'onglet **Administration**.

Etape 3 Dans la page User Types, cliquez sur **Create**.

Etape 4 Créez le type d'utilisateur et sélectionnez une des autorisations utilisateurs personnalisées pour le type d'utilisateur :

- **Configure QRadar Integration** : cochez cette case pour permettre aux utilisateurs d'accéder aux options d'intégration QRadar pour AppScan Enterprise.
- **Publish to QRadar** : cochez cette case pour autoriser QRadar SIEM à accéder aux données de rapport d'analyse publiées.
- **QRadar Service Account** : cochez cette case pour configurer la permission d'utiliser REST API sur le compte. Il n'accède pas à l'interface utilisateur.

Etape 5 Enregistrez le type d'utilisateur.

Vous êtes maintenant sur le point d'activer l'intégration de QRadar avec AppScan Enterprise.

Activation de QRadar Integration

Pour effectuer ces étapes, vous devez vous connecter en tant qu'utilisateur avec l'activation du type d'utilisateur Configuration QRadar Integration.

Pour activer AppScan Enterprise avec QRadar SIEM :

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

Etape 2 Dans le menu de navigation, cliquez sur **Network Security Systems**.

Etape 3 Dans le panneau QRadar Integration Settings, cliquez sur **Edit**.

La configuration QRadar Integration Settings s'affiche.

Etape 4 Cochez la case **Enable QRadar Integration**.

Tous les rapports précédemment publiés sur QRadar SIEM s'affichent. Si aucun des rapports affichés n'est requis, vous pouvez les supprimer de la liste. En publiant des rapports supplémentaires dans QRadar SIEM, les rapports s'affichent sur cette liste.

Vous êtes maintenant sur le point de configurer Application Deployment Mapping dans AppScan Enterprise.

Création d'une application Deployment Map

Application Deployment Map permet à AppScan Enterprise de déterminer les emplacements qui hébergent l'application dans votre environnement de production. Dès que les vulnérabilités sont reconnues, AppScan Enterprise connaît les emplacements des hôtes et les adresses IP concernés par la vulnérabilité. Si une application est déployée sur plusieurs hôtes, alors AppScan Enterprise génère la vulnérabilité pour chaque résultat dans les résultats d'analyse.

Pour créer une application Deployment Map:

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

Etape 2 Dans le menu de navigation, cliquez sur **Network Security Systems**.

Etape 3 Sur le panneau Application Deployment Mapping, cliquez sur **Edit**.

La configuration d'Application Deployment Mapping s'affiche.

Etape 4 Dans le zone **Application test location (host or canevas)**, entrez le test d'emplacement de votre application.

Etape 5 Dans le zone **Application production location (host)**, entrez l'adresse IP de votre environnement de production.

REMARQUE

Pour ajouter des informations de vulnérabilité à QRadar, votre Application Deployment Mapping doit inclure une adresse IP. Toutes les données de vulnérabilité sans adresse IP sont exclues de QRadar SIEM si l'adresse IP n'est pas disponible dans les résultats de recherche d'AppScan Enterprise.

Etape 6 Cliquez sur **Add**.

Etape 7 Répétez **Etape 3** à **Etape 6** pour mapper tous les environnements de production dans AppScan Enterprise.

Etape 8 Cliquez sur **Done** pour enregistrer les changements de configuration.

Vous êtes maintenant sur le point de publier des rapports complets sur QRadar SIEM.

Publication de rapports sur QRadar SIEM

Des rapports de vulnérabilité complets générés par AppScan Enterprise doivent être rendus accessibles sur QRadar SIEM en publiant le rapport. Pour effectuer ces étapes, vous devez vous connecter en tant qu'utilisateur avec l'activation du type d'utilisateur Publish sur QRadar.

Pour publier un rapport de vulnérabilité dans AppScan Enterprise :

Etape 1 Cliquez sur l'onglet **Jobs & Reports.**

Etape 2 Accédez au le rapport de sécurité que vous souhaitez rendre disponible sur QRadar SIEM.

Etape 3 Sur la barre de menus de tous les rapports de sécurité, sélectionnez **Publish >. Grant report accès to QRadar**.

Vous êtes maintenant sur le point d'ajouter votre scanner AppScan Enterprise à QRadar SIEM.

Configuration d'AppScan Enterprise dans QRadar SIEM

Après avoir configuré AppScan Enterprise et publié les rapports, vous pouvez ajouter le scanner AppScan Enterprise à QRadar SIEM. L'ajout d'un scanner permet à QRadar SIEM de connaître les rapports d'analyse à collecter. Vous pouvez ajouter plusieurs scanners AppScan Enterprise dans QRadar SIEM, chacun avec une configuration différente. L'ajout de plusieurs configurations pour un scanner AppScan Enterprise unique vous permet de créer des scanners individuels pour les données relatives aux résultats spécifiques. Le planning d'analyse que vous avez configuré dans QRadar SIEM vous permet de déterminer la fréquence à laquelle QRadar SIEM importe les données relatives aux résultats d'analyse dans AppScan Enterprise à l'aide du service Web REST.

REMARQUE

Vos données relatives aux résultats d'analyse doivent inclure l'adresse IP de l'hôte dans Application Deployment Mapping. Toutes les données de vulnérabilité sans adresse IP sont exclues de QRadar SIEM si l'adresse IP n'est pas disponible dans les résultats de recherche d'AppScan Enterprise.

Cette section comprend les rubriques suivantes :

- **Ajout d'un scanner AppScan Enterprise sur QRadar SIEM**
- **Edition d'un scanner AppScan Enterprise**
- **Suppresion d'un scanner AppScan Enterprise**

Ajout d'un scanner AppScan Enterprise sur QRadar SIEM

Pour ajouter un scanner AppScan Enterprise :

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs pour les paramètres suivants :

Tableau 2-1 Paramètres du scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez affecter à ce scanner. Le nom peut contenir jusqu'à 255 caractères.
Description	Entrez une description pour ce scanner. La description peut contenir jusqu'à 255 caractères.

Tableau 2-1 Paramètres du scanner (suite)

Paramètre	Description
Managed Host	Dans la zone de liste, sélectionnez la description que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **IBM AppScan Scanner.**

La liste des zones du scanner sélectionné s'affiche.

Etape 6 Configurez les valeurs pour les paramètres suivants :

Tableau 2-2 Paramètres IBM AppScan Enterprise

Paramètre	Description
ASE Instance Base URL	Entrez l'URL de base complète de l'instance AppScan Enterprise. Ce champ prend en charge les URL pour les HTTP et HTTPS. Par exemple, **`http://myasehostname/ase/`**.
Authentication Type	Sélectionnez un type d'authentification : • **Windows Authentication** : Sélectionnez cette option pour utiliser Windows Authentication lorsque vous utilisez le service Web REST pour extraire les rapports des données de l'analyse AppScan Enterprise. • **Jazz™ Authentication** - Sélectionnez cette option pour utiliser Jazz Authentication lorsque vous utilisez le service Web REST pour récupérer les données de rapport d'analyse pour AppScan Enterprise.
Username	Entrez le nom d'utilisateur requis pour extraire les résultats de l'analyse requis depuis AppScan Enterprise.
Password	Entrez le mot de passe requis pour extraire les résultats de l'analyse requis depuis AppScan Enterprise.
Report Name Pattern	Entrez une expression régulière (regex) requise pour filtrer la liste des rapports de vulnérabilité disponibles depuis AppScan Enterprise. Tous les fichiers correspondants sont inclus et traités par QRadar SIEM. Vous pouvez spécifier un groupe de rapports de vulnérabilité ou un rapport individuel à l'aide du canevas d'expression régulière. Par défaut, le champ **Report Name Pattern** contient.**`*`** comme canevas d'expression régulière. Le canevas.* importe tous les rapports qui sont publiés sur QRadar SIEM. L'utilisation de ce paramètre requiert la connaissance de l'expression régulière (regex). Pour plus d'informations, consultez le site Web suivant : *http://download.oracle.com/javase/tutorial/essential/regex//*.

Etape 7 Pour configurer les intervalles CIDR que ce scanner doit prendre en considération :

a Dans la zone de texte, entrez le routage CIDR ou cliquez sur **Browse** pour sélectionner le routage CIDR à partir de la liste réseaux.

La plage CIDR vous permet de filtrer la liste des adresses IP que les scanners prennent en compte lors de la récupération des résultats dans les périphériques AppScan Enterprise. Puisque vous pouvez configurer et planifier plusieurs scanners AppScan Enterprise dans QRadar, la plage CIDR agit comme un filtre lorsque vous recherchez le réseau pour vos données relatives au résultats d'analyse. Pour collecter tous les résultats au sein de tous les rapports AppScan Enterprise publiés, vous pouvez utiliser une plage CIDR de 0.0.0.0/0.

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

Etape 9 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

Vous êtes maintenant sur le point de créer un planning d'analyse dans QRadar SIEM. Pour plus d'informations, voir **Gestion des plannings d'analyse**.

Edition d'un scanner AppScan Enterprise

Pour éditer un scanner AppScan Enterprise :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez éditer.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Mettez à jours les paramètres, si nécessaire.Voir **Table 2-2**.

Etape 7 Cliquez sur **Save**.

Etape 8 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

Suppression d'un scanner AppScan Enterprise

Pour supprimer un scanner AppScan Enterprise :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez sur **OK**.

Etape 7 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

3 SCANNER IBM SITEPROTECTOR

Le module de scanner IBM SiteProtector® QRadar SIEM accède aux données de vulnérabilité à partir des scanners IBM SiteProtector à l'aide de JDBC. Le scanner IBM SiteProtector récupère des données à partir de la table RealSecureDB et interroge les informations disponibles sur la vulnérabilité. Le champ de comparaison permet à QRadar SIEM de récupérer uniquement les informations les plus récentes à partir de la table RealSecureDB et d'importer toutes les nouvelles vulnérabilités dans QRadar SIEM.

Lorsque vous configurez votre IBM SiteProtector, nous vous recommandons de créer un compte utilisateur SiteProtector spécifiquement pour QRadar SIEM. La création d'un compte utilisateur garantit que QRadar SIEM dispose de données d'identification pour interroger la base de données IBM SiteProtector pour récupérer les données de vulnérabilité. Après la création d'un compte utilisateur pour QRadar SIEM, vous devez vérifier la communication entre QRadar SIEM et votre système IBM SiteProtector pour vous assurer qu'il n'existe pas de pare-feu bloquant la communication sur le port que vous utilisez pour interroger RealSecureDB.

Cette section fournit des informations sur les éléments suivants :

Ajout d'un scanner IBM SiteProtector

Vous pouvez ajouter plusieurs scanners IBM SiteProtector dans QRadar SIEM, chacun avec une configuration différente pour déterminer les intervalles CIDR que vous voulez que le scanner doit prendre en compte. L'ajout de plusieurs configurations pour un scanner IBM SiteProtector unique vous permet de créer des scanners individuels pour collecter des données de résultats spécifiques à partir d'emplacements spécifiques. Après avoir ajouté et configuré le scanner IBM SiteProtector dans QRadar SIEM, vous pouvez créer un planning d'analyse pour déterminer la fréquence à laquelle QRadar SIEM interroge la base de données IBM SiteProtector.

Pour ajouter un scanner IBM SiteProtector à QRadar SIEM :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners**.

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 3-1 Paramètres du scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez attribuer à ce scanner. Le nom peut contenir jusqu'à 255 caractères.
Description	Entrez une description pour ce scanner. La description peut contenir jusqu'à 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **IBM SiteProtector Scanner**.

La liste des champs pour le type de scanner sélectionné s'affiche.

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 3-2 Paramètres du scanner IBM SiteProtector.

ParamètreParamètre	Description
Hostname	Entrez l'adresse IP ou le nom d'hôte de d'IBM SiteProtector contenant les vulnérabilités que vous souhaitez ajouter à QRadar SIEM.

Tableau 3-2 Paramètres du scanner IBM SiteProtector.

ParamètreParamètre	**Description**
Port	Entrez le numéro de port utilisé par le serveur de base de données. Le numéro par défaut affiché est fonction du type de base de données sélectionné. L'intervalle valide se trouve entre 0 et 65536. Le numéro de port par défaut pour MSDE est 1433. Le port de configuration JDBC doit correspondre au port d'écoute de la base de données. Les connexions TCP entrantes de la base de données doivent être activées pour communiquer avec QRadar SIEM. Le numéro de port par défaut pour toutes les options incluent : • **MSDE** - 1433 • **Postgres** - 5432 • **MySQL** - 3306 • **Oracle** - 1521 • **Sybase** - 1521
Username	Entrez le nom d'utilisateur requis pour accéder à IBM SiteProtector.
Password	Entre le mot de passe requis pour accéder à IBM SiteProtector.
Domain	Entrez le domaine requis, si nécessaire, pour vous connecter à votre base de données IBM SiteProtector. Si vous sélectionnez MSDE en tant que type de base de données et que la base de données est configurée pour Windows, vous devez définir un domaine Windows. Sinon, laissez ce champ vide. Le domaine peut contenir jusqu'à 255 caractères alphanumériques. Le domaine peut inclure les caractères spéciaux suivants : trait de soulignement :(_), tiret demi-cadratin (-), et point (.).
Database Name	Entrez le nom de la base de données à laquelle vous souhaitez vous connecter. Le nom de la base de données par défaut est **RealSecureDB**.
Database Instance	Entrez l'instance de base de données de votre base de données IBM SiteProtector. Si vous n'utilisez pas une instance de base de données, vous pouvez laisser ce champ vide. Si vous sélectionnez MSDE en tant que type de base de données et que vous avez plusieurs instances de serveur SQL sur un serveur, définissez l'instance à laquelle vous souhaitez vous connecter.

Tableau 3-2 Paramètres du scanner IBM SiteProtector.

ParamètreParamètre	Description
Use Named Pipe Communication	Cochez cette case pour utiliser des canaux de communication nommés lorsque vous communiquez avec la base de données IBM SiteProtector. Par défaut, cette case est désélectionnée. En utilisant une connexion dont le canal de communication est nommé, le nom d'utilisateur et le mot de passe doivent être ceux de l'authentification Windows appropriés et non ceux de la base de données. Lorsque vous sélectionnez cette case, vous utilisez le canal de communication nommé de votre système.
Use NTLMv2	Sélectionnez cette case si votre IBM SiteProtector utilise NTLMv2 en tant que protocole d'authentification. Par défaut, cette case est désélectionnée. La case Use NTLMv2 force les connexions MSDE à utiliser le protocole NTLMv2 lorsqu'elles communiquent avec les serveurs SQL nécessitant l'authentification NTLMv2 Si la case **Use NTLMv2** est cochée, cela n'a aucun effet sur les connexions MSDE avec les serveurs SQL qui ne nécessitent pas d'authentification NTLMv2.

Etape 7 Pour configurer les intervalles CIDR que ce scanner doit prendre en considération :

a Dans le champ de texte, entrez l'intervalle CIDR que vous souhaitez que ce scanner prenne en compte ou cliquez sur **Browse** pour sélectionner l'intervalle CIDR à partir de la liste réseaux.Pour collecter toutes les vulnérabilités IBM SiteProtector, vous pouvez entrer 0.0.0.0/0 en tant qu'adresse CIDR.

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

Etape 9 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Edition d'un scanner IBM SiteProtector

Editer un scanner:

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

Etape 2 Dans le menu de navigation, cliquez **Data Sources**.

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez éditer.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Mettez à jour les paramètres, si nécessaire. Voir **Tableau 3-2**.

Etape 7 Cliquez sur **Save**.

Etape 8 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

Suppression d'un scanner IBM SiteProtector

Pour supprimer un scanner :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez sur **OK**.

Etape 7 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

4 IBM TIVOLI ENDPOINT MANAGER

Le module de scanner IBM Tivoli® Endpoint Manager accède aux données de vulnérabilité à partir d'IBM Tivoli Endpoint Manager à l'aide de l'interface de programme d'application du protocole SOAP installée avec l'application Web Reports. L'application Web Reports de Tivoli Endpoint Manager est nécessaire pour récupérer les données de vulnérabilité de Tivoli Endpoint Manager pour QRadar SIEM. Nous vous recommandons de créer un utilisateur dans IBM Tivoli Endpoint Manager pour QRadar SIEM.

REMARQUE

QRadar SIEM est compatible avec les versions 8.2.x d'IBM Tivoli Endpoint Manager. Toutefois, nous vous recommandons de mettre à jour et d'utiliser la dernière version d'IBM Tivoli Endpoint Manager disponible.

Cette section fournit des informations sur les éléments suivants :

- **Ajout d'un scanner IBM Tivoli Endpoint Manager**
- **Modification d'un scanner IBM Tivoli Endpoint Manager**
- **Suppression d'un scanner IBM Tivoli Endpoint Manager**

Ajout d'un scanner IBM Tivoli Endpoint Manager

Vous pouvez ajouter plusieurs scanners IBM Tivoli Endpoint Manager à QRadar SIEM, chacun avec une configuration différente pour déterminer les plages de routage CIDR à prendre en compte par le scanner. L'ajout de plusieurs configurations pour un scanner IBM Tivoli Endpoint Manager vous permet de créer des scanners individuels pour la collecte de données relatives aux résultats spécifiques à partir d'emplacements spécifiques. Une fois que vous avez ajouté et configuré IBM Tivoli Endpoint Manager sous QRadar SIEM, vous pouvez programmer la fréquence à laquelle QRadar SIEM accède à IBM Tivoli Access Manager. Cela vous permet de programmer la fréquence à laquelle QRadar SIEM demande les données à partir d'IBM Tivoli Endpoint Manage à l'aide de l'interface de programme d'application du protocole SOAP.

Pour ajouter un scanner IBM Tivoli Endpoint Manager dans QRadar SIEM:

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners**.

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 3-1 Paramètres du scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez attribuer à ce scanner. Le nom peut contenir jusqu'à 255 caractères.
Description	Entrez une description pour ce scanner. La description peut contenir jusqu'à 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **IBM Tivoli Endpoint Manager**.

La liste des zones du type de scanner sélectionné s'affiche.

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 3-2 Paramètres IP360

Paramètre	Description
Hostname	Entrez l'adresse IP ou le nom d'hôte d'IBM Tivoli Endpoint Manager contenant les vulnérabilités à ajouter à QRadar SIEM.
Port	Entrez le numéro de port utilisé pour se connecter à IBM Tivoli Endpoint Manager à l'aide de l'interface de programme d'application du protocole SOAP. Par défaut, le port 80 est le numéro de port permettant de communiquer avec IBM Tivoli Endpoint Manager. Si vous utilisez le protocole HTTPS, vous devez mettre cette zone à jour vers le numéro de port HTTPS de votre réseau. La plupart des configurations utilisent le port 443 pour les communications HTTPS.

Tableau 3-2 Paramètres IP360 (suite)

Paramètre	Description
Use HTTPS	Cochez cette case pour vous connecter à l'aide du protocole HTTPS. Si vous cochez cette case, le nom d'hôte ou l'adresse IP que vous spécifiez utilise le protocole HTTPS pour se connecter à votre IBM Tivoli Endpoint Manager. Si un certificat est requis pour se connecter à l'aide du protocole HTTPS, vous devez copier les certificats exigés par la console QRadar ou les hôtes gérés vers le répertoire suivant : `/opt/qradar/conf/trusted_certificates` ***Remarque :*** *QRadar prend en charge les certificats ayant les extensions suivantes :.crt,.cert ou.der. Tous les certificats requis doivent être copiés dans le répertoire des certificats de confiance avant d'enregistrer et de déployer vos modifications.*
Username	Entrez le nom d'utilisateur requis pour accéder à IBM Tivoli Endpoint Manager.
Password	Entrez le mot de passe requis pour accéder à IBM Tivoli Endpoint Manager.

Etape 7 Pour configurer les intervalles de routage CIDR que vous souhaitez que ce scanner prenne en compte :

a Dans la zone de texte, entrez l'intervalle de routage CIDR que ce scanner doit prendre en considération ou cliquez sur **Browse** pour sélectionner l'intervalle de routage CIDR à partir de la liste réseaux.

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

Etape 9 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Modification d'un scanner IBM Tivoli Endpoint Manager

Editer un scanner :

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez éditer.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Mettez à jour les paramètres, si nécessaire. Voir **Tableau 3-2**.

Etape 7 Cliquez sur **Save**.

Etape 8 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

Suppression d'un scanner IBM Tivoli Endpoint Manager

Pour supprimer un scanner :

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez sur **OK**.

Etape 7 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

5 GESTION DES SCANNERS NCIRCLE IP360

QRadar SIEM utilise SSH pour accéder au serveur distant (serveur d'exportation SSH) pour récupérer et interpréter les données numérisées. QRadar SIEM prend en charge les versions VnE Manager IP360 allant de la 6.5.2 à la 6.8.2.8.

Vous pouvez configurer un dispositif d'analyse nCircle IP360 pour exporter les résultats d'analyse vers un serveur distant. Ces résultats d'analyse sont exportés en format XML2 vers un serveur SSH. Pour intégrer avec succès un périphérique IP 360 dans QRadar SIEM, ces fichiers en format XML2 doivent être lus à partir du serveur distant (via SSH). QRadar SIEM peut être configuré pour programmer une analyse ou interroger le serveur SSH afin de mettre à jour les résultats de l'analyse et d'importer les résultats les plus récents pour traitement. Le terme serveur distant renvoie à un système qui est séparé du périphérique nCircle. Il est impossible de connecter directement QRadar SIEM aux périphériques nCircles. Pour de plus amples informations sur l'exportation des résultats d'analyse, consultez **Exporter des rapports d'analyse**.

Les résultats de l'analyse contiennent des informations d'identification relatives à la configuration d'examen à partir de laquelle elles ont été produites. Les résultats d'analyse les plus récents sont utilisés lorsqu'une analyse est importée par QRadar SIEM. QRadar SIEM ne prend en charge que les résultats d'analyse exportés à partir du scanner IP360 dans le format XML2.

Cette section fournit des informations sur les éléments suivants :

- **Ajouter un scanner IP360**
- **Editer un Scanner IP360**
- **Supprimer un Scanner IP360**
- **Exporter des rapports d'analyse**

Ajouter un scanner IP360

Pour ajouter un scanner IP360:

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur Add.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 3-1 Paramètres du scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez attribuer à ce scanner. Le nom peut comporter jusqu'à 255 caractères.
Description	Entrez une description pour ce scanner. La description peut comporter jusqu'à 255 caractères.
Managed Host	Dans la liste déroulante, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la liste déroulante, sélectionnez nCircle IP360 Scanner.

La liste des champs pour le type de scanner sélectionné s'affiche.

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 3-2 Paramètres IP360

Paramètre	Description
SSH Server Host Name	Entrez l'adresse IP ou le nom d'hôte pour le serveur distant hébergeant les fichiers des résultats d'analyse. Nous recommandons un système d'exploitation UNIX avec SSH activé.
SSH Username	Entrez le nom d'utilisateur SSH du serveur distant.
SSH Password	Entrez le mot de passe du serveur distant correspondant au nom d'utilisateur SSH. Si vous sélectionnez la case **Enable Key Authentication**, vous n'aurez plus besoin d'un mot de passe.
SSH Port	Entrez le numéro de port utilisé pour se connecter au serveur distant.
Remote Directory	Entrez l'emplacement du répertoire des fichiers des résultats d'analyse.
Age maximum du fichier (en jours)	Entrez l'âge maximum du fichier à inclure lors de l'exécution de l'analyse programmée. Les fichiers qui sont plus anciens que la date précisée sont exclus du processus d'importation des données de résultat dans QRadar SIEM.

Tableau 3-2 Paramètres IP360 (suite)

Paramètre	Description
File Pattern	Entrez une expression régulière (regex), une étape obligatoire pour filtrer la liste des fichiers spécifiés dans la **zone** Remote Directory. Tous les fichiers correspondants sont inclus et traités. Par exemple, si vous voulez répertorier tous les fichiers xml2 se terminant par XML, utilisez l'entrée suivante : **`XML2.*\.xml`** L'utilisation de ce paramètre nécessite la connaissance des expressions régulières (regex) Pour de plus amples informations, consultez le site suivant: *http://download.oracle.com/javase/tutorial/essential/regex/*
Enable Key Authorization	Cochez cette case pour activer la clé d'autorisation d'accès au serveur. Si vous sélectionnez la case **Enable Key Authentication,** l'authentification SSH se fait via une clé privée. Vous pouvez ainsi vous passer du mot de passe. La valeur par défaut est désactivée.
Private Key Path	Entrez le chemin d'accès de la clé privée. Le chemin d'accès de la clé privée est le chemin complet du répertoire sur votre système QRadar SIEM dans lequel est conservée la clé privée à utiliser pour l'authentification par clé de SSH. Le chemin par défaut est /opt/qradar/conf/vis.ssh.key. Cependant ce chemin n'existe pas. Vous devez créer un fichier vis.ssh.key pour votre hôte distant ou taper un autre nom de fichier. Si la case **Enable Key Authentication** n'est pas cochée, alors Private Key Path est ignoré.

REMARQUE

Si le scanner est configuré pour utiliser un mot de passe, il est nécessaire que le serveur du scanner SSH auquel est connecté QRadar SIEM prenne en charge l'authentification par mot de passe. Si ce n'est pas le cas, l'authentification SSH pour le scanner échoue. Assurez-vous que la ligne suivante s'affiche dans votre fichier sshd_config qui se trouve généralement dans le répertoire / etc / ssh sur le serveur SSH: **`PasswordAuthentication yes. Si le serveur de votre scanner n'utilise pas OpenSSH, la configuration peut être différée.`** Pour plus d'informations, consultez le schéma de montage du scanner du fournisseur.

Etape 7 Pour configurer les plages de routage CIDR que vous voulez que le scanner doit prendre en compte:

a Dans la zone de texte, entrez l'intervalle CIDR que vous souhaitez que le scanner doit prendre en compte ou cliquez sur **Browse** pour sélectionner l'intervalle CIDR à partir de la liste de réseaux.

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

Etape 9 Dans le menu de l'onglet **Admin**, cliquez sur **Deploy Changes**.

Editer un Scanner IP360

Editer un scanner:

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez éditer.

Etape 5 Cliquer sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Mettez à jour les paramètres si nécessaire. Voir **Tableau 3-2**.

Etape 7 Cliquez sur **Save**.

Etape 8 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

Supprimer un Scanner IP360

Pour supprimer un scanner :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez sur **OK**.

Etape 7 Dans l'onglet **Admin**, cliquez **Deploy Changes**.

Exporter des rapports d'analyse

Configurez votre périphérique nCircle en vue d'exporter des rapports d'analyse :

Etape 1 Connexion à l'interface utilisateur VNE Manager IP360.

Etape 2 Dans la barre de navigation, sur le côté gauche de l'écran, sélectionnez **Administer > System > VNE Manager > Automated Export**.

Le menu Automated Export s'affiche.

Etape 3 Cliquez sur l'onglet **Export to File**.

Etape 4 Configurez les paramètres d'exportation.

Pour plus d'informations sur la configuration des paramètres d'exportation, cliquez sur le lien Aide. Pour assurer une bonne intégration des rapports d'analyse dansQRadar SIEM, le processus d'exportation doit être configuré de façon à ce que ces rapports soient exportés au format XML.

Etape 5 Enregistrez les paramètres de cible qui s'affichent dans l'interface utilisateur. Ces paramètres sont nécessaires pour configurer QRadar SIEM et l'intégrer dans votre périphérique nCircle.

6 GESTION DES SCANNERS NESSUS

QRadar SIEM peut récupérer les rapports d'analyse de vulnérabilité à propos de vos ressources réseau en mettant à profit la relation du client et du Nessus serveur ou en utilisant l'interface API XMLRPC de Nessus pour accéder directement aux données d'analyse.

Lorsque vous configurez votre client Nessus, nous vous recommandons de créer un compte utilisateur Nessus pour QRadar SIEM. La création d'un compte utilisateur vous assure que QRadar SIEM dispose de données d'identification nécessaires à la connexion via SSH et pour communiquer avec le serveur Nessus afin de récupérer les données de rapport d'analyse grâce à la relation serveur client ou grâce à l'interface API XMLRPC. Après avoir créé un compte utilisateur pour QRadar SIEM, vous devez tenter d'effectuer un SSH, depuis QRadar SIEM jusqu'à votre client Nessus, de vérifier les données d'identification de QRadar SIEM. Ceci garantit une communication entre QRadar SIEM et le client Nessus avant que vous tentiez de collecter les données d'analyse ou démarrer une analyse opérationnelle.

Les options de collection de données sont disponibles pour Nessus :

- **Scheduled Live Scan** - Permet à QRadar SIEM de se connecter avec un client Nessus et de lancer une analyse préconfigurée. QRadar SIEM utilise SSH pour récupérer les données du rapport d'analyse à partir du répertoire de résultats temporaires du client une fois l'analyse opérationnelle terminée.
- **Scheduled Results Import** - Permet à QRadar SIEM de se connecter à l'emplacement hébergeant vos rapports d'analyse Nessus. QRadar SIEM se connecte au référentiel via SSH et importe les fichiers de rapport d'analyse depuis le répertoire distant. QRadar SIEM prend en charge l'importation des rapports d'analyse Nessus ou rapports d'analyse dans un format de sortie Nessus pris en charge.
- **Scheduled Live Scan - XMLRPC API** - Permet à QRadar SIEM d'utiliser XMLRPC API pour démarrer une analyse préconfigurée. Pour démarrer une analyse opérationnelleà partir de QRadar SIEM, vous devez indiquer le nom de la règle des données de l'analyse opérationnelle à récupérer. Lors de l'exécution de l'analyse opérationnelle, QRadar SIEM met à jour le pourcentage complet dans l'état de l'analyse. A la fin de l'analyse opérationnelle, QRadar SIEM récupère les données et met à jour les informations d'évaluation de vulnérabilité pour vos actifs.

- **Scheduled Completed Report Import - XMLRPC API** : Permet à QRadar SIEM de se connecter au serveur Nessus et de télécharger des données depuis tout rapport complété qui correspond au nom du rapport et aux filtres rapport d'âge.

Les données de vulnérabilité Nessus peuvent être intégrées dans QRadar SIEM en ajoutant un scanner Nessus à l'aide de l'icône VA Scanners sur l'onglet**Admin**. Après avoir ajouté votre client Nessus, vous pouvez ajouter un planning d'analyse pour récupérer les données de vulnérabilité sur une intervalle ponctuelle ou répétée. Pour en savoir plus sur le planning d'une analyse, voir **Planification d'un scanner**

REMARQUE

Nous vous recommandons de ne pas installer votre logiciel Nessus sur un système critique en raison des exigences élevées de l'unité centrale.

Cette section comprend les rubriques suivantes :

- **Ajout d'un scanner Nessus**
- **Modification d'un scanner Nessus**
- **Suppression d'un scanner Nessus**

Ajout d'un scanner Nessus

Le module du scanner Nessus pour QRadar SIEM fournit plusieurs types de collection pour la récupération de données de vulnérabilité depuis votre serveur Nessus.

Cette section comprend les rubriques suivantes :

- **Ajout de Nessus Scheduled Live Scan**
- **Ajout de Nessus Scheduled Results Import**
- **Ajout de Nessus Scheduled Live Scan à l'aide de XMLPRC API**
- **Ajout de Nessus Completed Report Import via le XMLRPC API**

REMARQUE

Nessus XMLRPC API n'est disponible que sur les serveurs Nessus et les clients qui utilisent le logiciel v4.2 et supérieur.

Ajout de Nessus Scheduled Live Scan

Une analyse opérationnelle peut être démarrée sur le serveur Nessus et permet d'importer les données relatives au résultat à partir d'un répertoire temporaire contenant les données de rapport d'analyse opérationnelle. A la fin de l'analyse, QRadar SIEM télécharge les données d'analyse à partir du répertoire temporaire et met à jour les informations relatives à la vulnérabilité de vos actifs.

Pour ajouter une analyse opérationnelle Nessus dans QRadar SIEM :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 4-1 Paramètres du scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez attribuer à ce scanner. Le nom peut comporter jusqu'à 255 caractères.
Description	Entrez une description pour ce scanner. La description peut comporter jusqu'à 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **Nessus Scanner**.

La liste des paramètres du type de scanner sélectionné s'affiche.

Etape 6 Dans la zone de liste **Collection Type**, sélectionnez **Scheduled Live Scan**.

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 4-2 Paramètres d'analyse planifiée pour Nessus

Paramètre	Description
Server Hostname	Entrez l'adresse IP ou le nom d'hôte du serveur Nessus comme indiqué par le client Nessus. Si le processus serveur et le client sont situés sur le même hôte, vous pouvez utiliser le système d'hôte local comme nom d'hôte du serveur.
Port du serveur	Entrez le numéro de port pour le serveur Nessus. Le numéro de port par défaut est 1241.
Server Username	Entrez le nom d'utilisateur Nessus utilisé par le client pour l'authentification du serveur.
Server Password	Entrez le mot de passe Nessus correspondant au nom d'utilisateur. ***Remarque :*** *Votre mot de passe de serveur Nessus ne doit pas contenir le caractère !. Ce caractère peut provoquer des échecs d'authentification via SSH.*
Client Temp Dir	Entrez le chemin d'accès au répertoire du client Nessus pouvant être utilisé par QRadar SIEM afin de stocker des fichiers temporaires. QRadar SIEM utilise un répertoire temporaire du client Nessus comme emplacement de lecture et d'écriture pour télécharger des cibles d'analyse et lire des résultats d'analyse. Les fichiers temporaires sont supprimés lorsque QRadar SIEM termine l'analyse et récupère les rapports d'analyse à partir du client Nessus. Le chemin d'accès au répertoire par défaut du client Nessus est /tmp.

Tableau 4-2 Paramètres d'analyse planifiée pour Nessus (suite)

Paramètre	Description
Nessus Executable	Entrez le chemin d'accès au répertoire du fichier exécutable Nessus sur le serveur qui héberge le client Nessus. Par défaut, le chemin d'accès au répertoire pour le fichier exécutable est **/usr/bin/nessus**.
Nessus Configuration File	Entrez le chemin d'accès au répertoire du fichier de configuration Nessus sur le client Nessus.
Client Hostname	Entrez le nom d'hôte ou l'adresse IP du système qui héberge le client Nessus.
Client SSH Port	Entrez le numéro de port SSH du serveur Nessus pouvant être utilisé afin de récupérer les fichiers du résultat d'analyse. Le numéro de port par défaut est 22.
Client Username	Entrez le nom d'utilisateur utilisé par QRadar SIEM pour authentifier la connexion SSH.
Client Password	Entrez le mot de passe correspondant à la zone **Client Username**. Cette zone est obligatoire si la case **Enable Key Authentication** est vide. Si la case Enable Key Authentication est activée, le paramètre de mot de passe est ignoré. ***Remarque :*** *Si le scanner est configuré pour utiliser un mot de passe, le serveur SSH auquel QRadar SIEM se connecte doit prendre en charge l'authentification par mot de passe. Si ce n'est pas le cas, l'authentification par SSH du scanner échoue. Assurez-vous que la ligne suivante s'affiche dans votre fichier de configuration sshd, qui est généralement disponible dans le répertoire /etc/ssh du serveur SSH :* **`PasswordAuthentication yes.`** *Si votre serveur de scanner n'utilise pas OpenSSH, la configuration peut différer. Pour en savoir plus, contactez votre fournisseur de scanner.*
Enable Key Authentication	Sélectionnez cette case pour activer une authentification par clé publique ou privée. Si la case est sélectionnée, QRadar SIEM tente d'authentifier la connexion SSH à l'aide de la clé privée fournie et la zone **SSH Password** est ignorée.

Etape 8 Pour configurer les plages du routage CIDR que le scanner doit prendre en considération :

a Dans la zone de texte, entrez la plage du routage CIDR que le scanner doit prendre en considération ou cliquez sur **Browse** pour sélectionner la plage du routage CIDR à partir de la liste réseaux.

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

Etape 10 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

Etape 11 Après avoir déployé les modifications, vous devez créer un planning d'analyse pour l'analyse opérationnelle.

Les rapports d'analyse peuvent être créés comme un événement ponctuel ou comme une importation planifiée qui se reproduit. Pour en savoir plus sur le planning d'une analyse, voir **Planification d'un scanner**.

Ajout de Nessus Scheduled Results Import

Une importation des résultats planifiés récupère des rapports d'analyse Nessus depuis un emplacement externe. L'emplacement externe peut être un serveur Nessus ou un référentiel de fichiers contenant un rapport d'analyse complet. QRadar SIEM se connecte à l'emplacement de vos rapports d'analyse à l'aide de SSH importe des fichiers de rapports d'analyse complets depuis le répertoire distant en utilisant l'expression régulière ou un maximum d'âge de rapports à filtrer pour vos rapports d'analyse. QRadar SIEM prend en charge l'importation de rapports d'analyse Nessus (.Nessus) ou des rapports d'analyse exportés sous un format de sortie Nessus, tel que XML.

Pour ajouter une importation de résultats planifiés Nessus dans QRadar SIEM :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 4-3 Paramètres du scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez attribuer à ce scanner. Le nom peut comporter jusqu'à 255 caractères.
Description	Entrez une description pour ce scanner. La description peut comporter jusqu'à 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **Nessus Scanner**.

La liste des paramètres du type de scanner sélectionné s'affiche.

Etape 6 Dans la zone de liste **Collection Type**, sélectionnez **Scheduled Results Import.**

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 4-4 Paramètres Nessus Scheduled Results Import

Paramètre	Description
Remote Results Hostname	Entrez l'adresse IP, le nom d'hôte du client Nessus ou le nom du serveur qui héberge vos fichiers de résultat d'analyse XML.
Remote Results SSH Port	Entrez le numéro de port SSH du serveur Nessus pouvant être utilisé afin de récupérer les fichiers du résultat d'analyse. Le numéro de port par défaut est 22.
SSH Username	Entrez un nom d'utilisateur pouvant être utilisé par QRadar SIEM pour authentifier la session SSH à l'aide du serveur Nessus.
SSH Password	Entrez le mot de passe correspondant au nom d'utilisateur SSH. ***Remarque :*** *Votre mot de passe de serveur Nessus ne doit pas contenir le caractère !. Ce caractère peut provoquer des échecs d'authentification via SSH.*
Enable Key Authentication	Sélectionnez cette case pour activer une authentification par clé publique ou privée. Si la case est sélectionnée, QRadar SIEM tente d'authentifier la connexion SSH à l'aide de la clé privée fournie et la zone **SSH Password** est ignorée.
Remote Results Directory	Entrez le chemin d'accès au répertoire contenant les fichiers du rapport d'analyse Nessus du client Nessus. Le chemin d'accès au répertoire utilise./ comme valeur par défaut.
Remote Results File Pattern	Entrez le modèle de fichier à l'aide d'une expression régulière (regex), pour les fichiers de résultats d'analyse que vous tentez d'importer. Par défaut, le modèle de fichier suivant est inclus pour les fichier Nessus :.***\.nessus**. Si vous utilisez un masque de sortie pour exporter votre rapport d'analyse dans un autre format Nessus pris en charge, tel que XML, vous devez en conséquence mettre à jour l'expression regex pour le modèle de fichier. ***Remarque :*** *Si vous mettez à jour l'expression regex dans la zone* ***Remote Results File Pattern*** *, vous devez mettre en évidence les changements pour la mise à jour de votre configuration de scanner.*
Results File Max Age (Days)	Entrez la durée de validité maximale du fichier à inclure au moment d'importer les fichiers de résultats d'analyse Nessus lors d'une analyse planifiée. Par défaut, la durée de validé maximale du fichier de résultats est 7 jours. Les fichiers ayant une durée de validité supérieure au nombre de jours indiqué et d'horodatage sont exclus du processus d'importation des résultats.

Etape 8 Pour configurer les plages du routage CIDR que ce scanner doit prendre en considération :

a. Dans la zone de texte, entrez la plage du routage CIDR que ce scanner doit prendre en considération ou cliquez sur **Browse** pour sélectionner la plage du routage CIDR à partir de la liste réseaux.

b. Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

Etape 10 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

Etape 11 Après avoir déployé les modifications, vous devez créer un planning d'analyse pour importer les données de vulnérabilité.

Les rapports d'analyse peuvent être créés comme un événement ponctuel ou comme une importation planifiée qui se reproduit. Pour en savoir plus sur le planning d'une analyse, voir **Planification d'un scanner**.

Ajout de Nessus Scheduled Live Scan à l'aide de XMLPRC API

XMLRPC API permet à QRadar SIEM de démarrer une analyse opérationnelle préconfigurée sur votre serveur Nessus. Pour démarrer une analyse opérationnelle depuis QRadar SIEM vous devez indiquer le nom de la politique des données d'analyse opérationnelle que vous souhaitez récupérer. Au fur et à mesure que l'analyse progresse, vous pouvez placer le curseur de votre souris sur le scanner Nessus dans la fenêtre Scheduling pour visualiser le pourcentage de l'analyse qui est terminée. A la fin de l'analyse opérationnelle, QRadar SIEM utilise XMLRPC API pour récupérer les données d'analyse et mettre à jour les informations de vulnérabilité de vos actifs.

REMARQUE

Nessus XMLRPC API n'est disponible que sur les serveurs Nessus et les clients qui utilisent le logiciel v4.2 et version supérieure.

Pour ajouter une analyse opérationnelle Nessus XMLRPC API dans QRadar SIEM:

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 4-5 Paramètres du scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez attribuer à ce scanner. Le nom peut comporter jusqu'à 255 caractères.

Tableau 4-5 Paramètres du scanner (suite)

Paramètre	Description
Description	Entrez une description pour ce scanner. La description peut comporter jusqu'à 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **Nessus Scanner**.

La liste des paramètres du type de scanner sélectionné s'affiche.

Etape 6 Dans la zone de liste **Collection Type**, sélectionnez **Scheduled Live Scan - XMLRPC API**.

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 4-6 Paramètres d'interface API XMLRPC pour les importations planifiées

Paramètre	Description
Hostname	Entrez l'adresse IP ou le nom d'hôte du serveur Nessus.
Port	Entrez le numéro de port QRadar SIEM afin d'accéder au serveur Nessus à l'aide de l'interface API XMLRPC. Le numéro de port par défaut est 8834.
Username	Entrez le nom d'utilisateur requis pour accéder au serveur Nessus.
Password	Entrez le mot de passe correspondant au nom d'utilisateur.
Scan Name	Facultatif. Entrez le nom d'analyse que vous souhaitez afficher au moment de l'exécution de l'analyse sur le serveur Nessus. Si cette zone est zone vide, l'interface API tente de démarrer une analyse optionnelle pour “QRadar Scan”. ***Remarque :*** *QRadar SIEM ne prend pas en charge l'utilisation du signe (&) dans cette zone.*

Tableau 4-6 Paramètres d'interface API XMLRPC pour les importations planifiées (suite)

Paramètre	Description
Policy Name	Entrez le nom de la règle sur votre serveur Nessus pour démarrer une analyse opérationnelle. La règle que vous définissez doit exister sur le serveur Nessus lorsque QRadar SIEM tente de lancer l'analyse. Si la règle n'existe pas, un message d'erreur s'affiche dans la partie d'état lorsque QRadar SIEM tente de démarrer l'analyse opérationnelle. Dans la plupart des cas le nom de la règle est adapté à votre serveur Nessus, mais plusieurs règles par défaut sont incluses sous Nessus. Par exemple, • Analyse réseau externe • Analyse réseau interne • Tests d'application Web • Préparation aux audits PCI DSS Pour en savoir plus sur les règles, contactez votre fournisseur Nessus.

Etape 8 Pour configurer les plages de routage CIDR que cette analyse doit prendre en considération :

a Dans la zone de texte, entrez la plage de routage CIDR que ce scanner doit prendre en considération ou cliquez sur **Browse** pour sélectionner la plage de routage CIDR à partir de la liste réseaux.

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

Etape 10 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

Etape 11 Après que les changements aient été déployés, vous devez créer un analyse planifiée pour votre analyse opérationnelle.

Les rapports d'analyse peuvent être créés en tant qu'événement unique ou en tant qu'importation planifiée récurrente. Pour en savoir plus sur le planning d'analyse, voir **Planification d'un scanner**.

Ajout de Nessus Completed Report Import via le XMLRPC API

L'importation des résultats planifiés via l'utilisation de XMLRPC API permet à QRadar SIEM de récupérer les rapports complets d'analyse Nessus à partir du serveur Nessus. QRadar SIEM se connecte à votre serveur Nessus et télécharge les données de tous les rapports complets qui correspondent aux filtre du nom du rapport et de l'age maximal des rapports.

REMARQUE

Nessus XMLRPC API est uniquement disponible sur les serveurs et les clients Nessus via l'utilisation du logiciel v4.2 et plus.

Pour ajouter une importation d'analyse Nessus complète dans QRadar SIEM :

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 4-7 Paramètres du scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez attribuer à ce scanner. Le nom peut comporter jusqu'à 255 caractères.
Description	Entrez une description pour ce scanner. La description peut comporter jusqu'à 255 caractères.
Hôte géré	Dans la zone de liste, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **Nessus Scanner**.

La liste des paramètres du type de scanner sélectionné s'affiche.

Etape 6 Dans la zone de liste **Collection Type**, sélectionnez **Scheduled Completed Report Import - XMLRPC API**.

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 4-8 Paramètres d'interface API XMLRPC pour les importations planifiées

Paramètre	Description
Hostname	Entrez l'adresse IP, le nom d'hôte du client Nessus ou le nom du serveur qui héberge vos fichiers de résultat d'analyse XML.
Port	Entrez le numéro de port QRadar SIEM afin d'accéder au serveur Nessus à l'aide de l'interface API XMLRPC. Le numéro de port par défaut est 8834.
Username	Entrez le nom d'utilisateur requis pour accéder au serveur Nessus.
Password	Entrez le mot de passe correspondant au nom d'utilisateur.

Tableau 4-8 Paramètres d'interface API XMLRPC pour les importations planifiées (suite)

Paramètre	Description
Report Name Filter	Entrez le modèle de fichier à l'aide d'une expression régulière (regex), pour les fichiers de résultats d'analyse que vous tentez d'importer. Par défaut, le modèle de fichier suivant est inclus afin de collecter tous les rapports d'analyse disponibles :.*****. ***Remarque :*** *Si vous mettez à jour l'expression regex dans la zone* ***Report Name Filter****, vous devez déployer les modifications pour mettre à jour votre configuration de scanner.*
Results File Max Age (Days)	Entrez la durée de validité maximale du fichier à inclure au moment d'importer les fichiers de résultats d'analyse Nessus lors d'une analyse planifiée. Par défaut, la durée de validé maximale du fichier de résultats est 7 jours. Les fichiers ayant une durée de validité supérieure au nombre de jours indiqué et d'horodatage sont exclus du processus d'importation des résultats.

Etape 8 Pour configurer les plages de routage CIDR que cette analyse doit prendre en considération :

a Dans la zone de texte, entrez la plage de routage CIDR que ce scanner doit prendre en considération ou cliquez sur **Browse** pour sélectionner la plage de routage CIDR à partir de la liste réseaux.

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

Etape 10 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

Etape 11 Après que les changements aient été déployés, vous devez créer un planning d'analyse pour importer les données du rapport d'analyse.

Les rapports d'analyse peuvent être créés en tant qu'événement unique ou en tant qu'importation planifiée récurrente. Pour en savoir plus sur le planning d'analyse, voir **Planification d'un scanner**.

Modification d'un scanner Nessus

Pour modifier la configuration d'un scanner Nessus dans QRadar SIEM:

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez modifier.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Mettez à jour les paramètres, si nécessaire.

- Pour les paramètres Scheduled Live Scan, voir **Tableau 4-2**.
- Pour les paramètres Scheduled Results Import, voir **Tableau 4-4**.
- Pour les paramètres Schedule Live Scan XMLRPC API, voir **Tableau 4-6**.
- Pour les paramètres Scheduled Completed Report Import XMLRPC API, voir **Tableau 4-8**.

Etape 7 Cliquez sur **Save**.

Etape 8 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Suppression d'un scanner Nessus

Pour supprimer un scanner Nessus de QRadar SIEM:

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners**.

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez **OK**.

Etape 7 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

7 GESTION DES SCANNERS NMAP

Vous pouvez intégrer des scanners Network Mapper (Nmap) à QRadar SIEM. QRadar SIEM utilise SSH pour communiquer avec le serveur de scanner, démarrer des analyses distants Nmap et télécharger des résultats d'analyse. QRadar SIEM prend en charge deux méthodes d'importation de données de vulnérabilité Nmap :

- **Remote Live Scan** - permet à QRadar SIEM de se connecter à un scanner Nmap et de lancer une analyse à l'aide du fichier binaire Nmap. QRadar SIEM surveille l'état du processus d'analyse et attend que le serveur Nmap termine l'analyse. Une fois l'analyse terminée, QRadar SIEM télécharge les résultats de vulnérabilité à l'aide de SSH.

  Plusieurs types d'analyse de port Nmap nécessitent Nmap pour s'exécuter en tant que root. Par conséquent, QRadar SIEM doit avoir accès en tant que root ou vous devez vider la case **OS Detection**. Pour exécuter des analyses Nmap avec **OS Detection** activé, vous devez fournir à QRadar SIEM un accès root ou configurer le fichier binaire Nmap avec setuid root. Pour obtenir une assistance, contactez votre administrateur Nmap.
- **Remote Results Import** - Permet à QRadar SIEM de se connecter à un scanner Nmap à l'aide de SSH et de télécharger des fichiers de résultat d'analyse stockés dans un dossier distant du scanner Nmap. QRadar SIEM importe uniquement des résultats distants stockés au format XML. Lors de la configuration de votre scanner Nmap afin de générer un fichier pour l'importation de QRadar SIEM, vous devez générer le fichier de résultats à l'aide de l'option `-oX <file>`.

  D'où `<file>` est le chemin d'accès permettant de créer et de stocker les résultats d'analyse XML formatés sur votre scanner Nmap.

Une fois que vous avez ajouté et configuré soit Remote Live Scan, soit Remote Results Import sous QRadar SIEM, vous pouvez programmer la fréquence à laquelle QRadar SIEM importe les données de vulnérabilité. Pour plus d'informations, voir **Managing Scan Schedules**.

Cette section fournit des informations sur les éléments suivants :

Ajout d'une analyse Nmap Remote Live Scan

L'ajout d'une analyse Remote Live Scan permet à QRadar SIEM de lancer une analyse Nmap, d'attendre qu'elle se termine, puis d'importer les résultats. Après avoir ajouté une analyse opérationnelle, vous devez affecter un planning d'analyse à QRadar SIEM. Le planning d'analyse détermine la fréquence à laquelle QRadar SIEM lance des analyses opérationnelles sur votre scanner Nmap et récupère des données de vulnérabilité pour vos actifs.

Pour ajouter une analyse Remote Live Scan Nmap :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 5-1 Paramètres du scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez attribuer à ce scanner. Le nom peut comporter jusqu'à 255 caractères.
Description	Entrez une description pour ce scanner. La description peut comporter jusqu'à 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **Nmap Scanner**.

La liste de paramètres pour le type de scanner sélectionné s'affiche.

Etape 6 Dans la zone de liste **Scan Type**, sélectionnez **Remote Live Scan**.

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 5-2 Paramètres Nmap Live Scan

Paramètre	Description
Server Hostname	Entrez le nom d'hôte ou l'adresse IP du système distant hébergeant le client Nmap. Nous vous recommandons d'utiliser un système UNIX qui exécute SSH.
Server Username	Entrez le nom d'utilisateur requis pour accéder au système distant hébergeant le client Nmap à l'aide de SSH.

Tableau 5-2 Paramètres Nmap Live Scan (suite)

Paramètre	Description
Enable Key Authentication	Sélectionnez cette case pour permettre à QRadar SIEM d'utiliser une authentification par clé publique ou privée. Lorsque vous sélectionnez cette case, spécifiez le chemin de répertoire de votre clé dans QRadar SIEM à l'aide de la zone **Private Key File**. Par défaut, la case est vide.
Login Password	Entrez le mot de passe associé au nom d'utilisateur dans la zone **Server Username**.
Private Key File	Entrez le chemin d'accès au fichier contenant les informations sur la clé privée. Cette zone s'affiche uniquement si la case **Enable Key Authentication** sélectionnée. Si vous utilisez une authentification par clé basée sur SSH, QRadar SIEM utilise la clé privée pour authentifier la connexion SSH. Le répertoire par défaut est /opt/qradar/conf/vis.ssh.key. Cependant, ce fichier n'existe pas par défaut. Vous devez créer le fichier de clé vis.ssh.ou entrer un autre nom de fichier. Ce paramètre est obligatoire si la case **Enable Key Authentication** est sélectionnée, sinon il est ignoré.
Nmap Executable	Entrez le chemin de répertoire complet et le nom de fichier du fichier exécutable pour le fichier binaire Nmap. Le répertoire par défaut du fichier exécutable est /usr/bin/Nmap.
Disable Ping	Dans certains réseaux, le protocole ICMP est partiellement ou complètement désactivé. Dans les cas où ICMP n'est pas activé, vous pouvez sélectionner cette case pour permettre aux pings ICMP d'améliorer la précision de l'analyse. Par défaut, la case est vide.
OS Detection	OS Detection permet à Nmap d'identifier le système d'exploitation d'un périphérique ou d'un appareil dans le réseau cible. Par défaut, la case OS Detection est sélectionnée. Les options comprennent : **Selected** - Si vous sélectionnez la case **OS Detection**, vous devez fournir un nom d'utilisateur et un mot de passe avec des privilèges root dans les zones **Server Username** et **Login Password**. **Cleared** - Si la case **OS Detection** est vide et les résultats renvoyés ne contiennent pas d'informations sur le système d'exploitation. Les zones **Server Username** et **Login Password** ne nécessitent pas de privilèges root.

Tableau 5-2 Paramètres Nmap Live Scan (suite)

Paramètre	Description
Max RTT Timeout	Sélectionnez le délai maximal d'aller-retour (RTT) dans la zone de liste. Le délai d'attente détermine si une analyse doit être arrêtée ou réexécutée en raison du temps d'attente entre le scanner et la cible d'analyse. La valeur par défaut est de 300 millisecondes (ms). ***Note:*** *Si vous entrez 50 millisecondes comme temps d'aller-retour maximal, il est recommandé que les périphériques en cours d'analyse soient situés sur un réseau local. Si vous analysez des périphériques situés sue des réseaux distants, il est recommandé de sélectionner 1 seconde comme valeur maximale.*

REMARQUE

Si le scanner est configuré pour utiliser un mot de passe, le serveur du scanner SSH auquel QRadar SIEM se connecte doit prendre en charge l'authentification par mot de passe. Si ce n'est pas le cas, l'authentification par SSH pour le scanner échoue. Assurez-vous que la ligne suivante s'affiche dans votre fichier de configuration sshd, qui est généralement disponible dans le répertoire /etc/ssh du serveur SSH : `PasswordAuthentication yes.` Si votre serveur de scanner n'utilise pas OpenSSH, la configuration peut différer. Pour en savoir plus, contactez votre fournisseur de scanner.

Etape 8 Pour configurer le routage CIDR que ce scanner doit prendre en considération :

a Dans la zone de texte, entrez le routage CIDR ou cliquez sur **Browse** pour sélectionner le routage CIDR à partir de la liste réseaux.

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

Etape 10 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Vous pouvez maintenant ajouter un planning d'analyse pour déterminer la fréquence à laquelle QRadar SIEM lance une analyse opérationnelle sur votre scanner Nmap. QRadar SIEM peut importer des données de vulnérabilité uniquement si l'analyse est terminée. Pour en savoir plus sur le planning d'analyse, voir **Gestion des plannings d'analyse**.

Ajout d'une analyse Nmap Remote Results Import Scan

L'ajout d'un scanner Remote Results Import Nmap vous permet de générer et de stocker des analyses sur votre scanner Nmap. Les analyses doivent être générées au format XML à l'aide de la commande -oX <file> de votre scanner Nmap. Après avoir ajouté et configuré votre scanner Nmap, vous devez affecter un planning d'analyse pour indiquer la fréquence à laquelle QRadar SIEM importe des analyses Nmap.

Pour ajouter une importation de résultats distants Nmap :

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

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

La fenêtre Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 définit les valeurs des paramètres suivants:

Tableau 5-3 Paramètres du scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez attribuer à ce scanner. Le nom peut comporter jusqu'à 255 caractères.
Description	Entrez une description pour ce scanner. La description peut comporter jusqu'à 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **Nmap Scanner**.

La liste de paramètres pour le type de scanner sélectionné s'affiche.

Etape 6 Dans la zone de liste **Scan Type**, sélectionnez **Remote Results Import**.

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 5-4 Paramètres Nmap Nmap Remote Results Import

Paramètre	Description
Server Hostname	Entrez le nom d'hôte ou l'adresse IP du système distant hébergeant le client Nmap. Nous vous recommandons d'utiliser un système UNIX qui exécute SSH.
Server Username	Entrez le nom d'utilisateur requis pour accéder au système distant hébergeant le client Nmap.
Enable Key Authentication	Sélectionnez cette case pour permettre à QRadar SIEM d'utiliser une authentification par clé publique ou privée. Lorsque vous sélectionnez cette case, spécifiez le chemin de répertoire de votre clé dans QRadar SIEM à l'aide de la zone **Private Key File**. Par défaut, la case est vide.
Login Password	Entrez le mot de passe associé au nom d'utilisateur dans la zone **Server Username**.

Tableau 5-4 Paramètres Nmap Nmap Remote Results Import (suite)

Paramètre	Description
Private Key File	Entrez le chemin d'accès au fichier contenant les informations sur la clé privée. Cette zone s'affiche uniquement si la case **Enable Key Authentication** est sélectionnée. Si vous utilisez une authentification par clé basée sur SSH, QRadar SIEM utilise la clé privée pour authentifier la connexion SSH. Le répertoire par défaut est /opt/qradar/conf/vis.ssh.key. Cependant, ce fichier n'existe pas par défaut. Vous devez créer le fichier de clés vis.ssh. ou entrer un autre nom de fichier. Ce paramètre est obligatoire si la case **Enable Key Authentication** est sélectionnée, sinon il est ignoré.
Remote Folder	Entrez le chemin d'accès au scanner Nmap contenant des données de vulnérabilité XML.
Remote File Pattern	Entrez un modèle d'expression régulière (regex) pour déterminer les fichiers de résultats Nmap XML à inclure dans le rapport d'analyse. Tous les noms de fichier correspondant au modèle regex sont inclus lors de l'importation du rapport d'analyse de vulnérabilité. Vous devez utiliser un modèle regex valide dans la zone. Par exemple, le modèle suivant importe tous les fichiers XML situés dans le dossier distant : `.*\.xml` ***Note:*** *Les rapports d'analyse importés et traités par QRadar SIEM ne sont pas supprimés du dossier distant. Nous vous recommandons de planifier une tâche cron afin de supprimer les rapports d'analyse précédemment traités sur une base planifiée.*

REMARQUE

Si le scanner est configuré pour utiliser un mot de passe, le serveur du scanner SSH auquel QRadar SIEM se connecte doit prendre en charge l'authentification par mot de passe. Si ce n'est pas le cas, l'authentification par SSH pour le scanner échoue. Assurez-vous que la ligne suivante s'affiche dans votre fichier de configuration sshd, qui est généralement disponible dans le répertoire /etc/ssh du serveur SSH : `PasswordAuthentication yes.` Si votre serveur de scanner n'utilise pas OpenSSH, la configuration peut différer. Pour en savoir plus, consultez votre fournisseur de scanner.

Etape 8 Pour configurer le routage CIDR que ce scanner doit prendre en considération :

a Dans la zone de texte, entrez l'intervalle CIDR dont vous souhaitez que ce scanner prenne en considération ou cliquez sur **Browse** pour sélectionner l'intervalle CIDR à partir de la liste réseaux.

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

Etape 10 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Vous pouvez maintenant ajouter un planning d'analyse pour déterminer la fréquence à laquelle QRadar SIEM importe des rapports d'analyse XML formatés sur votre scanner NMap. Pour en savoir plus sur le planning d'une analyse, voir **Gestion des plannings d'analyse**.

Modification d'un scanner Nmap

Pour modifier un scanner Nmap :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez modifier.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Paramètres de mise à jour, si nécessaire.

- Pour les paramètres Nmap Live Scan, voir **Tableau 5-2**.
- Pour les paramètres Nmap Remote Results Import, voir **Tableau 5-4**.

Etape 7 Cliquez sur **Save**.

Etape 8 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Suppression d'un scanner Nmap

Pour supprimer un scanner Nmap :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez sur **OK**.

Etape 7 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

8 MANAGING QUALYS SCANNERS

IBM Security QRadar SIEM récupère les informations de vulnérabilité des scanners Qualys de deux manières différentes ; via Qualys Application Programming Interface (API) et en téléchargeant les rapports d'analyse générés par les diispositifs QualysGuard. La vulnérabilité QualysGuard et les informations d'actifs sont prises en charge sur les diispositifs QualysGuard via l'utilisation du logiciel version 4.7 to 7.2.

QRadar SIEM offre deux modules de scanner pour la récupération des données Qualys :

- **Qualys Detection Scanner** - Le module Qualys Detection Scanner accède aux données de vulnérabilité via l'utilisation de Qualys Host List Detection API de l'diispositif QualysGuard. Qualys Detection Scanner vous permet de récupérer des résultats à travers plusieurs rapports d'analyse afin de collecter les données de vulnérabilité. Le module Qualys Detection Scanner pour QRadar SIEM exige que vous indiquiez un utilisateur Qualys pouvant télécharger Qualys KnowledgeBase.

  Pour plus d'informations sur Qualys Detection Scanner, voir **Configuration de Qualys Detection Scanner**.

- **Qualys Scanner** - Le module Qualys Scanner accède aux rapport d'analyse de l'actif et de vulnérabilité via le serveur Web distant de l'diispositif QualysGuard via l'utilisation d'une connexion HTTPS.

  Pour plus d'informations sur Qualys Detection Scanner, voir **Configuration d'un Scanner Qualys**

Après avoir configuré le module Qualys Detection Scanner ou Qualys Scanner dans QRadar SIEM, vous pouvez planifier une analyse dans QRadar SIEM afin de collecter les vulnérabilités via l'utilisation d'API ou en téléchargeant le rapport d'analyse. Les plannings d'analyse vous permettent de planifier la fréquence de mise à jour de QRadar SIEM avec les données de vulnérabilité à partir des diispositifs de vulnérabilité externes, telles que Qualys Vulnerability Manager. Pour plus d'informations, voir **Gestion des plannings d’analyse**.

Cette section fournit des informations sur les éléments suivants :

- **Configuration de Qualys Detection Scanner**
- **Configuration d'un Qualys Scanner**

Configuration de Qualys Detection Scanner

Qualys Detection Scanner utilise l'interface de programme d'application QualysGuard Host Detection List pour analyser plusieurs rapports d'analyse afin de collecter les données de vulnérabilité des actifs. Les données renvoyées contiennent la vulnérabilité comme numéro d'identification, que QRadar SIEM compare par rapport la dernière version de Qualys Vulnerability Knowledge Base. Qualys Detection Scanner ne prend pas en charge les analyses opérationnelles mais autorise Qualys Detection Scanner à récupérer les informations de vulnérabilité regroupées à travers plusieurs rapports d'analyse. QRadar SIEM prend en charge les paramètres de recherche essentiels, tels que les zones **Operating System Filter** et **Asset Group Name**.

Qualys Detection Scanner fournit également une option permettant de configurer la fréquence de récupération et de mise en cache de Qualys par Vulnerability Knowledge Base par QRadar SIEM. Il s'agit de la zone **Qualys Vulnerability Retention Period**. Pour forcer QRadar SIEM à mettre à jour Qualys Vulnerability Knowledge Base pour chaque analyse planifiée, Qualys Detection Scanner comprend une case à cocher **Force Qualys Vulnerability Update**. Le compte utilisateur Qualys que vous indiquez pour QRadar SIEM doit disposer d'autorisations activées pour télécharger Qualys KnowledgeBase. Pour plus d'informations, voir votre documentation Qualys.

Ajout de Qualys Detection Scanner

Pour ajouter Qualys Detection Scanner vers QRadar SIEM :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 6-1 Paramètres QualysDetection Scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez affecter à scanner. Le nom peut contenir plus de 255 caractères.
Description	Entrez une description pour ce scanner. La description peut contenir plus de 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **Qualys Detection Scanner**.

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 6-2 Paramètres QualysDetection Scanner

Paramètre	Description
Qualys Server Host Name	Entrez le nom de domaine complet ou l'adresse IP de la console de gestion QualysGuard en fonction de votre emplacement. En spécifiant le nom de domaine complet, vous devez entrer le nom d'hôte et non l'adresse URL. Par exemple : • Entrez **`qualysapi.qualys.com`** pour un serveur QualysGuard se trouvant aux États-Unis. • Entrez **`qualysapi.qualys.eu`** pour un serveur hôte du serveur QualysGuard se trouvant en Europe. • Entrez **`qualysapi.<management_console>`** si vous utilisez l'infrastructure de numérisation complète comprenant une console de gestion interne, où <management_console> **`est le nom d'hôte de votre dispositif de gestion interne.`**
Qualys Username	Entrez le nom d'utilisateur nécessaire pour des demandes d'analyse. Il s'agit du même nom d'utilisateur utilisé pour se connecter au serveur Qualys. ***Remarque :*** *L'utilisateur que vous indiquez doit avoir un accès pour télécharger Qualys KnowledgeBase ou vous devez activer le compte utilisateur avec l'option pour télécharger Qualys KnowledgeBase. Pour plus d'informations, voir votre documentation Qualys.*
Qualys Password	Entrez le mot de passe correspondant au nom d'utilisateur Qualys.
Filtre de système d'exploitation	Entrez l'expression régulière obligatoire pour filtrer les données renvoyées par le système d'exploitation. Le champ **Operating System Filter** contient.***** comme étant l'expression régulière par défaut et correspondant à tous les systèmes d'exploitation. Si vous entrez une expression régulière non valide dans le champ **Operating System Filter**, l'analyse échoue pendant que QRadar SIEM initialise le scanner. Pour afficher le message d'erreur à partir d'un échec d'analyse, déplacez votre souris sur le texte dans la colonne **Status**.

Tableau 6-2 Paramètres QualysDetection Scanner (suite) (suite)

Paramètre	Description
Noms du groupe de fichiers métadonnées	Entrez une liste séparée par des virgules, sans espace pour analyser les adresses IP via leur nom de groupe de fichiers métadonnées. Un groupe de fichiers métadonnées est un nom fourni par un utilisateur dans l'interface de gestion Qualys pour identifier une liste ou une plage d'adresses IP. Par exemple, un groupe de fichiers métadonnées intitulé Building1 peut contenir l'adresse IP 192.168.0.1. Un groupe de fichiers métadonnées intitulé Webserver peut contenir 192.168.255.255. Dans QRadar SIEM, pour récupérer des informations de vulnérabilité, à la fois de ces deux actifs, entrez **Building1,Webserver** sans espace dans le champ **Asset Group Names**. Une fois l'analyse terminée, l'onglet **Asset** dans QRadar SIEM affiche les vulnérabilités via leur adresse IP. Pour l'exemple ci-dessus, QRadar SIEM affiche toutes les vulnérabilités pour les actifs 192.168.0.1 et 191.168.255.255.
Host Scan Time Filter (days)	Entrez une valeur numérique (en jours) pour créer un filtre pour la dernière fois que l'hôte a été analysé. Les temps d'analyse hôte qui sont plus anciens que le nombre de jours indiqué sont exclus des résultats renvoyés par Qualys.
Qualys Vulnerability Retention Period (days)	Entrez le nombre de jours pour lesquels vous souhaitez enregistrer localement Qualys Vulnerability Knowledge Base dans QRadar SIEM. Le nombre par défaut est de 7 jours. Si une analyse est planifiée et la durée de conservation expirée, QRadar SIEM télécharge une mise de jour de Qualys Vulnerability Knowledge Base.
Force Qualys Vulnerability Update	Sélectionnez cette case à cocher pour obliger QRadar SIEM à récupérer et à cacher la version la plus récente de Qualys Vulnerability Knowledge Base. Si cette case est sélectionnée, la durée de conservation est définie à conversation zéro et chaque analyse planifiée récupère Qualys Vulnerability Knowledge Base.
Use Proxy	Sélectionnez cette case à cocher si votre scanner exige un proxy pour la communication ou l'authentification.
Proxy Host Name	Entrez le nom d'hôte ou l'adresse IP de votre serveur proxy si votre scanner exige un proxy.
Proxy Port	Entrez le numéro de port de votre serveur proxy si votre scanner exige un proxy.
Proxy Username	Entrez le nom d'utilisateur de votre serveur proxy si votre scanner exige un proxy.
Proxy Password	Entrez le mot de passe de votre serveur proxy si votre scanner exige un proxy.

Etape 7 Pour configurer les plages du routage CIDR que le scanner doit prendre en considération :

a. Dans la zone de texte, entrez la plage du routage CIDR que le scanner doit prendre en considération ou cliquez sur **Browse** pour sélectionner la plage du routage CIDR à partir de la liste réseaux.

b. Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

Etape 9 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Vous êtes prêt à configurer un planning d'analyse pour déterminer la fréquence avec laquelle QRadar SIEM collecte les informations du scanner Qualys Detection. Pour plus d'informations, voir **Gestion des plannings d'analyse**.

Modification de Qualys Detection Scanner

Pour modifier une configuration Qualys Detection Scanner dans QRadar SIEM :

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le nom du scanner que vous souhaitez modifier.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Mettez à jour les paramètres, si nécessaire. Voir **Tableau 6-2**.

Etape 7 Cliquez sur **Save**.

Etape 8 Choisissez l'une des options de déploiement suivantes :

- Si vous effectuez la reconfiguration de Qualys Detection Scanner sans mettre à jour les données d'identification du proxy Qualys Detection Scanner, cliquez sur **Deploy Changes** dans le menu de l'onglet de navigation **Admin**.
- Si vous effectuez la reconfiguration de votre Qualys Detection Scanner et mettez à jour les données d'identification dans la zone **Proxy Username** ou **Proxy Password**, sélectionnez **Advanced > Deploy Full Configuration** à partir du menu de navigation de l'onglet **Admin**.

ATTENTION

*La sélection de **Deploy Full Configuration** redémarre les services QRadar SIEM, produisant ainsi un écart dans la collecte des données d'événements et de flux jusqu'à la fin du déploiement.*

Les modifications apportées à votre scanner Qualys sont terminées.

Suppression de Qualys Detection Scanner

Pour supprimer un scanner Qualys à partir de QRadar SIEM :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez sur **OK**.

Etape 7 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Le scanner Qualys Detection est supprimé de la liste de scanner.

Configuration d'un Scanner Qualys

Le module Qualys Scanner télécharge et analyse les rapports d'analyse à partir du dispositif Qualys. Si vous sélectionnez Qualys Scanner, QRadar SIEM doit accéder au serveur Web distant via une connexion HTTPS pour récupérer les rapports d'analyse. Le module Qualys Scanner prend en charge trois méthodes de collecte de données d'analyse sur Qualys. Les options d'analyse pour un scanner Qualys comprennent :

- Démarrage d'une analyse opérationnelle sur Qualys et collecte complète de données d'analyse.
- Planification d'importations de rapports complets de données d'analyse.
- Planification d'importations de rapports d'analyse complets.

Cette section comprend les rubriques suivantes :

ATTENTION

*Si vous mettez votre Qualys Scanner à niveau à partir d'une version VIS-QualysQualysGuard-7.0-259655 moins récente, vous devez vérifier le paramètre **Collection Type** dans la fenêtre Add Scanner de toutes les configurations Qualys Scanner existantes dans QRadar SIEM.*

Ajout de Qualys Live Scan

Les analyses opérationnelles permettent à QRadar SIEM de lancer des analyses préconfigurées sur Qualys Scanner et de collecter les résultats d'analyse à la fin de l'analyse opérationnelle.

Pour ajouter une analyse opérationnelle Qualys dans QRadar SIEM :

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 6-3 Paramètres du scanner Qualys

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez attribuer à ce scanner. Le nom peut contenir plus de 255 caractères.
Description	Entrez une description pour ce scanner. La description peut contenir plus de 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **Qualys Scanner**.

Etape 6 Dans la zone de liste **Collection Type**, sélectionnez **Scheduled Live - Scan Report**.

Les options de configuration pour le lancement d'une analyse opérationnelle sur votre serveur Qualys s'affichent.

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 6-4 Paramètres Live Scan de Qualys

Paramètre	Description
Qualys Server Host Name	Entrez le nom de domaine complet ou l'adresse IP de la console de gestion QualysGuard en fonction de votre emplacement. En spécifiant le nom de domaine complet, vous devez entrer le nom d'hôte et non l'adresse URL. Par exemple : • Entrez **`qualysapi.qualys.com`** pour un serveur QualysGuard se trouvant aux États-Unis. • Entrez **`qualysapi.qualys.eu`** pour un serveur QualysGuard se trouvant en Europe. • Entrez **`qualysapi.<management_console>`** si vous utilisez l'infrastructure de numérisation complète comprenant une console de gestion interne, où <management_console> **`est le nom d'hôte de votre dispositif de gestion interne.`**
Qualys Username	Entrez le nom d'utilisateur nécessaire pour des demandes d'analyse. Il s'agit du même nom d'utilisateur utilisé pour se connecter au serveur Qualys.
Qualys Password	Entrez le mot de passe correspondant au nom d'utilisateur Qualys.
Use Proxy	Sélectionnez cette case à cocher si QRadar SIEM exige un serveur proxy pour communiquer avec votre scanner Qualys. Par défaut, cette case est désélectionnée. Cette case affiche les paramètres supplémentaires de configuration de proxy.

Tableau 6-4 Paramètres Live Scan de Qualys (suite)

Paramètre	Description
Proxy Host Name	Entrez le nom d'hôte ou l'adresse de votre serveur proxy.
Proxy Port	Entrez le numéro de port de votre serveur proxy.
Proxy Username	Entrez un nom d'utilisateur permettant à QRadar SIEM de s'authentifier avec votre serveur proxy.
Proxy Password	Entrez le mot de passe associé au champ **Proxy Username**.
Scanner Name	Entrez le nom du scanner dont vous souhaitez effectuer l'analyse, tel qu'il s'affiche sur le serveur QualysGuard. Pour obtenir le nom du scanner, contactez votre administrateur de réseau. ***Remarque :*** *Si vous utilisez un dispositif de numérisation public, vous devez effacer le nom à partir du champ* ***Scanner Name****.*
Option Profile(s)	Entrez le nom du profil d'option pour déterminer le rapport d'analyse existant démarrant en tant qu'analyse en direct sur le scanner Qualys. QRadar SIEM récupère les données complètes de l'analyse opérationnelle après que celle-ci soit terminée. ***Remarque :*** *Les analyses en direct prennent en charge un nom de profil d'option par configuration de scanner.*

Etape 8 Pour configurer les plages de routage CIDR que cette analyse doit prendre en considération :

a Dans la zone de texte, entrez la plage de routage CIDR que ce scanner doit prendre en considération ou cliquez sur **Browse** pour sélectionner la plage de routage CIDR à partir de la liste réseaux.

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

Etape 10 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Vous pouvez maintenant configurer un planning d'analyse pour déterminer la fréquence à laquelle QRadar SIEM lance l'analyse opérationnelle sur votre scanner Qualys. Pour plus d'informations, voir **Gestion des plannings d'analyse**.

Ajout d'un Qualys Asset Report Data Import

Une importation de données de rapports sur les actifs vous permet de planifier QRadar SIEM afin de récupérer un rapport d'actif à partir de votre scanner Qualys. QRadar SIEM détermine le rapport d'actif à importer du fichier indiqué dans la zone **Import File**. Si un fichier d'importation n'est pas indiqué, alors QRadar SIEM tente d'importer le rapport d'actif en fonction de la zone **Report Template Title**.

Pour ajouter une importation de rapport de données d'actif planifié Qualys QRadar SIEM :

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 6-5 Paramètres du Scanner Qualys

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez attribuer à ce scanner. Le nom peut contenir plus de 255 caractères.
Description	Entrez une description pour ce scanner. La description peut contenir plus de 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **Qualys Scanner**.

Etape 6 Dans la zone de liste **Collection Type**, sélectionnez **Scheduled Import - Asset Data Report**.

Les options de configuration pour l'importation d'un rapport d'actif Qualys s'affichent.

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 6-6 Paramètres Qualys Asset Data Import

Paramètre	Description
Qualys Server Host Name	Entrez le nom de domaine complet ou l'adresse IP de la console de gestion QualysGuard en fonction de votre emplacement. En spécifiant le nom de domaine complet, vous devez entrer le nom d'hôte et non l'adresse URL. Par exemple : • Entrez **`qualysapi.qualys.com`** pour un nom d'hôte de serveur QualysGuard se trouvant aux États-Unis. • Entrez **`qualysapi.qualys.eu`** pour un nom hôte du serveur QualysGuard se trouvant en Europe. • Entrez **`qualysapi.<management_console>`** si vous utilisez l'infrastructure de numérisation complète comprenant une console de gestion interne, où <management_console> **`est le nom d'hôte de votre dispositif de gestion interne.`**

Tableau 6-6 Paramètres Qualys Asset Data Import (suite)

Paramètre	Description
Qualys Username	Entrez le nom d'utilisateur nécessaire pour des demandes d'analyse. Il s'agit du même nom d'utilisateur utilisé pour se connecter au serveur Qualys.
Qualys Password	Entrez le mot de passe correspondant au nom d'utilisateur Qualys.
Use Proxy	Sélectionnez cette case à cocher si QRadar SIEM exige un serveur proxy pour communiquer avec votre scanner Qualys. Par défaut, cette case est désélectionnée. Cette case affiche les paramètres supplémentaires de configuration de proxy.
Proxy Host Name	Entrez le nom d'hôte ou l'adresse de votre serveur proxy.
Proxy Port	Entrez le numéro de port de votre serveur proxy.
Proxy Username	Entrez un nom d'utilisateur permettant à QRadar SIEM de s'authentifier avec votre serveur proxy.
Proxy Password	Entrez le mot de passe associé au champ **Proxy Username**.
Collection Type	Dans la zone de liste, sélectionnez **Scheduled Import - Asset Data Report**. Cette option permet au scanner de récupérer le dernier rapport d'actifs à partir du fichier spécifié dans le champ **Import File**.
Report Template Title	Entrez un titre de modèle de rapport pour remplacer le titre par défaut en récupérant les rapports de données d'actifs.
Max Report Age (Days)	Entrez l'âge maximal du fichier pour inclure en important Qualys Asset Data durant une analyse planifiée. Par défaut, l'âge maximal du fichier est de 7 jours. Les fichiers qui sont plus anciens que le nombre de jours indiqués et l'horodatage sur le fichier de rapport sont exclus de l'importation planifiée.

Tableau 6-6 Paramètres Qualys Asset Data Import (suite)

Paramètre	Description
Import File (Optional)	Facultatif. Entrez un chemin de répertoire pour télécharger et importer un rapport d'actif unique à partir de Qualys sur votre console QRadar SIEM ou sur votre hôte géré. Par exemple, pour télécharger un rapport d'actif appelé QRadar_scan.xml à partir d'un répertoire de journaux sur votre hôte géré, entrez la commande suivante : `/qualys_logs/QRadar_scan.xml` Si vous indiquez l'emplacement d'un fichier d'importation, QRadar SIEM télécharge les contenus du rapport d'actif de Qualys vers un répertoire local. Une fois le téléchargement du rapport d'actif terminé sur votre console, QRadar SIEM importe les informations liées à l'actif via l'utilisation du fichier local. Si la zone **Import File** ne contient aucune valeur ou si le fichier ou le répertoire e st introuvable, alors le scanner Qualys tente de récupérer le dernier rapport d'actifs en utilisant Qualys API en fonction des informations se trouvant dans la zone **Report Template Title**.

Etape 8 Pour configurer les plages de routage CIDR que cette analyse doit prendre en considération :

a Dans la zone de texte, entrez la plage de routage CIDR que ce scanner doit prendre en considération ou cliquez sur **Browse** pour sélectionner la plage de routage CIDR à partir de la liste réseaux.

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

Etape 10 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Vous pouvez maintenant configurer un planning d'analyse pour déterminer la fréquence à laquelle QRadar SIEM importe les rapports sur les ressources sur votre scanner Qualys. Pour plus d'informations, voir **Gestion des plannings d'analyse**.

Ajout de Qualys Scheduled Import Scan Report

Une importation planifiée d'un rapport d'analyse Qualys permet à QRadar SIEM de récupérer les analyses complètes de votre scanner Qualys.

Pour ajouter une importation de données de rapport d'analyse Qualys vers QRadar SIEM :

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 6-7 Paramètres du Scanner Qualys

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez affecter à ce scanner. Le nom peut contenir plus de 255 caractères.
Description	Entrez une description pour ce scanner. La description peut contenir plus de 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **Qualys Scanner**.

Etape 6 Dans la zone de liste **Collection Type**, sélectionnez **Scheduled Import - Scan Report**.

Les options de configuration pour l'importation des rapports d'analyse complètes Qualys s'affichent.

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 6-8 Paramètres Qualys Schedule Scan Import

Paramètre	Description
Qualys Server Host Name	Entrez le nom de domaine complet ou l'adresse IP de la console de gestion QualysGuard en fonction de votre emplacement. En spécifiant le nom de domaine complet, vous devez entrer le nom d'hôte et non l'adresse URL.

Tableau 6-8 Paramètres Qualys Schedule Scan Import (suite) (suite)

Paramètre	Description
	Par exemple : • Entrez **`qualysapi.qualys.com`** pour un nom d'hôte de serveur QualysGuard se trouvant aux États-Unis. • Entrez **`qualysapi.qualys.eu`** pour un nom hôte du serveur QualysGuard se trouvant en Europe. • Entrez **`qualysapi.<management_console>`** si vous utilisez l'infrastructure de numérisation complète comprenant une console de gestion interne, où <management_console> **`est le nom d'hôte de votre dispositif de gestion interne.`**
Qualys Username	Entrez le nom d'utilisateur nécessaire pour des demandes d'analyse. Il s'agit du même nom d'utilisateur utilisé pour se connecter au serveur Qualys.
Qualys Password	Entrez le mot de passe correspondant au nom d'utilisateur Qualys.
Use Proxy	Sélectionnez cette case à cocher si QRadar SIEM exige un serveur proxy pour communiquer avec votre scanner Qualys. Par défaut, cette case est désélectionnée. Cette case affiche les paramètres supplémentaires de configuration de proxy.
Proxy Host Name	Entrez le nom d'hôte ou l'adresse de votre serveur proxy.
Proxy Port	Entrez le numéro de port de votre serveur proxy.
Proxy Username	Entrez un nom d'utilisateur permettant à QRadar SIEM de s'authentifier avec votre serveur proxy.
Proxy Password	Entrez le mot de passe associé au champ **Proxy Username**.
Collection Type	Dans la zone de liste, sélectionnez **Scheduled Import - Scan Report**.
Option Profile(s)	Entrez un nom de profil d'option unique ou utilisez une liste de noms de profile d'option séparée par des virgules pour filtrer la liste des rapports d'analyse téléchargés depuis votre scanner Qualys. Tous les rapports d'analyse correspondant au nom du profil d'option sont importés. Si la zone **Option Profile(s)** ne contient pas de nom de profil d'option, la liste est filtrée en fonction de tous les Profils d'option et tous les rapports d'analyse pour tous les Profils Option sont récupérés. Pour plus d'informations, consultez votre documentation QualysGuard. ***Remarque :*** *Si les données ne sont pas récupérées Profil d'option dans votre liste séparée par des virgules, le rapport d'analyse peut être disponible pour le téléchargement. Assurez-vous que Qualys a terminé le rapport d'analyse associé au Profil option.*

Tableau 6-8 Paramètres Qualys Schedule Scan Import (suite) (suite)

Paramètre	Description
Scan Report Name Pattern	Entrez un masque de fichiers, en utilisant une expression régulière, pour les rapports d'analyse que vous tentez d'importer. Par défaut, QRadar SIEM tente de télécharger tous les rapports d'analyse disponibles en utilisant le masque de fichiers suivant :.*****.
Max Report Age (Days)	Entrez l'âge maximal du fichier à inclure lors de l'importation des rapports d'analyse Qualys durant une analyse planifiée. Par défaut, l'âge maximal du fichier est de 7 jours. Les fichiers qui sont plus anciens que le nombre de jours indiqués et l'horodatage sur le fichier de rapport sont exclus de l'importation planifiée.
Import File (Optional)	Facultatif. Entrez un chemin de répertoire pour télécharger et importer un rapport d'analyse unique à partir de Qualys sur votre console QRadar SIEM ou sur votre hôte géré. Par exemple, pour télécharger un rapport d'analyse appelé QRadar_scan.xml à partir d'un répertoire de journaux sur votre hôte géré, entrez la commande suivante : **`/qualys_logs/QRadar_scan.xml`** Si vous indiquez l'emplacement d'un fichier d'importation, QRadar SIEM télécharge les contenus du rapport d'analyse de l'actif de Qualys vers un répertoire local. Une fois le téléchargement du rapport d'analyse de l'actif terminé, QRadar SIEM importe les informations liées à l'actif via l'utilisation du fichier local. Si la zone **Import File** ne contient aucune valeur ou si le fichier ou le répertoire est introuvable, alors le scanner Qualys tente de récupérer le dernier rapport de données d'actifs en utilisant Qualys API en fonction des informations se trouvant dans la zone **Report Template Title**.

Etape 8 Pour configurer les plages de routage CIDR que ce scanner doit mettre en considération :

a Dans la zone de texte, tapez la plage CIDR que le scanner doit mettre en considération ou cliquez sur **Browse** pour sélectionner la plage CIDR à partir de la liste de réseaux.

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

Etape 10 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Vous êtes prêt à configurer un planning d'analyse pour déterminer la fréquence à laquelle QRadar SIEM importe le rapport de données d'actif à partir de votre scanner Qualys. Pour plus d'informations, voir **Gestion des plannings d'analyse**.

Modification de Qualys Detection Scanner

Pour modifier une configuration de Qualys Scanner dans QRadar SIEM :

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez modifier.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Mettez à jour les paramètres, si nécessaire.

- Pour les paramètres Qualys Live Scan, voir **Tableau 6-4**.
- Pour les paramètres Qualys Asset Report Data Import, voir **Tableau 6-6**.
- Pour les paramètres Qualys Scheduled Import Scan Report, voir **Tableau 6-8**.

Etape 7 Cliquez sur **Save**.

Etape 8 Choisissez l'une des méthodes de déploiement suivantes :

- Si vous effectuez la reconfiguration de Qualys Scanner sans mettre à jour les données d'identification du proxy Qualys Scanner, cliquez sur **Deploy Changes** sur le menu de l'onglet de navigation **Admin** pour terminer la modification de votre configuration.
- Si vous effectuez la reconfiguration de votre Qualys Detection Scanner et mettez à jour les données d'identification dans les zones **Proxy Username** ou **Proxy Password**, sélectionnez **Advanced > Deploy Full Configuration** sur le menu de l'onglet de navigation **Admin** pour terminer la modification de votre configuration.

ATTENTION

*La sélection de **Deploy Full Configuration** redémarre les services QRadar SIEM, produisant ainsi un écart dans la collecte des données d'événements et de flux jusqu'à la fin du déploiement.*

Les modifications apportées à votre scanner Qualys sont terminées.

Suppression d'un Scanner Qualys

Pour supprimer un scanner Qualys à partir de QRadar SIEM :

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez sur **OK**.

Etape 7 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Le scanner Qualys est supprimé de la liste des scanners.

9 GESTIONS DE SCANNERS FOUNDSCAN

Le scanner Foundstone FoundScan IBM Security QRadar SIEM permet à QRadar SIEM d'interroger FoundScan Engine l'aide de l'OpenAPI de FoundScan pour obtenir des informations sur l'hôte et la vulnérabilité. Le scanner FoundScan n'exécute pas directement les analyses mais rassemble les résultats de l'analyse actuelle affichée dans l'application de numérisation. QRadar SIEM prend en charge Foundstone FoundScan versions 5.0 à 6.5.

Votre système FoundScan doit inclure une configuration adéquate permettant l'utilisation deQRadar SIEM et une analyse qui s'exécute régulièrement pour rendre les résultats actuels. Pour s'assurer que votre scanner FoundScan peut extraire des informations de l'analyse, vérifiez que votre système FoundScan répond aux exigences suivantes :

- Puisque API fournit l'accès à l'application FoundScan, assurez-vous que l'application FoundScan s'exécute en continu sur le serveur FoundScan. Cela signifie que l'application FoundScan doit être active sur votre bureau.
- L'analyse qui inclut la configuration nécessaire pour se connecter à QRadar SIEM doit être complète et visible dans l'interface utilisateur FoundScan permettant à QRadar SIEM d'extraire les résultats de l'analyse. Si l'analyse ne s'affiche pas dans l'interface utilisateur FoundScan ou que sa suppression est planifiée après avoir terminé, QRadar SIEM doit extraire les résultats avant que l'analyse est supprimée ou les résultats de l'analyse échouent.
- Les privilèges utilisateurs appropriés doivent être configurés dans l'application FoundScan, permettant à QRadar SIEM de communiquer avec FoundScan.

Etant donné que FoundScan OpenAPI fournit uniquement des informations sur l'hôte et la vulnérabilité à QRadar SIEM, vos informations du profil de l'actif affichent toutes les vulnérabilités pour un hôte assigné au port 0.

Lors de l'utilisation de SSL (par défaut) pour se connecter à FoundScan, FoundScan Engine exige à QRadar SIEM de s'authentifier à l'aide des certificats côté client. Par défaut, FoundScan inclut l' autorité de certification et les certificats du client qui sont les mêmes pour toutes les installations. Le plug-in QRadar SIEM FoundScan inclut également les mêmes certificats pour utilisation avec FoundScan 5.0. Si FoundScan Server utilise les certificats personnalisés ou utilise une version de FoundScan autre que 5.0, vous devez importer les certificats et clés sur l'hôte QRadar SIEM. Pour plus d'informations, voir **Importation de certificats**.

Après avoir configuré le système FoundScan et le scanner FoundScan dans QRadar SIEM, vous devez planifier une analyse. La configuration du planning d'analyse vous autorise à configurer. La puissance, cependant, le scanner FoundScan ne prend pas en considération le paramètre potency lors de l'analyse. Pour plus d'informations, voir **Gestion des plannings d'analyse**.

Cette section fournit les informations les éléments suivants :

- **Ajout d'un scanner FoundScan**
- **Edition d'un scanner FoundScan**
- **Suppression d'un scanner FoundScan**
- **Utilisation de certificats**

Ajout d'un scanner FoundScan

Pour ajouter un scanner FoundScan :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs pour les paramètres suivants :

Tableau 7-1 Paramètres du scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez affecter à ce scanner. Le nom peut contenir jusqu'à 255 caractères.
Description	Entrez une description pour ce scanner. La description peut contenir jusqu'à 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez la description que vous souhaitez utiliser pour configurer le scanner. ***Remarque :*** *Les certificats de votre scanner FoundScan doivent résider sur l'hôte géré sélectionné dans la zone de liste* ***Managed Host****.*
Type	Dans la zone de liste, cochez **FoundScan Scanner**.

Etape 6 Configurez les valeurs pour les paramètres suivants :

Tableau 7-2 Paramètres FoundScan

Paramètre	Description
SOAP API URL	Entrez l'adresse Web de Foundscan OpenAPI sous le format suivant : **`https://<foundstone IP address>:<SOAP port>`** Où : **`<foundstone IP address>`** est l'adresse IP ou le nom d'hôte du serveur scanner FoundScan. **`<SOAP port>`** est le numéro de port de FoundScan Engine. L'URL par défaut est **`https://localhost:3800.`**
Customer Name	Entrez le nom du client auquel appartient le Login User Name.
User Name	Entrez le nom d'utilisateur que vous souhaitez que QRadar SIEM utilise pour authentifier FoundScan Engine dans API. Ceci doit avoir accès à la configuration de l'analyse.
Client IP Address	Entrez l'adresse IP du serveur QRadar SIEM que vous avez choisie pour effectuer les analyses. Cette valeur n'est pas utilisée par défaut, cependant elle est nécessaire pour la validation de certains environnements.
Password	Entrez le mot de passe correspondant au Login User Name pour l'accès à l'API.
Portal Name	Facultatif. Entrez le nom du portail. Vous pouvez laisser ce champ vide pour un usage de QRadar SIEM. Voir votre administrateur FoundScan pour plus d'informations.
Configuration Name	Entrez le nom de la configuration de l'analyse qui existe dans FoundScan et auquel l'utilisateur a accès. Vérifiez que cette analyse est activée ou, au moins, s'exécute au moins fréquemment.
CA Truststore	Affiche le chemin de répertoire et le nom de fichier pour le fichier de clés certifiées CA. Le chemin de répertoire par défaut est /opt/qradar/conf/foundscan.keystore.
Client Keystore	Affiche le chemin de répertoire et le nom de fichier pour le fichier de clés du client. Le chemin de répertoire par défaut est /opt/qradar/conf/foundscan.truststore.

Etape 7 Pour configurer les intervalles que CIDR dont vous souhaitez que ce scanner doit prendre en considération :

a Dans la zone de texte, entrez l'intervalle CIDR dont vous souhaitez que ce scanner doit prendre en considération ou cliquez sur **Browse** pour sélectionner l'intervalle CIDR à partir de la liste réseaux.

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

Etape 9 Dans l'onglet **Admin**, sélectionnez **Deploy Changes**.

Edition d'un scanner FoundScan

Pour éditer un scanner FoundScan :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez éditer.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Paramètre Update, si nécessaire. Voir **Tableau 7-2**.

Etape 7 Cliquez sur **Save**.

Etape 8 Dans l'onglet **Admin**, sélectionnez **Deploy Changes**.

Suppression d'un scanner FoundScan

Pour supprimer un scanner FoundScan :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez sur **OK**.

Etape 7 Dans l'onglet **Admin**, sélectionnez **Deploy Changes**.

Utilisation de certificats

FoundScan Engine utilise un certificat pour chiffrer la circulation et pour l'authentification. Lors de l'installation initiale de FoundScan, vous pouvez configurerFoundScan pour utiliser le certificat par défaut ou un certificat personnalisé.

Cette section fournit les informations les éléments suivants :

- **Obtention d'un certificat**

- **Importation de certificats**

Obtention d'un certificat

Pour obtenir le certificat requis :

Etape 1 Exécutez l'application FoundScan.

Etape 2 Dans la zone de liste, sélectionnez **Preferences**.

Etape 3 Dans la fenêtre Preferences, cliquez sur l'onglet **Communication**.

Etape 4 Localisez le champ Authentication Scheme.

Si le champ indique le certificat par défaut de FoundStone, alors le certificat par défaut est en cours d'utilisation.

Etape 5 Si vous utilisez le certificat par défaut, parcourez et obtenez les fichiers **TrustedCA.pem** et **Portal.pem** depuis le dossier de configuration sur votre système FoundScan.

Pour obtenir des informations sur les fichiers TrustedCA.pem et Portal.pem, voir **Exemple de fichiers TrustedCA.pem** et **Exemple de fichiers Portal.pem**.

Etape 6 Si vous utilisez un certificat personnalisé, générez un certificat à l'aide du gestionnaire de certificat FoundScan. Vérifiez que vous avez saisi l'adresse IP de l'hôte QRadar SIEM en tant que nom d'hôte pour le certificat.

Vous êtes maintenant sur le point d'importer le certificat sur chaque hôte géré QRadar SIEM qui héberge le composant du scanner. Voir **Importation de certificats**.

Importation de certificats

Si FoundScan Server utilise les certificats personnalisés ou utilise une version de FoundScan autre que 5.0, vous devez importer les certificats et clés vers l'hôte géré QRadar SIEM que vous avez sélectionnés dans **Table 7-1**. Avant d'essayer d'importer des certificats à l'aide de la procédure ci-dessous, vérifiez que le scanner FoundScan est ajouté à QRadar SIEM, voir **Ajout d'un scanner FoundScan**.

Pour importer des certificats vers QRadar SIEM:

Etape 1 Obtenir deux fichiers certificat et la phrase passe depuis votre administrateur FoundScan.

Le premier fichier est le certificat CA pour le moteur FoundScan. Le second certificat est la clé privée plus la chaîne de certificats pour le client.

L'ensemble des deux fichiers doivent être au format PEM. Pour obtenir des exemples de ces fichiers, voir **Exemple de fichiers TrustedCA.pem** et **Exemple de fichiers Portal.pem**.

Etape 2 Copiez les fichiers PEM sur votre système QRadar SIEM et sur le répertoire de base superutilisateur ou sur un nouveau répertoire créé pour les certificats.

Etape 3 Sur l'hôte QRadar SIEM, modifiez le répertoire vers lequel les deux fichiers PEM sont copiés.

Etape 4 Supprimez les certificats existants :

```
rm -f /opt/qradar/conf/foundscan.keystore
rm -f /opt/qradar/conf/foundscan.truststore
```

Etape 5 Entrez la commande suivante :

```
/opt/qradar/bin/foundstone-cert-import.sh <TrustedCA.pem>
<Portal.pem>
```

Où :

<TrustedCA.pem> est le nom de fichier du certificat de l'autorité de certification.

<Portal.pem> est le fichiers de la chaîne de clés privées PEM.

La sortie peut ressembler à ce qui suit :

```
Le certificat a été ajouté au fichier de clés
Utilisation de fichier de clés :
/opt/qradar/conf/foundscan.keystore
Un certificat, aucune chaîne.
Clé et certificat stockés.
Alias:Portal.pem Password:foundscan
Contenu de Trust Store:
Type de Keystore : jks
Fournisseur de Keystore : SUN
Votre Keystore contient 1 entrée
Alias name: trustedca.pem
Date de création : 8 mars 2007
Type d'entrée : trustedCertEntry
Owner: CN=Foundstone CA
Issuer: CN=Foundstone CA
Numéro de série : 0
Valable du : ven 12 Sep à 20:29:11 ADT 2003 au : Lun Oct 20
20:29:11 ADT empreintes digitales 2008 :
     MD5: 14:7E:68:02:38:EC:A5:A8:AE:3D:3C:C6:F5:F6:33:6C
     SHA1:
37:C3:48:36:87:B0:F2:41:48:6A:A2:F6:43:B7:76:55:92:C5:6E:11
**********************************************
**********************************************
Contenu de Key Store:
Type de Keystore : jks
Fournisseur de Keystore : SUN
Votre Keystore contient 1 entrée
Alias name: portal.pem
Date de création : 8 mars 2007
Type d'entrée : keyEntry
Longueur de la chaîne de certificats : 1
Certificat [1]:
Owner: CN=Foundstone Enterprise Manager
Issuer: CN=Foundstone CA
Numéro de série : 2
```

```
Valable du : Ven 12 à 20:36:54 ADT 2003 au : Lun 20 oct à
20:36:54 ADT empreintes digitale 2008 :
     MD5: 0A:CD:06:36:B2:ED:62:8C:98:8D:10:3C:99:95:BA:7D
     SHA1:
3A:B4:9C:59:D0:AD:26:C9:6D:B9:05:E9:F1:33:CB:23:F2:0A:E7:26
****************************************
****************************************
```

Etape 6 Répétition pour tous les hôtes gérés dans votre déploiement qui héberge le scanner.

Exemple de fichiers TrustedCA.pem

```
-----BEGIN CERTIFICATE-----
MIICFzCCAYCgAwIBAgIBADANBgkqhkiG9w0BAQQFADAYMRYwFAYDVQQDEw1Gb3Vu
ZHN0b25lIENBMB4XDTAzMDkxMjIzMjkxMVoXDTA4MTAyMDIzMjkxMVowGDEWMBQG
J9PUXhzRqqh8yzh795R9Dloj7hsyZtq4My6gKu8RuHVBscYvJVwPMUkPmDHMnpjl
A1UEAxMNRm91bmRzdG9uZSBDQTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
sWN8ZqqREMZ7qByvuIqr2q4XaP5TfP3hRCo8mjvqWsQjk2B8WMRAgZjHqvPN/qfG
5uZw5gm1M6IyoVbLkaQwDF34McRpqlTLvjeDadjPuRaZGVu4zVknC8s83EPqKU9+
fdqmhtCwwqVYq+sQFp1S3kKUvXIBEGV0r9mnFAD3InUCAwEAAaNxMG8wHQYDVR0O
BBYEFGQ8UJTPbqSP202Mygs2sqzU2h7LMEAGA1UdIwQ5MDeAFGQ8UJTPbqSP202M
ygs2sqzU2h7LoRykGjAYMRYwFAYDVQQDEw1Gb3VuZHN0b25lIENBggEAMAwGA1Ud
j0ynMtEM2mtuf95uxeGFe581k31w9d3IGt19uahtyqG860kr4/ys3r7LjA0f9rjf
J9PUXhzRqqh8yzh795R9Dloj7hsyZtq4My6gKu8RuHVBscYvJVwPMUkPmDHMnpjl
4p7dh7GKk7ymFYs=
-----END CERTIFICATE-----
```

Exemple de fichiers Portal.pem

Ceci est un exemple de fichier Portal.pem :

```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQC5DOnQtMtDXAHth/4M/lI9gVlyoch9EYvCiAsZmtO2JMTjEDse
mH0DQkxSKv0gvsCqKXHx6nNegyyiCM1GuEDvFYPCI5FrkrzEwtndTILGXT5asDXu
ncnAl/9am4jAhADDPFb9ZRMoE6aFE13XD21o49gJG4sH+VkCQQDrf6OGfnR6YaYz
SbPTMrBKR5pfMJoPJ/Sjc0vf6A48Nn8FiYLDiyBLKhunzM03EZ22VrZxBwIDAQAB
AoGARZfkqzgDJZ8JnpJBahOPTFBEGodbhiW+IPfW7Nc8fcjQPvDQuw3wHfSmDVTb
g6AZhyU1FBzvLIE6nOmggdMzn9KIN8WMD+XDAAR4AaWOGkN18Ib4h1VVnsa90hYS
BPIWVsfbAkEAySj6iwto1LVsXC5cIP4YzNzNsj2QBqeEhEfUmLtZl8vD1sj+EM2L
JggOcRpYMxIj64ob/hevavXeW1CFeRmpRQJBAKaq6OKQsILEhUoGHlJTt2BtOpEs
3JP4BBUV7QE0VTTKxA8byQqjGSu6zh/JxWk9hTjo5oSCmlcwahC5k1O4Cy0CQQCt
vnwv7mncFtsB/3TJdk67Wxc7FRs59CRsEJKaXG80weVjtXRj1PSTo6+9ltCJQ+jM
fxxQaeq0SqqEWlb+UuC1AkEAr6Z503v5p1rVUWTo+L8JaygumdzZRuBZi/EVuxqG
j79b6Xa+UvXtXquU2qlo1weanry/Glm47qSwPBcFoOse4Q==
-----END RSA PRIVATE KEY-----
Certificat :
```

```
    Données :
      Version: 3 (0x2) Numéro de série : 2 (0x2)
      Algorithme de signature : md5WithRSAEncryption
      Issuer: CN=Foundstone CA
      Validité
        Pas avant : le 12 Sept 2003 à 23:36:54 GMT
        Pas avant : le 20 oct 2008 à 20 23:36:54 GMT
      Objet : CN=Foundstone Enterprise Manager
      Informations objets de clé publique :
        Algorithme de clé publique : rsaEncryption
        Clé publique algorithme RSA : (1024 bit)
          Modulus (1024 bits):
            00:b9:0c:e9:d0:b4:cb:43:5c:01:ed:87:fe:0c:fe:
            52:3d:81:59:72:a1:c8:7d:11:8b:c2:88:0b:19:9a:
            d3:b6:24:c4:e3:10:3b:1e:98:7d:03:42:4c:52:2a:
fd:20:be:c0:aa:29:71:f1:ea:73:5e:83:2c:a2:08:
cd:46:b8:40:ef:15:83:c2:23:91:6b:92:bc:c4:c2:
d9:dd:4c:82:c6:5d:3e:5a:b0:35:ee:49:b3:d3:32:
b0:4a:47:9a:5f:30:9a:0f:27:f4:a3:73:4b:df:e8:
0e:3c:36:7f:05:89:82:c3:8b:20:4b:2a:1b:a7:cc:
            cd:37:11:9d:b6:56:b6:71:07
          Exposant : 65537 (0x10001)
      Extensions X509v3 :
        Contraintes de base X509v3 :
        CA:FALSE
        Commentaire Netscape :
        Certificat généré OpenSSL
        Identificateur de clé d'objet X509v3 Identifier:
        0D:52:54:EF:A0:B3:91:9D:3D:47:AC:D8:9E:62:2A:34:0F:09:FF:8D
        Identificateur de clé X509v3 Authority :
keyid:64:3C:50:94:CF:6E:A4:8F:DB:4D:8C:CA:0B:36:B2:AC:D4:DA:1E:CB
        DirName:/CN=Foundstone CA
        Série :00
    Algorithme de signature : md5WithRSAEncryption
4a:88:3f:51:34:5b:30:3b:5b:7c:57:31:86:22:3b:00:16:61:
ac:7b:b7:ae:cd:68:11:01:a2:52:b7:59:1e:c6:5b:af:2a:ed:
f9:ee:ef:64:11:b2:b9:14:21:7d:2c:35:d3:cb:09:08:a1:ab:
26:93:0f:aa:97:eb:cc:65:ab:95:a3:0d:77:0b:23:20:4a:0d:
04:18:47:2d:58:a7:de:61:9f:aa:3c:da:a5:00:9d:b5:eb:52:
fb:e2:5b:56:45:02:02:79:df:0f:87:bc:f3:82:d1:3d:39:79:
9e:ef:64:e2:f5:61:9b:ea:29:94:fb:00:8f:b8:08:7c:f0:ee:
    68:b6
```

```
-----BEGIN CERTIFICATE-----
MIICVDCCAb2gAwIBAgIBAjANBgkqhkiG9w0BAQQFADAYMRYwFAYDVQQDEw1Gb3Vu
ZHN0b25lIENBMB4XDTAzMDkxMjIzMzY1NFoXDTA4MTAyMDIzMzY1NFowKDEmMCQG
A1UEAxMdRm91bmRzdG9uZSBFbnRlcnByaXNlIE1hbmFnZXIwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBALkM6dC0y0NcAe2H/gz+Uj2BWXKhyH0Ri8KICxma07Yk
xOMQOx6YfQNCTFIq/SC+wKopcfHqc16DLKIIzUa4QO8Vg8IjkWuSvMTC2d1MgsZd
PlqwNe5Js9MysEpHml8wmg8n9KNzS9/oDjw2fwWJgsOLIEsqG6fMzTcRnbZWtnEH
AgMBAAGjgZ0wgZowCQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYdT3BlblNTTCBH
ZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFA1SVO+gs5GdPUes2J5iKjQP
Cf+NMEAGA1UdIwQ5MDeAFGQ8UJTPbqSP202Mygs2sqzU2h7LoRykGjAYMRYwFAYD
VQQDEw1Gb3VuZHN0b25lIENBggEAMA0GCSqGSIb3DQEBBAUAA4GBAEqIP1E0WzA7
W3xXMYYiOwAWYax7t67NaBEBolK3WR7GW68q7fnu72QRsrkUIX0sNdPLCQihqyaT
D6qX68xlq5WjDXcLIyBKDQQYRy1Yp95hn6o82qUAnbXrUvviW1ZFAgJ53w+HvPOC
0T05eZ7vZOL1YZvqKZT7AI+4CHzw7mi2
-----END CERTIFICATE-----
```

10 GESTION DES SCANNERS JUNIPER NETWORKS NSM PROFILER

La console The Juniper Networks Netscreen Security Manager (NSM) collecte de manière passive un outil d'information utile depuis votre réseau via un déploiement de détecteurs Juniper Networks IDP. QRadar SIEM se connecte à la base de données Profiler stockée sur le serveur NSM pour récupérer ces enregistrements. Le serveur QRadar SIEM doit avoir accès à la base de données Profiler. QRadar SIEM prend en charge les versions NSM 2007.1r2, 2007.2r2, 2008.1r2, 2009r1.1, et 2010.x. Pour en savoir plus, consultez la documentation de votre fournisseur.

QRadar SIEM collecte les données à partir de la base de données PostgreSQL sur NSM à l'aide de JDBC. Pour collecter des données, QRadar SIEM doit avoir accès au port de la base de données Postgres (port TCP 5432). Cet accès est fourni dans le fichier pg_hba.conf qui, généralement, se trouve dans /var/netscreen/DevSvr/pgsql/data/pg_hba.conf sur l'hôte NSM.

Après avoir configuré le scanner Juniper Networks NSM Profiler dans QRadar SIEM, vous pouvez planifier une analyse.Les plannings d'analyse vous permettent de configurer la fréquence à laquelle QRadar SIEM tente de récupérer des vulnérabilités.Pour plus d'informations, voir **Gestion des plannings d'analyse**.

Cette section fournit des informations sur les éléments suivants :

- **Ajout d'un scanner Juniper Networks NSM Profiler**
- **Edition d'un scanner Profiler**
- **Suppression d'un scanner Profiler**

Ajout d'un scanner Juniper Networks NSM Profiler

Pour ajouter un scanner Juniper Networks NSM Profiler :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs pour les paramètres suivants :

Tableau 8-1 Paramètres du scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez affecter à ce scanner. Le nom peut contenir jusqu'à 255 caractères.
Description	Entrez une description pour ce scanner. La description peut contenir jusqu'à 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez la description que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **Juniper NSM Profiler Scanner**.

Etape 6 Configurez les valeurs pour les paramètres suivants :

Tableau 8-2 Paramètres Juniper Networks NSM Profiler

Paramètre	Description
Server Host Name	Entrez le nom d'hôte ou l'adresse IP du serveur NetScreen Security Manager (NSM).
Database Username	Entrez le nom d'utilisateur Postgres pour se connecter à la base de données Profiler stockée sur le serveur NSM.
Database Password	Entrez le mot de passe associé à Database Username pour se connecter au serveur.
Database Name	Entrez le nom de la base de données Profiler. Le nom de la base de données par défaut est profilerDb.

Etape 7 Pour configurer les intervalles CIDR que ce scanner doit prendre en considération :

a Dans la zone de texte, entrez l'intervalle CIDR que vous souhaitez que ce scanner prenne en considération ou cliquez sur **Browse** pour sélectionner l'intervalle CIDR à partir de la liste réseaux.

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

Etape 9 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

Edition d'un scanner Profiler

Pour éditer un scanner Juniper Networks NSM Profiler :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez éditer.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Paramètre Update, si nécessaire. Voir **Tableau 8-2**.

Etape 7 Cliquez sur **Save**.

Etape 8 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

Suppression d'un scanner Profiler

Pour supprimer un scanner Juniper Networks NSM Profiler :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez sur **OK**.

Etape 7 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

11 GESTION DES SCANNERS RAPID7 NEXPOSE

Le scanner Rapid7 NeXpose utilise l'interface API basée sur le Web afin d'obtenir des résultats d'analyse pour QRadar SIEM à partir de tous les sites connectés à votre console de sécurité NeXpose. QRadar SIEM prend en charge deux méthodes pour importer les données de vulnérabilité Rapid7 NeXpose :

- Import Site Data - Adhoc Report via API

  L'importation de données de site permet à QRadar SIEM d'accéder au scanner Rapid7 NeXpose et de télécharger un rapport adhoc à partir des vulnérabilités découvertes de l'adresse IP configurée pour votre site. Pour plus d'informations, voir **Importation des données de vulnérabilité Rapid7 NeXpose à l'aide de l'interface API**.

- Import Site Data - Local File

L'importation de site de fichier local permet à QRadar SIEM d'importer des rapports d'analyse pour un site basé sur un fichier local téléchargé sur votre console QRadar SIEM. Le fichier XML Rapid7 NeXpose contenant des données de vulnérabilité doit être copié à partir du dispositif Radid7 NeXpose vers la console QRadar SIEM ou l'hôte géré qui effectue l'importation locale. Vous devez créer un répertoire sur la console QRadar SIEM ou l'hôte géré avant de copier les fichiers XML du rapport d'analyse. Les fichiers peuvent être copiés à l'aide de Secure Copy (SCP) ou Secure File Transfer Protocol (SFTP). Pour plus d'informations, voir **Importation de vulnérabilité Rapid7 NeXpose à partir d'un fichier local**.

Après avoir configuré le périphérique Rapid7 NeXpose et le scanner Rapid7 NeXpose dans QRadar SIEM, vous pouvez planifier une analyse. Planifier une analyse vous aide lorsque QRadar SIEM importe des données de vulnérabilité de Rapid7 NeXpose à l'aide de l'interface API ou lorsque QRadar SIEM importe le fichier XML contenant des données de vulnérabilité. Pour plus d'informations, voir **Gestion des plannings d'analyse**.

Cette section comprend les rubriques suivantes :

- **Suppression d'un scanner Rapid7 NeXpose**
- **Identification et résolution des problèmes Rapid7 NeXpose API Scan Import**

Pour en savoir plus, consultez votre documentation Rapid7 NeXpose.

Importation des données de vulnérabilité Rapid7 NeXpose à l'aide de l'interface API

L'importation des données de vulnérabilité du site à l'aide de l'interface API permet à QRadar SIEM d'importer des analyses complètes basées sur des noms de site configurés sur votre scanner Rapid7 NeXpose.

Cette section comprend les rubriques suivantes :

- **Configuration d'un scanner Rapid7 NeXpose**
- **Identification et résolution des problèmes Rapid7 NeXpose API Scan Import**

Configuration d'un scanner Rapid7 NeXpose

Pour configurer un scanner Rapid7 NeXpose afin d'importer des données de rapport du site ad-hoc :

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

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

La fenêtre Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 9-1 Paramètres du scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez attribuer à ce scanner. Le nom peut comporter jusqu'à 255 caractères.
Description	Entrez une description pour ce scanner. La description peut comporter jusqu'à 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **Rapid7 Nexpose Scanner**.

Etape 6 Dans la zone de liste **Import Type**, sélectionnez **Import Site Data - Adhoc Report via API**.

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 9-2 Paramètres Rapid7 NeXpose

Paramètre	Description
Remote Hostname	Entrez le nom d'hôte ou l'adresse IP de la console de sécurité Rapid7 NeXpose configurés avec le site des données de vulnérabilité que vous souhaitez importer.
Login Username	Entrez le nom d'utilisateur pour vous connecter à la console de sécurité Rapid7 NeXpose. ***Remarque :*** *Le nom d'utilisateur doit être valide et obtenu à partir de l'interface d'utilisateur de la console de sécurité Rapid7 NeXpose. Pour en savoir plus, contactez votre administrateur Rapid7 NeXpose.*
Login Password	Entrez le mot de passe pour accéder à la console de sécurité Rapid7 NeXpose.
Port	Entrez le port utilisé pour accéder à la console de sécurité Rapid7 NeXpose. ***Remarque :*** *Le numéro de port est le même port utilisé pour accéder à l'interface utilisateur de console de sécurité Rapid7 NeXpose. C'est généralement le port 3780. Pour en savoir plus, contactez votre administrateur de serveur Rapid7 NeXpose.*
Site Name Pattern	Entrez un modèle d'expression régulière (regex) pour déterminer les sites Rapid7 NeXpose qu'il faut inclure dans le rapport d'analyse. Le modèle de nom du site par défaut **.*** sélectionne tous les rapports de nom de site disponibles. Tous les noms de site correspondant au modèle regex sont inclus dans le rapport d'analyse. Vous devez utiliser un modèle regex valide dans cette zone.
Cache Timeout (Minutes)	Entrez le temps de stockage des données dans la mémoire à partir du dernier rapport d'analyse généré. ***Remarque :*** *Si la limite de temps indiquée expire, de nouvelles données de vulnérabilité sont requises à partir de la console de sécurité Rapid7 NeXpose à l'aide de l'interface API.*

Etape 8 Pour configurer le routage CIDR devant être pris en compte par ce scanner :

a Dans la zone de texte, entrez le routage CIDR devant être pris en compte par ce scanner ou cliquez sur **Browse** afin de sélectionner le routage CIDR à partir de la liste de réseau.

b Cliquez sur **Add**.

NOTE

Dans la mesure où QRadar SIEM importe des rapports d'analyse de Radip7 NeXpose, nous vous recommandons de configurer un routage CIDR de 0.0.0.0/0 pour importer des rapports d'analyse. Cela prouve que les rapports d'analyse sont bien présents lors d'une analyse planifiée lorsque QRadar SIEM tente d'importer des rapports à partir de l'appareil Rapid7 NeXpose.

Etape 9 Cliquez sur **Save**.

Etape 10 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Vous pouvez maintenant ajouter une planification d'analyse afin de déterminer la fréquence à laquelle QRadar SIEM importe des rapports de données de vulnérabilité adhoc depuis Rapid7 NeXpose à l'aide de l'interface API. Pour en savoir plus sur la Gestion des plannings d'analyse, consultez **Gestion des plannings d'analyse**.

Identification et résolution des problèmes Rapid7 NeXpose API Scan Import

Les scanners Rapid7 NeXpose qui utilisent l'interface API pour collecter des rapports de vulnérabilité d'actifs adhoc sont basés sur votre site de configuration. Selon le nombre d'adresses IP configurées, chaque site peut impacter sur la taille du rapport adhoc. Les configurations de site importantes peuvent augmenter le volume des rapports de site et prendre plusieurs heures avant de s'achever. Rapid7 NeXpose doit générer un rapport d'analyse avec succès avant que le délai d'attente de session n'expire. Si vous n'êtes pas en mesure de récupérer les résultats d'analyse à partir de vos sites Rapid7 NeXpose à l'aide de QRadar SIEM, vous devez augmenter le délai d'attente de session Rapid7 NeXpose.

Pour configurer votre délai d'attente de session Rapid7 NeXpose procédez comme suit :

Etape 1 Accédez à l'interface utilisateur Rapid7 NeXpose.

Etape 2 Sélectionnez l'onglet **Administration**.

NOTE

Vous devez disposer de privilèges d'administrateur sur votre périphérique Rapid7 NeXpose pour afficher l'onglet **Administration**.

Etape 3 Dans la console de sécurité NeXpose, sélectionnez **Manage**.

La fenêtre de configuration NeXpose Security Console s'affiche.

Etape 4 Dans le menu de navigation du côté gauche de la fenêtre de configuration NeXpose Security Console, sélectionnez **Web Server**.

Etape 5 Augmentez la valeur pour **Session timeout (en secondes)**.

Etape 6 Cliquez sur **Save**.

Pour en savoir plus sur votre périphérique Rapid7 NeXpose, consultez votre fournisseur.

Si vous rencontrez toujours des problèmes concernant l'importation de sites à l'aide de l'interface API, utilisez l'importation de fichier local en déplaçant des analyses XML vers votre console QRadar SIEM ou l'hôte géré responsable de l'importation de données de vulnérabilité. Pour plus d'informations, voir **Importation de vulnérabilité Rapid7 NeXpose à partir d'un fichier local**.

Importation de vulnérabilité Rapid7 NeXpose à partir d'un fichier local

Importer des données de vulnérabilité à l'aide de fichiers locaux permet à QRadar SIEM d'importer des analyses complètes basées sur des rapports complets copiés à partir de votre scanner Rapid7 NeXpose pour QRadar SIEM.

Pour configurer QRadar SIEM afin d'importer des fichiers Rapid7 NeXpose :

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

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

La fenêtre Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 9-1 Paramètres du scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez attribuer à ce scanner. Le nom peut comporter jusqu'à 255 caractères.
Description	Entrez une description pour ce scanner. La description peut comporter jusqu'à 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **Rapid7 Nexpose Scanner**.

Etape 6 Dans la zone de liste **Import Type**, sélectionnez **Import Site Data - Local File**.

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 9-2 Paramètres Rapid7 NeXpose

Paramètre	Description
Import Folder	Entrez le chemin d'accès au répertoire sur la console QRadar SIEM ou l'hôte géré contenant les données de vulnérabilité XML. Si vous spécifiez un dossier d'importation, vous devez déplacer vos données de vulnérabilité de votre console de sécurité Rapid7 NeXpose vers QRadar SIEM. QRadar SIEM importe les informations d'actif du dossier de fichier local à l'aide de la zone modèle de fichier d'importation.

Tableau 9-2 Paramètres Rapid7 NeXpose (suite)

Paramètre	Description
Modèle de fichier d'importation	Entrez un modèle d'expression régulière (regex) pour déterminer les fichiers Rapid7 NeXpose XML qu'il faut inclure dans le rapport d'analyse. Tous les noms de fichier correspondant au modèle regex sont inclus lors de l'importation du rapport d'analyse de vulnérabilité. Vous devez utiliser un modèle regex valide dans la zone. La valeur par défaut.*\.xml importe tous les fichiers situés dans le dossier d'importation. ***Remarque :*** *Les rapports d'analyse importés et traités par QRadar SIEM ne sont pas supprimés du dossier d'importation, mais renommés en processed0. Nous vous recommandons de planifier une tâche cron afin de supprimer les rapports d'analyse précédemment traités sur une base planifiée.*

Etape 8 Pour configurer le routage CIDR devant être pris en compte par ce scanner procédez comme suit :

a Dans la zone de texte, entrez le routage CIDR devant être pris en compte par ce scanner ou cliquez sur **Browse** afin de sélectionner le routage CIDR à partir de la liste de réseau.

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

Etape 10 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Vous pouvez maintenant ajouter une planification d'analyse afin de déterminer la fréquence à laquelle QRadar SIEM importe des rapports de données de vulnérabilité locaux depuis des fichiers locaux sur la console QRadar SIEM ou l'hôte géré. Pour en savoir plus sur la planification d'une analyse, consultez **Gestion des plannings d'analyse**.

Modification d'un scanner Rapid7 NeXpose

Pour modifier un scanner Rapid7 NeXpose procédez comme suit :

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

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

La fenêtre Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez modifier.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Paramètres de mise à jour, si nécessaire. Voir **Tableau 9-2**.

Etape 7 Cliquez sur **Save**.

Etape 8 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Suppression d'un scanner Rapid7 NeXpose

Pour supprimer un scanner Rapid7 NeXpose procédez comme suit :

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

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

La fenêtre Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez sur **OK**.

Etape 7 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

12 GESTION DE netVigilance SecureScout SCANNERS

Les deux périphériques SecureScout NX et SecureScout SP enregistrent tous les résultats d'analyse vers une base de données SQL (Microsoft MSDE ou SQL Server). IBM Security QRadar SIEM se connecte à la base de données, situe les résultats d'analyse les plus récents pour une adresse IP donnée et renvoie les services et vulnérabilités découverts vers le profil d'actif. Cela vous permet de rechercher des actifs et vulnérabilités en utilisant l'onglet **Asset** dans QRadar SIEM. QRadar SIEM prend en charge la version 2.6 du scanner SecureScout.

Pour connecter à QRadar SIEM vers la base de données SecureScout et analyser les résultats, vous devez disposer de l'accès administratif adéquat vers QRadar SIEM et vers votre périphérique SecureScout. Pour plus d'informations, voir votre documentation SecureScout. Assurez-vous que tous les pare-feux, y compris le pare-feu se trouvant sur l'hôteSecureScout, autorisent une connexion à Event Collector. IBM Security QRadar SIEM se connecte à un serveur SQL via une connexion TCP sur le port 1433.

Nous vous recommandons de créer un utilisateur dans votre configuration SecureScout, spécialement pour QRadar SIEM. L'utilisateur de base de données que vous créez doit avoir sélectionné les permissions aux tableaux suivants :

- HOST
- JOB
- JOB_HOST
- SERVICE
- TCRESULT
- TESTCASE
- PROPERTY
- PROP_VALUE
- WKS

REMARQUE

L'utilisateur doit avoir exécuté les permissions dans la procédure mémorisée IPSORT.

Après avoir ajouté le scanner SecureScout à QRadar SIEM, vous pouvez planifier une analyse. Pour plus d'informations, voir **Gestion des plannings d'analyse**.

Cette section contient des informations sur les rubriques suivantes :

- **Ajout d'un scanner SecureScout**
- **Modification d'un scanner SecureScout**
- **Suppression d'un scanner SecureScout**

Ajout d'un scanner SecureScout

Pour ajouter un scanner SecureScout :

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs pour les paramètres suivants :

Tableau 10-1 Paramètres SecureScout

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez affecter à scanner. Le nom peut contenir plus de 255 caractères.
Description	Entrez une description pour ce scanner. La description peut contenir plus de 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **SecureScout Scanner.**

Etape 6 Configurez les valeurs pour les paramètres suivants :

Tableau 10-2 Paramètres SecureScout

Paramètre	Description
Database Hostname	Entrez l'adresse IP ou le nom d'hôte du serveur de base de données SecureScout exécutant le serveur SQL.
Login Username	Entrez le nom d'utilisateur de base de données SQL dont vous souhaitez que QRadar SIEM utilise pour se connecter à la base de données SecureScout.
Login Password	Entrez le mot de passe correspondant au nom d'utilisateur de connexion.

Tableau 10-2 Paramètres SecureScout (suite)

Paramètre	Description
Database Name	Entrez le nom de la base de données dans le serveur SQL contenant les données SecureScout. La valeur par défaut est SCE.
Database Port	Entrez le port TCP dont vous souhaitez faire contrôler les connexions via le serveur SQL. La valeur par défaut est 1433.

Etape 7 Pour configurer les intervalles de routage CIDR que vous souhaitez mettre en évidence par cette analyse :

a Dans le champ de texte, entrez l'intervalle de routage CIDR que ce scanner doit prendre en considération ou cliquez sur **Browse** pour sélectionner l'intervalle de routage CIDR à partir de la liste réseaux.

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

Etape 9 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Modification d'un scanner SecureScout

Pour modifier un scanner SecureScout :

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez modifier.

Etape 5 Click **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Mettez à jour les paramètres, si nécessaire. Voir **Tableau 10-2**.

Etape 7 Cliquez sur **Save**.

Etape 8 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Suppression d'un scanner SecureScout

Pour supprimer un scanner a SecureScout à partir de QRadar SIEM:

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez sur **OK**.

Etape 7 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

13 GESTION DES scanners EEYE

IBM Security QRadar SIEM prend en charge à la fois les scanners eEye REM Security Management Console et eEye Retina CS. Les scanners eEye utilisent SNMPv1, SNMPv2 ou SNMPv3 pour envoyer des alertes SNMP vers QRadar SIEM.

Pour configurer les scanners eEye avecQRadar SIEM, vous devez :

1. Configurez votre scanner eEye pour transférer des alertes SNMP vers QRadar SIEM. Pour plus d'informations, voir la documentation du fournisseur eEye.
2. Ajoutez votre scanner à QRadar SIEM. Pour plus d'informations, voir **Ajout d'un scanner eEye**.
3. Facultatif. Installez Java™ Cryptography Extension pour obtenir des algorithmes de description SNMPv3 de niveau supérieur. Pour plus d'informations, voir **Installation de Java Cryptography Extension**.
4. Planifiez une analyse pour votre scanner eEye dans QRadar SIEM. Pour plus d'informations, voir **Gestion des plannings d'analyse**.

A la fin d'une analyse, les résultats sont envoyés vers QRadar SIEM à l'aide de SNMP et sont stockés dans QRadar SIEM ou votre hôte géré dans un répertoire temporaire.QRadar SIEM surveille constamment le port d'écoute pour obtenir des informations d'actifs et de vulnérabilité à partir du scanner eEye. Pour garantir que les informations sur les profils de port et d'hôte sont mises à jour dans QRadar SIEM, vous devez configurer un planning d'analyse pour votre scanner eEye. Le planning d'analyse détermine la fréquence à laquelle QRadar SIEM importe les données SNMP stockées dans le champ **Base Directory**. Ce planning d'analyse rend les profils de port et d'hôte disponibles dans la base de données de profils.

Pour connecter QRadar SIEM au scanner eEye, vous devez disposer d'un accès administrateur à QRadar SIEM et à votre dispositif eEye. Vous devez également vérifier que les pare-feu entre votre scanner eEye et QRadar SIEM autorisent le trafic SNMP.

Cette section comprend les rubriques suivantes :

- **Ajout d'un scanner eEye**
- **Edition d'un scanner eEye**
- **Suppression d'un scanner eEye.**

Ajout d'un scanner eEye

Pour ajouter un scanner eEye REM :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs pour les paramètres suivants :

Tableau 11-1 Paramètres eEye REM

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez affecter à ce scanner. Le nom peut contenir jusqu'à 255 caractères.
Description	Entrez une description pour ce scanner. La description peut contenir jusqu'à 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez la description que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **eEye REM Scanner.**

Etape 6 Configurez les valeurs pour les paramètres suivants :

Tableau 11-2 Paramètres eEye

Paramètre	Description
Base Directory	Entrez l'emplacement dans lequel vous souhaitez stocker les fichiers temporaires résultant du scan. L'emplacement par défaut est /store/tmp/vis/eEye/.
Cache Size	Entrez le nombre de transactions que vous souhaitez stocker dans le cache avant d'écrire les informations sur le disque. La valeur par défaut est 40.
Retention Period	Entrez la plage de temps, en jours, à laquelle le système stocke les informations de scan. Si vous n'avez pas planifié une analyse à la fin de la durée de conservation, les informations sont supprimées. La durée de conservation par défaut est 5 jours.

Tableau 11-2 Paramètres eEye (suite)

Paramètre	Description
Use Vulnerability Data	Cochez la case pour corréler les données de vulnérabilité aux identifiants Common Vulnerabilities and Exposures (CVE) et les informations de description à partir de votre scanner eEye REM ou eEye CS Retina. Par défaut, fichier de données de vulnérabilité audits.xml se trouve dans le répertoire suivant : **`%ProgramFiles(x86)%\eEye Digital Security\Retina CS\Applications\RetinaManager\Database\audits.xml`** ***Note:*** *Cette option requiert une copie du fichier audits.xml à partir de votre dispositif eEye REM ou eEye Retina CS vers QRadar SIEM.*
Vulnerability Data File	Entrez le chemin de répertoire pour accéder au fichier eEye audits.xml. Le chemin de répertoire par défaut est **`/opt/qradar/conf/audits.xml`**. ***Note:*** *Pour obtenir les informations d'audit les plus récentes d'eEye, vous devez mettre QRadar SIEM à jour de manière périodique avec le plus récent fichier audits.xml à partir de votre scanner eEye REM ou eEye Retina. Pour plus d'informations, voir la documentation du fournisseur eEye.*
Listen Port	Entrez le numéro de port utilisé pour surveiller les informations de vulnérabilité SNMP entrantes depuis votre scanner eEye. La valeur par défaut est 1162.
Source Host	Entrez l'adresse IP du scanner eEye REM ou eEye Retina CS.
SNMP Version	Dans la zone de liste, sélectionnez la version SNMP que vous souhaitez configurer pour que votre scanner eEye la transfère. Les options incluent : • **v1** - Sélectionnez v1 si votre scanner eEye transfère des messages d'alerte SNMPv1. • **v2** - Sélectionnez v2 si votre scanner eEye transfère des messages d'alerte SNMPv2. • **v3** - Sélectionnez v3 si votre scanner eEye transfère des messages d'alerte SNMPv3. Le message d'alerte par défaut est SNMPv2.
Community String	Entrez le nom de communauté SNMP pour le protocole SNMPv2, par exemple, Public. Le paramètre est uniquement utilisé si vous sélectionnez v2 pour la version SNMP. Le nom de communauté par défaut est public.

Tableau 11-2 Paramètres eEye (suite)

Paramètre	Description
Authentication Protocol	Dans la zone de liste, sélectionnez l'algorithme que vous souhaitez utiliser pour authentifier les alertes SNMP. Ce paramètre est obligatoire si vous utilisez SNMPv3. Les options incluent : • **SHA** - Sélectionnez cette option pour utiliser Secure Hash Algorithm (SHA) en tant que protocole d'authentification. • **MD5** - Sélectionnez cette option pour utiliser Message Digest 5 (MD5) en tant que protocole d'authentification. Le protocole par défaut est SHA.
Authentication Password	Entrez le mot de passe que vous souhaitez utiliser pour authentifier SNMP. Ce paramètre ne s'applique qu'à SNMPv3. ***Note:*** *Votre mot de passe d'authentification doit inclure 8 caractères au minimum.*
Encryption Protocol	Dans la zone de liste, sélectionnez l'algorithme que vous souhaitez utiliser pour déchiffrer les alertes SNMP. Ce paramètre est obligatoire si vous utilisez SNMPv3. Les algorithmes de description comprennent : • DES • AES128 • AES192 • AES256 L'algorithme de description par défaut est DES. ***Note:*** *Si vous sélectionnez AES192 ou AES256 en tant que votre algorithme de description, vous devez installer des logiciels supplémentaires pour QRadar SIEM. Pour plus d'informations, voir* **Installation de Java Cryptography Extension**.
Encryption Password	Entrez le mot de passe utilisé pour déchiffrer les alertes SNMP. Ce paramètre est obligatoire si vous utilisez SNMPv3. ***Note:*** *Votre mot de passe de chiffrement doit inclure 8 caractères au minimum.*

Etape 7 Pour configurer les intervalles CIDR que ce scanner doit prendre en considération :

a Dans la zone de texte, entrez l'intervalle CIDR que vous souhaitez que ce scanner doit prendre en considération ou cliquez sur **Browse** pour sélectionner l'intervalle CIDR à partir de la liste réseaux.

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

Etape 9 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

Les modifications apportées à votre configuration SNMP pour votre scanner eEye ne prennent effet qu'au début de la prochaine analyse planifiée. Si la modification de la configuration requiert une mise à jour immédiate, vous devez achever un déploiement total dans QRadar SIEM. Pour plus d'informations, voir **Edition d'un scanner eEye**,**Step 9**.

La configuration dans QRadar SIEM est achevée.

Si vous avez sélectionné SNMPv3 comme étant votre configuration eEYe avec le chiffrement AES192 ou AES256, vous devez installer un composant Java™ supplémentaire sur votre console QRadar SIEM ou votre collecteur d'événement.

Installation de Java Cryptography Extension

Java™ Cryptography Extension (JCE) est une infrastructure Java™ requise pour que QRadar SIEM puisse décrypter les algorithmes de cryptographie avancée pour AES192 ou AES256. Les informations suivantes décrivent la manière d'installer Oracle JCE sur QRadar SIEM et sur votre dispositif McAfee ePO.

Pour installer Oracle JCE sur QRadar SIEM.

Etape 1 Téléchargez la plus récente version de Java™ Cryptography Extension:

http://www.oracle.com/technetwork/java/javase/downloads/index.html

Il est possible que plusieurs versions de JCE soient disponibles pour téléchargement. La version que vous devez télécharger correspond à la version de Java™ installée sur QRadar SIEM.

Etape 2 Extrayez le fichier JCE.

Les fichiers archive suivants sont inclus dans le téléchargement de JCE :

- local_policy.jar
- US_export_policy.jar

Etape 3 En utilisant SSH, connectez-vous à votre console QRadar SIEM ou hôte géré en tant que superutilisateur.

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

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

Etape 4 Copiez les fichiers JCE jar vers le répertoire suivant sur votre console QRadar SIEM ou hôte géré :

`/usr/java/latest/jre/lib/`

Les fichiers JCE jar sont uniquement copiés vers le système qui reçoit les fichiers AES192 ou AE256 à partir de McAfee ePolicy Orchestrator. En fonction de votre configuration, votre console QRadar SIEM ou un hôte géré peut être sollicité.

L'installation de Java™ Cryptography Extension pour QRadar SIEM est terminée. Vous pouvez maintenant planifier une analyse pour votre scanner eEye dans QRadar SIEM. Pour plus d'informations, voir **Gestion des plannings d'analyse**.

Edition d'un scanner eEye

Pour éditer un scanner eEye :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez éditer.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Paramètres de mise à jour, si nécessaire. Voir **Tableau 11-2**.

Etape 7 Cliquez sur **Save**.

Etape 8 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Les modifications apportées à la configuration SNMP pour votre scanner eEye ne prennent effet qu'au début de la prochaine analyse planifiée. Si la modification de la configuration requiert une mise à jour immédiate, vous devez achever un déploiement total dans QRadar SIEM.

Etape 9 Optionel. Sur l'onglet **Admin**, sélectionnez **Advanced > Deploy Full Configuration**.

ATTENTION

L'option Deploying Full Configuration redémarre plusieurs services sur QRadar SIEM. La collection d'événements ne sera pas disponible surQRadar SIEM tant que Deploy Full Configuration n'est pas terminé.

Suppression d'un scanner eEye.

Pour supprimer un scanner eEye REM :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez sur **OK**.

Etape 7 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

14 GESTION DES scanners PATCHLINK

Vous pouvez intégrer un scanner PatchLink (version 6.4.4. et supérieure) à IBM Security QRadar SIEM. Le scanner PatchLink envoie des requêtes au moteur afin d'utiliser l'interface API. QRadar SIEM collecte des données de vulnérabilité à partir des résultats d'analyse avec PatchLink. Par conséquent, votre système PatchLink doit inclure une configuration appropriée pour QRadar SIEM ainsi qu'un système d'analyse qui fonctionne correctement afin d'être sûr d'obtenir des résultats à jour. Etant donné que l'interface API fournit un accès à l'application PatchLink, assurez-vous que l'application fonctionne en permanence sur le serveur PatchLink.

REMARQUE

Le scanner PatchLink est désormais connu sous le nom de Lumension Security Management Console mais également sous Harris Stat Guardian.

Pour connecter QRadar SIEM au scanner PatchLink, vous devez avoir un accès administrateur approprié à QRadar SIEM et à votre périphérique PatchLink. Pour en savoir plus, consultez votre documentation du produit. Assurez-vous que tous les pare-feu entre votre dispositif PatchLink et QRadar SIEM sont configurés pour permettre les communications.

Après avoir configuré votre dispositif PatchLink et ajouté un scanner PatchLink à QRadar SIEM, vous pouvez planifier une analyse. Un planning d'analyse vous permet de déterminer la fréquence à laquelle QRadar SIEM demande des données à partir de votre dispositif PatchLink à l'aide de l'interface de programme d'application du protocole SOAP. Pour plus d'informations, voir **Gestion des plannings d'analyse**.

Cette section fournit des informations sur les éléments suivants :

Ajout d'un scanner PatchLink

Pour ajouter un scanner PatchLink, procédez comme suit :

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 12-1 Paramètres du scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez attribuer à ce scanner. Le nom peut comporter jusqu'à 255 caractères.
Description	Entrez une description pour ce scanner. La description peut comporter jusqu'à 255 caractères.
Managed Host	A partir de la zone de liste, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.
Type	A partir de la zone de liste, sélectionnez **Lumension PatchLink Scanner**.

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 12-2 Paramètres PatchLink

Paramètre	Description
Engine Address	Entrez l'adresse dans laquelle le scanner PatchLink est installé.
Port	L'interface de programmation d'application (API) transmet des demandes du protocole SOAP à travers HTTPS au port par défaut du moteur (205). Si le port par défaut est changé en modifiant la clé de registre **`HKLM\Software\Harris\reportcenter_listenport`**, indiquez le numéro du nouveau port.
Username	Entrez le nom d'utilisateur devant être utilisé par QRadar SIEM pour l'authentification du moteur PatchLink. L'utilisateur doit avoir accès à la configuration d'analyse (système administrateur par défaut).
Password	Entrez le mot de passe correspondant au nom d'utilisateur.
Job Name	Entrez le nom de tâche existant dans le scanner PatchLink. la tâche doit être terminée avant de planifier un processus d'analyse sous QRadar SIEM.

Tableau 12-2 Paramètres PatchLink (suite)

Paramètre	Description
Résultat de la fréquence de rafraîchissement (en minutes)	Entrez la fréquence à laquelle vous souhaitez que le scanner récupère les résultats à partir du serveur PatchLink. Ce processus de récupération est un processus qui exige d'importantes ressources et se fait uniquement après l'intervalle de temps défini dans cette zone. Les valeurs valides sont configurées en quelques minutes et les valeurs par défaut en 15 minutes.

Etape 7 Pour configurer les plages de routage CIDR que ce scanner doit prendre en compte :

a Dans la zone de texte, entrez le routage CIDR qui doit être pris en compte par le scanner ou cliquez sur **Browse** afin de sélectionner le routage CIDR à partir de la liste de réseau.

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

Etape 9 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Modification d'un scanner PatchLink

Pour modifier un scanner PatchLink :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez modifier.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Mettez à jour les paramètres, si nécessaire. Voir **Tableau 12-2**.

Etape 7 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Suppression d'un scanner PatchLink

Pour supprimer un scanner PatchLink de QRadar SIEM:

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez sur **OK**.

Etape 7 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

15 GESTION DES SCANNERS MCAFEE VULNERABILITY MANAGER

Le scanner McAfee Vulnerability Manager IBM Security QRadar SIEM autorise QRadar SIEM à interroger le moteur McAfee Foundstone Enterprise à l'aide de l'OpenAPI de McAfee. Le scanner McAfee Vulnerability Manager n'effectue pas directement des analyses mais rassemble les résultats d'analyse disponibles tels qu'ils sont affichés dans l'application de numérisation. QRadar SIEM prend en charge les versions 6.8 ou 7.0. de McAfee Vulnerability Manager.

REMARQUE

Seul McAfee Vulnerability Manager est pris en charge pour chaque QRadar SIEM Console ou remote Event Collector.

REMARQUE

Foundstone et ses produits de scanner ont été acquis par McAfee et sont commercialisés en tant que McAfee Vulnerability Manager. Si vous utilisez une version précédente du scanner Foundstone Foundscan, consultez **Gestion des scanners Foundscan.**

Votre système McAfee Foundstone Enterprise doit inclure une configuration appropriée pour QRadar SIEM ainsi qu'un système d'analyse fonctionnant régulièrement pour s'assurer que les résultats sont à jour. Pour vous assurer que votre scanner McAfee Vulnerability Manager est capable de récupérer des informations d'analyse, vérifiez que votre système McAfee Foundstone Enterprise satisfait aux exigences suivantes :

- Etant donné que l'API Open de Foundstone permet d'accéder au serveur McAfee Foundstone Enterprise Manager, assurez-vous que l'application McAfee Foundstone Enterprise McAfee Foundstone Enterprise) s'exécute en continu sur ledit serveur.
- L'analyse qui inclut la configuration requise pour se connecter à QRadar SIEM doit être entièrement exécutée et visible dans l'interface utilisateur McAfee Foundstone Enterprise QRadar SIEM pour récupérer les résultats d'analyse. Si l'analyse ne s'affiche pas dans l'interface utilisateur McAfee Foundstone Enterprise ou doit être supprimée après exécution, QRadar SIEM doit récupérer les résultats avant la suppression ou l'échec de l'analyse.

- Les privilèges d'utilisateur appropriés doivent être configurés dans l'application McAfee Foundstone Configuration Manager, ce qui permet à QRadar SIEM de communiquer avec McAfee Foundstone Enterprise.

Etant donné que FoundScan OpenAPI ne fournit à QRadar SIEM que des informations sur l'hôte et les vulnérabilités, les informations du profil de l'actif affichent toutes les vulnérabilités d'un port affecté au port 0.

SSL connecte le serveur McAfee Foundstone Enterprise Manager à l'OpenAPI Foundstone. QRadar SIEMauthentifie le serveur McAfee Foundstone Enterprise Manager en utilisant les certificats côté client. Vous devez créer et gérer les certificats appropriés sur le serveur McAfee Foundstone Enterprise Manager, puis importer les clés sur QRadar SIEM. Pour plus d'informations, voir **Utilisation des certificats**.

Après avoir configuré le système McAfee Foundstone Enterprise et le scanner McAfee Vulnerability Manager dansQRadar SIEM, vous pouvez programmer l'analyse. Les plannings d'analyse vous permettent de déterminer la fréquence à laquelle QRadar SIEM demande des données à votre dispositif McAfee en utilisant l'Open API de McAfee. Pour plus d'informations, voir **Gestion des plannings d'analyse.**

Cette section fournit des informations sur les éléments suivants :

- **Ajouter un scanner McAfee Vulnerability Manager**
- **Editer un scanner McAfee Vulnerability Manager**
- **Supprimer un scanner McAfee Vulnerability Manager**
- **Utilisation des certificats**

Ajouter un scanner McAfee Vulnerability Manager

Pour ajouter un scanner McAfee Vulnerability Manager :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 définit les valeurs des paramètres suivants:

Tableau 13-1 Paramètres du scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez attribuer à ce scanner. Le nom peut comporter jusqu'à 255 caractères.
Description	Entrez une description pour ce scanner. La description peut comporter jusqu'à 255 caractères.
Managed Host	Dans la liste déroulante, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **McAfee Vulnerability Manager**.

Etape 6 définit les valeurs des paramètres suivants:

Tableau 13-2 Paramètres de McAfee Vulnerability Manager

Paramètre	Description
SOAP API URL	Saisissez l'adresse Web de l'API de Foundscan Open au format suivant : **`https://<IP address>:<SOAP port>`** Où : **`<IP address>`** est l'adresse IP ou le nom d'hôte de McAfee Foundstone Enterprise Manager Server. **`<SOAP port>`** est le numéro de port pour la connexion entrante au serveur API Open. L'adresse par défaut est **`https://localhost:3800.`**
Customer Name	Entrez un nom pour identifier à quel client ou organisation appartient le nom d'utilisateur. Le nom du client doit correspondre à l'ID de l'organisation requise pour se connecter à McAfee Foundstone Enterprise Manager.
User Name	Entrez le nom d'utilisateur que vous voulez que QRadar SIEM utilise pour authentifier le serveur McAfee Foundstone Enterprise Manager dans l'API Open Cet utilisateur doit avoir accès à la configuration d'examen.
Password	Entrez le mot de passe correspondant au nom de connexion pour avoir accès à l'API Open.
Client IP Address	Entrez l'adresse IP du serveur QRadar SIEM que vous avez choisi pour effectuer les analyses. Par défaut, cette valeur n'est pas utilisée. Cependant, elle est requise pour valider certains environnements.
Portal Name	Facultatif. Entrez le nom du portail. Ce champ peut être laissé vide pour QRadar SIEM. Consultez l'administrateur de McAfee Vulnerability Manager administrator pour de plus amples informations.
Configuration Name	Entrez le nom de la configuration d'examen qui existe dans McAfee Foundstone Entreprise et auquel l'utilisateur a accès.

Tableau 13-2 Paramètres de McAfee Vulnerability Manager (suite)

Paramètre	Description
CA Truststore	Entrez le chemin de répertoire et le nom du fichier de clés certifiées CA. Le chemin de répertoire par défaut est /opt/qradar/conf/mvm.keystore. ***Note:*** *Pour plus d'informations, sur les certificats McAfee Vulnerability Manager, voir* **Utilisation des certificats**.
Client Keystore	Entrez le chemin de répertoire et le nom du fichier des fichiers de clés du client. Le chemin de répertoire par défaut est /opt/qradar/conf/mvm.truststore. ***Note:*** *Pour plus d'informations sur les certificats McAfee Vulnerability Manager, voir* **Utilisation des certificats**.
McAfee Vulnerability Manager Version	Dans la liste déroulante, spécifiez la version de votre McAfee Vulnerability Manager.

Etape 7 Pour configurer les plages de routage CIDR que vous voulez que le scanner doit prendre en compte:

a Dans la zone de texte, tapez la plage CIDR que vous souhaitez que le scanner doit prendre en compte ou cliquez sur Browse pour sélectionner la plage CIDR à partir de la liste de réseaux.

REMARQUE

McAfee Vulnerability Manager n'accepte que les adresses CIDR dans un sous-réseau 0/0 ajouté en tant que 0.0.0.0/0. Les adresses CIDR qui se terminent par 0/0 ne sont plus acceptées dans la configuration. Cela est dû aux limitations de l'Open API de McAfee.

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

Etape 9 Dans le menu de l'onglet **Admin**, sélectionnez **Deploy Changes**.

Editer un scanner McAfee Vulnerability Manager

Pour éditer un scanner McAfee Vulnerability Manager :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez éditer.

Etape 5 Cliquer sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Mettez à jour les paramètres si nécessaire. Voir **Table 13-2**.

Etape 7 Cliquez sur **Save**.

Etape 8 Dans le menu de l'onglet **Admin**, sélectionnez **Deploy Changes**.

Supprimer un scanner McAfee Vulnerability Manager

Pour supprimer un scanner McAfee Vulnerability Manager:

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez sur **OK**.

Etape 7 Dans le menu de l'onglet **Admin**, sélectionnez **Deploy Changes**.

Utilisation des certificats

McAfee Certificate Manager Tool est requis pour créer des certificats tiers et se connecter à travers l'Open Api Foundstone. Si le Certificate Manager Tool n'est pas encore installé sur le serveur McAfee Foundstone Enterprise Manager, contactez l'équipe d'assistance technique de McAfee.

Vous devez traiter les certificats côté client de sorte que vous ayez des fichiers de clés et de clés certifiées pour QRadar SIEM sur le serveur McAfee Foundstone Enterprise Manager. Le serveur McAfee Foundstone Enterprise Manager doit être compatible avec la version d'OpenSSL répondant aux normes FIPS utilisée par le Foundstone Certficate Manager pour générer correctement les certificats. Un kit de développement de logiciels Java ™ (Java™ SDK) doit être installé sur ce serveur pour ce traitement. Pour acquérir la dernière version du kit de développement de logiciels Java ™ consultez *http://java.sun.com*.

Cette section fournit des informations sur l'obtention et l'importation du certificats requis, notamment :

- **Obtention de certificats**
- **Traitement des certificats**
- **Importer des certificats**

Obtention de certificats

Pour obtenir les certificats requis :

Etape 1 Exécutez Foundstone Certificate Manager.

Etape 2 Cliquez sur l'onglet **Create SSL Certificates.**

Etape 3 Configurez l'adresse hôte de QRadar SIEM.

REMARQUE

Si vous utilisez un collecteur d'événements à distance, le certificat doit être généré en utilisant l'adresse hôte du collecteur d'événements à distance.

Etape 4 Facultatif. Cliquez sur **Resolve**.

REMARQUE

Nous vous recommandons de saisir une adresse IP dans le champ adresse de l'hôte lorsque Foundstone Certificate Manager génère un message d'erreur

Si vous n'avez le programme de résolution du nom d'hôte, consultez **Etape 6**.

Etape 5 Cliquez sur **Create Certificate Using Common Name**.

Etape 6 Cliquez sur **Create Certificate Using Host Address**.

McAfee Certificate Manager Tool génère un fichier zip et fournit une phrase passe pour le certificat.

Etape 7 Enregistrer le fichier zip contenant les fichiers de certificat dans un répertoire accessible.

Etape 8 Copier dans le même emplacement la phrase passe fournie dans un fichier texte

REMARQUE

Nous vous recommandons de sauvegarder cette phrase de passe pour une utilisation future. Si vous perdez votre phrase de passe de **Etape 8**, vous devez créer de nouveaux certificats.

Vous êtes maintenant prêt pour traiter les certificats de QRadar SIEM. Voir **Traitement des certificats**.

Traitement des certificats

Pour traiter les certificats :

Etape 1 Extrayez le fichier zip contenant les certificats de **Etape 7** vers un répertoire de votre McAfee Vulnerability Manager

Etape 2 A partir du site Qmmunity, téléchargez les fichiers suivants dans le même répertoire que celui des fichiers de certificat extraits.

```
VulnerabilityManager-Cert.bat.gz
```

```
q1labs_vis_mvm_cert.jar
```

Etape 3 Extraire le fichier:

```
gzip -d VulnerabilityManager-Cert.bat.gz
```

Etape 4 Exécutez la commande **`VulnerabilityManager-Cert.bat`**, notamment le chemin d'accès à votre répertoire de base Java™.

Par exemple :

```
VulnerabilityManager-Cert.bat "C:\Program Files\Java\jdk1.6.0_20"
```

REMARQUE

Il est nécessaire d'utiliser des guillemets lorsque vous spécifiez le répertoire de base Java ™ de votre fichier de commandes.

Si **`VulnerabilityManager-Cert.bat`** n'est pas en mesure de trouver les fichiers Java™ et que les fichiers de commandes ne peuvent trouver leur emplacement, un message d'erreur est alors généré.

Etape 5 Lorsque vous y êtes invité, saisissez la phrase de passe fournie dans **Etape 6**.

Après avoir saisi la phrase de passe, le message suivant s'affiche pour vous informer de la création des fichiers.

```
Keystore File Created
Truststore File Created
```

Vous pouvez maintenant importer les certificats dans QRadar SIEM. Voir **Importer des certificats**.

Importer des certificats

Les fichiers de clés ainsi que les fichiers de clés certifiées doivent être importés vers QRadar SIEM. Nous vous recommandons vivement d'utiliser une méthode sécurisée pour copier les fichiers de certificat, comme SCP.

REMARQUE

Avant d'importer des fichiers, nous vous recommandons de supprimer ou renommer les fichiers de clés ainsi que les fichiers de clés certifiées des configurations précédentes.

Etape 1 Pour importer les certificats, assurez-vous que vous avez copié les fichiers **mvm.keystore** et **mvm.truststore** sur les répertoires suivants dans QRadar SIEM :

`/opt/qradar/conf`

`/opt/qradar/conf/trusted_certificates`

ATTENTION

En fonction de votre configuration, votre système pourrait ne pas contenir le répertoire **`/opt/qradar/conf/trusted_certificates`***. Si ce répertoire n'existe pas, ne le créez pas et n'oubliez pas de copier le fichier dans* **`/opt/qradar/conf/trusted_certificates.`**

Etape 2 Se connectez à QRadar SIEM.

`https://<IP Address>`

Où <IP Address> est l'adresse IP de la console QRadar SIEM.

Etape 3 Cliquez sur l'onglet **Admin**.

L'onglet Administration s'affiche.

Etape 4 Sur l'onglet **Admin**, sélectionnez **Advanced > Deploy Full Configuration**.

ATTENTION

Le fait de sélectionner Deploy Full Configuration permet de redémarrer QRadar SIEM les services avec comme résultat un écart dans la collecte de données pour les événements et les flux, ceci jusqu'à exécution complète du processus de déploiement

16 GESTION DES SCANNERS SAINT

Vous pouvez intégrer un scanner de vulnérabilité Security Administrator's Integrated Network Tool (SAINT) avec QRadar SIEM via l'utilisation de la version 7.4.x de SAINT. En utilisant QRadar SIEM, vous pouvez planifier et lancer les analyses de vulnérabilité SAINT ou générer des rapports à l'aide des données de vulnérabilité existantes. Le scanner SAINT identifie les vulnérabilités basées sur le niveau d'analyse indiqué et utilise SAINTwriter pour générer les rapports personnalisés pour QRadar SIEM. Votre système SAINT doit donc comprendre un modèle de rapport SAINTwriter convenable pour QRadar SIEM et une analyse qui s'effectue régulièrement pour garantir que les résultats sont récents.

Pour intégrer QRadar SIEM au scanner SAINT, vous devez avoir l'accès administrateur adéquat à QRadar SIEM et à votre dispositif SAINT. Vous devez également vous assurer que les pare-feu sont configurés pour autoriser une communication entre votre dispositif SAINT et QRadar SIEM. Pour plus d'informations, voir la documentation de votre produit.

Après avoir configuré SAINTwriter, vous pouvez planifier une analyse. Un planning d'analyse vous permet de déterminer la fréquence à laquelle QRadar SIEM demande des données à partir de votre dispositif SAINT. Pour plus d'informations, voir **Gestion des scanners SAINT**.

Cette section fournit des informations sur les éléments suivants :

- **Configuration du modèle de rapport SAINTwriter**
- **Ajout d'un scanner de vulnérabilité SAINT**
- **Modification d'un scanner de vulnérabilité SAINT**
- **Suppression d'un scanner de vulnérabilité SAINT**

Configuration du modèle de rapport SAINTwriter

Pour configurer un modèle de rapport SAINTwriter :

Etape 1 Connectez-vous à l'interface utilisateur SAINT.

Etape 2 Sélectionnez **Data > SAINTwriter**.

Etape 3 Cliquez sur **Type**.

Etape 4 Dans la zone de liste, sélectionnez **Custom**.

Etape 5 Dans la zone **File Name**, indiquez le nom d'un fichier de configuration.

Le nom du fichier de configuration doit correspondre au paramètre QRadar SIEM Saint Writer Config dans **Tableau 14-2**.

Etape 6 Dans la zone de liste **Template Type**, sélectionnez **Technical Overview**.

Etape 7 Cliquez sur **Continue**.

Le menu Category s'affiche.

Etape 8 Sélectionnez **Lists**.

Etape 9 Dans **Columns to include in host list**, modifiez toutes les colonnes marquées comme None sur **MAC Address**.

Etape 10 Dans **Columns to include in vulnerability list**, modifiez toutes les colonnes marquées comme None sur **Port**.

Etape 11 Dans **Columns to include in vulnerability list**, modifiez toutes les colonnes marquées comme None sur **Service**.

Etape 12 Cliquez sur **Save**.

Vous pouvez maintenant ajouter un scanner de vulnérabilité SAINT à QRadar SIEM, voir **Ajout d'un scanner de vulnérabilité SAINT**.

Ajout d'un scanner de vulnérabilité SAINT

Pour ajouter un scanner de vulnérabilité SAINT à QRadar SIEM:

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 14-1 Paramètres du scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez affecter au scanner. Le nom peut contenir jusqu'à 255 caractères.
Description	Entrez une description pour ce scanner. La description peut contenir jusqu'à 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.

Tableau 14-1 Paramètres du scanner (suite)

Paramètre	Description
Type	Dans la zone de liste, sélectionnez **SAINT Scanner**.

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 14-2 Paramètres du scanner SAINT

Paramètre	Description
Remote Hostname	Entrez le nom d'hôte ou l'adresse IP du système hébergeant le scanner SAINT.
Login Username	Entrez le nom d'utilisateur utilisé par QRadar SIEM pour authentifier la connexion SSH.
Enable Key Authorization	Cochez cette case pour activer l'authentification par clé publique/privée. Si la case à cocher est sélectionnée, QRadar SIEM tente d'authentifier la connexion SSH en utilisant la clé privée fournie et le paramètre Login Password est ignoré. Par défaut, la case à cocher est vide. Pour plus d'informations, voir votre documentation SSH pour configurer l'authentification par clé publique.
Login Password	Entrez le mot de passe associé à Login Username pour l'accès SSH. Si Enable Key Authentication est activé, ce paramètre est ignoré.
Private Key File	Entrez le chemin de répertoire au fichier contenant les informations de la clé privée. Si vous utilisez une authentification basée sur la clé SSH, QRadar SIEM utilise la clé privée pour authentifier la connexion SSH. La valeur par défaut est /opt/qradar/conf/vis.ssh.key. Toutefois, par défaut, ce fichier n'existe pas. Vous devez créer le fichier vis.ssh.key ou le nom d'un autre type de fichier. Ce paramètre est obligatoire si la case Enable Key Authentication est cochée. Si la case à cocher Enable Key Authentication est vide, ce paramètre est ignoré.
SAINT Base Directory	Entrez le chemin d'accès vers le répertoire d'installation pour SAINT.
Scan Type	Vous pouvez configurer un scanner pour récupérer les données SAINT en utilisant Live Scan ou vous pouvez sélectionner Report Only. Dans la zone de texte, sélectionnez le type de collection : • **Live Scan** - Lance une analyse de vulnérabilité et génère des données de rapport à partir des résultats d'analyse basés sur le nom de session. • **Report Only** - Génère un rapport d'analyse basé sur le nom de session.

Tableau 14-2 Paramètres du scanner SAINT (suite)

Paramètre	Description
Ignore Existing Data	Cette option s'applique uniquement lorsque Live Scan est le type d'analyse sélectionné. Cette option indique si l'analyse opérationnelle ignore les données existantes et regroupe les nouvelles informations de vulnérabilité pour le réseau. Si la case Ignore Existing Data est cochée, le scanner SAINT supprime les données de session existantes avant qu'une analyse opérationnelle ne soit lancée. Par défaut, la case à cocher est vide.
Scan Level	Sélectionnez le niveau d'analyse en utilisant la zone de liste : • **Vulnerability Scan** - Analyse toutes les vulnérabilités. • **Port Scan** - Analyse les services TCP et UDP en mode écoute sur le réseau. • **PCI Compliance Scan** - Evalue les ports et les services avec mise en évidence sur la conformité DSS PCI. • **SANS Top 20 Scan** - Analyse les 20 vulnérabilités de sécurité les plus importantes. • **FISMA Scan** - Analyse toutes les vulnérabilités en incluant toutes les analyses personnalisées et les niveaux PCI.
Session Name	Entrez le nom de session pour la configuration de session du scanner SAINT.
SAINT Writer Config	Entrez le nom du fichier de configuration pour SAINTwriter.

Etape 7 Pour configurer les plages de routage CIDR que ce scanner doit prendre en considération :

a Dans la zone de texte, entrez la plage de routage CIDR que ce scanner doit prendre en compte ou cliquez sur **Browse** pour sélectionner la plage de routage CIDR à partir de la liste réseaux.

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

Etape 9 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Modification d'un scanner de vulnérabilité SAINT

Pour modifier un scanner de vulnérabilité SAINT dans QRadar SIEM:

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez modifier.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Mettez à jour les paramètres si nécessaire. Voir **Tableau 14-2**.

Etape 7 Cliquez sur **Save**.

Etape 8 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Suppression d'un scanner de vulnérabilité SAINT

Pour supprimer un scanner de vulnérabilité SAINT depuis QRadar SIEM :

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez sur **OK**.

Etape 7 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

17 GESTION DES SCANNERS AXIS

Le scanner Asset Export Information Source (AXIS) permet à IBM Security QRadar SIEM d'extraire les résultats d'analyse des périphériques de scanner inconnus pour la corrélation. Cela permet l'utilisation d'AXIS pour l'importation de résultats d'analyse pour les périphériques créés par les fournisseurs de scanner XML qui présentent les vulnérabilités dans un format XML qui respecte le schéma du format AXIS. De ce fait, les fournisseurs de logiciels et produits de scanner peuvent créer un format générique compatible avec IBM Security QRadar SIEM. Le scanner AXIS QRadar SIEM est conçu pour récupérer périodiquement les résultats d'analyse au format XML et interpréter les données scannées. QRadar SIEM surveille le serveur SSH pour les mises à jour vers les résultats d'analyse et télécharge les derniers résultats pour le traitement. QRadar SIEM ne prend en charge que les résultats d'analyse au format AXIS XML.

Pour réussir l'intégration d'un scanner AXIS à QRadar SIEM, les fichiers de résultats XML doivent être lus à partir d'un serveur distant à l'aide de SSH ou du serveur qui crée le fichier de résultat, si le scanner lui-même prend en charge l'accès à l'aide de SSH. Le terme serveur distant fait référence à un système ou dispositif tiers pour héberger les résultats d'analyse qui est séparé de QRadar SIEM.

Les résultats d'analyse contiennent des informations d'identification concernant la configuration du scan depuis le périphérique de scanner inconnu. Les résultats d'analyse les plus récents sont utilisés lorsqu'une nouvelle analyse est demandée depuis QRadar SIEM. Les plannings d'analyse vous permettent de déterminer la fréquence à laquelle QRadar SIEM demande des données à votre scanner compatible avec AXIS. Pour plus d'informations, voir **Gestion des plannings d'analyse.**

Cette section fournit les informations sur les éléments suivants :

- **Ajout d'un scanner AXIS**
- **Edition d'un scanner an AXIS**
- **Suppression d'un scanner AXIS**

Ajout d'un scanner AXIS

Pour ajouter un scanner AXIS à QRadar SIEM:

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs pour les paramètres suivants :

Tableau 15-1 Paramètres AXIS Scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez affecter à ce scanner. Le nom peut contenir jusqu'à 255 caractères.
Description	Entrez une description pour ce scanner. La description peut contenir jusqu'à 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez la description que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, cochez **Axis Scanner**.

Etape 6 Configurez les valeurs pour les paramètres suivants :

Tableau 15-2 Paramètres AXIS Scanner

Paramètre	Description
Remote Hostname	Entrez le nom d'hôte ou l'adresse IP du serveur distant.
Login Username	Entrez le nom d'utilisateur utilisé parQRadar SIEM pour authentifier la connexion SSH.
Login Password	Si Enable Key Authentication s'affiche, vous devez entrer le mot de passe correspondant au paramètre Login Username qu'utilise QRadar SIEM pour authentifier la connexion SSH. Si Enable Key Authentication est activé, le paramètre Login Password est ignoré.
Enable Key Authorization	Cochez cette case pour activer l'autorisation de la clé privée pour le serveur. Si la case est cochée, l'authentification SSH est effectuée à l'aide de la clé privée et le mot de passe est ignoré. La valeur par défaut est désactivée.

Tableau 15-2 Paramètres AXIS Scanner (suite)

Paramètre	Description
Private Key File	Entrez le chemin de répertoire qui mène vers le fichier contenant les informations de la clé privée. Si vous utilisez une authentification SSH basée sur la clé privée, QRadar SIEM utilise la clé privée pour authentifier la connexion SSH. Le chemin de répertoire par défaut est /opt/qradar/conf/vis.ssh.key. Cependant, par défaut, ce fichier n'existe pas. Vous devez créer le fichier vis.ssh.key ou entrer un autre nom de fichier. Ce paramètre est obligatoire si la case Enable Key Authentication est cochée. Si la case Enable Key Authentication est décochée, ce paramètre est ignoré.
Remote Directory	Entrez l'emplacement du répertoire des fichiers résultats d'analyse.
File Name Pattern	Entrez une expression régulière (regex) requise pour filtrer la liste des fichiers spécifiés dans Remote Directory. Tous les fichiers correspondants sont inclus dans le traitement. Par exemple, si vous souhaitez lister tous les fichiers se terminant par XML, utilisez l'entrée suivante : `.*\.xml` L'utilisation de ce paramètre requiert la connaissance de l'expression régulière (regex). Pour plus d'informations, consultez le site Web suivant : *http://download.oracle.com/javase/tutorial/essential/regex/*
Ignore Duplicates	Cochez cette case pour pister les fichiers qui ont déjà été traités et les fichiers que dont vous ne souhaitez pas traiter une seconde fois. ***Remarque :*** *Si un fichier résultat ne s'affiche pas pendant 10 jours, il est supprimé de la liste de suivi et traité à la prochaine reconnaissance du fichier.*

Etape 7 Pour configurer les intervalles CIDR que ce scanner doit prendre en considération :

a Dans la zone de texte, entrez l'intervalle CIDR que vous souhaitez que ce scanner prenne en considération ou cliquez sur **Browse** pour sélectionner l'intervalle CIDR à partir de la liste réseaux.

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

Etape 9 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

Edition d'un scanner an AXIS

Pour éditer un scanner AXIS :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez éditer.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Paramètre Update, si nécessaire. Voir **Table 15-2**.

Etape 7 Cliquez sur **Save**.

Etape 8 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

Suppression d'un scanner AXIS

Pour supprimer un scanner AXIS de QRadar SIEM:

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez sur **OK**.

Etape 7 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

18 GESTION DE TENABLE SECURITYCENTER

Un scanner Tenable SecurityCenter peut être utilisé avec IBM Security QRadar SIEM pour planifier et récupérer tous les enregistrements de rapports ouverts d'analyse de vulnérabilité à partir de plusieurs scanners de vulnérabilité Nessus sur votre réseau. QRadar SIEM accède à distance à Tenable SecurityCenter via une connexion HTTPS.

Après avoir ajouté le scanner Tenable SecurityCenter dans QRadar SIEM, vous pouvez planifier une analyse afin de récupérer les enregistrements de rapports ouverts de vulnérabilité. Les plannings d'analyse vous permettent de déterminer la fréquence à laquelle QRadar SIEM demande des données à votre dispositif Tenable SecurityCenter. Pour plus d'informations, voir **Gestion des plannings d'analyse**.

Cette section fournit des informations sur les éléments suivants :

- **Ajout de Tenable SecurityCenter**
- **Edition de Tenable SecurityCenter**
- **Suppression de SecurityCenter**

Ajout de Tenable SecurityCenter

Pour ajouter Tenable SecurityCenter à QRadar SIEM:

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs pour les paramètres suivants :

Tableau 16-1 Paramètres du scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez affecter au scanner. Le nom peut contenir plus de 255 caractères.
Description	Entrez une description pour ce scanner. La description peut contenir plus de 255 caractères.
Managed Host	Dans la zone de liste, sélectionnez l'hôte géré que vous souhaitez utiliser pour configurer le scanner.
Type	Dans la zone de liste, sélectionnez **Tenable Security Center**.

Etape 6 Configurez les valeurs des paramètres :

Tableau 16-2 Paramètres Tenable SecurityCenter

Paramètre	Description
Server Address	Entrez l'adresse IP ou le nom d'hôte du dispositif Tenable SecurityCenter.
API Location	Entrez le chemin d'accès au fichier request.php pour votre version de Tenable SecurityCenter. Par défaut, le chemin d'accès à l'interface de programme d'application est **`sc4/request.php`**. Si vous rencontrez des problèmes en vous connectant à votre Tenable SecurityCenter depuis QRadar SIEM, vous pouvez vérifier le chemin d'accès vers votre fichier request.php puis mettre ce champ à jour.
Username	Entrez le nom d'utilisateur requis pour se connecter à votre dispositif Tenable SecurityCenter.
Password	Entrez le mot de passe correspondant au nom d'utilisateur pour votre dispositif Tenable SecurityCenter.

Etape 7 Pour configurer les intervalles de routage CIDR que vous souhaitez que ce scanner prenne en compte :

a Dans le champ de texte, entrez l'intervalle de routage CIDR que ce scanner doit prendre en considération ou cliquez sur **Browse** pour sélectionner l'intervalle de routage CIDR à partir de la liste réseaux.

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

Etape 9 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Edition de Tenable SecurityCenter

Pour éditer un scanner Tenable SecurityCenter précédemment configuré dans QRadar SIEM:

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez modifier.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Mettre à jour les paramètres, si nécessaire. Voir **Tableau 16-2**.

Etape 7 Cliquez sur **Save**.

Etape 8 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Suppression de SecurityCenter

Pour supprimer le scanner Tenable SecurityCenter à partir de QRadar SIEM :

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **VA Scanners.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez sur **OK**.

Etape 7 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

19 GESTION DES PLANNINGS D'ANALYSE

Après avoir configuré les scanners individuels pour permettre à IBM Security QRadar SIEM d'accéder aux données de vulnérabilité du client ou du dispositif, vous devez créer une planification afin que QRadar SIEM récupère les données de vulnérabilité. Un planning d'analyse doit être effectué une fois ou configuré afin de récupérer les données de vulnérabilité sur une base de reproduction. Lorsqu'un planning d'analyse est terminé, QRadar SIEM est mis à jour avec les données de vulnérabilité les plus récentes.

Cette section fournit des informations sur les éléments suivants :

- **Viewing Scheduled Scans**
- **Planification d'une analyse**
- **Modification d'un planning d'analyse**
- **Suppression d'une analyse planifiée**

REMARQUE

Vous pouvez gérer des plannings d'analyse à partir des onglets **Admin** ou **Assets** dans QRadar SIEM.

Viewing Scheduled Scans

La fenêtre Scan Scheduling s'affiche lorsque QRadar SIEM est planifié pour la collecte des données de l'évaluation de vulnérabilité à partir des dispositifs de vulnérabilité sur votre réseau. Le nom de chaque analyse s'affiche, tout au long de la plage de routage CIDR, du port ou de la plage de ports, de priorité, de puissance, de statut, du masque de concurrence et de la prochaine phase d'exécution.

Pour afficher les analyses planifiées :

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **Schedule VA Scanners.**

Scan Scheduling s'affiche.

Les informations suivantes sont fournies pour chaque analyse planifiée :

Tableau 17-1 Scheduled Scan Paramètres

Paramètre	Description
VA Scanner	Affiche le nom de l'analyse planifiée.
routage CIDR	Affiche les adresses IP à inclure à cette analyse.
Ports	Affiche la plage de ports incluse dans l'analyse. Si l'analyse de l'exécution du scanner exécute directement l'analyse (NMap, Nessus ou Nessus Scan Results Importer), les ports indiqués restreignent le nombre de ports analysés. Toutefois, pour tous les autres scanners, la plage de ports n'est pas considérée pendant la demande d'informations d'actifs à partir d'un scanner. Par exemple, les scanners nCircle IP360 et Qualys scanners rapportent des vulnérabilités sur tous les ports mais vous exigent d'indiquer les informations de port adéquates afin de récupérer le rapport complet pour l'affichage de l'interface utilisateur.
Priority	Affiche la priorité de l'analyse. Les analyses planifiées ayant une priorité élevée sont mises en attente, au-delà de la priorité et s'effectuent avant les analyses à priorité faible.
Potency	Affiche la gravité de l'analyse.L'interprétation précise des niveaux dépend du scanner. Cependant, les niveaux indiquent généralement : • **Very safe** - Indique une évaluation sûre et non-intrusive. Il peut générer de faux résultats. • **Safe** - Indique une évaluation intermédiaire et produit des résultats sûrs, basés sur des bannières. • **Medium** - Indique une évaluation intermédiaire sûre avec des résultats précis. • **Somewhat safe** - Indique une évaluation intermédiaire, mais peut rendre le service inactif. • **Somewhat unsafe** - Indique une évaluation intermédiaire, cependant, il peut arrêter le fonctionnement de votre hôte ou de votre serveur. • **Unsafe** - Indique une évaluation intermédiaire, cependant, il peut rendre votre service inactif. • **Very unsafe** - Indique une évaluation peu sûre, dangereuse qui peut rendre votre hôte ou votre serveur inactif. ***Remarque :*** *Les niveaux de puissance ne s'appliquent qu'aux scanners NMap. Nous vous recommandons de sélectionner* ***Medium*** *dans la zone de liste* ***Potency*** *pour plus d'analyses NMap.*

Tableau 17-1 Scheduled Scan Paramètres (suite)

Paramètre	Description
Status	Affiche le statut de l'analyse. Un message d'état descriptif s'affiche en maintenant (pointant) la souris sur le message d'état : • **New** - Indique que l'entrée de l'analyse planifiée est récemment créée. Lorsque le statut est New, vous pouvez modifier l'entrée de l'analyse. Lorsque l'heure de début initiale pour l'analyse a été atteinte, le statut change à Pending et vous ne pouvez plus modifier l'entrée de l'analyse. • **Pending** - Indique que l'analyse a été placée dans la file d'attente de travaux. Le statut reste Pending jusqu'à ce que la file d'attente via le module de scanner, ou le statut change en pourcentage (%) terminé ou échoue. Le scanner VA soumet un résultat d'analyse pour chaque adresse IP planifiée. • **Percentage Complete** - Chaque fois qu'une adresse IP est planifiée, le scanner VA calcule la fin de l'analyse. Percentage Complete indique le statut du pourcentage (%) complet pour l'analyse en tant que valeur numérique. • **Complete** - Lorsque Percentage Complete atteint les 100%, le statut de l'analyse change en Complete. • **Failed** - Indique qu'une erreur s'est produite dans le processus d'analyse. ***Remarque :*** *Placez votre souris sur n'importe quel scanner pour afficher informations détaillées sur les erreurs ou analyses opérationnelles qui peuvent être en cours.*
Concurrency Mask	Affiche la taille du sous-réseau analysé lors d'une analyse VA (Vulnerability Assessment).
Next Run Time	Affiche un compte à rebours pour indiquer l'intervalle jusqu'à ce que la prochaine analyse de vulnérabilité soit planifiée pour le redémarrage. Si l'analyse est planifiée avec un intervalle de 0, cela indique que l'analyse n'est pas planifiée pour la répétition. Les analyses ne répètent pas l'affichage de la prochaine exécution en tant que N/A. Mises à jour Next Run Time au moment de l'actualisation de la fenêtre Scan Scheduling.

Planification d'une analyse

Après avoir configuré les scanners de vulnérabilité dans QRadar SIEM, vous pouvez dès lors créer un planning d'analyse. Les plannings d'analyse sont créés pour chaque produit de scanner dans votre réseau et sont utilisés pour récupérer les données de vulnérabilité pour QRadar SIEM.

Pour planifier une analyse Vulnerability Assessment :

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

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

Le panneau Data sources s'affiche.

Etape 3 Cliquez sur l'icône **Schedule VA Scanners.**

La fenêtre Scan Scheduling s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Schedule s'affiche.

REMARQUE

Si vous ne disposez d'aucun scanner configuré, un message d'erreur s'affiche. Vous devez configurer le scanner avant de pouvoir planifier une analyse.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 17-2 Paramètres Scan Schedule

Paramètre	Description
VA Scanner	Dans la zone de liste, sélectionnez le scanner pour lequel vous souhaitez créer une planification.
Network CIDR	Choisissez une des options suivantes : • **Network CIDR** - Sélectionnez l'option, puis la plage de réseaux CIDR à laquelle vous souhaitez que cette analyse s'applique. • **Subnet/CIDR** - Sélectionnez le sous-réseau ou la plage de routage CIDR de l'option et du type auxquels que vous souhaitez que cette analyse s'applique. Ce sous-réseau/routage CIDR doit apparaître dans le Network CIDR sélectionné. Les valeurs Network CIDR ou Subnet/CIDR doivent être disponibles via le scanner sélectionné dans la zone de liste **VA Scanner**.

Tableau 17-2 Paramètres Scan Schedule (suite)

Paramètre	Description
Potency	Dans la zone de liste **Potency**, sélectionnez le niveau de l'analyse à effectuer. L'interprétation précise des niveaux dépend du scanner. Pour en savoir plus sur la puissance, contactez votre fournisseur. En général, les niveaux de puissance indiquent la gravité de l'analyse : • **Very safe** - Indique une évaluation sûre et non-intrusive. Il peut générer de faux résultats. • **Safe** - Indique une évaluation intermédiaire et produit des résultats sûrs, basés sur des bannières. • **Medium** - Indique une évaluation intermédiaire sûre avec des résultats précis. • **Somewhat safe** - Indique une évaluation intermédiaire, mais peut rendre le service inactif. • **Somewhat unsafe** - Indique une évaluation intermédiaire, cependant, il peut arrêter le fonctionnement de votre hôte ou de votre serveur. • **Unsafe** - Indique une évaluation intermédiaire, cependant, il peut rendre votre service inactif. • **Very unsafe** - Indique une évaluation peu sûre, dangereuse qui peut rendre votre hôte ou votre serveur inactif. ***Remarque :*** *Les niveaux de puissance ne s'appliquent qu'aux scanners NMap.*
Priority	Dans la zone de liste **Priority**, sélectionnez le niveau de priorité à affecter à l'analyse. • **Low** - Indique que l'analyse est en priorité normale. La priorité basse est la valeur d'analyse par défaut. • **High** - Indique que l'analyse est la priorité élevée. Les analyses de priorité élevée sont toujours placées au-dessus des analyses de priorité basse dans la file d'attente des analyses.
Ports	Entrez la plage de ports que le scanner doit analyser.
Start Time	Configurez l'heure et la date de début de l'analyse. La configuration par défaut est l'heure locale de votre QRadar SIEM. ***Remarque :*** *Si vous sélectionnez une heure de début réglée auparavant, l'analyse commence immédiatement après l'enregistrement de sa planification.*
Interval	Entrez un intervalle de temps pour indiquer la fréquence souhaitée pour l'exécution de l'analyse. Les intervalles d'analyse peuvent être planifiés par heure, jour, semaine ou mois. Un intervalle de 0 indique que l'analyse planifiée s'effectue une fois et ne se répète pas.

Tableau 17-2 Paramètres Scan Schedule (suite)

Paramètre	Description
Concurrency Mask	Entrez CIDR pour indiquer la taille du sous-réseau devant être analysé lors d'une analyse de vulnérabilité. La valeur configurée pour le masque de concurrence représente la plus grande portion du sous-réseau que le scanner est autorisé à analyser à un moment donné. Le masque de concurrence permet à l'ensemble du réseau CIDR ou sous-réseau/CIDR d'être analysé en segments de sous-réseau afin d'optimiser l'analyse. L'analyse maximale de segment de sous-réseau est /24 et l'analyse minimale est /32.
Clean Vulnerability Ports	Cochez cette case si vous souhaitez que l'analyse exclut les données de vulnérabilité précédemment collectées.

Etape 6 Cliquez sur **Save**.

Modification d'un planning d'analyse

Après avoir créé un nouveau planning d'analyse, vous pouvez modifier ses paramètres. La modification d'un planning d'analyse n'est possible qu'après le déploiement de la configuration dans QRadar SIEM. Après le déploiement des modifications de configuration dans QRadar SIEM, le bouton Editer est non disponible et vous ne pouvez plus modifier un planning d'analyse.

Pour modifier un planning d'analyse Vulnerability Assessment :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **Schedule VA Scanners.**

La fenêtre Scan Scheduling s'affiche.

Etape 4 Sélectionnez la planification que vous souhaitez modifier.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Schedule s'affiche.

Etape 6 Mettez à jour les valeurs, si nécessaire. Voir **Tableau 17-2**.

Etape 7 Cliquez sur **Save**.

Suppression d'une analyse planifiée

Pour supprimer un planning d'analyse Vulnerability Assessment :

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

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

Le panneau Data Sources s'affiche.

Etape 3 Cliquez sur l'icône **Schedule VA Scanner.**

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez l'analyse que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez sur **OK**.

20 SCANNERS PRIS EN CHARGE

T : Tableau 18-1 fournit des informations sur les prises en charge de scanners pour l'évaluation de la vulnérabilité QRadar.

QRadar s'intègre à de nombreux fabricants et fournisseurs de produits de sécurité. Notre liste de scanners et documentation pris en charge est en constante augmentation. Si votre scanner n'est pas répertorié dans le présent document, contactez votre représentant commercial.

T : Tableau 18-1 Scanners pour l'évaluation de vulnérabilité

Fabricant	Scanner	Version	Option dans QRadar	Type de Connexion
Sécurité numérique eEye	eEye REM ou Retina CS eEye	REM v3.5.6 or Retina CS v3.0 à v4.0	Scanner REM eEye	Alerte SNMP
Générique	AXE	N/A	Scanner Axis	Importez des fichiers de données de vulnérabilité à l'aide de SSH
IBM	IBM Security AppScan Enterprise	AppScan Enterprise 8.6	Scanner IBM AppScan	IBM gère le service web à l'aide du protocole HTTP ou HTTPS
IBM	SiteProtector	SiteProtector v2.9.x	Scanner IBM SiteProtector	Sondage JDBC
IBM	Tivoli EndPoint Manager	IBM Tivoli EndPoint Manager v8.2.x	IBM Tivoli EndPoint Manager	Interface API basée sur le protocole SOAP à l'aide de HTTP ou HTTPS
Juniper	NSM Profiler	2007.1r2, 2007.2r2, 2008.1r2, 2009r1.1, et 2010.x	Scanner Juniper NSM Profiler	Sondage JDBC
Lumenison	Patchlink	version 6.4.4 et supérieure	Scanner Patchlink Lumenison	interface API basée sur le protocole SOAP à l'aide de HTTPS
McAfee	Foundstone	version 5.0 vers 6.5	Scanner Foundscan	interface API basée sur le protocole SOAP à l'aide de HTTPS
	Gestionnaire de Vulnérabilité	Version 6.8 ou 7.0.	McAfee Vulnerability Manager	interface API basée sur le protocole SOAP à l'aide de HTTPS

T : Tableau 18-1 Scanners pour l'évaluation de vulnérabilité (suite)

Fabricant	Scanner	Version	Option dans QRadar	Type de Connexion
nCircle	ip360	VnE Manager version 6.5.2 vers 6.8.28	Scanner nCircle ip360	Importation des fichiers de données de vulnérabilité à l'aide de SSH
Nessus	Nessus	Linux version 4.0.2 vers 4.4.x, Windows version 4.2 vers 4.4.x	Scanner Nessus	Importation de fichiers via SSH et exécution de la commande SSH
	Nessus	Linux version 4.2 vers 5.x, Windows version 4.2 vers 5.x	Scanner Nessus	Interface API Nessus XMLRPC via HTTPS
netVigilance	SecureScout	2.6	Scanner SecureScout	Sondage JDBC
Open Source	NMap	Version 3.7 vers 5.50	Scanner NMap	Importation de données de vulnérabilité via SSH et exécution de la commande SSH
Qualys	QualysGuard	Version 4.7 vers 7.2	Scanner Qualys	Interface APIv2 via HTTPS
	QualysGuard	Version 4.7 vers 7.2	Scanner de détection Qualys	Liste de détection d'hôte API via HTTPS
Rapid7	NeXpose	4.x à v5.4	Scanner Rapid7 NeXpose	Appel de procédure à distance via HTTPS
				Importation de fichiers locaux à partir d'un répertoire QRadar
Saint Corporation	SAINT	7.4.x	Scanner Saint	Importation de données de vulnérabilité via SSH et exécution de la commande SSH
Tenable	Centre de sécurité		Centre de sécurité Tenable	Appel de procédure à distance via HTTPS

A AVIS ET MARQUES

Dans cette annexe :

Cette section décrit quelques avis et marques importants et fournit des informations sur la conformité.

Avis

Ces informations étaient destinées aux produits et services offerts aux Etats-Unis.

IBM peut ne pas offrir les produits, les services ou les fonctions décrits dans ce document dans d'autres pays. Contactez votre interlocuteur IBM habituel pour obtenir des informations sur les produits et services actuellement disponibles dans votre région. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre produit, programme ou service fonctionnellement équivalent peut être utilisé, s'il n'enfreint pas les droits de propriété intellectuelle d'IBM. Toutefois, il est de la responsabilité de l'utilisateur d'évaluer et de vérifier le fonctionnement de tout produit, programme ou service non IBM.

IBM peut détenir des brevets ou des demandes de brevet en instance couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets. Vous pouvez soumettre des demandes de licences par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues auprès du service IBM Intellectual Property Department de votre pays ou par écrit à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Le paragraphe suivant ne s’applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales : INTERNATIONAL BUSINESS MACHINES CORPORATION LIVRE LE PRESENT DOCUMENT "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE, Y COMPRIS MAIS SANS S'Y LIMITER, TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties explicites ou implicites pour certaines transactions, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Ces informations peuvent contenir des inexactitudes techniques ou des erreurs typographiques. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

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, USA

Ces informations peuvent être soumises à des dispositions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions d'IBM Customer Agreement, d'IBM International Program License Agreement ou de tout autre accord équivalent.

Les données de performance indiquées dans ce 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 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 de ces 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 prix IBM indiqués sont des prix de détail suggérés par IBM, sont à jour et peuvent être modifiés sans préavis. Les prix distributeurs peuvent donc varier.

Ces informations contiennent des exemples de données et de rapports utilisés dans les opérations métier habituelles. Pour les illustrer aussi complètement que possible, les exemples incluent les noms des personnes, des sociétés, des marques et des produits. Tous ces noms sont fictifs et toute ressemblance avec des noms et adresses utilisés par une société réelle serait purement fortuite.

Si vous visualisez la copie électronique de ces informations, les photographies et illustrations en couleur peuvent ne pas apparaître.

Marques

IBM, le logo IBM et ibm.com sont des marques ou des marques déposées d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. Une liste actualisée des marques IBM est disponible sur la page Web “Copyright and trademark information” 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 ou des marques déposées d'Oracle et/ou de ses filiales.

Linux est une marque de Linus Torvalds aux Etats-Unis, dans d'autres pays ou les deux.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux États-Unis, dans d'autres pays ou les deux.

UNIX est une marque de The Open Group aux Etats-Unis et dans d'autres pays.

INDEX

R

S

T

V