IBM Security QRadar
Version 7.1.0

Gestion de l'évaluation de la vulnérabilité

CONTENU

A PROPOS DE CE MANUEL

Le Guide de gestion de l'évaluation de la vulnérabilité QRadar *fournit des informations sur la gestion de la vulnérabilité des scanners et la configuration des scanners destinés à protéger les données vulnérables de QRadar.*Détection des anomalies QRadar.

Utilisateurs concernés

Ce manuel est destiné à tous les administrateurs système responsables de la configuration de l'importation des données vulnérables .Ce manuel suppose que vous disposez d'un accès en tant qu'Administrateur à et d'une connaissance de votre réseau d'entreprise et des technologies réseau.

Conventions

Les conventions suivantes s'appliquent dans ce manuel :

► Indique que la procédure contient une seule instruction.

NOTE

Indique que les informations fournies viennent complêter 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.

 **WARNING**

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

Vous pouvez accéder à la documentation technique, aux notes techniques et aux notes sur l' édition directement à partir du site Web Qmmunity à l'adresse

https://qmmunity.q1labs.com/. Lorsque vous accédez au site Web Qmmunity, localisez le produit et l'édition logicielle pour lesquels vous avez besoin d'une documentation.

Vos commentaires sont les bienvenus. Envoyez par email vos commentaires à propos de ce manuel ou de la documentation Q1 Labs :

documentation@q1labs.com

Intégrez les informations suivantes à vos commentaires :

- Titre du document
- Numéro de page

Contacter le service clients

Pour vous aider à résoudre vos éventuels problèmes lors de l'installation ou de maintenance de Détection des anomalies QRadar, vous pouvez contacter le service clients à l'adresse suivante :

- Consignation d'une demande de support 24/7 :*https://qmmunity.q1labs.com/*

  Pour demander un nouveau Qmmunity et un nouveau compte de support libre-service, envoyez votre demande à *welcomecenter@q1labs.com*. Vous devez fournir votre numéro de facture pour accéder à votre compte.
- Assistance téléphonique :
  - **Etats-Unis et Canada** - 1.866.377.7000
  - **International** - (01) 506.462.9117
  - **Royaume-Uni** - 028 9031 7991
- Forums : Accédez à nos Qmmunity forums pour profiter des expériences de nos clients.

Marques

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.

1 PRÉSENTATION

L'intégration d'évaluation de la vulnérabilité permet à QRadar de générer des profils d'évaluation de vulnérabilité. Les profils d'évaluation de la vulnérabilité utilise 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 élèments métier essentiels.

L'intégration de QRadar aux outils d'évaluation de la vulnérabilité vous permet d'importer des rapports d'analyses terminées ou en fonction du scanner, vous pouvez lancer une analyse en direct et importer les résultats par la suite. La planification des analyses vous permet de maintenir à jour vos données en permettant à QRadar d'importer des données du rapport d'analyse dans un intervalle de temps défini. Après l'ajout des données de vulnérabilité à QRadar à travers une analyse planifiée, affichez les résultats à partir de l'onglet **Asset**.

NOTE

Vous devez disposer d'autorisations appropriées pour accéder aux réseaux contenant des adresses CIDR que vous planifiez afin de récupérer des analyses d'évaluation de vulnérabilité à partir des appareils de vulnérabilité.

NOTE

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 ce qui suit :

- **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 en savoir plus, consultez **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 le hôte, les ports, et les vulnérabilités potentielles.

NOTE

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. Pour en savoir plus, consultez la section **Managing Scan Schedules**.

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 services.

Installation des Scanners

Pour mettre à jour ou installer un nouveau scanner, vous devez soit configurer QRadar 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 sur votre console QRadar :

Etape 1 téléchargez les fichiers rpm du scanner à partir du site webQmmunity :

https://qmmunity.q1labs.com/

Etape 2 Copiez les fichiers sur votre console QRadar.

Etape 3 A l'aide de SSH, connectez-vous à votre console QRadar 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 requête suivante :

`rpm -Uvh <filename>`

O **`<filename>`** est le nom du fichier t l charg .

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

Etape 6 Connectez-vous à QRadar.

`https://<IP Address>`

O <IP Address> est l'adresse IP du système QRadar.

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 :

Table 1-1 Paramètres du sacanner

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 devant être pris en compte par le scanner. Plusieurs routages CIDR sont affichés à l'aide d'une liste séparée par une virgule.
Description	Affiche une description pour ce scanner.
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* **Table 17-1** *pour en savoir plus sur l'état d'analyse.*

2 GESTION DE SCANNERS IBM SECURITY APPSCAN ENTERPRISE

QRadar peut importer des résultats d'analyse depuis le rapport de données 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 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.

Pour intégrer AppScan Enterprise avec QRadar, vous devez :

1. Générer des rapports d'analyse dans AppScan Enterprise. Pour en savoir plus sur la g n ration de rapports d'analyse, voir la documentation du fournisseur AppScan Enterprise.
2. Configurer AppScan Enterprise pour accorder l'accès QRadar aux données de rapport. Pour en savoir plus, voir **Configuration d'AppScan Enterprise pour autoriser l'accès QRadar.**.
3. Configurer votre scanner AppScan Enterprise dans QRadar. Pour en savoir plus, voir **Configuration d'AppScan Enterprise dans QRadar**.
4. créer une planification dans QRadar pour importer les résultats AppScan Enterprise. Pour en savoir plus, voir **Managing Scan Schedules**.

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

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. Apr s avoir configuré les utilisateurs AppScan Enterprise, les rapports générés par AppScan Enterprise peuvent être publiés sur QRadar, les rendant disponibles pour téléchargement.

Pour configurer AppScan Enterprise afin d'accorder l'accès QRadar 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. Voir. **Activation de QRadar Integration**.
3. Cr ez une Application Deployment Map. Voir **Création d'une Application Deployment Map**.
4. Publiez vos résultats d'analyse sur QRadar. Voir **Publication de rapports sur QRadar**.

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 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 :

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

Etape 5 Enregistrez le type d'utilisateur.

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

Activation de QRadar Integration

Pour remplir 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 :

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 surQRadar s'affichent. Si aucun des rapports affichés n'est requis, vous pouvez les supprimer de la liste. En publiant des rapports supplémentaires sur QRadar, les rapports s'affichent dans la 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 vulnérabilité s 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 champ **Application test location (h te ou canevas)**, entrez le test d'emplacement pour votre application.

Etape 5 Dans le champ **Application production location (h te)**, entrez l'adresse IP pour votre environnement de production.

NOTE

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 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.

Publication de rapports sur QRadar

Des rapports de vulnérabilité complets générés par AppScan Enterprise doivent être rendus accessibles sur QRadar en publiant le rapport. Pour remplir 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 Naviguez vers le rapport de sécurité que vous souhaitez rendre disponible sur QRadar.

Etape 3 Sur la barre de menus de tous les rapports de sécurité, sélectionnez **Publish >. Autorisez l'accès au rapport surQRadar**.

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

Configuration d'AppScan Enterprise dans QRadar

Après avoir configuré AppScan Enterprise et publié des rapports sur QRadar, vous pouvez ajouter le scanner AppScan Enterprise dans QRadar. L'ajout d'un scanner permet à QRadar de connaître les rapports d'analyse à configurer. Vous pouvez ajouter plusieurs scanners AppScan Enterprise dans QRadar, 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 vous permet de déterminer la fréquence à laquelle QRadar importe les données relatives aux résultats d'analyse dans AppScan Enterprise à l'aide du service Web REST.

NOTE

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 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**
- **Edition d'un scanner AppScan Enterprise**
- **Suppresion d'un scanner AppScan Enterprise**

Ajout d'un scanner AppScan Enterprise sur QRadar

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 fen tre Add Scanner s'affiche.

Etape 5 Configurez les valeurs pour les paramètres suivants :

Table 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.
Managed Host	Dans la zone de liste, sélectionnez la description que vous souhaitez utiliser pour configurer le scanner.

Table 2-1 Paramètres du scanner (suite)

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

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

Etape 6 Configurez les valeurs pour les param ères suivants :

Table 2-2 Paramètres IBM AppScan Enterprise

Param tre	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 extraire les rapports des données de l'analyse depuis 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. 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. 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 vous souhaitez que ce scanner prenne 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 réseau.

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 tes maintenant sur le point de créer un planning d'analyse dans QRadar. Pour en savoir plus, voir **Managing Scan Schedules**.

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 souhaiter éditer.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

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

Etape 7 Cliquez sur **Save**.

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

Suppresion 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 GESTION DES SCANNERS IP360

QRadar utilise SSH pour accéder au serveur distant (serveur d'exportation SSH) pour récupérer et interpréter les données numérisées. QRadar prend en charge les versions VnE Manager IP360 allant de la 6.5.2 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, ces fichiers en format XML2 doivent être lus à partir du serveur distant (via SSH). QRadar 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 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 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. QRadar 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 points 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 Définit les valeurs des paramètres suivants:

Table 3-1 paramètres du scanner

Paramètre	Description
Scanner Name	Tapez le nom que vous souhaitez attribuer à ce scanner. Le nom peut comporter jusqu' à 255 caractères.
Description	Décrivez ce scanner par saisie 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, s éectionnez nCircle IP360 Scanner **.**

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

Etape 6 définit les valeurs des paramètres suivants:

Table 3-2 paramètres IP360

Paramètre	Description
SSH Server Host Name	Tapez 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	Tapez le nom d'utilisateur SSH du serveur distant.
SSH Password	Tapez 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	Tapez le numéro de port utilisé pour se connecter au serveur distant.
Remote Directory	Tapez l'emplacement du répertoire des fichiers des résultats d'analyse.
Age maximum du fichier (en jours)	Tapez l' âge maximum du fichie à inclure lors de l'exécution de l'analyse programmée. Les fichiers qui sont plus anciens que la date précis e sont exclus du processus d'importation des données de résultat dans QRadar.

Table 3-2 paramètres IP360 (suite)

Paramètre	Description
File Pattern	Tapez une expression régulière (regex), une étape obligatoire pour filtrer la liste des fichiers spécifiés dans le Répertoire distant **champ**. 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 clef 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	Tapez 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 dans lequel est conservé la clé privée devant tre utilisée 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.

NOTE

Si le scanner est configuré pour utiliser un mot de passe, il est nécessaire que le serveur du scanner SSH auquel est connecté QRadar 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 prenne en compte:

a Dans la zone de texte, tapez la plage CIDR vous souhaitez que le scanner prenne en compte ou cliquez sur **Browse** pour sélectionner la plage 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 **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. Consultez Table 3-2.

Etape 7 Cliquez sur **Save**.

Etape 8 Dans le menu de 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 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Exporter des rapports d'analyse

Configurer 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, à la 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 Configurer 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, le processus d'exportation doit être configuré de façon à ce que ces rapports soient exportés au format XML.

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

4 GESTION DE SCANNERS NESSUS

QRadar peut récupérer les rapports d'analyse de vulnérabilité à propos de vos ressources réseau en mettant à profit la relation client Nessus et 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. La création d'un compte utilisateur vous assure que QRadar 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, vous devez tenter depuis QRadar jusqu' à votre client Nessus, de vérifier les données d'identification de QRadar. Ceci garantit une communication entre QRadar et le client Nessus avant que vous tentiez de collecter les données d'analyse ou démarrer une analyse en direct.

Les options de collection de données sont disponibles pour Nessus :

- **Scheduled Live Scan** - Permet QRadar de se connecter avec un client Nessus et de lancer une analyse préconfigurée. QRadar utilise SSH pour récupérer les données du rapport d'analyse à partir du répertoire de résultats temporaires client une fois l'analyse en direct terminée.
- **Scheduled Results Import** - Permet à QRadar de se connecter l'emplacement hébergeant vos rapports d'analyse Nessus. QRadar se connecte au référentiel via SSH et importe les fichiers de rapport d'analyse depuis le répertoire distant. QRadar 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 d'utiliser XMLRPC API pour démarrer une analyse préconfigurée. Pour démarrer un scan à partir de QRadar, vous devez spécifier le nom de règles pour les données de scan que vous voulez récupérer. Lors de l'exécution de l'analyse opérationnelle, QRadar met à jour le pourcentage complet dans l' état de l'analyse. A la fin de l'analyse opérationnelle, QRadar 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 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 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 un intervalle ponctuel ou répété. Pour en savoir plus sur le planning d'une analyse, voir **Scheduling a Scan**.

NOTE

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

Cette section comprend les rubriques suivantes :

- **Ajout d'un Live Scan planifié Nessus**
- **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**

NOTE

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

Ajout d'un Live Scan planifié Nessus

Un Live scan vous permet de démarrer une analyse opérationnelle sur le serveur Nessus et d'importer les données relatives au résultat depuis un répertoire temporaire contenant les données de rapport d'analyse opérationnelle. A la fin de l'analyse, QRadar télécharge les données d'analyse depuis répertoire temporaire et met à jour les informations relatives à a vulnérabilité pour vos actifs.

Pour ajouter une analyse opérationnelle Nessus dans QRadar:

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 fenêre Add Scanner s'affiche.

Etape 5 Configurez les valeurs pour les paramètres suivants :

Table 4-1 Paramètres du scanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez affecter 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 pour le type de scanner sélectionné s'affiche.

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

Etape 7 Configurez les valeurs pour les paramètres suivants :

Table 4-2 Paramètres d'analyse planifiée pour Nessus

Paramètre	Description
Nom d'hôte du serveur	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.
Nom d'utilisateur du serveur	Entrez le nom d'utilisateur Nessus utilisé par le client pour l'authentification du serveur.
Mot de passe de serveur	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.*
répertoire temporaire client	Entrez le chemin d'accès au répertoire du client Nessus pouvant tre utilisé par QRadar afin de stocker des fichiers temporaires. QRadar 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 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.

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

Paramètre	Description
Nessus Exécutable	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**.
Fichier de configuration Nessus	Entrez le chemin d'accès au répertoire du fichier de configuration Nessus sur le client Nessus.
Nom d'hôte du client	Entrez le nom d'hôte ou l'adresse IP du système qui héberge le client Nessus.
Port SSH du client	Entrez le numéro de port SSH du serveur Nessus pouvant tre utilis afin de récupérer les fichiers du résultat d'analyse. Le numéro de port par défaut est 22.
Nom d'utilisateur client	Entrez le nom d'utilisateur utilis par QRadar pour authentifier la connexion SSH.
Mot de passe client	Entrez le mot de passe correspondant 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 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, consultez votre fournisseur de scanner.*
Activation d'authentification par clé	Sélectionnez cette case pour activer une authentification par clé publique ou privée. Si la case est sélectionnée, QRadar 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 intervalles CIDR dont vous souhaitez que ce scanner prenne 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 réseau.

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 tre créés comme un évènement ponctuel ou comme une importation planifiée qui se reproduit. Pour en savoir plus sur le planning d'une analyse, voir **Scheduling a Scan**.

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 se connecte à l'emplacement de vos rapports d'analyse à l'aide de SSH, importe des rapports d'analyse complets depuis le répertoire distant en utilisant l'expression régulière ou un maximum de rapports âge à filtrer pour vos rapports d'analyse. QRadar 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 :

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 :

Table 4-3 Paramètres du sacanner

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez affecter 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 pour le type de scanner sélectionné s'affiche.

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

Etape 7 Configurez les valeurs pour les paramètres suivants :

Table 4-4 Paramètres d'importation des résultats planifiés pour Nessus

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 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 :*** *Le mot de passe de votre 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 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 du 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 mettre à jour la configuration de votre scanner.*
durée de validité maximale du fichier de résultats (jours)	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 validité maximale du fichier de résultats est 7 jours. Les fichiers ayant une durée de validité supérieure au nombre de jours indiqué et l'horodatage du fichier résultats sont exclus du processus d'importation des résultats.

Etape 8 Pour configurer les intervalles CIDR dont vous souhaitez que ce scanner prenne 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 réseau.

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 vulnérabilités.

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

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

XMLRPC API permet à QRadar de démarrer une analyse opérationnelle préconfigurée sur votre serveur Nessus. Pour démarrer une analyse opérationnelle depuis QRadar 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. Après l'achèvement de l'analyse opérationnelle, QRadar utilise XMLRPC API pour récupérer les données d'analyse et mettre à jour les informations de vulnérabilités pour vos actifs.

NOTE

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

Pour ajouter une analyse en direct Nessus XMLRPC API dans QRadar :

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 :

Table 4-5 Paramètres du scanner

Paramètre	Description
Nom du scanner	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.

Table 4-5 Paramètres du scanner (suite)

Paramètre	Description
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 pour le 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 pour les paramètres suivants :

Table 4-6 paramètres d'interface API XMLRPC pour les importations planifiées

Paramètre	Description
Nom d'hôte	Entrez l'adresse IP ou le nom d'hôte du serveur Nessus.
Port	Entrez le numéro de port QRadar afin d'accéder au serveur Nessus à l'aide de l'interface API XMLRPC. Le numéro de port par défaut est 8834.
Nom d'utilisateur	Entrez le nom d'utilisateur requis pour accéder au serveur Nessus.
Mot de passe	Entrez le mot de passe correspondant au nom d'utilisateur.
Nom d'analyse	Facultatif. Entrez le nom d'analyse que vous souhaitez afficher au moment de l'exécution de l'analyse sur le serveur Nessus. Si elle est vide, l'interface API tente de démarrer une analyse directe pour QRadar Scan. ***Remarque :*** *QRadar ne prend pas en charge si vous utilisez le signe (&) dans cette zone.*
Nom de la règle	Entrez le nom de la régle sur votre serveur Nessus pour démarrer une analyse directe. La régle que vous définissez doit exister sur le serveur Nessus lorsque QRadar tente de lancer l'analyse. Si la régle n'existe pas, un message d'erreur s'affiche dans la partie d'état lorsque QRadar tente de démarrer l'analyse directe. Dans la plupart des cas le nom de la régle est adaptée à votre serveur Nessus, mais plusieurs régles par défaut sont inclues sous Nessus. Par exemple, • Analyse réseau externe • Analyse réseau interne • Tests d'application web • Préparer pour les audits PCI DSS Pour en savoir plus sur les régles, consultez votre fournisseur Nessus.

Etape 8 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 vous souhaitez mettre en évidence via ce scanner ou cliquez sur **Browse** pour sélectionner l'intervalle de routage CIDR à partir de la liste réseau.

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

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

Etape 11 Après que les changements aient été déployés, vous devez créer une analyse planifiée pour votre analyse en directe.

Les rapports d'analyse peuvent être créés en tant qu' évènement unique ou en tant qu'importation planifiée récurrente. Pour plus d'informations sur la planification d'une analyse, voir **Scheduling a Scan**.

Ajout de Nessus Completed Report Import via le XMLRPC API

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

NOTE

Le Nessus XMLRPC API est disponible uniquement sur les serveurs et les clients Nessus via l'utilisation du logiciel et une version supérieure.

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

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:

Table 4-7 paramètres du scanner

Paramètre	Description
Nom du scanner	Entrez le nom que vous souhaitez affecter 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.

Table 4-7 paramètres du scanner (suite)

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

La liste des paramètres pour le 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 pour les paramètres suivants :

Table 4-8 paramètres d'interface API XMLRPC pour les importations planifiées

Param tre	Description
Nom d'hôte	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 afin d'accéder au serveur Nessus à l'aide de l'interface API XMLRPC. Le numéro de port par défaut est 8834.
Nom d'utilisateur	Entrez le nom d'utilisateur requis pour accéder au serveur Nessus.
Mot de passe	Entrez le mot de passe correspondant au nom d'utilisateur.
Filtre de nom du rapport	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 inclu 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 mettre en évidence les changements pour la mise à jour de votre configuration de scanner.*
durée de validité maximale du fichier de résultats (jours)	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 validité 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 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 vous mettre en évidence via ce scanner ou cliquez sur **Browse** pour sélectionner l'intervalle de routage CIDR à partir de la liste réseau.

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

Etape 10 Sur 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'évènement unique ou en tant qu'importation planifiée récurrente. Pour plus d'informations sur la planification d'une analyse, voir **Scheduling a Scan**.

Modification d'un scanner Nessus

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

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.

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

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**.

5 GESTION DES SCANNERS NMAP

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

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

  Plusieurs types d'analyse de port NMap nécessite NMap pour s'exécuter en tant que root. Par conséquent, QRadar doit avoir accés 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 un accés root ou configurer le fichier binaire NMap avec setuid root. Pour obtenir une assistance, contactez votre administrateur système.

- **Remote Results Import** - Permet à QRadar 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 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, vous devez générer le fichier de résultats à l'aide de l'option **`-oX <file>`**.

  D'o **`<file>`** est le chemin d'accés permettant de créer et 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, vous pouvez programmer la fréquence à laquelle QRadar importe les données de vulnérabilité. Pour en savoir plus, consultez la section **Managing Scan Schedules**.

Cette section fournit des renseignements sur ce qui suit :

Ajout d'une analyse Remote Live Scan NMap

L'ajout d'une analyse Remote Live Scan sous QRadar permet à QRadar de lancer une analyse NMap, d'attendre quelle se termine, puis d'importer les résultats. Après avoir configuré une analyse en direct, attribuez une planification pour déterminer la fréquence à laquelle QRadar lance des analyses sur votre scanner NMap afin de récupérer des données de vulnérabilité pour vos documents.

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 pour les paramètres suivants :

Table 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 pour les paramètres suivants :

Table 5-2 paramètres d'analyse NMap

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 ex cute SSH.
Server Username	Entrez le nom d'utilisateur obligatoire sous SSH, pour accéder au système distant qui héberge le client NMap.
Enable Key Authentication	Sélectionnez cette case pour permettre à QRadar d'utiliser une authentification par clé public ou privée. Lorsque vous sélectionnez cette case, spécifiez le chemin de répertoire de votre clé dans QRadar à l'aide de la zone **Private Key File**. Par défaut, la case est vide.

Table 5-2 paramètres d'analyse NMap (suite)

Paramètre	Description
Login Password	Entrez le mot de passe associé au nom d'utilisateur dans la zone **Server Username**.
Private Key File	Entrez le chemin d'accés 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 utilise la clé privée pour authentifier la connexion SSH. La clé 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. Si cette case est vide, le paramètre est ignoré .
NMap Executable	Entrez le chemin complet du répertoire et le nom du 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.
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 abandonnée 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 sur des réseaux distants, il est recommandé de sélectionner 1 seconde comme valeur maximale.*

Table 5-2 paramètres d'analyse NMap (suite)

Paramètre	Description
Timing Template	Sélectionnez le niveau d'intensité d'analyse devant être exécuté par NMap. L'interprétation précise des niveaux dépend du scanner. Pour en savoir plus sur la puissance, consultez votre fournisseur. En général, les niveaux de puissance indiquent sur l'intensité d'analyse : • **Paranoid** - Indique une évaluation sûre, et non-intrusive. Cette option d'analyse prend du temps et peut ne plus répondre. Cette analyse prend le plus de temps pour s'accomplir. • **Sneaky** - Indique une évaluation sûre et fournit des résultats concrets. Sneak est similaire à paranoid, mais introduit une période d'attente entre les paquets. • **Polite** - Indique une évaluation quelque peu sécuritaire, vise à réduire les risques de panne et génère des résultats précis. • **Normal** - est l'option d'analyse NMap par défaut, qui correspond à une intensité d'analyse moyenne. Cette option d'analyse s'exécute aussi rapidement possible sans hôtes ou ports manquants lors de l'analyse. • **Aggressive** - Indique une évaluation quelque peu risquée. • **Insane** - Indique une évaluation trés risquée ou risquée. C'est l'option d'analyse la plus rapide. Cependant, c'est l'option d'analyse la plus intense et peut omettre des données de vulnérabilité ou rendre votre service inactif. ***Note:*** *Nous vous recommandons de sélectionner* ***Normal*** *dans la zone de liste* ***Timing Template*** *pour plus d'analyses NMap.*
CIDR Mask	Entrez CIDR pour configurer 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 CIRD 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.

NOTE

Si le scanner est configuré pour utiliser un mot de passe, le serveur du scanner SSH auquel QRadar 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 devant être considéré par ce scanner :

a Dans la zone de texte, entrez le routage CIDR ou cliquez sur **Browse** pour sélectionner le routage CIDR à partir de la liste 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 pour déterminer la fréquence à laquelle QRadar lance une analyse sur votre scanner NMap. QRadar peut importer des données de vulnérabilité uniquement si l'analyse est terminée. Pour en savoir plus sur la planification d'une analyse, consultez **Managing Scan Schedules**.

Ajout d'une analyse Remote Results Import Scan NMap

Ajouter un scanner Remote Results Import NMap vous permet de générer et stocker des analyses sur votre scanner NMap. Les analyses doivent être générées en format XML à l'aide de la commande -oX <file> de votre scanner NMap. Vous pouvez ensuite récupérer les résultats à l'aide de QRadar sur une base planifiée. Après avoir configuré votre scanner NMap, vous devez attribuer une planification pour déterminer la fréquence à laquelle QRadar récupére des informations de vulnérabilité NMap pour vos documents.

Pour ajouter une importation de résulats distant 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 pour les paramètres suivants :

Table 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 sélectionn s'affiche.

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

Etape 7 Configurez les valeurs pour les paramètres suivants :

Table 5-2 paramètres NMap pour importer des résultats distants

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 ex cute SSH.
Server Username	Entrez le nom d'utilisateur obligatoire sous SSH, pour accéder au système distant qui héberge le client NMap.
Enable Key Authentication	Sélectionnez cette case pour permettre à QRadar d'utiliser une authentification par clé public ou privée. Lorsque vous sélectionnez cette case, spécifiez le chemin de répertoire de votre clé dans QRadar 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'accés 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 utilise la clé privée pour authentifier la connexion SSH. La clé 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. Si cette case est vide, le paramètre est ignoré .
Remote Folder	Entrez le chemin d'accés au scanner NMap contenant des données de vulnérabilité XML.
Remote File Pattern	Entrez un modèle d'expression régulière (regex) pour déterminer quels fichiers de résultats NMap XML faut-il 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 ne sont pas supprimés du dossier distant. Nous vous recommandons de planifier une tâche cron afin de supprimer les rapports d'analyse précèdemment traités sur une base planifiée.*

NOTE

Si le scanner est configuré pour utiliser un mot de passe, le serveur du scanner SSH auquel QRadar 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 devant être considéré par ce scanner :

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 du 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 importe les rapports d'analyse de vulnérabilité formatés de type XML sur votre scanner NMap. Pour en savoir plus sur la planification d'une analyse, consultez **Managing Scan Schedules**.

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. Consultez **Table 5-2**.

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**.

6 MANAGING QUALYS SCANNERS

QRadar récupére les informations de vulnérabilité à des scanners Qualys de deux manières différentes ; via Qualys Application Programming Interface (API) et en téléchargeant les rapports d'analyse générés par les appliances QualysGuard. La vulnérabilité à QualysGuard et les informations d'actifs est prise en charge sur les appliances QualysGuard via l'utilisation de la version de logiciel 4.7 to 7.2.

QRadar 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'appliance 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 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'appliance QualysGuard via l'utilisation d'une connexion HTTPS.

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

Après avoir configuré le module Qualys Detection Scanner ou Qualys Scanner dans QRadar, vous pouvez planifier une analyse dans QRadar 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 avec les données de vulnérabilité à partir des appliances de vulnérabilité externes, telles que Qualys Vulnerability Manager. Pour plus d'informations, voir **Managing Scan Schedules**.

Cette section fournit des informations sur l' étape suivant :

- **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 via plusieurs rapports d'analyse pour collecter les données de vulnérabilité pour les actifs. Les données renvoyées contiennent la vulnérabilité comme numéro d'identification, que QRadar compare par rapport à la dernière version de Qualys Vulnerability KnowledgeBase. Qualys Detection Scanner ne prend pas en charge les analyses en direct mais autorise Qualys Detection Scanner de récupérer les informations de vulnérabilité regroupées à travers plusieurs rapports d'analyse. QRadar prend en charge les paramètres de recherche essentiels, tels que les champs **Operating System Filter** et **Asset Group Name**.

Qualys Detection Scanner fournit également une option afin de configurer la fréquence de récupération et de mis en cache de Qualys par Vulnerability KnowledgeBase par QRadar. La durée de conservation de KnowledgeBase par QRadar est déterminée par le champ **Qualys Vulnerability Retention Period**. Pour forcer QRadar 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 doit disposer d'autorisations activées pour télécharger Qualys KnowledgeBase. Pour plus d'informations, voir votre documentation Qualys.

Adding the Qualys Detection Scanner

Pour ajouter Qualys Detection Scanner vers QRadar:

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

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

Le panneau des sources de données 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 :

Table 6-1 Qualys Detection Scanner Parameters

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 pour les paramètres suivants :

Table 6-2 Qualys Detection Scanner Parameters

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 Etats-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, dans lequel **`<management_console>`** est le nom d'hôte de votre appliance 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 tant 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 initialise le scanner. Pour afficher le message d'erreur partir d'un échec d'analyse, déplacez votre souris sur le texte dans la colonne **Status**.

Table 6-2 Qualys Detection Scanner Parameters (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, 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 affiche les vulnérabilités via leur adresse IP. Pour l'exemple ci-dessus, QRadar 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 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. Le nombre par défaut est de 7 jours. Si une analyse est planifiée et la durée de conservation expirée, QRadar télécharge une mise de jour de Qualys Vulnerability Knowledge Base.
Force Qualys Vulnerability Update	Sélectionnez cette case à cocher pour obliger QRadar 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 récupére 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 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 vous mettre en évidence via ce scanner ou cliquez sur **Browse** pour sélectionner l'intervalle de routage CIDR à partir de la liste réseau.

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 collecte les informations du scanner Qualys Detection. Pour plus d'informations, voir **Managing Scan Schedules**.

Editing a Qualys Detection Scanner

Pour modifier une configuration Qualys Detection Scanner dans QRadar :

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

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

Le panneau des sources de données 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 Mettre à jour les paramètres, si nécessaire. Voir **Table 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 et ne mets pas à jour données d'identification de proxy Qualys Detection Scanner, cliquez sur **Deploy Changes** sur 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 le champ **Proxy Username** ou **Proxy Password**, sélectionnez **Advanced > Deploy Full Configuration** partir du menu de navigation de l'onglet **Admin**.

ATTENTION

*La sélection de **Deploy Full Configuration** redémarre les services QRadar, résultant à un écart dans la collecte des données d'événements et flows until the deployment completes.*

Vos changements de scanner Qualys sont terminés.

Deleting a Qualys Detection Scanner

Pour supprimer un scanner Qualys à partir QRadar:

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

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

Le panneau des sources de données 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 Qualys Scanner

Le module Qualys Scanner télécharge et analyse les rapports d'analyse à partir de l'appliance Qualys. Si vous sélectionnez Qualys Scanner, QRadar doit accèder 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 comprend :

- Le démarrage d'une analyse en direct sur Qualys et la collecte complète de données d'analyses.
- Les importations de planification des rapports complets de données d'analyse.
- Les importations de planification des rapports complets d'analyse.

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 que le paramètre **Collection Type** dans la fenêtre Add Scanner pour toutes les configurations Qualys Scanner existantes dans QRadar.*

Ajout de Qualys Live Scan

Live scans allow QRadar to launch preconfigured scans on the Qualys Scanner and collect the scan results in QRadar when the live scan completes.

Pour ajouter une analyse Qualys dans QRadar:

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

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

Le panneau des sources de données 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 :

Table 6-3 paramètres du scanner Qualys

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 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 en direct sur votre serveur Qualys s'affichent.

Etape 7 Configurez les valeurs pour les paramètres suivants :

Table 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 Etats-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, dans lequel **`<management_console>`** est le nom d'hôte de votre appliance 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 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.

Table 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 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 une appliance de numérisation publique, 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 récupére les données complètes de l'analyse en direct 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 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 vous mettre en évidence via ce scanner ou cliquez sur **Browse** pour sélectionner l'intervalle de routage CIDR à partir de la liste réseau.

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 avec laquelle QRadar lance l'analyse en direct sur votre scanner Qualys. Pour plus informations, voir **Managing Scan Schedules**.

Ajout d'un Qualys Asset Report Data Import

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

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

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 :

Table 6-5 Paramètres du scanner Qualys

Paramètres	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 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 pour les paramètres suivants :

Table 6-6 Paramètres d' Importation de données d'actifs Qualys

Paramètres	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 Etats-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, dans lequel **`<management_console>`** est le nom d'hôte de votre appliance de gestion interne.

Table 6-6 Paramètres d’ (suite)Importation de données d’actifs Qualys

Paramètres	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 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 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 nom de jour indiqué et l'horodatage sur le fichier de rapport sont exclus de l'importation planifiée.
Import File (Optional)	Facultatif. Entrez un chemin de répertoire pour enregistrer le rapport d'analyse de l'actif téléchargé . Si vous indiquez l'emplacement d'un fichier d'importation, QRadar télécharge les contenus du rapport d'analyse de l'actif vers un répertoire local. Une fois le téléchargement terminé , QRadar importe les informations de l'actif en utilisant le fichier local. Si le champ Import File ne contient aucune valeur, 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 le champ **Report Template Title**.

Etape 8 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 vous mettre en évidence via ce scanner ou cliquez sur **Browse** pour sélectionner l'intervalle de routage CIDR à partir de la liste réseau.

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 avec laquelle QRadar importe le rapport de données d'actif à partir de votre scanner Qualys. Pour plus d'informations, voir **Managing Scan Schedules**.

Ajout d'un Qualys Scheduled Import Scan Report

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

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

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 :

Table 6-7 Paramètres du scanner Qualys

Paramètres	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 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 pour les paramètres suivants :

Table 6-8 Paramètres d'importation pour la planification Qualys

Paramètres	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 Etats-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, dans lequel **`<management_console>`** est le nom d'hôte de votre appliance 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 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 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**.

Table 6-8 Paramètres d'importation pour la planification Qualys (suite)

Paramètres	Description
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 le champ **Option Profile(s)** ne contient un nom Option Profile, alors la liste est filtrée en fonction de tous les Option Profiles et tous les rapports d'analyse pour tous les Option Profiles sont récupérés. Pour plus d'informations, voir votre documentation QualysGuard. ***Remarque :*** *Si les données ne sont pas récupérées d'un Option Profile 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 Option Profile.*
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 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 nom de jours indiqué et l'horodatage sur le fichier de rapport sont exclus de l'importation planifiée.
Import File (Optional)	Facultatif. Entrez un chemin de répertoire pour enregistrer les rapports d'analyse téléchargés. Si vous indiquez l'emplacement d'un fichier d'importation, QRadar télécharge les contenus du rapport d'analyse de l'actif vers un répertoire local. Une fois le téléchargé du rapport de données de l'actif terminé , QRadar importe les informations liées l'actif via l'utilisation du fichier local. Si le champ Import File ne contient aucune valeur, 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 le champ **Report Template Title**.

Etape 8 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 vous mettre en évidence via ce scanner ou cliquez sur**Browse** pour sélectionner l'intervalle de routage CIDR à partir de la liste réseau.

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 avec laquelle QRadar importe le rapport de données d'actif à partir de votre scanner Qualys. Pour plus d'informations, voir **Managing Scan Schedules**.

Editing a Qualys Detection Scanner

Pour modifier une configuration de Qualys Scanner dans QRadar:

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.

- Pour les paramètres Qualys Live Scan, voir **Table 6-4**.
- Pour les paramètres Qualys Asset Report Data Import, voir **Table 6-6**.
- Pour les paramètres Qualys Scheduled Import Scan Report, voir **Table 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 et ne mettez pas à jour données d'identification de 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 champs **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, aboutissant à un écart dans la collecte de données pour les événements et flux jusqu' à achèvement du déploiement.*

Vos changements de scanner Qualys sont terminés.

Deleting the Qualys Scanner

Pour supprimer un scanner Qualys de QRadar:

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 de scanner.

7 GESTIONS DE SCANNERS FOUNDSCAN

Le scanner QRadar Foundstone FoundScan, le scanner interroge FoundScan Engine à l'aide de FoundScan OpenAPI. Le scanner FoundScan n'exécute pas directement les analyses mais rassemble les résultats de l'analyse actuelle affichée dans l'application de numérisation. QRadar prend en charge Foundstone FoundScan versions 5.0 6.5.

Votre système FoundScan doit inclure une configuration adéquate permettant l'utilisation deQRadar 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 continue sur le serveur FoundScan. Cela signifie que l'application FoundScan doit être active sur votre bureau.
- L'analyse qui inclut la configuration nécessaire permettant de se connecter QRadar doit être complète et visible dans l'interface utilisateur FoundScan. Cela permet à QRadar 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 à la fin, QRadar doit extraire les résultats avant la suppression ou l'échec de l'analyse.
- Les droits utilisateur appropri s doivent être configurés dans l'application FoundScan, permettant à QRadar de communiquer avec FoundScan.

Puisque FoundScan OpenAPI ne fournit que des informations d'hôte et de vulnérabilité à QRadar, vos informations Asset Profile QRadar affichent toutes les vulnérabilités d'un hôte affecté au port 0.

Lors de l'utilisation de SSL (par défaut) pour se connecter à FoundScan, FoundScan Engine exige à QRadar 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 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 les clés appropriés sur l'hôteQRadar. Pour en savoir plus, voir **Importation de certificats**.

Après avoir configur le système FoundScan et le scanner FoundScan dans QRadar, 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 de la puissance lors de l'analyse. Pour en savoir plus, voir **Managing Scan Schedules**.

Cette section fournit des informations sur 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**.

La 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 :

Table 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, cohez **FoundScan Scanner**.

Etape 6 Configurez les valeurs des paramètres suivants :

Table 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>`** O : **`<foundstone IP address>`** correspond l'adresse IP ou au nom d'hôte du serveur scanner FoundScan. **`<SOAP port>`** correspond au numéro de port de FoundScan Engine. L'URL par défaut est **`https://localhost:3800.`**
Customer Name	Entrez le nom du client auquel appartient le nom d'utilisateur.
User Name	Entrez le nom d'utilisateur dont vous souhaitez que QRadar utilise pour authentifier FoundScan Engine dans API. Cet utilisateur doit avoir accès à la configuration d'examen.
Client IP Address	Entrez l'adresse IP du serveur QRadar devant exécuter 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 nom d'utilisateur pour accéder à l'API (interface de programme d'application).
Portal Name	Facultatif. Entrez le nom du portail. Vous pouvez laisser ce champ vide pour QRadar. Contactez votre administrateur FoundScan pour plus d'informations.
Configuration Name	Entrez le nom de la configuration de l'analyse qui se trouve dans FoundScan et auquel l'utilisateur a accès. Vérifiez que cette analyse est active ou s'exécute au moins fréquemment.
CA Truststore	Affiche le chemin de répertoire et le nom de fichier du 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 du fichier de clés du client. Le chemin de répertoire par défaut est /opt/qradar/conf/foundscan.truststore.

Etape 7 Pour configurer les intervalles CIDR dont vous souhaitez que ce scanner prenne 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 réseau.

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

Etape 9 Sur l'onglet **Admin**, s lectionnez **Deploy Changes**.

Edition d'un scanner FoundScan

Pour modifier un scanner FoundScan :

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

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

La panneau Data Sources s'affiche.

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

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner à modifier.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Mettre à jour les paramètres, si nécessaire. Voir Table 7-2.

Etape 7 Cliquez sur **Save**.

Etape 8 Sur 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**.

La 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**, 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 configurer FoundScan pour utiliser le certificat par défaut ou un certificat personnalisé.

Cette section fournit des informations sur 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 Accédez à la zone Authentication Scheme.

Si la zone indique le certificat par défaut FoundStone, cela signifie que le certificat par défaut est en cours d'utilisation.

Etape 5 Si vous utilisez le certificat par défaut, localisez et obtenez les fichiers **TrustedCA.pem** et **Portal.pem** dans le dossier de configuration de 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. Assurez-vous que vous avez saisi l'adresse IP de l'hôteQRadar en tant que nom d'hôte du certificat.

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

Importation de certificats

Si FoundScan Server utilise les certificats personnalisés ou utilise une version FoundScan autre que 5.0, vous devez importer les certificats et les clés appropriés vers l'hôte géré QRadar que vous avez sélectionné 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, voir **Ajout d'un scanner FoundScan**.

Pour importer des certificats vers QRadar:

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

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

Les 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 et sur le répertoire de base utilisateur ou sur un nouveau répertoire créé pour les certificats.

Etape 3 Sur l'hôte QRadar, 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>
```

O :

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

<Portal.pem> est le fichier PEM de la cha ne de cl s priv es.

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  Mot de passe :foundscan
Contenu du fichier de clés certifiées :
Type de magasin de clés : jks
Fournisseur de fichier de clés : SUN
Votre fichier de clés contient 1 entrée
Alias : trustedca.pem
Date de création : 8 mars 2007
Type d'entrée : trustedCertEntry
Propriétaire : CN=Foundstone CA
Emetteur : CN=Foundstone CA
Numéro de série : 0
Valable du ven 12 sep  20:29:11 ADT 2003 au lun 20 oct 20:29:11
ADT 2008 - Empreintes digitale du certificat :
         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 du fichier de clés :
Type de magasin de clés : jks
Fournisseur de fichier de clés : SUN
Votre fichier de clés contient 1 entr e
Alias : portal.pem
Date de création : 8 mars 2007
Type d'entrée : keyEntry
Longueur de la chaîne de certificats : 1
Certificat [1] :
Propriétaire : CN=Foundstone Enterprise Manager
Emetteur : CN=Foundstone CA
Numéro de série : 2
```

```
Valable du ven 12 sep  20:36:54 ADT 2003 au lun 20 oct 20:36:54
ADT 2008 - Empreintes digitales du certificat :
         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
        Emetteur : CN=Foundstone CA
        Validité
            Pas avant : le 12 sept 2003   23:36:54 GMT
            Pas avant : le 20 oct 2008   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 :
ID de clé
: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-----
```

8 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 se connecte à la base de données Profiler stockée sur le serveur NSM pour récupérer ces enregistrements. Le serveur QRadar doit avoir accès à la base de données Profiler. QRadar 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 collecte les données partir de la base de données PostgreSQL sur NSM l'aide de JDBC. Pour collecter des données, QRadar 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 configur le périphérique Juniper Networks NSM Profiler et le scanner Juniper Networks NSM Profiler dans QRadar, vous pouvez planifier une analyse. La configuration du planning d'analyse vous permet de configurer la puissance, cependant, le scanner Juniper Networks NSM Profiler ne prend pas en considération le paramètre de puissance lors de l'analyse. Pour en savoir plus, voir **Managing Scan Schedules**.

Cette section fournit les informations les l ments 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 :

Table 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 :

Table 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 vous souhaitez que ce scanner prenne 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 réseau.

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 **Table 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**.

9 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 à partir de tous les sites connectés à votre console de sécurité NeXpose. QRadar 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 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 en savoir plus, consultez la section **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 d'importer des rapports d'analyse pour un site basé sur un fichier local de la console QRadar ou l'hôte géré . Le fichier XML Rapid7 NeXpose contenant des données de vulnérabilité doit être copié à partir du dispositif Radid7 NeXpose vers la console QRadar ou l'hôte géré qui effectue l'importation locale. Vous devez créer un répertoire sur la console QRadar ou l'hôte géré avant de copier les fichiers XML du rapport d'analyse. Les fichiers peuvent être copiés vers QRadar à l'aide de Secure Copy (SCP) ou Secure File Transfer Protocol (SFTP). Pour en savoir plus, consultez **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, vous pouvez planifier une analyse. Planifier une analyse vous aide lorsque QRadar importe des données de vulnérabilité de Rapid7 NeXpose à l'aide de l'interface API ou lorsque QRadar importe le fichier XML contenant des données de vulnérabilité . Pour en savoir plus, consultez **Managing Scan Schedules**.

Cette section comprend les rubriques suivantes :

- **Importation des données de vulnérabilité Rapid7 NeXpose à l'aide de l'interface API**
- **Importation de vulnérabilité Rapid7 NeXpose à partir d'un fichier local**
- **modification d'un scanner Rapid7 NeXpose**

- **Suppression d'un scanner Rapid7 NeXpose**
- **Troubleshooting 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 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**
- **Troubleshooting 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 pour les paramètres suivants :

Table 9-1 paramètres du scanner

Paramètre	Description
Nom du scanner	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 pour les paramètres suivants :

Table 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 correspondants 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 le délai de temps expire, de nouvelles données de vulnérabilité sont requises à partir de la console de sécurité Rapid7 NeXpose à l'aide de l'interface API (Interface de Programmation d'Application).*

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

a Dans la zone de txte, 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 du réseau.

b Cliquez sur **Add**.

NOTE

Dans la mesure où QRadar 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 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 importe des rapports de données de vulnérabilité adhoc depuis Rapid7 NeXpose à l'aide de l'interface API. Pour en savoir plus sur la planification d'une analyse, consultez **Managing Scan Schedules**.

Troubleshooting 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, vous devez augmenter 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 ou l'hôte géré responsable de l'importation de données de vulnérabilité . Pour en savoir plus, consultez **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 d'importer des analyses complètes basées sur des rapports complets copiés à partir de votre scanner Rapid7 NeXpose pour QRadar.

Pour configurer QRadar 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 pour les paramètres suivants :

Table 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.
hôte g r	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 pour les paramètres suivants :

Table 9-2 paramètres Rapid7 NeXpose

Paramètre	Description
Import Folder	Entrez le chemin d'accès au répertoire sur la console QRadar 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. QRadar importe les informations d'actif du dossier de fichier local à l'aide de la zone modèle de fichier d'importation.

Table 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 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 précèdemment 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 txte, 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 du 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 importe des rapports de données de vulnérabilité locaux depuis des fichiers locaux sur la console ou l'hôte géré . Pour en savoir plus sur la planification d'une analyse, consultez **Managing Scan Schedules**.

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. Consultez **Table 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**.

10 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). QRadar se connecte la base de données, localise les derniers résultats de scannage pour une adresse IP donnée et renvoie les services et vulnérabilités reconnues vers le profil d'actif QRadar. QRadar prend en charge la version 2.6 du scanner SecureScout.

Pour connecter à QRadar vers la base de données SecureScout et analyser les résultats, vous devez disposer de l'accès administratif adéquat vers QRadar 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'hôte SecureScout, autorisez une connexion Event Collector. QRadar 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. L'utilisateur de base de données QRadar doit avoir sélectionné les permissions aux tableaux suivants :

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

NOTE

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

Après avoir configuré le périphérique SecureScout et le scanner SecureScout dans QRadar, vous pouvez planifier une analyse. La configuration de planification

de l'analyse vous permet configurer la puissance, néanmoins, le scanner SecureScout ne considère pas le paramètre de puissance pendant l'exécution de l'analyse. Pour plus d'informations, voir **Managing Scan Schedules**.

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 :

Table 10-1 Paramètres SecureScout

Paramètre	Description
Nom du scanner	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.
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 **SecureScout Scanner.**

Etape 6 Configurez les valeurs pour les paramètres suivants :

Table 10-2 paramètres SecureScout

paramètre	Description
Nom d'hôte de base de données	Entrez l'adresse IP ou le nom d'hôte du serveur de base de données SecureScout exécutant le serveur SQL.
Nom d'utilisateur de connexion	Entrez le nom d'utilisateur de base de données SQL dont vous souhaitez que QRadar utilise pour se connecter à la base de données SecureScout.
Mot de passe de connexion	Entrez le mot de passe correspondant au nom d'utilisateur de connexion.

Table 10-2 paramètres SecureScout (suite)

paramètre	Description
Nom de base de données	Entrez le nom de la base de données dans le serveur SQL contenant les données SecureScout. La valeur par défaut est SCE.
Port de la base de données	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 vidence par cette analyse :

a Dans le champ de texte, entrez l'intervalle de routage CIDR que vous mettre en vidence via ce scanner ou cliquez sur**Browse** pour sélectionner l'intervalle de routage CIDR à partir de la liste r seau.

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 Mettre jour les paramètres, si nécessaire. Voir **Table 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:

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**.

11 GESTION DE scanners EEYE

QRadar 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.

Pour configurer les scanners eEye avecQRadar, vous devez :

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

A la fin d'une analyse, les résultats sont envoyés vers QRadar à l'aide de SNMP. QRadar 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 de profil du port sont conservées, vous devez configurer une planification d'analyse pour votre scanner eEye. Ce planning d'analyse rend les profils de port et d'hôte disponibles dans la base de données de profils.

Pour connecter QRadar au scanner eEye, vous devez disposer d'un accès administrateur à QRadar et à votre dispositif eEye. Vous devez également vous assurer que n'importe quel pare-feu entre votre scanner eEye et QRadar autorise le trafic SNMP à travers votre consoleQRadar.

NOTE

La configuration de planification d'analyse vous permet de définir la puissance. Toutefois le scanner eEye REM ne prend pas en compte le paramètre de puissance lorsqu'il effectue l'analyse.Pour en savoir plus, voir **Managing Scan Schedules**.

Cette section comprend les rubriques suivantes :

- **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 :

Table 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 :

Table 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 la fin de la durée de conservation, les informations sont supprimées. La durée de conservation par défaut est 5 jours.

Table 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. ***Note:*** *Cette option requiert une copie du fichier audits.xml à partir de votre dispositif eEye REM ou eEye Retina CS vers QRadar.*
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 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 vers QRadar. • **v2** : Sélectionnez v2 si votre scanner eEye transfère des messages d'alerte SNMPv2 vers QRadar. • **v3** : Sélectionnezv3 si votre scanner eEye transfère des messages d'alerte SNMPv3 vers QRadar. 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.
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.

Table 11-2 paramètres eEye (suite)

paramètre	Description
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 d faut est DES. ***Note:*** *Si vous sélectionnez AES192 ou AES256 comme votre algorithme de description, vous pouvez installer un composant logiciel facultatif pour QRadar. Pour en savoir plus, 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 vous souhaitez que ce scanner prenne 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 réseau.

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. Pour plus d'informations, voir **Edition d'un scanner eEye**, **Etape 9**.

La configuration dans QRadar 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 ou votre collecteur d' évènement.

Installation de Java Cryptography Extension

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

Pour installer Oracle JCE sur QRadar.

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™ install e sur QRadar.

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 sur votre consoleQRadar ou votre collecteur d' évènement en tant qu'utilisateur root.

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

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

Etape 4 Copiez les fichiers JCE jar sur le répertoire suivant sur votre consoleQRadar ou votre collecteur d' évènement :

`/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, ceci peut être votre console QRadar ou votre collecteur d' évènements.

L'installation de Java™ Cryptography Extension pour QRadar est terminée. Vous pouvez maintenant planifier une analyse pour votre scanner eEye dans QRadar.

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 souhaiter éditer.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 paramètres de mise à jour, si nécessaire. Voir **Table 11-2**.

Etape 7 Cliquez sur **Save**.

Etape 8 Dans 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 our immédiate, vous devez achever un déploiement total dans QRadar.

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

ATTENTION

Deploying Full Configuration redémarre plusieurs services sur le système QRadar. La collection d' évènements ne sera pas disponible surQRadar 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**.

12 GESTION DES scanners PATCHLINK

Vous pouvez intégrer un scanner PatchLink (version 6.4.4. et supérieure) QRadar. Le scanner PatchLink envoie des requêtes au moteur afin d'utiliser l'interface API. QRadar collecte des données de vulnérabilités à partir des résultats d'analyse avec PatchLink. Par conséquent, votre système PatchLink doit inclure une configuration appropriée pour QRadar 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.

NOTE

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

Pour connecter QRadar au scanner PatchLink, vous devez avoir un accès administrateur approprié QRadar ainsi que votre périphérique PatchLink. Pour en savoir plus, consultez votre documentation du produit. Assurez-vous que tous les pare-feu sont configurés pour permettre une connexion avec votre système QRadar.

après avoir configuré votre périphérique PatchLink et votre scanner PatchLink sous QRadar, vous pouvez planifier un processus d'analyse. La configuration de planification d'analyse vous permet également de configurer la puissance, toutefois, le scanner PatchLink ne tient pas compte du paramêtre de puissance lors de l'exécution du processus d'analyse. Pour en savoir plus, consultez la section **Managing Scan Schedules**.

Cette section fournit des renseignements sur ce qui suit :

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

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 pour les paramètres suivants :

Table 12-1 paramètres du scanner

Paramêtre	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 pour les paramètres suivants :

Table 12-2 paramètres PatchLink

Paramêtre	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 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.

Table 12-2 paramètres PatchLink (suite)

Paramêtre	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 le routage CIDR que vous souhaitez que ce scanner prenne 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 du 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. Consultez **Table 12-2**.

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

Suppression d'un scanner PatchLink

Pour supprimer un scanner PatchLink de QRadar :

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 MCAFEE VULNERABILITY MANAGER

Le scanner McAfee Vulnerability Manager QRadar scanner interroge le moteur de McAfee Foundstone Enterprise en utilisant l'OpenAPI de FoundScan.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 prend en charge les versions 6.8 ou 7.0. de McAfee Vulnerability Manager.

NOTE

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

NOTE

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 **Managing FoundScan Scanners**.

Votre système McAfee Foundstone Enterprise doit inclure une configuration appropri e pour QRadar 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 QRadar doit être entièrement exécué e et visible dans l'interface utilisateur McAfee Foundstone Enterprise QRadar 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 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 de communiquer avec McAfee Foundstone Enterprise.

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

SSL connecte le serveur McAfee Foundstone Enterprise Manager à OpenAPI Foundstone. QRadarauthentifie 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. Pour plus d'informations, consultez **Utiliser les certificats**.

Après avoir configuré le système McAfee Foundstone Enterprise et le scanner McAfee Vulnerability Manager dansQRadar, vous pouvez programmer l'analyse. La configuration du planning d'analyse vous permet de configurer la puissance. Cependant, le scanner McAfee Vulnerability Manager ne tient pas compte du paramètre de puissance lors de l'exécution de l'analyse. Pour plus d'informations, consultez **Managing Scan Schedules**.

Cette section fournit des informations sur les points suivants:

- **Ajouter un scanner McAfee Vulnerability Manager**
- **Editer un scanner McAfee Vulnerability Manager**
- **Supprimer un scanner McAfee Vulnerability Manager**
- **Utiliser les 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:

Table 13-1 Paramètres du scanner

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

Table 13-1 Paramètres du scanner (suite)

Paramètre	Description
Description	Décrivez ce scanner par saisie 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:

Table 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>`** O : **`<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 d faut est **`https://localhost:3800.`**
Customer Name	Tapez un nom pour identifier à quel client ou organisation appartient le nom d'utilisateur. Le nom du client doit correspondre l'ID de l'organisation requise pour se connecter à McAfee Foundstone Enterprise Manager.
User Name	Tapez le nom d'utilisateur que vous voulez que QRadar utilise pour authentifier le serveur McAfee Foundstone Enterprise Manager dans l'API Open Cet utilisateur doit avoir accès à la configuration d'examen.
Password	Tapez le mot de passe correspondant au nom de connexion pour avoir accès à l'API Open.
Client IP Address	Tapez l'adresse IP du serveur QRadar 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. Tapez le nom du portail. Ce champ peut être laissé vide pour QRadar. Consultez l'administrateur de McAfee Vulnerability Manager administrator pour de plus amples informations.
Configuration Name	Tapez le nom de la configuration d'examen qui existe dans McAfee Foundstone Entreprise et auquel l'utilisateur a accès.

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

Paramètre	Description
CA Truststore	Tapez 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 pour McAfee Vulnerability Manager, consultez* **Utiliser les certificats**.
Client Keystore	Tapez 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, consultez* **Utiliser les 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 prenne en compte:

a Dans la zone de texte, tapez la plage CIDR vous souhaitez que le scanner prenne en compte ou cliquez sur Browse pour sélectionner la plage 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**, 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**.

Utiliser les 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 à avoir des fichiers de clés valides pour 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) peut être installé sur le même système en charge de créer des certificats à l'aide de McAfee Certificate Management Tool. 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 Exécuter the Foundstone Certificate Manager.

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

Etape 3 Configurez l'adresse hôte de QRadar.

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

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

NOTE
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 Step 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

NOTE
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. Voir **Traitement des certificats**.

Traitement des certificats

Pour traiter les certificats :

Etape 1 Extraire 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"
```

NOTE

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. Voir **Importer des certificats**.

Importer des certificats

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

NOTE

Avant d'importer des fichiers, nous vous recommandons de supprimer ou renommer les fichiers de clés ainsi que les fichiers de clés certifiés 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 :

`/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 connecter à QRadar.

`https://<IP Address>`

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

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

L'onglet Administration s'affiche.

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

ATTENTION

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

14 GESTION DE SCANNERS SAINT

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

Pour intégrer QRadar au scanner SAINT, vous devez avoir l'accès administrateur adéquat au QRadar et votre périphérique SAINT. Vous devez également vous assurer que les pare-feux sont configurés pour autoriser une connexion avec votre système QRadar. Pour plus d'informations, voir la documentation de votre produit.

Après avoir configuré SAINTwriter, vous pouvez planifier une analyse. Pour plus d'informations, voir **Managing SAINT Scanners**.

Cette section fournit des informations sur l'étape suivante :

- **Configuring SAINTwriter Report Template**
- **Adding a SAINT Vulnerability Scanner**
- **Modification d'un groupe**
- **Deleting a SAINT Vulnerability Scanner**

Configuration d’un modèle de raport 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 le champ **File Name**, indiquez le nom d'un fichier de configuration.

Le nom du fichier de configuration doit correspondre au paramètre QRadar Saint Writer Config dans Table 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** **inclure dans la liste d'hôtes** , changez toute colonne marquée comme None **MAC Address**.

Etape 10 Dans **Columns** **inclure dans la liste de vulnérabilité**, changez toute colonne marquée comme None **Port**.

Etape 11 Dans **Columns** **inclure dans la liste de vulnérabilité** , changez toute colonne marquée comme None **Service**.

Etape 12 Cliquez sur **Save**.

Vous êtes prêts à ajouter un scanner de vulnérabilité SAINT à QRadar, voir Adding a SAINT Vulnerability Scanner.

Ajout d'un scanner de vunérabilité SAINT

Pour ajouter un scanner de vulnérabilité SAINT à QRadar:

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 :

Table 14-1 Scanner Parameters

Parameter	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 **SAINT Scanner**.

Etape 6 Configurez les valeurs pour les paramètres suivants :

Table 14-2 Paramètres de Scanner SAINT

Paramètres	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 pour authentifier la connexion SSH.
Enable Key Authorization	Sélectionnez cette case à cocher pour activer l'authentification par clé publique/privée. Si la case à cocher est sélectionnée, QRadar 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 documentation SSH pour configurer l'authentification par clé publique.
Login Password	Entrez le mot de passe associé 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 clé privée. Si vous utilisez une authentification basée sur la clé SSH, QRadar 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 à cocher Enable Key Authentication est sélectionnée. 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 un scannage de vulnérabilité et génére des données de rapport à partir des résultats basés sur le nom de session. • **Report Only** - génére un rapport d'analyse basé sur le nom de session.
Ignore Existing Data	Cette option s'applique uniquement lorsque Live Scan est le type d'analyse sélectionné . Cette option indique si l'analyse en direct ignore les données existantes et regroupe les nouvelles informations de vulnérabilité pour le réseau. Si la case à cocher Ignore Existing Data est sélectionne, le scanner SAINT supprime les données de session existantes avant qu'une analyse en direct ne soit lancée. Par défaut, la case cocher est vide.

Table 14-2 Paramètres de Scanner SAINT (suite)

Paramètres	Description
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 vidence sur la conformité DSS PCI. • **SANS Top 20 Scan** - Analyse les 20 vulnérabilités de sécurité les plus importantes. • **FISMA Scan** - Analyse toutes les vulnérabilités et 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 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 vous mettre en évidence via ce scanner ou cliquez sur **Browse** pour sélectionner l'intervalle de routage CIDR à partir de la liste réseau.

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

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

Modification d'un groupe

Pour modifier un scanner de vulnérabilit SAINT dans QRadar:

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 Mettre à jour les paramètres, si nécessaire. Voir **Table 14-2**.

Etape 7 Cliquez sur **Save**.

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

Suppression d’un scanner de vunérabilité SAINT

Pour supprimer un scanner de vulnérabilité SAINT depuis QRadar:

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**.

15 GESTION DE SCANNERS AXIS

Le scanner Asset Export Information Source (AXIS) permet à QRadar d'extraire les résultats d'analyse des périphériques de scanner inconnus pour la corrélation. Le scanner AXIS interroge périodiquement l'écoute de fichiers pour extraire les résultats d'analyse au format XML et interpr ter les données analysées. QRadar surveille le serveur SSH pour les mises à jour vers les résultats d'analyse et télécharge les derniers résultats pour le traitement.

Pour intégrer correctement le scanner AXIS dans QRadar, les fichiers résultats XML doivent être lus à partir d'un serveur distant utilisant SSH ou du scanner créant les fichiers résultat, si le scanner prend en charge SSH. Le terme serveur distant fait référence à un système indépendant de QRadar.

Les résultats d'analyse contiennent des informations d'identification concernant la configuration de l'analyse à partir du périphérique de scanner inconnu. Les derniers résultats d'analyse sont utilisés lorsqu'une analyse est demandée depuis QRadar. QRadar ne prend en charge que le format XML.

Pour en savoir plus, voir **Managing Scan Schedules**.

Cette section fournit des informations sur les éléments suivants :

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

Ajout d'un scanner AXIS

Pour ajouter un scanner AXIS QRadar:

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

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

La 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 :

Table 15-1 Paramètres du scanner AXIS

Paramètre	Description
Scanner Name	Entrez le nom que vous souhaitez affecter 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 **Axis Scanner**.

Etape 6 Configurez les valeurs des paramètres suivants :

Table 15-2 Paramètres du scanner AXIS

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 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 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 du 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.
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 bas e sur la clé privée, QRadar 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 d cochée, ce paramètre est ignoré.
Remote Directory	Entrez l'emplacement du répertoire des fichiers des résultats d'analyse.

Table 15-2 Paramètres du scanner AXIS (suite)

Paramètre	Description
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 répertorier 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 déjà traités et les fichiers à ne 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 la prochaine reconnaissance du fichier.*

Etape 7 Pour configurer les intervalles CIDR dont vous souhaitez que ce scanner prenne 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 réseau.

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

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

Modification d'un scanner AXIS

Pour modifier un scanner AXIS :

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

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

La panneau Data Sources s'affiche.

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

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner à modifier.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Mettre à jour les paramètres, si nécessaire. Voir **Table 15-2**.

Etape 7 Cliquez sur **Save**.

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

Suppression d'un scanner AXIS

Pour supprimer un scanner AXIS de QRadar:

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**.

16 GESTION DE TENABLE SECURITYCENTER

Un scanner Tenable SecurityCenter peut être utilisé avec QRadar pour planifier et récupérer tous les enregistrements de rapports ouverts d'analyse de vulnérabilités à partir de plusieurs scanners de vulnérabilités Nessus sur votre réseau. QRadar accède à distance à Tenable SecurityCenter via une connexion HTTPS. QRadar prend en charge la version 4.0 de Tenable SecurityCenter.

Après avoir ajouté le scanner Tenable SecurityCenter dans QRadar, vous pouvez planifier une analyse afin de récupérer les enregistrements de rapports ouverts de vulnérabilités. Pour plus d'informations, voir **Managing Scan Schedules**.

Cette section fournit des informations sur l'étape suivante :

- **Ajout de Tenable SecurityCenter**
- **Modification de Tenable SecurityCenter**
- **Suppression de SecurityCenter**

Ajout de Tenable SecurityCenter

Pour ajouter Tenable SecurityCenter QRadar :

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 :

Table 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:

Table 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 du programme d'application est **`sc4/request.php`**. Si vous rencontrez des problèmes en vous connectant à votre Tenable SecurityCenter depuis QRadar, vous pouvez vérifier le chemin d'accès vers votre fichier request.php puis mettez 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 si vous souhaitez que ce scanner prenne en compte :

a Dans le champ de texte, entrez l'intervalle de routage CIDR que vous souhaitez mettre en évidence via ce scanner ou cliquez sur **Browse** pour sélectionner l'intervalle de routage CIDR à partir de la liste réseau.

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

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

Modification de Tenable SecurityCenter

Pour modifier un scanner Tenable SecurityCenter précédemment configuré dans QRadar:

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 **Table 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:

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 MANAGING SCAN SCHEDULES

Après avoir configuré les scanners individuels pour permettre à QRadar à accéder aux données de vulnérabilité du client ou de l'appliance, vous devez créer une planification afin que QRadar récupére 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 est mis à jour avec les données de vulnérabilité les plus récentes.

Cette section fournit des informations sur l' étape suivant :

- **Viewing Scheduled Scans**
- **Scheduling a Scan**
- **Editing a Scan Schedule**
- **Deleting a Scheduled Scan**

NOTE

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

Viewing Scheduled Scans

La fenêtre Scan Scheduling s'affiche lorsque QRadar est planifié pour la collecte des données de l'évaluation de vulnérabilité à partir des appliances 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 :

Table 17-1 Scheduled Scan Parameters

Parameter	Description
VA Scanner	Affiche le nom de l'analyse planifiée.
routage CIDR	Affiche les adress(es) IP à inclure à cette analyse.
Ports	Affiche la plage de ports inclue 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 et restreint le nombre de ports planifiés. 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 les vulnérabilités sur tous les ports mais vous exigent d'indiquer les informations de port adéquatesafin 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.
Status	Affiche le statut de l'analyse. Un message d' état descriptif s'affiche via le maintient du message d' état de la souris (en pla ant dessus) : • **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 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 l'achèvement de l'analyse. Percentage Complete indique le statut du pourcentage (%) complet pour l'analyse en tant que valeur num rique. • **Complete** - Lorsque Percentage Complete atteind 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 en direct qui peuvent être en cours.*

Table 17-1 Scheduled Scan Parameters (suite)

Parameter	Description
Next Run Time	Affiche un compte à rebours pour indiquer l'intervalle jusqu' à ce que le prochain scannage de vulnérabilité soit planifié pour le redémarrage. Si l'analyse est planifiée avec une 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.

Scheduling a Scan

Après avoir configuré les scanners configurés de vulnérabilité dans QRadar, vous êtes alors prêts à 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.

Pour planifier une analyser 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.

NOTE

Si vous ne disposez pas 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 pour les paramètres suivants :

Table 17-2 Scan Schedule Parameters

Parameter	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 sélectionnez la plage de réseaux CIDR à laquelle vous souhaitez que cette 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**.
Priority	Dans la zone de liste **Priority**, sélectionnez le niveau de priorité 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.

Table 17-2 Scan Schedule Parameters (suite)

Parameter	Description
Ports	Entrez la plage de ports que vous souhaitez faire analyser par le scanner.
Start Time	Configurez l'heure et la date de début pour l'analyse. La configuration par défaut est l'heure locale de votre système QRadar. ***Remarque :*** *Si vous sélectionnez une heure de début réglée auparavant, l'analyse commence immédiatement après l'enregistrement de sa planification.*
Interval	Entrez une intervalle de temps pour indiquer la fréquence souhaitée pour l'exécution de l'analyse. Les intervalles d'analyse peuvent être planifiées par heure, jour, semaine ou mois. Une intervalle de 0 indique que l'analyse planifiée s'effectue une fois et ne se répéte pas.

Etape 6 Cliquez sur **Save**.

L'analyse est planifiée et démarre immédiatement. Le statut de l'analyse, tel que le niveau d'achèvement ou les messages d'échec sont affichables dans la colonne Status.

Editing a Scan Schedule

Après avoir créé un nouveau planning d'analyse, vous pouvez modifier les paramètres du planning d'analyse. La modification d'un planning d'analyse n'est possible qu'une fois le déploiement de la configuration dans QRadar. Après que les changements de configuration aient été déployés dans QRadar, 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 Click **Edit**.

La fenêtre Edit Schedule s'affiche.

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

Etape 7 Cliquez sur **Save**.

Deleting a Scheduled Scan

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** .

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 **OK**.

L8 SCANNERS PRIS EN CHARGE

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

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 préser document, contactez votre représentant commercial.

au 18-1 Scanners pour l' évaluation de vulnérabilité

nt	Scanner	Version	Option dans QRadar	Type de Connexion
ue eEye	REM eEye ou Retina CS eEye	REM version 3.5.6 ou Retina CS version 3.0.0	Scanner REM eEye	Alerte SNMP
ue	AXE	N/A	Axis Scanner	Importez des fichiers de données de vulnérabilité à l'aide de SSH
	IBM Security AppScan Enterprise	AppScan Enterprise 8.6	Scanner IBM AppScan	IBM gére le service web à l'aide du protocole HTTP ou HTTPS
	NSM Profiler	2007.1r2, 2007.2r2, 2008.1r2, 2009r1.1, et 2010.x	Scanner Juniper NSM Profiler	Sondage JDBC
on	Patchlink	version 6.4.4 et supérieure	Scanner Patchlink Lumenison	interface API basée sur le protocole SOAP l'aide de HTTPS
	Foundstone	version 5.0 vers 6.5	Scanner Foundscan	interface API basée sur le protocole SOAP l'aide de HTTPS
	Gestionnaire de vulnérabilité	Version 6.8 ou 7.0.	McAfee Vulnerability Manager	interface API basée sur le protocole SOAP l'aide de HTTPS
	ip360	VnE Manager version 6.5.2 vers 6.8.28	nCircle ip360 Scanner	Importez des fichiers de données de vulnérabilité à l'aide de SSH

eau 18-1 Scanners pour l' évaluation de vulnérabilité (suite)

ant	Scanner	Version	Option dans QRadar	Type de Connexion
s	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 exécution de 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
ance	SecureScout	2.6	Scanner SecureScout	Sondage JDBC
Source	NMap	Version 3.7 vers 5.50	Scanner NMap	Importation de fichiers de données de vulnérabilité à l'aide de SSH et l'exécution de commande SSH
	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
	NeXpose	Version 4.0 et version supérieure	Scanner Rapid7 NeXpose	Appel de procédure à distance via HTTPS
				Importation des fichiers XML files à partir d'u répertoire local QRadar
orporation	Saintscanner	7.4.x	Scanner Saint	Importation de données de vulnérabilité via SSH et l'exécution de la commande SSH
e	Centre de sécurité		Centre de sécurité Tenable	Appel de procédure à distance via HTTPS

INDEX

T

V