IBM Security QRadar
Version 7.1.0 (MR2)

Guide de configuration de l'évaluation de la vulnérabilité

Remarque : Avant d'utiliser ces informations et le produit associé, prenez connaissance des informations figurant à la section “Avis et marques” du document page 143.

SOMMAIRE

A PROPOS DE CE GUIDE

Le *Guide de configuration de l'évaluation de la vulnérabilité IBM Security QRadar* vous fournit des informations sur la gestion des scanners de vulnérabilité et la configuration des plannings d'analyse à utiliser avec QRadar.

Public cible

Ce guide est destiné à l'administrateur système chargé de configurer QRadar dans votre réseau. Ce guide suppose que vous disposez d'un accès à QRadar en tant qu'administrateur et que vous maîtrisez le réseau de votre entreprise et les technologies de mise en réseau.

Conventions

Les conventions suivantes s'appliquent dans ce guide :

u Indique que la procédure contient une seule instruction.

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

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

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

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

1 PRÉSENTATION

L'intégration de l'évaluation de la vulnérabilité permet à QRadar de générer des profils d'évaluation de vulnérabilité.

Les profils d'évaluation de la vulnérabilité utilisent des données d'événement corrélées, l'activité du réseau, ainsi que des changements de comportement afin de déterminer le niveau de menace pour les éléments métier essentiels de votre réseau.

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

Remarque : Vous devez disposer d'autorisations appropriées pour accéder aux réseaux contenant des adresses CIDR sur lesquels vous planifiez d'effectuer des analyses d'évaluation de vulnérabilité.

Remarque : Les informations trouvées dans cette documentation sur la configuration des scanners sont basées sur les derniers fichiers RPM se trouvant sur *http://www.ibm.com/support*.

Configuration de l'évaluation de vulnérabilité

Afin de configurer les analyses d'évaluation de vulnérabilité QRadar, vous devez :

1. Installer le scanner RPM, si nécessaire.

   Pour plus d'informations, voir **Installation manuelle d'un scanner**.
2. Configurer votre scanner à l'aide de la liste suivante des scanners pris en charge :
   - **Gestion des scanners IBM Security AppScan Enterprise**
   - **Gestion des scanners nCircle IP360**
   - **Gestion des scanners Nessus**
   - **Gestion des scanners Nmap**
   - **Gestion des scanners Qualys**
   - **Gestion des scanners FoundScan**
   - **Gestion des scanners Juniper Networks NSM Profiler**

- **Gestion des scanners Rapid7 NeXpose**
- **Gestion des scanners netVigilance SecureScout**
- **Gestion des scanners eEye**
- **Gestion des scanners PatchLink**
- **Gestion des scanners McAfee Vulnerability Manager**
- **Gestion des scanners SAINT**
- **Gestion des scanners AXIS**
- **Gestion des scanners Tenable SecurityCenter**

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

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

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

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

Installation manuelle d'un scanner

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 d'installer une mise à jour manuelle du scanner, le dernier fichier d'installation rpm pour votre scanner est disponible sur le site Web *http://www.ibm.com/support*.

Pour installer un scanner manuellement :

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

http://www.ibm.com/support

Etape 2 Copiez les fichiers sur votre QRadar.

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

`rpm -Uvh <nom_de_fichier>`

Où **`<nom_de_fichier>`** représente le nom du fichier téléchargé.

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

Etape 6 Connectez-vous à QRadar.

`https://<adresse_IP>`

Où <adresse_IP> représente l'adresse IP de QRadar.

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

L'onglet Administration s'affiche.

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

Affichage des scanners configurés

Pour afficher les scanners configurés, procédez comme suit :

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

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

Le panneau Data Sources s'affiche.

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

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

Tableau 1-1 Paramètres du scanner

Paramètre	Description
Name	Affiche le nom du scanner.
Type	Affiche le type de scanner, par exemple, Nessus Scan Results Importer.
Host	Affiche l'adresse IP ou le nom de l'hôte sur lequel le scanner fonctionne.
Approved CIDR ranges	Affiche la plage du routage CIDR devant être prise en compte par le scanner. Plusieurs plages du routage CIDR sont affichées à l'aide d'une liste séparée par des virgules.
Description	Affiche une description pour ce scanner.
Status	Affiche le statut de planification du scanner. ***Remarque :*** *Lorsque le statut d'une analyse planifiée change, la zone de statut située dans la liste des scanners installés se met à jour, consultez le* **Tableau 22-1** *pour en savoir plus sur le statut d'analyse.*

2 GESTION DES SCANNERS BEYOND SECURITY AVDS

Le dispositif ADVS (Automated Vulnerability Detection System) de Beyond Security utilise le format de fichier XML AXIS (Asset Export Information Source) afin de collecter les vulnérabilités pour IBM Security QRadar.

Afin de réussir l'intégration des vulnérabilités Beyond Security AVDS avec QRadar, vous devez configurer votre dispositif Beyond Security AVDS pour publier les données de vulnérabilités dans un fichier de résultats XML au format AXIS. Les données de vulnérabilité XML doivent être publiées sur un serveur distant qui est accessible pour QRadar via SFTP. Le terme serveur distant renvoie à un système ou à un dispositif tiers ou à un emplacement de stockage en réseau, accessible via SFTP qui peut héberger les résultats de l'analyse XML publiés.

Les résultats XML les plus récents contenant les vulnérabilités Beyond Security AVDS sont importés dans QRadar lorsqu'un planning d'analyse est lancé par QRadar. Les plannings d'analyse vous permettent de déterminer la fréquence à laquelle QRadar demande des données à un scanner compatible avec AXIS, tel que Beyond Security AVDS. Après l'ajout du dispositif Beyond Security AVDS dans QRadar, vous pouvez ajouter un planning d'analyse afin de récupérer les informations de vulnérabilité. Les vulnérabilités des actifs dans votre réseau s'affichent dans l'onglet **Assets** de QRadar.

Ajout d'un scanner Beyond Security AVDS

Pour ajouter un scanner Beyond Security AVDS 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 des paramètres suivants :

Tableau 2-1 Paramètres du scanner Beyond Security AVDS

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 **Beyond Security AVDS Scanner**.

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 2-2 Paramètres du scanner Beyond Security AVDS

Paramètre	Description
Remote Hostname	Entrez le nom d'hôte ou l'adresse IP du serveur distant.
Login Username	Entrez le nom d'utilisateur utilisé par QRadar pour authentifier la connexion.
Enable Key Authorization	Cochez cette case pour activer l'autorisation via une clé privée pour le serveur. Si la case est cochée, l'authentification est effectuée à l'aide d'une clé privée et le mot de passe est ignoré. Ce paramètre est désactivé par défaut. La sélection de cette option active la zone **Private Key File** dans la configuration du scanner.
Login Password	Si le paramètre Enable Key Authentication est désactivé, vous devez entrer le mot de passe correspondant au paramètre Login Username qu'utilise QRadar pour authentifier la connexion. Si le paramètre Enable Key Authentication est activé, le paramètre Login Password est ignoré.
Remote Directory	Entrez l'emplacement du répertoire des fichiers des résultats d'analyse.
File Name Pattern	Entrez une expression régulière (regex) requise pour filtrer la liste des fichiers spécifiés dans le paramètre 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 nécessite la connaissance des expressions régulières (regex). Pour plus d'informations, consultez le site Web suivant : *http://download.oracle.com/javase/tutorial/essential/regex/*

Tableau 2-2 Paramètres du scanner Beyond Security AVDS (suite)

Paramètre	Description
Private Key File	Entrez le chemin de répertoire qui mène vers le fichier contenant les informations sur la clé privée. Si vous utilisez une authentification basée sur une clé, QRadar utilise la clé privée pour authentifier la connexion. 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 entrer un autre nom de fichier. Ce paramètre est obligatoire si la case Enable Key Authentication est cochée. Si la case Enable Key Authentication est décochée, ce paramètre est ignoré.
Max Report Age (Days)	Entrez l'âge maximal du fichier à inclure au moment de l'importation du fichier de vulnérabilités XML lors d'une analyse planifiée. Par défaut, la valeur est de 7 jours. Les fichiers qui sont plus anciens que le nombre de jours indiqué et que l'horodatage sur le fichier de rapport sont exclus de l'importation planifiée.
Ignore Duplicates	Cochez cette case pour suivre les fichiers qui ont déjà été traités et les fichiers que vous ne souhaitez pas traiter une seconde fois. ***Remarque :*** *Si un fichier de résultat n'est pas consulté pendant 10 jours, il est supprimé de la liste de suivi et est traité à la prochaine reconnaissance du fichier.*

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

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

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

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

Modification d'un scanner Beyond Security AVDS

Pour modifier la configuration de votre scanner Beyond Security ADVS :

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

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

Le panneau Data Sources s'affiche.

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

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez modifier.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

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

Etape 7 Cliquez sur **Save**.

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

Suppression d'un scanner Beyond Security AVDS

Pour supprimer un scanner Beyond Security ADVS 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 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

3 GESTION DES SCANNERS IBM SECURITY APPSCAN ENTERPRISE

QRadar peut importer des résultats d'analyse à partir des données du rapport IBM Security AppScan® Enterprise, ce qui vous offre un environnement de sécurité centralisé pour une analyse d'application avancée et une création de rapports de conformité de sécurité.

L'importation des résultats d'analyse d'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 violations dans QRadar pour votre équipe de sécurité.

Pour intégrer AppScan Enterprise à QRadar, vous devez :

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

Configuration d'AppScan Enterprise

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.

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

Pour configurer AppScan Enterprise afin d'accorder à QRadar l'accès aux rapports de l'analyse :

1. Créez un type d'utilisateur personnalisé.
2. Activez AppScan Enterprise et l'intégration QRadar.
3. Créez une Application Deployment Map.
4. Publiez vos résultats d'analyse sur QRadar.

Création d'un type d'utilisateur personnalisé

Les types d'utilisateurs personnalisés permettent aux administrateurs d'effectuer des tâches administratives spécifiques et limitées et doivent être créés avant l'affectation des autorisations.

Pour créer un type d'utilisateur personnalisé :

Etape 1 Connectez-vous à IBM Security AppScan Enterprise.

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

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

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

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

Etape 5 Enregistrez le type d'utilisateur.

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

Activation de l'intégration QRadar

Pour effectuer ces étapes, vous devez vous connecter en tant qu'utilisateur en activant le 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, sélectionnez **Network Security Systems**.

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

La configuration QRadar Integration Settings s'affiche.

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

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

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

Création d'une Application Deployment Map

Application Deployment Map permet à AppScan Enterprise de déterminer les emplacements qui hébergent l'application dans votre environnement de production.

Dès que les vulnérabilités sont reconnues, AppScan Enterprise connaît les emplacements des hôtes et des adresses IP concernées par la vulnérabilité. Si une application est déployée sur plusieurs hôtes, cela signifie qu'AppScan Enterprise génère une vulnérabilité pour chaque hôte 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 la zone **Application test location (host or pattern)**, entrez l'emplacement test de votre application.

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

Remarque : Pour ajouter des informations sur la vulnérabilité à QRadar, votre Application Deployment Mapping doit avoir 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 d'analyse d'AppScan Enterprise.

Etape 6 Cliquez sur **Add**.

Etape 7 Répétez l'**Etape 3** à l'**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 d'un rapport dans QRadar

Des rapports complets sur la vulnérabilité générés par AppScan Enterprise doivent être rendus accessibles sur QRadar en publiant le rapport.

Pour effectuer ces étapes, vous devez vous connecter en tant qu'utilisateur en activant le type d'utilisateur Publish sur QRadar.

Pour publier un rapport de vulnérabilité dans AppScan Enterprise :

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

Etape 2 Accédez au 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 > Grant report access to QRadar**.

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

Configuration d'un scanner dans QRadar

Après avoir configuré AppScan Enterprise et publié les rapports, vous pouvez ajouter le scanner AppScan Enterprise à QRadar.

L'ajout d'un scanner permet à QRadar de connaître les rapports d'analyse à collecter. 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.

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

Cette section comprend les rubriques suivantes :

Ajout d'un scanner AppScan Enterprise

Pour ajouter un scanner AppScan Enterprise :

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

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

Le panneau Data Sources s'affiche.

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

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 3-1 Paramètres du scanner

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

Tableau 3-1 Paramètres du scanner (suite)

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

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

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 3-2 Paramètres IBM AppScan Enterprise

Paramètre	Description
ASE Instance Base URL	Entrez l'URL de base complète de l'instance AppScan Enterprise. Cette zone prend en charge les URL pour les protocoles HTTP et HTTPS. Par exemple, **`http://myasehostname/ase/`**.
Authentication Type	Sélectionnez un type d'authentification : • **Windows Authentication** - Sélectionnez cette option pour utiliser Windows Authentication lorsque vous utilisez le service Web REST pour extraire les rapports des données de l'analyse AppScan Enterprise. • **Jazz™ Authentication** - Sélectionnez cette option pour utiliser Jazz Authentication lorsque vous utilisez le service Web REST pour récupérer les données de rapport d'analyse pour AppScan Enterprise.
Username	Entrez le nom d'utilisateur requis pour extraire les résultats de l'analyse requis depuis AppScan Enterprise.
Password	Entrez le mot de passe requis pour extraire les résultats de l'analyse 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 d'un modèle regex d'expression régulière. Par défaut, la zone **Report Name Pattern** contient **`.*`** comme modèle d'expression régulière. Le modèle .* importe tous les rapports d'analyse qui sont publiés dans QRadar. L'utilisation de ce paramètre nécessite la connaissance des expressions régulières (regex). Pour plus d'informations, consultez le site Web suivant : *http://download.oracle.com/javase/tutorial/essential/regex//*.

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

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

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

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

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

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

Modification d'un scanner AppScan Enterprise

Pour modifier 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 modifier.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

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

Etape 7 Cliquez sur **Save**.

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

Suppression d'un scanner 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**.

4 GESTION DES SCANNERS IBM GUARDIUM

Les dispositifs IBM InfoSphere™ Guardium® sont capables d'exporter des informations sur la vulnérabilité de la base de données qui peuvent être essentielles pour protéger les données des clients.

Les processus de vérification d'IBM Guardium exportent les résultats des tests qui ont échoué aux tests du Common Vulnerability and Exposures (CVE) générés au moment du démarrage des tests d'évaluation de la sécurité sur le dispositif IBM Guardium. Les données de vulnérabilité d'IBM Guardium doivent être exportées vers un serveur distant ou un serveur de transfert au format Security Content Automation Protocol (SCAP). QRadar peut ensuite récupérer les résultats de l'analyse à partir du serveur distant qui stocke la vulnérabilité via SFTP.

Remarque : IBM Guardium exporte uniquement la vulnérabilité à partir des bases de données contenant les résultats des tests CVE qui ont échoué. Si aucun test CVE n'a échoué, IBM Guardium peut ne pas exporter de fichier à la fin de l'évaluation de la sécurité.

Pour plus d'informations sur la configuration des tests d'évaluation de la sécurité et sur la création d'un processus de vérification pour exporter les données de vulnérabilité au format SCAP, consultez votre documentation IBM InfoSphere Guardium.

Une fois que vous avez configuré votre dispositif IBM Guardium, vous êtes prêt à configurer QRadar pour importer les résultats à partir du serveur distant hébergeant les données de vulnérabilité. Vous devez ajouter un scanner IBM Guardium à QRadar et configurer le scanner pour récupérer des données à partir de votre serveur distant. Les vulnérabilités les plus récentes sont importées par QRadar lorsque vous créez un planning d'analyse. Les plannings d'analyse vous permettent de déterminer la fréquence à laquelle QRadar demande des données à partir du serveur distant qui héberge vos données de vulnérabilité IBM Guardium. Pour plus d'informations, voir **Gestion des plannings d'analyse**

Ajout d'un scanner IBM Guardium

Pour ajouter un scanner IBM Guardium 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 des paramètres suivants :

Tableau 4-1 Paramètres du scanner IBM Guardium SCAP

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 **IBM Guardium SCAP Scanner**.

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 4-2 Paramètres du scanner IBM Guardium SCAP

Paramètre	Description
Remote Hostname	Entrez le nom d'hôte ou l'adresse IP du serveur distant qui héberge vos fichiers SCAP XML.
Remote Port	Entrez le numéro du port du serveur distant afin de récupérer les fichiers du résultat d'analyse à l'aide de SFTP. Le numéro de port par défaut est 22.
Login Username	Entrez le nom d'utilisateur utilisé par QRadar pour authentifier la connexion SFTP.
Login Password	Si le paramètre Enable Key Authentication est désactivé, vous devez entrer le mot de passe correspondant au paramètre Login Username qu'utilise QRadar pour authentifier la connexion SFTP. Si le paramètre Enable Key Authentication est activé, le paramètre Login Password est ignoré.
Enable Key Authorization	Cochez cette case pour activer l'autorisation via une clé privée pour le serveur. Si la case est cochée, l'authentification est effectuée à l'aide d'une clé privée et le mot de passe est ignoré. Ce paramètre est désactivé par défaut.

Tableau 4-2 Paramètres du scanner IBM Guardium SCAP (suite)

Paramètre	Description
Private Key File	Entrez le chemin de répertoire qui mène vers le fichier contenant les informations sur la clé privée. Si vous utilisez une authentification basée sur une clé, QRadar utilise la clé privée pour authentifier la connexion. Ce paramètre est obligatoire si la case Enable Key Authentication est cochée. Si la case Enable Key Authentication est décochée, ce paramètre est ignoré.
Remote Directory	Entrez l'emplacement du répertoire des fichiers des résultats d'analyse sur le serveur distant qui héberge vos vulnérabilités IBM Guardium.
File Name Pattern	Entrez une expression régulière (regex) requise pour filtrer la liste des fichiers spécifiés dans le paramètre 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 nécessite la connaissance des expressions régulières (regex). Pour plus d'informations, consultez le site Web suivant : *http://download.oracle.com/javase/tutorial/essential/regex/*
Max Report Age (Days)	Entrez l'âge du fichier maximal à inclure au moment d'importer votre fichier de résultats XML lors d'une analyse planifiée. Les fichiers qui sont plus anciens que le nombre de jours indiqué et que l'horodatage sur le fichier de rapport sont exclus de l'importation planifiée.

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

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

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

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

Modification d'un scanner IBM Guardium

Pour modifier un scanner IBM Guardium :

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

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

Le panneau Data Sources s'affiche.

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

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez modifier.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Mettez à jour les paramètres, si nécessaire. Voir **Tableau 4-2**.

Etape 7 Cliquez sur **Save**.

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

Suppression d'un scanner IBM Guardium

Pour supprimer un scanner IBM Guardium 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 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

5 GESTION DES SCANNERS IBM SITEPROTECTOR

Le module de scanner IBM SiteProtector® QRadar accède aux données de vulnérabilité à partir des scanners IBM SiteProtector à l'aide de JDBC.

Le scanner IBM SiteProtector récupère des données à partir de la table RealSecureDB et demande les informations disponibles sur la vulnérabilité. La zone de comparaison permet à QRadar de récupérer uniquement les informations les plus récentes à partir de la table RealSecureDB et d'importer toutes les nouvelles vulnérabilités dans QRadar.

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

Ajout d'un scanner IBM SiteProtector

Vous pouvez ajouter plusieurs scanners IBM SiteProtector dans QRadar, chacun avec une configuration différente pour déterminer les plages du routage CIDR que ce scanner doit prendre en compte.

L'ajout de plusieurs configurations pour un scanner IBM SiteProtector unique vous permet de créer des scanners individuels pour collecter les données de résultat spécifiques à partir d'emplacements spécifiques. Après avoir ajouté et configuré le scanner IBM SiteProtector dans QRadar, vous pouvez créer un planning d'analyse pour déterminer la fréquence à laquelle QRadar interroge la base de données IBM SiteProtector.

Pour ajouter un scanner IBM SiteProtector 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 des paramètres suivants :

Tableau 5-1 Paramètres du scanner

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

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

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 5-2 Paramètres du scanner IBM SiteProtector

Paramètre	Description
Hostname	Entrez l'adresse IP ou le nom d'hôte d'IBM SiteProtector contenant les vulnérabilités que vous souhaitez ajouter à QRadar.
Port	Entrez le numéro de port utilisé par le serveur de base de données. Le numéro par défaut affiché est fonction du type de base de données sélectionné. La plage valide est comprise entre 0 et 65536. Le numéro de port par défaut pour MSDE est 1433. Le port de configuration JDBC doit correspondre au port d'écoute de la base de données. Les connexions TCP entrantes de la base de données doivent être activées pour communiquer avec QRadar. Le numéro de port par défaut pour toutes les options inclut : • **MSDE** - 1433 • **Postgres** - 5432 • **MySQL** - 3306 • **Oracle** - 1521 • **Sybase** - 1521
Username	Entrez le nom d'utilisateur requis pour accéder à IBM SiteProtector.
Password	Entrez le mot de passe requis pour accéder à IBM SiteProtector.

Tableau 5-2 Paramètres du scanner IBM SiteProtector (suite)

Paramètre	Description
Domain	Entrez le domaine requis, si nécessaire, pour vous connecter à votre base de données IBM SiteProtector. Si vous sélectionnez MSDE en tant que type de base de données et que la base de données est configurée pour Windows, vous devez définir un domaine Windows. Sinon, laissez cette zone vide. Le domaine peut comporter jusqu'à 255 caractères alphanumériques. Le domaine peut inclure les caractères spéciaux suivants : trait de soulignement (_), tiret demi-cadratin (-) et point (.).
Database Name	Entrez le nom de la base de données à laquelle vous souhaitez vous connecter. Le nom de la base de données par défaut est **RealSecureDB**.
Database Instance	Entrez l'instance de base de données pour votre base de données IBM SiteProtector. Si vous n'utilisez pas une instance de base de données, vous pouvez laisser cette zone vide. Si vous sélectionnez MSDE en tant que type de base de données et que vous avez plusieurs instances de serveur SQL sur un serveur, définissez l'instance à laquelle vous souhaitez vous connecter.
Use Named Pipe Communication	Cochez cette case pour utiliser des canaux de communication nommés lorsque vous communiquez avec la base de données IBM SiteProtector. Par défaut, cette case est désélectionnée. Lorsque vous utilisez une connexion dont le canal de communication est nommé, le nom d'utilisateur et le mot de passe doivent être ceux de l'authentification Windows appropriés et non ceux de la base de données. Lorsque vous sélectionnez cette case, vous utilisez le canal de communication nommé par défaut de votre système.
Use NTLMv2	Sélectionnez cette case à cocher si votre IBM SiteProtector utilise NTLMv2 en tant que protocole d'authentification. Par défaut, cette case est désélectionnée. La case **Use NTLMv2** force les connexions MSDE à utiliser le protocole NTLMv2 lorsqu'elles communiquent avec les serveurs SQL nécessitant l'authentification NTLMv2. Si la case **Use NTLMv2** est cochée, cela n'a aucun effet sur les connexions MSDE avec les serveurs SQL qui ne nécessitent pas d'authentification NTLMv2.

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

a Dans la zone de texte, entrez la plage du routage CIDR que ce scanner doit prendre en compte ou cliquez sur **Browse** pour sélectionner la plage du routage CIDR à partir de la liste des réseaux. Pour collecter toutes les vulnérabilités IBM SiteProtector disponibles, vous pouvez entrer 0.0.0.0/0 en tant qu'adresse CIDR.

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

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

Modification d'un scanner IBM SiteProtector

Pour modifier un scanner 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 Mettez à jour les paramètres, si nécessaire. Voir **Tableau 5-2**.

Etape 7 Cliquez sur **Save**.

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

Suppression d'un scanner IBM SiteProtector

Pour supprimer un scanner 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 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

6 SCANNER IBM TIVOLI ENDPOINT MANAGER

Le module de scanner Tivoli® Endpoint Manager accède aux données de vulnérabilité à partir d'IBM Tivoli Endpoint Manager à l'aide de l'interface de programme d'application SOAP installée avec l'application Web Reports.

L'application Web Reports de Tivoli Endpoint Manager est nécessaire pour récupérer les données de vulnérabilité de Tivoli Endpoint Manager pour QRadar. Nous vous recommandons de créer un utilisateur dans IBM Tivoli Endpoint Manager pour QRadar.

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

Ajout d'un scanner IBM Tivoli Endpoint Manager

Vous pouvez ajouter plusieurs scanners IBM Tivoli Endpoint Manager à QRadar, chacun avec une configuration différente pour déterminer les plages du routage CIDR à prendre en compte par le scanner.

L'ajout de plusieurs configurations pour un scanner IBM Tivoli Endpoint Manager unique vous permet de créer des scanners individuels pour la collecte de données relatives aux résultats spécifiques à partir d'emplacements spécifiques. Une fois que vous avez ajouté et configuré IBM Tivoli Endpoint Manager sous QRadar, vous pouvez créer un planning d'analyse afin de déterminer la fréquence à laquelle QRadar accède à IBM Tivoli Access Manager. Cela vous permet de programmer la fréquence à laquelle QRadar demande les données à partir d'IBM Tivoli Endpoint Manage à l'aide de l'interface de programme d'application du protocole SOAP.

Pour ajouter un scanner IBM Tivoli Endpoint Manager dans QRadar :

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

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

Le panneau Data Sources s'affiche.

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

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 6-1 Paramètres 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 **IBM Tivoli Endpoint Manager**.

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

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 6-2 Paramètres IP360

Paramètre	Description
Hostname	Entrez l'adresse IP ou le nom d'hôte d'IBM Tivoli Endpoint Manager contenant les vulnérabilités à ajouter à QRadar.
Port	Saisissez le numéro de port utilisé pour vous connecter à IBM Tivoli Endpoint Manager à l'aide de l'API SOAP. Par défaut, le port 80 est le numéro de port autorisant la communication avec IBM Tivoli Endpoint Manager. Si vous utilisez le protocole HTTPS, vous devez mettre cette zone à jour vers le numéro de port HTTPS de votre réseau. La plupart des configurations utilisent le port 443 pour les communications HTTPS.
Use HTTPS	Cochez cette case pour vous connecter à l'aide du protocole HTTPS. Si vous cochez cette case, le nom d'hôte ou l'adresse IP que vous spécifiez utilise le protocole HTTPS pour se connecter à votre IBM Tivoli Endpoint Manager. Si un certificat est requis pour se connecter à l'aide du protocole HTTPS, vous devez copier les certificats exigés par la console QRadar ou les hôtes gérés vers le répertoire suivant : `/opt/qradar/conf/trusted_certificates` ***Remarque :*** *QRadar prend en charge les certificats ayant les extensions suivantes :.crt, .cert ou.der. Tous les certificats requis doivent être copiés dans le répertoire des certificats de confiance avant d'enregistrer et de déployer vos modifications.*
Username	Entrez le nom d'utilisateur requis pour accéder à IBM Tivoli Endpoint Manager.
Password	Entrez le mot de passe requis pour accéder à IBM Tivoli Endpoint Manager.

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

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

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

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

Modification d'un scanner IBM Tivoli Endpoint Manager

Pour modifier un scanner 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 Mettez à jour les paramètres, si nécessaire. Voir **Tableau 6-2**.

Etape 7 Cliquez sur **Save**.

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

Suppression d'un scanner IBM Tivoli Endpoint Manager

Pour supprimer un scanner 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 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

7 GESTION DES SCANNERS NCIRCLE IP360

QRadar utilise SSH pour accéder au serveur distant (serveur d'exportation SSH) pour récupérer et interpréter les données analysées.

QRadar prend en charge les versions VnE Manager IP360 allant de la 6.5.2 à la 6.8.2.8.

Vous pouvez configurer un périphérique d'analyse nCircle IP360 pour exporter les résultats d'analyse vers un serveur distant. Ces résultats d'analyse sont exportés au format XML2 vers un serveur SSH. Pour intégrer avec succès un périphérique IP360 dans QRadar, ces fichiers au format XML2 doivent être lus à partir du serveur distant (via SSH). QRadar peut être configuré pour programmer une analyse ou pour interroger le serveur SSH à propos de mises à jour des résultats de l'analyse pour 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, voir **Exportation de rapports d'analyse nCircle**.

Les résultats de l'analyse contiennent des informations d'identification relatives à la configuration de l'analyse à partir de laquelle ils ont été produits. 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 au format XML2.

Ajout d'un scanner nCircle IP360

Pour ajouter un scanner nCircle IP360 :

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

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

Le panneau Data Sources s'affiche.

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

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 7-1 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 liste déroulante, sélectionnez **nCircle IP360 Scanner.**

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

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 7-2 Paramètres IP360

Paramètre	Description
SSH Server Host Name	Entrez l'adresse IP ou le nom d'hôte pour le serveur distant hébergeant les fichiers des résultats d'analyse. Nous recommandons un système d'exploitation UNIX avec SSH activé.
SSH Username	Entrez le nom d'utilisateur SSH du serveur distant.
SSH Password	Entrez le mot de passe du serveur distant correspondant au nom d'utilisateur SSH. Si vous sélectionnez la case **Enable Key Authentication**, vous n'aurez plus besoin d'un mot de passe.
SSH Port	Entrez le numéro de port utilisé pour se connecter au serveur distant.
Remote Directory	Entrez l'emplacement du répertoire des fichiers des résultats d'analyse.
File Max Age (days)	Entrez l'âge maximum du fichier à inclure lors de l'exécution de l'analyse programmée. Les fichiers qui sont plus anciens que la date précisée sont exclus du processus d'importation des données de résultat dans QRadar.
File Pattern	Entrez une expression régulière (regex), pour filtrer la liste des fichiers spécifiés dans la zone **Remote Directory**. Tous les fichiers correspondants sont inclus et traités. Par exemple, si vous voulez répertorier tous les fichiers xml2 se terminant par XML, utilisez l'entrée suivante : `XML2.*\.xml` L'utilisation de ce paramètre nécessite la connaissance des expressions régulières (regex). Pour plus d'informations, consultez le site Web suivant : *http://download.oracle.com/javase/tutorial/essential/regex/*

Tableau 7-2 Paramètres IP360 (suite)

Paramètre	Description
Enable Key Authorization	Cochez cette case pour activer l'autorisation via une clé pour le serveur. Si la case **Enable Key Authentication** est cochée, l'authentification SSH se fait via une clé privée. Vous pouvez ainsi vous passer du mot de passe. Ce paramètre est désactivé par défaut.
Private Key Path	Entrez le chemin d'accès de la clé privée. Le chemin d'accès de la clé privée est le chemin complet du répertoire sur votre système QRadar dans lequel est conservée la clé privée à utiliser pour l'authentification par clé SSH. Le chemin par défaut est /opt/qradar/conf/vis.ssh.key. Cependant ce fichier 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, le paramètre Private Key Path est ignoré.

Remarque : 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 du 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 différente. Pour plus d'informations, consultez la documentation du fournisseur de votre scanner.

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

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

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

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

Modification d'un scanner nCircle IP360

Pour modifier un scanner 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 Mettez à jour les paramètres, si nécessaire. Voir **Tableau 7-2**.

Etape 7 Cliquez sur **Save**.

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

Suppression d'un scanner nCircle IP360

Pour supprimer un scanner 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 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

Exportation de rapports d'analyse nCircle

Pour configurer votre périphérique nCircle afin d'exporter des rapports d'analyse :

Etape 1 Connectez-vous à l'interface utilisateur VNE Manager IP360.

Etape 2 Dans la barre de navigation à gauche, sélectionnez **Administer > System > VNE Manager > Automated Export**.

Le menu Automated Export s'affiche.

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

Etape 4 Configurez les paramètres d'exportation.

Pour plus d'informations sur la configuration des paramètres d'exportation, cliquez sur le lien Help. Pour être intégrée dans QRadar, l'exportation doit être configurée de façon à utiliser le format XML.

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

8 GESTION DES SCANNERS NESSUS

QRadar peut récupérer les rapports d'analyse de vulnérabilité à propos de vos ressources réseau en mettant à profit la relation entre le client et le serveur Nessus 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 des 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 d'effectuer une identification SSH, depuis QRadar vers votre client Nessus afin de vérifier les données d'identification de QRadar. Ceci permet de vous assurer que QRadar et le client Nessus communiquent avant de tenter de collecter les données d'analyse ou de démarrer une analyse opérationnelle.

Les options de collection de données suivantes sont disponibles pour Nessus :

- **Scheduled Live Scan** - Permet à QRadar de se connecter à 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 du client une fois l'analyse opérationnelle terminée.
- **Scheduled Results Import** - Permet à QRadar de se connecter à l'emplacement hébergeant vos rapports d'analyse Nessus. QRadar se connecte au référentiel via SSH et importe les fichiers de rapport d'analyse complet depuis le répertoire distant. QRadar prend en charge l'importation des rapports d'analyse Nessus ou des rapports d'analyse dans un format de sortie pris en charge par Nessus.
- **Scheduled Live Scan - XMLRPC API** - Permet à QRadar d'utiliser l'interface API XMLRPC pour démarrer une analyse préconfigurée. Pour démarrer une analyse opérationnelle à partir de QRadar, vous devez indiquer le nom de la règle pour les données de l'analyse opérationnelle à récupérer. Lors de l'exécution de l'analyse opérationnelle, QRadar met à jour le pourcentage effectué dans le statut 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 complet qui correspond au filtre de nom et d'âge des rapports.
- 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 Nessus selon un intervalle ponctuel ou répété. Pour en savoir plus sur la planification d'une analyse, voir **Planification d'une analyse**.

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

Ajout d'un scanner Nessus

Le module du scanner Nessus 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'une analyse opérationnelle planifiée Nessus**
- **Ajout d'une importation de résultats planifiée Nessus**
- **Ajout d'une analyse opérationnelle planifiée Nessus à l'aide de l'interface de programme d'application XMLPRC**
- **Ajout d'une importation de rapport complet Nessus à l'aide de l'interface programme d'application API XMLRPC**

Remarque : L'interface API Nessus XMLRPC n'est disponible que sur les serveurs et les clients Nessus qui utilisent le logiciel v4.2 et plus.

Ajout d'une analyse opérationnelle planifiée Nessus

Une analyse opérationnelle peut être démarrée sur le serveur Nessus et permet d'importer les données relatives aux résultats à partir d'un répertoire temporaire contenant les données de rapport d'analyse opérationnelle.

A la fin de l'analyse, QRadar télécharge les données d'analyse à partir du répertoire temporaire et met à jour les informations relatives à la vulnérabilité de vos actifs.

Pour ajouter une analyse opérationnelle Nessus dans QRadar :

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

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

Le panneau Data Sources s'affiche.

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

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 8-1 Paramètres du scanner

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

La liste des paramètres 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 des paramètres suivants :

Tableau 8-2 Paramètres d'analyse opérationnelle planifiée pour Nessus

Paramètre	Description
Server Hostname	Entrez l'adresse IP ou le nom d'hôte du serveur Nessus comme indiqué par le client Nessus. Si le processus serveur et le client sont situés sur le même hôte, vous pouvez utiliser localhost comme nom d'hôte du serveur.
Server Port	Entrez le numéro de port pour le serveur Nessus. Le numéro de port par défaut est 1241.
Server Username	Entrez le nom d'utilisateur utilisé par le client Nessus pour l'authentification sur le serveur Nessus.
Server Password	Entrez le mot de passe Nessus correspondant au nom d'utilisateur. ***Remarque :*** *Votre mot de passe de serveur Nessus ne doit pas contenir le caractère !. Ce caractère peut provoquer des échecs d'authentification via SSH.*
Client Temp Dir	Entrez le chemin d'accès au répertoire du client Nessus pouvant être utilisé par QRadar 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.
Nessus Executable	Entrez le chemin d'accès au répertoire du fichier exécutable Nessus sur le serveur qui héberge le client Nessus. Par défaut, le chemin d'accès au répertoire pour le fichier exécutable est **/usr/bin/nessus**.

Tableau 8-2 Paramètres d'analyse opérationnelle planifiée pour Nessus (suite)

Paramètre	Description
Nessus Configuration File	Entrez le chemin d'accès au répertoire du fichier de configuration Nessus sur le client Nessus.
Client Hostname	Entrez le nom d'hôte ou l'adresse IP du système qui héberge le client Nessus.
Client SSH Port	Entrez le numéro de port SSH du serveur Nessus pouvant être utilisé afin de récupérer les fichiers de résultat d'analyse. Le numéro de port par défaut est 22.
Client Username	Entrez le nom d'utilisateur utilisé par QRadar pour authentifier la connexion SSH.
Client Password	Entrez le mot de passe correspondant à la zone **Client Username**. Cette zone est obligatoire si la case **Enable Key Authentication** est décochée. Si le paramètre Enable Key Authentication est activé, le paramètre Login Password est ignoré. ***Remarque :*** *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 du scanner échoue. Assurez-vous que la ligne suivante s'affiche dans votre fichier sshd_config, qui est généralement disponible dans le répertoire /etc/ssh du serveur SSH :* `PasswordAuthentication yes.` *Si le serveur de votre scanner n'utilise pas OpenSSH, la configuration peut être différente. Pour plus d'informations, consultez la documentation du fournisseur de votre scanner.*
Enable Key Authentication	Sélectionnez cette case pour activer l'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 plages du routage CIDR que ce scanner doit prendre en compte :

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

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

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

Etape 11 Après que les changements ont été déployés, vous devez créer un planning d'analyse pour l'analyse opérationnelle.

Les rapports d'analyse peuvent être créés en tant qu'événement unique ou en tant qu'importation planifiée récurrente. Pour en savoir plus sur la planification d'une analyse, voir **Planification d'une analyse**.

Ajout d'une importation de résultats planifiée Nessus

Une importation des résultats planifiée récupère les 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 via SSH et importe les fichiers de rapports d'analyse complets depuis le répertoire distant en utilisant une expression régulière ou un âge de rapports maximum pour filtrer vos rapports d'analyse. QRadar prend en charge l'importation de rapports d'analyse Nessus (.Nessus) ou des rapports d'analyse exportés dans un format de sortie pris en charge par Nessus, tel que XML.

Pour ajouter une importation de résultats planifiée 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 des paramètres suivants :

Tableau 8-3 Paramètres du scanner

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

La liste des paramètres 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 des paramètres suivants :

Tableau 8-4 Paramètres de l'importation des résultats planifiés Nessus

Paramètre	Description
Remote Results Hostname	Entrez l'adresse IP ou le nom d'hôte du client Nessus ou du serveur qui héberge vos fichiers de résultat d'analyse XML ou Nessus.

Tableau 8-4 Paramètres de l'importation des résultats planifiés Nessus (suite)

Paramètre	Description
Remote Results SSH Port	Entrez le numéro de port SSH du serveur Nessus pouvant être utilisé afin de récupérer les fichiers de 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 avec le serveur Nessus.
SSH Password	Entrez le mot de passe correspondant au nom d'utilisateur SSH. ***Remarque :*** *Votre mot de passe de serveur Nessus ne doit pas contenir le caractère !. Ce caractère peut provoquer des échecs d'authentification via SSH.*
Enable Key Authentication	Sélectionnez cette case pour activer l'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 complet au répertoire contenant les fichiers du rapport d'analyse Nessus sur le client Nessus. Le chemin d'accès au répertoire utilise **./** comme valeur par défaut.
Remote Results File Pattern	Entrez un 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 fichiers 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 mettre à jour l'expression regex pour le modèle de fichier en conséquence. ***Remarque :*** *Si vous mettez à jour l'expression regex dans la zone* ***Remote Results File Pattern,*** *vous devez déployer le changement pour mettre à jour la configuration de votre scanner.*
Results File Max Age (Days)	Entrez l'âge maximal du fichier à inclure au moment d'importer les fichiers de résultats d'analyse Nessus lors d'une analyse planifiée. Par défaut, l'âge maximal du fichier est de 7 jours. Les fichiers dont l'âge est supérieur au nombre de jours indiqué et à l'horodatage sont exclus du processus d'importation des résultats.

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

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

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

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

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

Les rapports d'analyse peuvent être créés en tant qu'événement unique ou en tant qu'importation planifiée récurrente. Pour en savoir plus sur la planification d'une analyse, voir **Planification d'une analyse**

Ajout d'une analyse opérationnelle planifiée Nessus à l'aide de l'interface de programme d'application XMLPRC

L'interface API XMLRPC 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 l'analyse et le nom de la règle pour les 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 Scan Scheduling pour visualiser le pourcentage d'avancement de l'analyse opérationnelle. A la fin de l'analyse opérationnelle, QRadar utilise l'interface API XMLRPC pour récupérer les données d'analyse et mettre à jour les informations de vulnérabilité de vos actifs.

Remarque : L'interface API Nessus XMLRPC n'est disponible que sur les serveurs et les clients Nessus qui utilisent le logiciel v4.2 et plus.

Pour ajouter une analyse opérationnelle de l'interface API Nessus XMLRPC 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 des paramètres suivants :

Tableau 8-5 Paramètres du scanner

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

La liste des paramètres 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 des paramètres suivants :

Tableau 8-6 Paramètres de l'interface API XMLRPC pour les importations opérationnelles planifiées

Paramètre	Description
Hostname	Entrez l'adresse IP ou le nom d'hôte du serveur Nessus.
Port	Entrez le numéro de port afin que QRadar puisse accéder au serveur Nessus via l'interface API XMLRPC. Le numéro de port par défaut est 8834.
Username	Entrez le nom d'utilisateur requis pour se connecter au serveur Nessus.
Password	Entrez le mot de passe correspondant au nom d'utilisateur.
Scan Name	Facultatif. Entrez le nom de l'analyse que vous souhaitez afficher au moment de l'exécution de l'analyse opérationnelle sur le serveur Nessus. Si cette zone est vide, l'interface API tente de démarrer une analyse opérationnelle pour “QRadar Scan”. ***Remarque :*** *QRadar ne prend pas en charge l'utilisation du signe perluète (&) dans cette zone.*
Policy Name	Entrez le nom de la règle sur votre serveur Nessus pour démarrer une analyse opérationnelle. La règle que vous définissez doit exister sur le serveur Nessus lorsque QRadar tente de lancer l'analyse. Si la règle n'existe pas, un message d'erreur s'affiche dans le status lorsque QRadar tente de démarrer l'analyse opérationnelle. Dans la plupart des cas, le nom de la règle est adapté à votre serveur Nessus, mais plusieurs règles par défaut sont incluses dans Nessus. Par exemple, • Analyse réseau externe • Analyse réseau interne • Tests d'application Web • Préparation aux audits PCI DSS Pour en savoir plus sur les règles, consultez la documentation de votre fournisseur Nessus.

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

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

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

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

Etape 11 Après que les changements ont été déployés, vous devez créer un planning d'analyse pour votre analyse opérationnelle.

Les rapports d'analyse peuvent être créés en tant qu'événement unique ou en tant qu'importation planifiée récurrente. Pour en savoir plus sur la planification d'une analyse, voir **Planification d'une analyse**.

Ajout d'une importation de rapport complet Nessus à l'aide de l'interface programme d'application API XMLRPC

Une importation des résultats planifiée à l'aide de l'interface API XMLRPC 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 à partir des rapports complets qui correspondent aux filtres de nom d'âge maximal des rapports.

Remarque : L'interface API Nessus XMLRPC n'est disponible que sur les serveurs et les clients Nessus qui utilisent le logiciel v4.2 et plus.

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 des paramètres suivants :

Tableau 8-7 Paramètres du scanner

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

La liste des paramètres 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 des paramètres suivants :

Tableau 8-8 Paramètres d'interface API XMLRPC pour les importations planifiées de rapports complet

Paramètre	Description
Hostname	Entrez l'adresse IP ou le nom d'hôte du client Nessus ou du serveur qui héberge vos fichiers de résultat d'analyse XML ou Nessus.
Port	Entrez le numéro de port afin que QRadar puisse accéder au serveur Nessus via l'interface API XMLRPC. Le numéro de port par défaut est 8834.
Username	Entrez le nom d'utilisateur requis pour se connecter au serveur Nessus.
Password	Entrez le mot de passe correspondant au nom d'utilisateur.
Report Name Filter	Entrez le modèle de fichier à l'aide d'une expression régulière (regex), pour les fichiers de résultats d'analyse que vous tentez d'importer. Par défaut, le modèle de fichier suivant est inclus afin de collecter tous les rapports d'analyse complets disponibles : .*. ***Remarque :*** *Si vous mettez à jour l'expression regex dans la zone* ***Report Name Filter,*** *vous devez déployer les modifications pour mettre à jour la configuration de votre scanner.*
Results File Max Age (Days)	Entrez l'âge maximal du fichier à inclure au moment d'importer les fichiers de résultats d'analyse Nessus lors d'une analyse planifiée. Par défaut, l'âge maximal du fichier est de 7 jours. Les fichiers dont l'âge est supérieur au nombre de jours indiqué et à l'horodatage sont exclus du processus d'importation des résultats.

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

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

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

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

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

Les rapports d'analyse peuvent être créés en tant qu'événement unique ou en tant qu'importation planifiée récurrente. Pour en savoir plus sur la planification d'une analyse, voir **Planification d'une analyse**

Modification d'un scanner Nessus

Pour modifier une configuration de 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 Mettez à jour les paramètres, si nécessaire.

- Pour connaître les configurations de l'analyse opérationnelle planifiée, voir **Tableau 8-2**.
- Pour connaître les configurations de l'importation de résultats planifiée, voir **Tableau 8-4**.
- Pour connaître les configurations de l'interface API XMLRPC d'analyse opérationnelle planifiée, voir **Tableau 8-6**.
- Pour connaître les configurations de l'interface API XMLRPC d'importation de rapport complet, voir **Tableau 8-8**.

Etape 7 Cliquez sur **Save**.

Etape 8 Dans 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 sur **OK**.

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

9 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 distantes Nmap et télécharger les résultats de l'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 de lancer une analyse à l'aide du fichier binaire Nmap. QRadar surveille l'état du processus d'analyse opérationnelle 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 requièrent Nmap pour être exécutés en tant que root. Par conséquent, QRadar doit avoir accès en tant que root ou vous devez désélectionner la case **OS Detection**. Pour exécuter des analyses Nmap avec le paramètre **OS Detection** activé, vous devez fournir à QRadar un accès root ou configurer le fichier binaire Nmap avec setuid root. Pour obtenir de l'aide, contactez votre administrateur Nmap.
- **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 sur le 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 <fichier>`**.

  Où **`<fichier>`** représente le chemin d'accès permettant de créer et de stocker les résultats d'analyses XML sur votre scanner Nmap.

Une fois que vous avez ajouté et configuré une analyse opérationnelle distante ou une importation de résultats distante dans QRadar, vous pouvez programmer la fréquence à laquelle QRadar importe les données de vulnérabilité. Pour plus d'informations, voir **Gestion des plannings d'analyse**.

Ajout d'une analyse opérationnelle distante Nmap

L'ajout d'une analyse opérationnelle distante permet à QRadar de lancer une analyse Nmap, d'attendre qu'elle se termine, puis d'importer les résultats.

Après avoir ajouté une analyse opérationnelle, vous devez affecter un planning d'analyse à QRadar. Le planning d'analyse détermine la fréquence à laquelle QRadar lance des analyses opérationnelles sur votre scanner Nmap et récupère des données de vulnérabilité pour vos actifs.

Pour ajouter une analyse opérationnelle distante Nmap :

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

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

Le panneau Data Sources s'affiche.

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

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 9-1 Paramètres du scanner

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

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

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

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 9-2 Paramètres d'analyse opérationnelle 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 exécute SSH.
Server Username	Entrez le nom d'utilisateur requis pour accéder au système distant hébergeant le client Nmap à l'aide de SSH.

Tableau 9-2 Paramètres d'analyse opérationnelle Nmap (suite)

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

Tableau 9-2 Paramètres d'analyse opérationnelle Nmap (suite)

Paramètre	Description
Max RTT Timeout	Sélectionnez le délai maximal d'aller-retour (RTT) dans la zone de liste. Le délai d'attente détermine si une analyse doit être arrêtée ou réexécutée en raison du temps d'attente entre le scanner et la cible d'analyse. La valeur par défaut est de 300 millisecondes (ms). ***Remarque :*** *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 de temps d'aller-retour.*

Remarque : 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 du 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 différente. Pour plus d'informations, consultez la documentation du fournisseur de votre scanner.

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

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

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

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

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

Ajout d'une analyse d'importation distante des résultats Nmap

L'ajout d'un scanner d'importation distante de résultat Nmap vous permet de générer et de stocker des analyses sur votre scanner Nmap.

Les analyses doivent être générées au format XML à l'aide de la commande -oX <fichier> dans votre scanner Nmap. Après avoir ajouté et configuré votre scanner Nmap, vous devez affecter un planning d'analyse pour indiquer la fréquence à laquelle vous souhaitez que QRadar importe des analyses Nmap.

Pour ajouter une importation distante de résultats Nmap :

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

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

Le panneau Data Sources s'affiche.

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

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 9-3 Paramètres du scanner

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

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

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

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 9-4 Paramètres d'importation distante des résultats 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 exécute SSH.
Server Username	Entrez le nom d'utilisateur requis pour accéder au système distant hébergeant le client Nmap.
Enable Key Authentication	Sélectionnez cette case pour permettre à QRadar d'utiliser une authentification par clé publique ou privée. Lorsque vous sélectionnez cette case, spécifiez le chemin de répertoire de votre fichier de clés dans QRadar à l'aide de la zone **Private Key File**. Par défaut, la case est décochée.
Login Password	Entrez le mot de passe associé au nom d'utilisateur dans la zone **Server Username**.

Tableau 9-4 Paramètres d'importation distante des résultats Nmap (suite)

Paramètre	Description
Private Key File	Entrez le chemin d'accès au fichier contenant les informations sur la clé privée. Cette zone s'affiche uniquement si la case **Enable Key Authentication** est sélectionnée. Si vous utilisez une authentification par clé basée sur SSH, QRadar utilise la clé privée pour authentifier la connexion SSH. Le répertoire 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 entrer un autre nom de fichier. Ce paramètre est obligatoire si la case **Enable Key Authentication** est sélectionnée, sinon il est ignoré.
Remote Folder	Entrez le chemin d'accès au scanner Nmap contenant des données de vulnérabilité XML.
Remote File Pattern	Entrez un modèle d'expression régulière (regex) pour déterminer les fichiers de résultats Nmap XML à inclure dans le rapport d'analyse. Tous les noms de fichier correspondant au modèle regex sont inclus lors de l'importation du rapport d'analyse de vulnérabilité. Vous devez utiliser un modèle regex valide dans la zone. Par exemple, le modèle suivant importe tous les fichiers XML situés dans le dossier distant : `.*\.xml` ***Remarque :*** *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 précédemment traités selon un planning.*

Remarque : 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 du 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 différente. Pour plus d'informations, consultez la documentation du fournisseur de votre scanner.

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

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

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

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

Vous pouvez maintenant ajouter un planning d'analyse pour déterminer la fréquence à laquelle vous souhaitez que QRadar importe les rapports d'analyse XML depuis votre scanner NMap. Pour en savoir plus sur la planification d'une analyse, voir **Gestion des plannings d'analyse**

Modification d'un scanner Nmap

Pour modifier la configuration d'un scanner Nmap 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 Mettez à jour les paramètres, si nécessaire.

- Pour les configurations d'analyse opérationnelle Nmap, voir **Tableau 9-2**.
- Pour les configurations d'importation distante de résultats Nmap, voir **Tableau 9-4**.

Etape 7 Cliquez sur **Save**.

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

Suppression d'un scanner Nmap

Pour supprimer un scanner Nmap 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 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

10 GESTION DES SCANNERS QUALYS

IBM Security QRadar récupère les informations de vulnérabilité des scanners Qualys de deux manières différentes ; via l'interface API Qualys et en téléchargeant les rapports d'analyse générés par les dispositifs QualysGuard.

Les informations d'actifs de vulnérabilité QualysGuard sont prises en charge sur les dispositifs QualysGuard via l'utilisation du logiciel aux versions 4.7 à 7.2.

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

- **Qualys Detection Scanner** - Le module du scanner de détection Qualys accède aux données de vulnérabilité à l'aide de l'interface API Qualys Host List Detection du dispositif QualysGuard. Le scanner de détection Qualys vous permet de récupérer des résultats à partir de plusieurs rapports d'analyse afin de collecter des données de vulnérabilité. Le module du scanner de détection Qualys pour QRadar requiert que vous indiquiez un utilisateur Qualys pouvant télécharger la base Qualys KnowledgeBase.

  Pour plus d'informations sur le scanner de détection Qualys, voir **Configuration d'un scanner de détection Qualys**.

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

  Pour plus d'informations sur le scanner de détection Qualys, voir **Configuration d'un scanner Qualys**

Après avoir configuré le module du scanner de détection Qualys ou du scanner Qualys dans QRadar, vous pouvez planifier une analyse dans QRadar afin de collecter les vulnérabilités à l'aide de l'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 dispositifs de vulnérabilité externes, tels que Qualys Vulnerability Manager. Pour plus d'informations, voir **Gestion des plannings d'analyse**

Configuration d'un scanner de détection Qualys

Le scanner de détection Qualys utilise l'interface de programme d'application QualysGuard Host Detection List pour analyser plusieurs rapports d'analyse afin de collecter les données de vulnérabilité des actifs.

Les données renvoyées contiennent la vulnérabilité comme numéro d'identification, que QRadar compare par rapport à la dernière version de la base Qualys Vulnerability Knowledge Base. Le scanner de détection Qualys ne prend pas en charge les analyses opérationnelles mais autorise le scanner de détection Qualys à récupérer les informations de vulnérabilité regroupées à partir de plusieurs rapports d'analyse. QRadar prend en charge les paramètres de recherche essentiels, tels que les zones **Operating System Filter** et **Asset Group Name**.

Le scanner de détection Qualys fournit également une option permettant de configurer la fréquence de récupération et de mise en cache de la base Qualys Vulnerability Knowledge Base par QRadar. Il s'agit de la zone **Qualys Vulnerability Retention Period**. Pour forcer QRadar à mettre à jour la base Qualys Vulnerability Knowledge Base pour chaque analyse planifiée, le scanner de détection Qualys 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 la base Qualys KnowledgeBase. Pour plus d'informations, voir votre documentation Qualys.

Ajout d'un scanner de détection Qualys

Pour ajouter un scanner de détection Qualys 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 des paramètres suivants :

Tableau 10-1 Paramètres du scanner de détection Qualys

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 **Qualys Detection Scanner**.

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 10-2 Paramètres du scanner de détection 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. Lorsque vous indiquez le nom de domaine complet, vous devez entrer le nom d'hôte et non l'adresse URL. Par exemple : • Entrez **`qualysapi.qualys.com`** pour un serveur QualysGuard se trouvant aux États-Unis. • Entrez **`qualysapi.qualys.eu`** pour un serveur hôte du serveur QualysGuard se trouvant en Europe. • Entrez **`qualysapi.<`**`console_gestion`**`>`** si vous utilisez l'infrastructure d'analyse complète comprenant une console de gestion interne, où `<console_gestion>` est le nom d'hôte de votre dispositif de gestion interne**`.`**
Qualys Username	Entrez le nom d'utilisateur nécessaire pour des demandes d'analyse. Il s'agit du même nom d'utilisateur utilisé pour se connecter au serveur Qualys. ***Remarque :*** *L'utilisateur que vous indiquez doit disposer d'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.
Operating System Filter	Entrez l'expression régulière (regex) requise pour filtrer les données renvoyées par le système d'exploitation. La zone **Operating System Filter** contient **.*** comme expression régulière par défaut et correspond à tous les systèmes d'exploitation. Si vous entrez une expression régulière non valide dans la zone **Operating System Filter**, l'analyse échoue lorsque QRadar initialise le scanner. Pour afficher le message d'erreur à partir d'un échec d'analyse, déplacez votre souris sur le texte dans la colonne **Status**.

Tableau 10-2 Paramètres du scanner de détection Qualys (suite)

Paramètre	Description
Asset Group Names	Entrez une liste séparée par des virgules, sans espace pour analyser les adresses IP en fonction de leur nom de groupe d'actifs. Un groupe d'actifs 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 d'actifs intitulé Building1 peut contenir l'adresse IP 192.168.0.1. Un groupe d'actifs intitulé Webserver peut contenir 192.168.255.255. Dans QRadar, pour récupérer les informations de vulnérabilité de ces deux actifs, entrez **Building1,Webserver** sans espace dans la zone **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 portant sur la dernière analyse de l'hôte. Les analyses d'hôte qui sont plus anciennes que le nombre de jours indiqué sont exclues des résultats renvoyés par Qualys.
Qualys Vulnerability Retention Period (days)	Entrez le nombre de jours pendant lesquels vous souhaitez enregistrer localement la base Qualys Vulnerability Knowledge Base dans QRadar. La valeur par défaut est de 7 jours. Si une analyse est planifiée et que la durée de conservation a expiré, QRadar télécharge une mise de jour de la base Qualys Vulnerability Knowledge Base.
Force Qualys Vulnerability Update	Sélectionnez cette case à cocher pour obliger QRadar à récupérer et à mettre en cache la version la plus récente de la base Qualys Vulnerability Knowledge Base. Si cette case est sélectionnée, la durée de conservation est définie sur zéro et chaque analyse planifiée récupère la base Qualys Vulnerability Knowledge Base.
Use Proxy	Sélectionnez cette case à cocher si votre scanner requiert 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 requiert un proxy.
Proxy Port	Entrez le numéro de port de votre serveur proxy si votre scanner requiert un proxy.
Proxy Username	Entrez le nom d'utilisateur de votre serveur proxy si votre scanner requiert un proxy.
Proxy Password	Entrez le mot de passe de votre serveur proxy si votre scanner requiert un proxy.

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

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

b. Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

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

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

Modification d'un scanner de détection Qualys

Pour modifier une configuration de scanner de détection Qualys 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 nom du scanner que vous souhaitez modifier.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

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

Etape 7 Cliquez sur **Save**.

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

- Si vous reconfigurez le scanner de détection Qualys sans avoir mis à jour les données d'identification du proxy du scanner de détection Qualys, cliquez sur **Deploy Changes** dans le menu de navigation de l'onglet **Admin**.
- Si vous reconfigurez le scanner de détection Qualys et que vous mettez à jour les données d'identification dans la zone **Proxy Username** ou **Proxy Password**, sélectionnez **Advanced > Deploy Full Configuration** à partir du menu de navigation de l'onglet **Admin**.

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

Les modifications apportées à votre scanner Qualys sont terminées.

Suppression d'un scanner de détection Qualys

Pour supprimer un scanner Qualys 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 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

Le scanner de détection Qualys est supprimé de la liste des scanners.

Configuration d'un scanner Qualys

Le module de scanner Qualys télécharge et analyse les rapports d'analyse à partir du dispositif Qualys.

Si vous sélectionnez le scanner Qualys, QRadar doit accéder au serveur Web distant via une connexion HTTPS pour récupérer les rapports d'analyse. Le module du scanner Qualys prend en charge trois méthodes de collecte de données d'analyse depuis Qualys.

Les options d'analyse pour un scanner Qualys comprennent :

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

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

Ajout d'un rapport d'analyse opérationnelle planifiée Qualys

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

Pour ajouter une analyse opérationnelle Qualys 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 des paramètres suivants :

Tableau 10-3 Paramètres du scanner Qualys

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 **Qualys Scanner**.

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

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

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 10-4 Paramètres d'analyse opérationnelle 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. Lorsque vous indiquez le nom de domaine complet, vous devez entrer le nom d'hôte et non l'adresse URL. Par exemple : • Entrez **`qualysapi.qualys.com`** pour un serveur QualysGuard se trouvant aux États-Unis. • Entrez **`qualysapi.qualys.eu`** pour un serveur QualysGuard se trouvant en Europe. • Entrez **`qualysapi.<`**`console_gestion`**`>`** si vous utilisez l'infrastructure d'analyse complète comprenant une console de gestion interne, où <`console_gestion`> est le nom d'hôte de votre dispositif de gestion interne**`.`**
Qualys Username	Entrez le nom d'utilisateur nécessaire pour des demandes d'analyse. Il s'agit du même nom d'utilisateur utilisé pour se connecter au serveur Qualys.
Qualys Password	Entrez le mot de passe correspondant au nom d'utilisateur Qualys.
Use Proxy	Sélectionnez cette case à cocher si QRadar requiert 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 IP de votre serveur proxy.

Tableau 10-4 Paramètres d'analyse opérationnelle de Qualys (suite)

Paramètre	Description
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 à la zone **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 réseau. ***Remarque :*** *Si vous utilisez un dispositif d'analyse public, vous devez effacer le nom dans la zone* ***Scanner Name****.*
Option Profile(s)	Entrez le nom du profil d'option pour déterminer le rapport d'analyse existant démarrant en tant qu'analyse opérationnelle sur le scanner Qualys. QRadar récupère les données complètes de l'analyse opérationnelle après que celle-ci soit terminée. ***Remarque :*** *Les analyses opérationnelles prennent en charge un nom de profil d'option par configuration de scanner.*

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

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

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

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

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

Ajout d'une importation planifiée de rapport de données d'actifs Qualys

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

Pour ajouter une importation de rapport de données d'actifs 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 des paramètres suivants :

Tableau 10-5 Paramètres du scanner Qualys

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 **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'actifs Qualys s'affichent.

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 10-6 Paramètres d'importation des données d'actifs 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. Lorsque vous indiquez le nom de domaine complet, vous devez entrer le nom d'hôte et non l'adresse URL. Par exemple : • Entrez **`qualysapi.qualys.com`** pour un nom d'hôte de serveur QualysGuard se trouvant aux États-Unis. • Entrez **`qualysapi.qualys.eu`** pour un nom d'hôte de serveur QualysGuard se trouvant en Europe. • Entrez **`qualysapi.<management_console>`** si vous utilisez l'infrastructure d'analyse complète comprenant une console de gestion interne, où <management_console> **`est le nom d'hôte de votre dispositif de gestion interne.`**
Qualys Username	Entrez le nom d'utilisateur nécessaire pour des demandes d'analyse. Il s'agit du même nom d'utilisateur utilisé pour se connecter au serveur Qualys.
Qualys Password	Entrez le mot de passe correspondant au nom d'utilisateur Qualys.

Tableau 10-6 Paramètres d'importation des données d'actifs Qualys (suite)

Paramètre	Description
Use Proxy	Sélectionnez cette case à cocher si QRadar requiert 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 IP 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 à la zone **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 la zone **Import File**.
Report Template Title	Entrez un titre de modèle de rapport pour remplacer le titre par défaut lors de la récupération des rapports de données d'actifs.
Max Report Age (Days)	Entrez l'âge maximal du fichier à inclure lors de l'importation des données d'actifs Qualys durant une analyse planifiée. Par défaut, l'âge maximal du fichier est de 7 jours. Les fichiers qui sont plus anciens que le nombre de jours indiqué et que l'horodatage sur le fichier de rapport sont exclus de l'importation planifiée.
Import File (Optional)	Facultatif. Entrez un chemin de répertoire pour télécharger et importer un rapport d'actifs unique à partir de Qualys sur votre console QRadar ou sur votre hôte géré. Par exemple, pour télécharger un rapport d'actifs appelé QRadar_scan.xml à partir d'un répertoire de journaux sur votre hôte géré, entrez la valeur suivante : **`/qualys_logs/QRadar_scan.xml`** Si vous indiquez l'emplacement d'un fichier d'importation, QRadar télécharge les contenus du rapport d'actifs depuis Qualys vers un répertoire local. Une fois le téléchargement du rapport d'actifs sur votre console terminé, QRadar importe les informations d'actif en utilisant le fichier local. Si la zone **Import File** ne contient aucune valeur ou si le fichier ou le répertoire est introuvable, le scanner Qualys tente de récupérer le dernier rapport d'actifs à l'aide de l'interface API Qualys en fonction des informations se trouvant dans la zone **Report Template Title**.

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

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

b. Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

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

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

Ajout d'une importation planifiée de rapport d'analyse Qualys

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

Pour ajouter une importation de données de rapport d'analyse Qualys 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 des paramètres suivants :

Tableau 10-7 Paramètres du scanner Qualys

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 **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 terminées Qualys s'affichent.

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 10-8 Paramètres de l'importation d'analyse planifiée 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. Lorsque vous indiquez le nom de domaine complet, vous devez entrer le nom d'hôte et non l'adresse URL.

Tableau 10-8 Paramètres de l'importation d'analyse planifiée Qualys (suite) (suite)

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

Tableau 10-8 Paramètres de l'importation d'analyse planifiée Qualys (suite) (suite)

Paramètre	Description
Scan Report Name Pattern	Entrez un masque de fichiers, en utilisant une expression régulière (regex), 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 nombre de jours indiqué et que l'horodatage sur le fichier de rapport sont exclus de l'importation planifiée.
Import File (Optional)	Facultatif. Entrez un chemin de répertoire pour télécharger et importer un rapport d'analyse unique à partir de Qualys sur votre console QRadar ou sur votre hôte géré. Par exemple, pour télécharger un rapport d'analyse appelé QRadar_scan.xml à partir d'un répertoire de journaux sur votre hôte géré, entrez la valeur suivante : **`/qualys_logs/QRadar_scan.xml`** Si vous indiquez l'emplacement d'un fichier d'importation, QRadar télécharge les contenus du rapport d'analyse d'actif de Qualys vers un répertoire local. Une fois le téléchargement du rapport d'analyse d'actif terminé, QRadar importe les informations liées à l'actif à l'aide du fichier local. Si la zone **Import File** ne contient aucune valeur ou si le fichier ou le répertoire est introuvable, le scanner Qualys tente de récupérer le dernier rapport de données d'actifs en utilisant l'interface API Qualys en fonction des informations se trouvant dans la zone **Report Template Title**.

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

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

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

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

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

Modification d'un scanner Qualys

Pour modifier une configuration de scanner Qualys 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 Mettez à jour les paramètres, si nécessaire.

- Pour les paramètres d'analyses opérationnelles Qualys, voir **Tableau 10-4**.
- Pour les paramètres d'importation des données de rapports d'actifs Qualys, voir **Tableau 10-6**.
- Pour les paramètres d'importation planifiée rapport d'analyse Qualys, voir **Tableau 10-8**.

Etape 7 Cliquez sur **Save**.

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

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

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

Les modifications apportées à votre scanner Qualys sont terminées.

Suppression d'un scanner Qualys

Pour supprimer un scanner Qualys à partir de QRadar :

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**.

Le scanner Qualys est supprimé de la liste des scanners.

11 GESTION DES SCANNERS FOUNDSCAN

Le scanner Foundstone FoundScan IBM Security QRadar permet à QRadar d'interroger FoundScan Engine via l'OpenAPI de FoundScan pour obtenir des informations sur l'hôte et la vulnérabilité.

Le scanner FoundScan n'exécute pas directement les analyses mais rassemble les résultats de l'analyse actuelle tels qu'ils sont affichés dans l'application d'analyse. QRadar prend en charge les versions 5.0 à 6.5 Foundstone FoundScan.

Votre système FoundScan doit inclure une configuration adéquate permettant l'utilisation de QRadar et une analyse qui s'exécute régulièrement pour disposer de résultats mis à jour. Pour vous assurer que votre scanner FoundScan peut extraire des informations de l'analyse, vérifiez que votre système FoundScan répond aux exigences suivantes :

- Puisque l'interface API fournit l'accès à l'application FoundScan, assurez-vous que l'application FoundScan s'exécute en continu sur le serveur FoundScan. Cela signifie que l'application FoundScan doit être active sur votre bureau.
- L'analyse qui inclut la configuration nécessaire pour se connecter à QRadar doit être terminée et visible dans l'interface utilisateur FoundScan permettant 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 après exécution, QRadar doit extraire les résultats avant la suppression de l'analyse ou l'échec de l'analyse.
- Les privilèges utilisateurs appropriés doivent être configurés dans l'application FoundScan, permettant à QRadar de communiquer avec FoundScan.

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

Lors de l'utilisation de SSL (par défaut) pour se connecter à FoundScan, FoundScan Engine requiert que QRadar s'authentifie via des certificats côté client. Par défaut, FoundScan inclut l'autorité de certification et les certificats du client par défaut qui sont les mêmes pour toutes les installations. Le plug-in QRadar FoundScan inclut également les mêmes certificats à utiliser avec FoundScan 5.0. Si FoundScan Server utilise les certificats personnalisés ou utilise une version de

FoundScan autre que 5.0, vous devez importer les certificats et clés dans l'hôte QRadar. Pour plus d'informations, voir **Importation de certificats**.

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

Ajout d'un scanner FoundScan

Pour ajouter un scanner FoundScan 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 des paramètres suivants :

Tableau 11-1 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. ***Remarque :*** *Les certificats de votre scanner FoundScan doivent résider sur l'hôte géré sélectionné dans la zone de liste* ***Managed Host****.*
Type	Dans la zone de liste, cochez **FoundScan Scanner**.

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 11-2 Paramètres FoundScan

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

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

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

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

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

Modification d'un scanner FoundScan

Pour modifier la configuration d'un scanner FoundScan 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 Mettez à jour les paramètres, si nécessaire. Voir **Tableau 11-2**.

Etape 7 Cliquez sur **Save**.

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

Suppression d'un scanner FoundScan

Pour supprimer un scanner FoundScan 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 Dans l'onglet **Admin**, sélectionnez **Deploy Changes**.

Configuration des certificats

Le moteur FoundScan 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 Localisez la zone Authentication Scheme.

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

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

Pour obtenir des exemples de fichiers TrustedCA.pem et Portal.pem, voir **Exemple de fichier TrustedCA.pem** et **Exemple de fichier Portal.pem**.

Etape 6 Si vous utilisez un certificat personnalisé, générez un certificat à l'aide du gestionnaire de certificat FoundScan. Vérifiez que vous avez saisi l'adresse IP de l'hôte QRadar en tant que nom d'hôte pour le 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 de FoundScan autre que 5.0, vous devez importer les certificats et clés vers l'hôte géré QRadar que vous avez sélectionné dans **Tableau 11-1**.

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 dans QRadar :

Etape 1 Demandez les deux fichiers de certificat et la phrase passe à votre administrateur FoundScan.

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

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

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

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

Etape 4 Supprimez les certificats existants :

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

Etape 5 Entrez la commande suivante :

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

Où :

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

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

La sortie peut ressembler à ce qui suit :

```
Le certificat a été ajouté au fichier de clés
Utilisation de fichier de clés :
/opt/qradar/conf/foundscan.keystore
Un certificat, aucune chaîne.
Clé et certificat stockés.
Alias: Portal.pem Mot de passe : foundscan
Contenu de Trust Store :
Type de fichier de clés : jks
Fournisseur de fichier de clés : SUN
Votre fichier de clés contient 1 entrée
Nom d'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 sept à 20:29:11 ADT 2003 au : Lun 20 oct
20:29:11 ADT 2008 Empreintes digitales de 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 de fichier de clés :
Type de fichier de clés : jks
Fournisseur de fichier de clés : SUN
Votre fichier de clés contient 1 entrée
Nom d'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 à 20:36:54 ADT 2003 au : Lun 20 oct à
20:36:54 ADT 2008 Empreintes digitales de 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 Répétez l'opération pour tous les hôtes gérés dans votre déploiement qui hébergent le scanner.

Exemple de fichier TrustedCA.pem

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

Exemple de fichier 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 à 23:36:54 GMT
      Pas après : le 20 oct 2008 à 20 23:36:54 GMT
    Objet : CN=Foundstone Enterprise Manager
    Informations sur la clé publique de l'objet :
      Algorithme de clé publique : rsaEncryption
      Clé publique RSA : (1024 bits)
        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 :
      AC : FAUX
      Commentaire Netscape :
      Certificat généré OpenSSL
      Identificateur de clé d'objet X509v3 :
      0D:52:54:EF:A0:B3:91:9D:3D:47:AC:D8:9E:62:2A:34:0F:09:FF:8D
      Identificateur de clé d'autorité X509v3 :
keyid:64:3C:50:94:CF:6E:A4:8F:DB:4D:8C:CA:0B:36:B2:AC:D4:DA:1E:CB
      DirName:/CN=Foundstone CA
      Série :00
  Algorithme de signature : md5WithRSAEncryption
4a:88:3f:51:34:5b:30:3b:5b:7c:57:31:86:22:3b:00:16:61:
ac:7b:b7:ae:cd:68:11:01:a2:52:b7:59:1e:c6:5b:af:2a:ed:
f9:ee:ef:64:11:b2:b9:14:21:7d:2c:35:d3:cb:09:08:a1:ab:
26:93:0f:aa:97:eb:cc:65:ab:95:a3:0d:77:0b:23:20:4a:0d:
04:18:47:2d:58:a7:de:61:9f:aa:3c:da:a5:00:9d:b5:eb:52:
fb:e2:5b:56:45:02:02:79:df:0f:87:bc:f3:82:d1:3d:39:79:
9e:ef:64:e2:f5:61:9b:ea:29:94:fb:00:8f:b8:08:7c:f0:ee:
    68:b6
```

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

12 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 à partir de la base de données PostgreSQL sur NSM à 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 se situe normalement dans /var/netscreen/DevSvr/pgsql/data/pg_hba.conf sur l'hôte NSM.

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

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 des paramètres suivants :

Tableau 12-1 Paramètres du scanner

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

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 12-2 Paramètres de 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 plages du routage CIDR que ce scanner doit prendre en compte :

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

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

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

Modification d'un scanner Juniper Networks NSM Profiler

Pour modifier une configuration de scanner Juniper Networks NSM Profiler 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 Mettez à jour les paramètres, si nécessaire. Voir **Tableau 12-2**.

Etape 7 Cliquez sur **Save**.

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

Suppression d'un scanner Juniper Networks NSM Profiler

Pour supprimer un scanner Juniper Networks NSM Profiler 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 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

13 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 du scanner en fonction des vulnérabilités découvertes depuis l'adresse IP configurée pour votre site. Pour plus d'informations, voir **Importation des données de vulnérabilité Rapid7 NeXpose à l'aide de l'interface API**.

- Import Site Data - Local File

L'importation de site de fichier local permet à QRadar d'importer des rapports d'analyse pour un site en fonction d'un fichier local téléchargé sur votre console QRadar. 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 à l'aide du protocole Secure Copy (SCP) ou Secure File Transfer. Pour plus d'informations, voir **Importation de données 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 plus d'informations, voir **Gestion des plannings d'analyse**

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.

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**.

Le panneau Data Sources s'affiche.

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

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 13-1 Paramètres du scanner

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

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

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 13-2 Paramètres Rapid7 NeXpose

Paramètre	Description
Remote Hostname	Entrez le nom d'hôte ou l'adresse IP de la console de sécurité Rapid7 NeXpose configuré avec les données de vulnérabilité du site que vous souhaitez importer.

Tableau 13-2 Paramètres Rapid7 NeXpose (suite)

Paramètre	Description
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 la console de sécurité Rapid7 NeXpose. Il s'agit généralement du port 3780. Pour en savoir plus, contactez votre administrateur de serveur Rapid7 NeXpose.*
Site Name Pattern	Entrez un modèle d'expression régulière (regex) pour déterminer les sites Rapid7 NeXpose qu'il faut inclure dans le rapport d'analyse. Le modèle de nom du site par défaut .***** sélectionne tous les rapports de nom de site disponibles. Tous les noms de site correspondant au modèle regex sont inclus dans le rapport d'analyse. Vous devez utiliser un modèle regex valide dans cette zone.
Cache Timeout (Minutes)	Entrez le temps de stockage dans la mémoire cache des données du dernier rapport d'analyse généré. ***Remarque :*** *Si la limite de temps indiquée expire, de nouvelles données de vulnérabilité sont requises à partir de la console de sécurité Rapid7 NeXpose à l'aide de l'interface API.*

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

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

b Cliquez sur **Add**.

Remarque : Dans la mesure où QRadar importe des rapports d'analyse de Rapid7 NeXpose, nous vous recommandons de configurer une plage du 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 Dans 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, voir **Gestion des plannings d'analyse**

Identification et résolution des problèmes d'une importation d'analyse Rapid7 NeXpose API.

Les scanners Rapid7 NeXpose qui utilisent l'interface API pour collecter des rapports de vulnérabilité d'actifs adhoc sont basés sur la configuration de votre site.

Le nombre d'adresses IP configurées pour chaque site peut avoir un impact sur la taille du rapport adhoc. Les configurations de site important 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 le délai d'attente de session Rapid7 NeXpose.

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

Etape 1 Accédez à l'interface utilisateur Rapid7 NeXpose.

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

Remarque : 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 NeXpose Security Console Configuration 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 (in seconds)**.

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 importants à l'aide de l'interface API, utilisez l'importation de fichier local en déplaçant les analyses XML vers votre console QRadar ou l'hôte géré responsable de l'importation de données de vulnérabilité. Pour plus d'informations, voir **Importation de données de vulnérabilité Rapid7 NeXpose à partir d'un fichier local**.

Importation de données 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 les analyses de vulnérabilité terminées basées sur des rapports d'analyse 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**.

Le panneau Data Sources s'affiche.

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

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 13-1 Paramètres du scanner

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

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

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 13-2 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 Import File Pattern.

Tableau 13-2 Paramètres Rapid7 NeXpose (suite)

Paramètre	Description
Import File Pattern	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 précédemment traités selon un planning.*

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

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

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

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

Vous pouvez maintenant ajouter un planning 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 QRadar ou l'hôte géré. Pour en savoir plus sur la planification d'une analyse, voir **Gestion des plannings d'analyse**

Modification d'un scanner Rapid7 NeXpose

Pour modifier la configuration d'un scanner Rapid7 NeXpose 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 Mettez à jour les paramètres, si nécessaire. Voir **Tableau 13-2**.

Etape 7 Cliquez sur **Save**.

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

Suppression d'un scanner Rapid7 NeXpose

Pour supprimer un scanner Rapid7 NeXpose 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 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

14 GESTION DES SCANNERS netVigilance SecureScout

Vous pouvez collecter des vulnérabilités à partir des périphériques netVigilance SecureScout NX et SecureScout SP.

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

Pour connecter QRadar à 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, autorisent une connexion au collecteur d'événement. IBM Security 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 que vous créez doit disposer des autorisations de sélection pour les tables suivantes :

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

Remarque : L'utilisateur doit disposer des autorisations d'exécution pour la procédure IPSORT enregistrée.

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

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 des paramètres suivants :

Tableau 14-1 Paramètres SecureScout

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 **SecureScout Scanner.**

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 14-2 Paramètres SecureScout

Paramètre	Description
Database Hostname	Entrez l'adresse IP ou le nom d'hôte du serveur de base de données SecureScout exécutant le serveur SQL.
Login Username	Entrez le nom d'utilisateur de base de données SQL que QRadar doit utiliser pour se connecter à la base de données SecureScout.
Login Password	Entrez le mot de passe correspondant au nom d'utilisateur de connexion.
Database Name	Entrez le nom de la base de données dans le serveur SQL contenant les données SecureScout. La valeur par défaut est SCE.
Database Port	Entrez le port TCP dont vous souhaitez faire contrôler les connexions via le serveur SQL. La valeur par défaut est 1433.

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

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

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

Etape 9 Dans 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 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

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

Etape 7 Cliquez sur **Save**.

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

Suppression d'un scanner SecureScout

Pour supprimer un scanner 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 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

15 GESTION DES SCANNERS eEye

IBM Security QRadar prend en charge 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 avec QRadar, vous devez :

1. Configurer votre scanner eEye pour transférer des alertes SNMP vers QRadar. Pour plus d'informations, voir la documentation du fournisseur eEye.
2. Ajouter votre scanner eEye à QRadar.
3. Facultatif. Installer Java™ Cryptography Extension pour obtenir des algorithmes de description SNMPv3 de niveau supérieur.
4. Planifier une analyse pour votre scanner eEye dans QRadar.

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

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

Ajout d'un scanner eEye

Pour ajouter un scanner eEye REM 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 des paramètres suivants :

Tableau 15-1 Paramètres eEye REM

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 **eEye REM Scanner.**

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 15-2 Paramètres eEye

Paramètre	Description
Base Directory	Entrez l'emplacement dans lequel vous souhaitez stocker les fichiers temporaires résultant de l'analyse. 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 de 40.
Retention Period	Entrez la plage de temps, en jours, selon laquelle le système stocke les informations sur l'analyse. Si vous ne disposez pas d'une analyse planifiée à la fin de la durée de conservation, les informations sont supprimées. La durée de conservation par défaut est de 5 jours.
Use Vulnerability Data	Cochez la case pour corréler les données de vulnérabilité aux identifiants CVE (Common Vulnerabilities and Exposures) et les informations relatives à la description à partir de votre scanner eEye REM ou eEye CS Retina. Par défaut, le fichier de données de vulnérabilité audits.xml se trouve dans le répertoire suivant : **`%ProgramFiles(x86)%\eEye Digital Security\Retina CS\Applications\RetinaManager\Database\audits.xml`** ***Remarque :*** *Cette option nécessite que vous effectuez une copie du fichier audits.xml à partir de votre dispositif eEye REM ou eEye Retina CS vers QRadar.*

Tableau 15-2 Paramètres eEye (suite)

Paramètre	Description
Vulnerability Data File	Entrez le chemin de répertoire qui mène vers le fichier eEye audits.xml. Le chemin de répertoire par défaut est **`/opt/qradar/conf/audits.xml`**. ***Remarque :*** *Pour obtenir les informations d'audit les plus récentes sur eEye, vous devez régulièrement mettre à jour QRadar avec le fichier audits.xml le plus récent 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 entrantes sur la vulnérabilité SNMP 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 avez configurée pour que votre scanner eEye la transfère. Les options incluent : • **v1** - Sélectionnez v1 si votre scanner eEye transfère des messages d'alerte SNMPv1. • **v2** - Sélectionnez v2 si votre scanner eEye transfère des messages d'alerte SNMPv2. • **v3** - Sélectionnez v3 si votre scanner eEye transfère des messages d'alerte SNMPv3. La valeur par défaut est SNMPv2.
Community String	Entrez le nom de communauté SNMP pour le protocole SNMPv2, par exemple, Public. Utilisez ce paramètre uniquement 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.
Authentication Password	Entrez le mot de passe que vous souhaitez utiliser pour authentifier SNMP. Ce paramètre ne s'applique qu'à SNMPv3. ***Remarque :*** *Votre mot de passe d'authentification doit inclure 8 caractères au minimum.*

Tableau 15-2 Paramètres eEye (suite)

Paramètre	Description
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 décryptage comprennent : • DES • AES128 • AES192 • AES256 L'algorithme de décryptage par défaut est DES. ***Remarque :*** *Si vous sélectionnez AES192 ou AES256 en tant qu'algorithme de décryptage, vous devez installer des logiciels supplémentaires pour QRadar. Pour plus d'informations, voir* **Installation de Java Cryptography Extension**.
Encryption Password	Entrez le mot de passe utilisé pour déchiffrer les alertes SNMP. Ce paramètre est obligatoire si vous utilisez SNMPv3. ***Remarque :*** *Votre mot de passe de cryptage doit inclure 8 caractères au minimum.*

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

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

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

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

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

Installation de Java Cryptography Extension

Java™ Cryptography Extension (JCE) est une infrastructure Java™ nécessaire pour que QRadar puisse décrypter les algorithmes de cryptographie avancée pour AES192 ou AES256.

Les informations suivantes décrivent l'installation d'Oracle JCE sur QRadar.

Pour installer les fichiers de règles Unrestricted JCE sur QRadar.

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

https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk

Il est possible que plusieurs versions de JCE soient disponibles pour téléchargement. La version que vous téléchargerez doit correspondre à la version de Java™ installée 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 à votre console QRadar ou à votre hôte géré en tant que superutilisateur.

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

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

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

`/opt/ibm/java-x86_64-60/jre/lib/security/US_export_policy.jar`

`/opt/ibm/java-x86_64-60/jre/lib/security/local_policy.jar`

Les fichiers jar sont copiés sur le système recevant les fichiers cryptés AES192 ou AE256. Selon votre configuration, il peut s'agir de votre console QRadar ou d'un hôte géré.

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

Modification d'un scanner eEye

Pour modifier la configuration d'un scanner eEye 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 Mettez à jour les paramètres, si nécessaire. Voir **Tableau 15-2**.

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 jour immédiate, vous devez effectuer un déploiement total dans QRadar.

Etape 9 Facultatif. Dans l'onglet **Admin**, sélectionnez **Advanced > Deploy Full Configuration**.

ATTENTION : *L'option Deploying Full Configuration redémarre plusieurs services sur QRadar. La collection d'événements ne sera pas disponible sur QRadar tant que l'opération Deploy Full Configuration n'est pas terminée.*

Suppression d'un scanner eEye

Pour supprimer un scanner eEye REM 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 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

16 GESTION DES SCANNERS PatchLink

Vous pouvez intégrer un scanner PatchLink (version 6.4.4. et supérieure) à IBM Security QRadar.

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

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

Pour connecter QRadar au scanner PatchLink, vous devez avoir un accès administrateur approprié à QRadar et à votre périphérique PatchLink. Pour plus d'informations, voir la documentation de votre produit. Assurez-vous que tous les pare-feu entre votre dispositif PatchLink et QRadar sont configurés pour permettre les communications.

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

Ajout d'un scanner PatchLink

Pour ajouter un scanner PatchLink 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 des paramètres suivants :

Tableau 16-1 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	A partir de la zone de liste, sélectionnez **Lumension PatchLink Scanner**.

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 16-2 Paramètres PatchLink

Paramètre	Description
Engine Address	Entrez l'adresse dans laquelle le scanner PatchLink est installé.
Port	L'interface de programmation d'application (API) transmet des demandes du protocole SOAP via 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.
Result Refresh Rate (mins)	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 requiert d'importantes ressources et se fait uniquement après l'intervalle de temps défini dans cette zone. Les valeurs valides sont configurées en minutes et la valeur par défaut est de 15 minutes.

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

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

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

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

Modification d'un scanner PatchLink

Pour modifier la configuration d'un scanner PatchLink 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 Mettez à jour les paramètres, si nécessaire. Voir **Tableau 16-2**.

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

17 GESTION DES SCANNERS MCAFEE VULNERABILITY MANAGER

Le scanner McAfee Vulnerability Manager de IBM Security QRadar permet à QRadar d'importer les vulnérabilités à l'aide d'un fichier XML ou de faire une requête pour un fichier de résultats à l'aide de l'interface de programme d'application ouverte McAfee.

Le scanner McAfee Vulnerability Manager de QRadar ne démarre pas les analyses à distance, mais regroupe les données du résultat de l'analyse à la fin d'une analyse sur le dispositif McAfee Vulnerability Manager. QRadar prend en charge les versions 6.8 ou 7.0. de McAfee Vulnerability Manager.

Après avoir configuré le système McAfee Foundstone Enterprise et le scanner McAfee Vulnerability Manager dans QRadar, vous pouvez programmer l'analyse. Un planning d'analyse vous permet de déterminer la fréquence à laquelle QRadar demande des données à partir de votre dispositif McAfee. Pour plus d'informations, voir **Gestion des plannings d'analyse**

Les options de collection de données suivants sont disponibles pour McAfee Vulnerability Manager :

- **Remote XML Import** - Permet à QRadar de se connecter à un serveur distant et d'importer les données de vulnérabilité XML créées par le dispositif de votre McAfee Vulnerability Manager. Ceci vous permet de configurer votre McAfee Vulnerability Manager pour publier ou exporter vos résultats d'analyse vers un serveur distant, et ensuite importer les données XML. QRadar se connecte au référentiel via SFTP et importe les fichiers de rapport d'analyse complets depuis le répertoire distant.
- **SOAP API** - Permet à QRadar d'utiliser l'interface OpenAPI McAfee pour récupérer des données d'analyse de vulnérabilité complètes. Pour récupérer des données d'analyse via l'interface API ouverte, vous devez indiquer le nom de configuration pour les données de l'analyse opérationnelle que vous voulez récupérer. Lors de l'exécution de l'analyse opérationnelle, QRadar met à jour le pourcentage effectué dans le statut 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.

Ajout d'une analyse McAfee Vulnerability Manager

Le module du scanner McAfee Vulnerability Manager pour QRadar fournit plusieurs types de collection pour la récupération de données de vulnérabilité depuis votre serveur.

- **Configuration d'une importation XML distante**
- **Configuration d'une analyse OpenAPI**

Configuration d'une importation XML distante

Une importation XML distante vous permet de récupérer vos données McAfee Vulnerability Manager à partir d'un serveur distant. Les données sont récupérées via SFTP.

Pour ajouter un scanner McAfee Vulnerability Manager via une importation XML :

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

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

Le panneau Data Sources s'affiche.

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

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Scanner s'affiche.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 17-1 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 **McAfee Vulnerability Manager**.

Etape 6 A partir de la zone de liste **Collection Type**, sélectionnez **Remote XML Import**.

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 17-2 Paramètres d'importation XML distant de McAfee

Paramètre	Description
Remote Hostname	Entrez l'adresse IP ou le nom d'hôte du serveur distant qui héberge les données XML de McAfee Vulnerability Manager. Si le processus serveur et le client sont situés sur le même hôte, vous pouvez utiliser localhost comme nom d'hôte du serveur.

Tableau 17-2 Paramètres d'importation XML distant de McAfee (suite)

Paramètre	Description
Server Remote	Entrez le port afin que l'hôte distant puisse récupérer les données de vulnérabilité du XML via SFTP. Le numéro de port par défaut est 22.
Login Username	Entrez le nom d'utilisateur que QRadar peut utiliser pour l'authentification à l'aide du serveur distant.
Enable Key Authentication	Sélectionnez cette case pour activer l'authentification par clé publique ou privée. Si la case est sélectionnée, QRadar tente d'authentifier la connexion à l'aide de la clé privée fournie et la zone **Login Password** est ignorée.
Login Password	Entrez le mot de passe correspondant au nom d'utilisateur pour le serveur distant. ***Remarque :*** *Votre mot de passe de serveur ne doit pas contenir le caractère !. Ce caractère peut provoquer des échecs d'authentification via SFTP.*
Remote Directory	Entrez l'emplacement du répertoire des fichiers des résultats d'analyse.
File Name Pattern	Entrez une expression régulière (regex) requise pour filtrer la liste des fichiers spécifiés dans le paramètre 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 nécessite la connaissance des expressions régulières (regex). Pour plus d'informations, consultez le site Web suivant : *http://download.oracle.com/javase/tutorial/essential/regex/*
Max Report Age (Days)	Entrez l'âge du fichier maximal à inclure au moment d'importer votre fichier de résultats XML lors d'une analyse planifiée. Par défaut, l'âge maximal du fichier est de 7 jours. Les fichiers qui sont plus anciens que le nombre de jours indiqué et que l'horodatage sur le fichier de rapport sont exclus de l'importation planifiée.

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

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

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

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

La configuration est terminée. Vous êtes prêt à ajouter un planning d'analyse pour déterminer la fréquence à laquelle QRadar importe les données XML du dispositif de votre McAfee Vulnerability Manager.

Configuration d'une analyse OpenAPI

Votre système McAfee Foundstone Enterprise doit inclure une configuration appropriée 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 répond aux exigences suivantes :

- Etant donné que l'API Open de Foundstone permet d'accéder au serveur McAfee Foundstone Enterprise Manager, assurez-vous que l'application McAfee Foundstone Enterprise McAfee Foundstone Enterprise) s'exécute en continu sur ledit serveur.
- L'analyse qui inclut la configuration requise pour se connecter à QRadar doit être entièrement exécutée 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 FoundScan OpenAPI fournit uniquement des informations sur l'hôte et la vulnérabilité à QRadar, vos informations du profil de l'actif affichent toutes les vulnérabilités pour un hôte assigné au port 0.

SSL connecte le serveur McAfee Foundstone Enterprise Manager à l'OpenAPI Foundstone. QRadar authentifie 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, voir **Configuration des certificats**.

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 Configurez les valeurs des paramètres suivants :

Tableau 17-3 Paramètres du scanner

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

Etape 6 A partir de la zone de liste **Collection Type**, sélectionnez **importation API distante**.

Etape 7 Configurez les valeurs des paramètres suivants :

Tableau 17-4 Paramètres d'importation d'interface de programme d'application ouvert de McAfee

Paramètre	Description
SOAP API URL	Saisissez l'adresse Web de l'interface de programme d'application de Foundscan Open au format suivant : **`https://<address_IP>:<port_SOAP>`** Où : **`<l'adresse_IP>`** représente l'adresse IP ou le nom d'hôte du serveur de McAfee Foundstone Enterprise Manager. **`<port_SOAP>`** représente le numéro de port pour la connexion entrante au serveur API Open. La valeur par défaut est **`https://localhost:3800.`**
Customer Name	Entrez un nom pour identifier à quel client ou organisation appartient le nom d'utilisateur. Le nom du client doit correspondre à l'ID de l'organisation requise pour se connecter à McAfee Foundstone Enterprise Manager.
User Name	Entrez le nom d'utilisateur que vous voulez que QRadar utilise pour authentifier le serveur McAfee Foundstone Enterprise Manager dans l'interface de programme d'application ouverte Cet utilisateur doit avoir accès à la configuration de l'analyse.
Password	Entrez le mot de passe correspondant au nom de connexion pour avoir accès à l'interface de programme d'application ouverte.
Client IP Address	Entrez l'adresse IP du serveur QRadar que vous avez choisie pour effectuer les analyses. Par défaut, cette valeur n'est pas utilisée. Cependant, elle est requise pour valider certains environnements.
Portal Name	Facultatif. Entrez le nom du portail. Cette zone peut être laissée vide pour QRadar. Consultez l'administrateur de McAfee Vulnerability Manager administrator pour de plus amples informations.

Tableau 17-4 Paramètres d'importation d'interface de programme d'application ouvert de McAfee (suite)

Paramètre	Description
Configuration Name	Entrez le nom de la configuration de l'analyse qui existe dans McAfee Foundstone Entreprise et auquel l'utilisateur a accès.
CA Truststore	Entrez le chemin de répertoire et le nom du fichier de clés certifiées CA. Le chemin de répertoire par défaut est /opt/qradar/conf/mvm.keystore. ***Remarque :*** *Pour plus d'informations sur les certificats McAfee Vulnerability Manager, voir* **Configuration des certificats**.
Client Keystore	Entrez le chemin de répertoire et le nom du fichier des fichiers de clés du client. Le chemin de répertoire par défaut est /opt/qradar/conf/mvm.truststore. ***Remarque :*** *Pour plus d'informations sur les certificats McAfee Vulnerability Manager, voir* **Configuration des certificats**.
McAfee Vulnerability Manager Version	A partir de la zone de liste, spécifiez la version de votre McAfee Vulnerability Manager.

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

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

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

b Cliquez sur **Add**.

Etape 9 Cliquez sur **Save**.

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

La configuration est terminée. Vous êtes prêt à ajouter un planning d'analyse pour déterminer la fréquence à laquelle QRadar importe les données XML à partir du dispositif de votre McAfee Vulnerability Manager.

Modification d'un scanner McAfee Vulnerability Manager

Pour modifier la configuration d'un scanner McAfee Vulnerability Manager dans :

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

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

Le panneau Data Sources s'affiche.

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

La fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez le scanner que vous souhaitez modifier.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Mettez à jour les paramètres, si nécessaire.

- Pour les paramètres d'importation XML distante, voir **Tableau 17-2**.
- Pour les paramètres de l'interface OpenAPI, voir **Tableau 17-4**.

Etape 7 Cliquez sur **Save**.

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

Suppression d'un scanner McAfee Vulnerability Manager

Pour supprimer un scanner McAfee Vulnerability Manager 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 Dans l'onglet **Admin**, sélectionnez **Deploy Changes**.

Configuration des certificats

McAfee Certificate Manager Tool est requis pour créer des certificats tiers et se connecter à travers l'Open Api Foundstone.

Si le Certificate Manager Tool n'est pas encore installé sur le serveur McAfee Foundstone Enterprise Manager, contactez l'équipe d'assistance technique de McAfee.

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

serveur pour ce traitement. Pour acquérir la dernière version du kit de développement de logiciels Java ™ consultez *http://java.sun.com*.

Génération de certificats

Pour obtenir les certificats requis :

Etape 1 Exécutez Foundstone Certificate Manager.

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

Etape 3 Configurez l'adresse hôte de QRadar.

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

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

Remarque : Nous vous recommandons de saisir une adresse IP dans la zone adresse de l'hôte lorsque Foundstone Certificate Manager génère un message d'erreur

Si vous n'avez pas résolu le problème du nom d'hôte, consultez l'**Etape 6**.

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

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

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

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

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

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

Vous êtes maintenant prêt pour traiter les certificats de QRadar.

Traitement de certificats

Pour traiter les certificats :

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

Etape 2 A partir du site *http://www.ibm.com/support,* 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 Entrez la commande suivante pour extraire les fichiers gz :

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

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

Par exemple :

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

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

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

Etape 5 Lorsque vous y êtes invité, saisissez la phrase de passe fournie dans l'**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 **Importation de certificats**.

Importation de 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.

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

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

`/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 vous pouvez ignorer la copie du fichier dans* **`/opt/qradar/conf/trusted_certificates.`**

Etape 2 Connectez-vous à QRadar.

`https://<Adresse_IP>`

Où <Adresse_IP> représente l'adresse IP de la console QRadar.

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

L'onglet Administration s'affiche.

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

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

18 GESTION DES SCANNERS SAINT

Vous pouvez intégrer un scanner de vulnérabilité Security Administrator's Integrated Network Tool (SAINT) avec QRadar à l'aide de la version 7.4.x de SAINT

En utilisant QRadar, vous pouvez planifier et lancer les analyses de vulnérabilité SAINT ou générer des rapports à l'aide des données de vulnérabilité existantes. Le scanner SAINT identifie les vulnérabilités en fonction du niveau d'analyse indiqué et utilise SAINTwriter pour générer les rapports personnalisés pour QRadar. Votre système SAINT doit donc 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 disposer de l'accès administrateur adéquat à QRadar et à votre dispositif SAINT. Vous devez également vous assurer que les pare-feu sont configurés pour autoriser une communication entre votre dispositif SAINT et QRadar. Pour plus d'informations, voir la documentation de votre produit.

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

Configuration d'un modèle de rapports SAINTwriter

Pour configurer un modèle de rapport SAINTwriter :

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

Etape 2 Sélectionnez **Data > SAINTwriter**.

Etape 3 Cliquez sur **Type**.

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

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

Le nom du fichier de configuration doit correspondre au paramètre QRadar Saint Writer Config dans le **Tableau 18-2**.

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

Etape 7 Cliquez sur **Continue**.

Le menu Category s'affiche.

Etape 8 Sélectionnez **Lists**.

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

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

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

Etape 12 Cliquez sur **Save**.

Vous pouvez maintenant ajouter un scanner de vulnérabilité SAINT à QRadar.

Ajout d'un scanner 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 des paramètres suivants :

Tableau 18-1 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 **SAINT Scanner**.

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 18-2 Paramètres du scanner SAINT

Paramètre	Description
Remote Hostname	Entrez le nom d'hôte ou l'adresse IP du système hébergeant le scanner SAINT.

Tableau 18-2 Paramètres du scanner SAINT (suite)

Paramètre	Description
Login Username	Entrez le nom d'utilisateur utilisé par QRadar pour authentifier la connexion SSH.
Enable Key Authorization	Cochez cette case pour activer l'authentification par clé publique/privée. Si la case à cocher est sélectionnée, QRadar tente d'authentifier la connexion SSH en utilisant la clé privée fournie et le paramètre Login Password est ignoré. Par défaut, la case est décochée. Pour plus d'informations, voir votre documentation SSH pour configurer l'authentification par clé publique.
Login Password	Entrez le mot de passe associé à Login Username pour l'accès SSH. Si le paramètre Enable Key Authentication est activé, ce paramètre est ignoré.
Private Key File	Entrez le chemin de répertoire qui mène vers le fichier contenant les informations sur la 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 entrer un autre nom de fichier. Ce paramètre est obligatoire si la case Enable Key Authentication est cochée. Si la case Enable Key Authentication est décochée, ce paramètre est ignoré.
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 une analyse opérationnelle ou vous pouvez sélectionner Report Only. Dans la zone de texte, sélectionnez le type de collection : • **Live Scan** - Lance une analyse de vulnérabilité et génère des données de rapport à partir des résultats d'analyse basés sur le nom de session. • **Report Only** - Génère un rapport d'analyse basé sur le nom de session.
Ignore Existing Data	Cette option s'applique uniquement lorsque Live Scan est le type d'analyse sélectionné. Cette option indique si l'analyse opérationnelle ignore les données existantes et regroupe les nouvelles informations de vulnérabilité pour le réseau. Si la case Ignore Existing Data est cochée, le scanner SAINT supprime les données de session existantes avant qu'une analyse opérationnelle ne soit lancée. Par défaut, la case est décochée.

Tableau 18-2 Paramètres du scanner SAINT (suite)

Paramètre	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** - Analyse les ports et les services avec une mise en évidence sur la conformité DSS PCI. • **SANS Top 20 Scan** - Analyse les 20 vulnérabilités de sécurité les plus importantes. • **FISMA Scan** - Analyse toutes les vulnérabilités en incluant toutes les analyses personnalisées et les niveaux PCI.
Session Name	Entrez le nom de session pour la configuration de session du scanner SAINT.
SAINT Writer Config	Entrez le nom du fichier de configuration pour SAINTwriter.

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

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

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

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

Modification d'un scanner SAINT

Pour modifier un scanner de vulnérabilité 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 Cliquez sur **Edit**.

La fenêtre Edit Scanner s'affiche.

Etape 6 Mettez à jour les paramètres, si nécessaire. Voir **Tableau 18-2**.

Etape 7 Cliquez sur **Save**.

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

Suppression d'un scanner 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 sur **OK**.

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

19 GESTION DES SCANNERS AXIS

Le scanner Asset Export Information Source (AXIS) permet à IBM Security QRadar d'extraire les résultats d'analyse des périphériques d'analyse inconnus pour la corrélation.

Cela permet d'utiliser AXIS afin d'importer les résultats d'analyse pour les périphériques créés par les fournisseurs de scanner qui présentent les vulnérabilités au format XML qui respecte le schéma du format AXIS. De ce fait, les fournisseurs de logiciels et produits de scanner peuvent créer un format générique compatible avec IBM Security QRadar. Le scanner AXIS pour QRadar est conçu pour récupérer périodiquement les résultats d'analyse au format XML et interpréter les données analysées. QRadar surveille l'existence de mises à jour des résultats d'analyse sur le serveur et télécharge les derniers résultats pour le traitement. QRadar ne prend en charge que les résultats d'analyse au format AXIS XML.

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

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

Ajout d'un scanner AXIS

Pour ajouter un scanner AXIS 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 des paramètres suivants :

Tableau 19-1 Paramètres AXIS 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, cochez **Axis Scanner**.

Etape 6 Configurez les valeurs des paramètres suivants :

Tableau 19-2 Paramètres AXIS Scanner

Paramètre	Description
Remote Hostname	Entrez le nom d'hôte ou l'adresse IP du serveur distant.
Login Username	Entrez le nom d'utilisateur utilisé par QRadar pour authentifier la connexion SFTP.
Login Password	Si le paramètre Enable Key Authentication est désactivé, vous devez entrer le mot de passe correspondant au paramètre Login Username qu'utilise QRadar pour authentifier la connexion SFTP. Si le paramètre Enable Key Authentication est activé, le paramètre Login Password est ignoré.
Enable Key Authorization	Cochez cette case pour activer l'autorisation via une clé privée pour le serveur. Si la case est cochée, l'authentification est effectuée à l'aide d'une clé privée et le mot de passe est ignoré. Ce paramètre est désactivé par défaut.
Private Key File	Entrez le chemin de répertoire qui mène vers le fichier contenant les informations sur la clé privée. Si vous utilisez une authentification basée sur une clé, QRadar utilise la clé privée pour authentifier la connexion. 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 entrer un autre nom de fichier. Ce paramètre est obligatoire si la case Enable Key Authentication est cochée. Si la case Enable Key Authentication est décochée, ce paramètre est ignoré.
Remote Directory	Entrez l'emplacement du répertoire des fichiers des résultats d'analyse.

Tableau 19-2 Paramètres AXIS Scanner (suite)

Paramètre	Description
File Name Pattern	Entrez une expression régulière (regex) requise pour filtrer la liste des fichiers spécifiés dans le paramètre 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 nécessite la connaissance des expressions régulières (regex). Pour plus d'informations, consultez le site Web suivant : *http://download.oracle.com/javase/tutorial/essential/regex/*
Max Report Age (Days)	Entrez l'âge du fichier maximal à inclure au moment d'importer votre fichier de résultats XML lors d'une analyse planifiée. Par défaut, l'âge maximal du fichier est de 7 jours. Les fichiers qui sont plus anciens que le nombre de jours indiqué et que l'horodatage sur le fichier de rapport sont exclus de l'importation planifiée.
Ignore Duplicates	Cochez cette case pour suivre les fichiers qui ont déjà été traités et les fichiers que vous ne souhaitez pas traiter une seconde fois. ***Remarque :*** *Si un fichier de résultat n'est pas consulté pendant 10 jours, il est supprimé de la liste de suivi et est traité à la prochaine reconnaissance du fichier.*

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

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

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

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

Modification d'un scanner AXIS

Pour modifier la configuration d'un scanner AXIS 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 Mettez à jour les paramètres, si nécessaire. Voir **Tableau 19-2**.

Etape 7 Cliquez sur **Save**.

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

Suppression d'un scanner AXIS

Pour supprimer un scanner AXIS de QRadar :

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**.

20 GESTION DES SCANNERS TENABLE SECURITYCENTER

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

QRadar accède à distance au scanner Tenable SecurityCenter via une connexion HTTPS.

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

Ajout d'un scanner Tenable SecurityCenter

Pour ajouter Tenable SecurityCenter 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 des paramètres suivants :

Tableau 20-1 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 **Tenable Security Center**.

Etape 6 Configurez les valeurs des paramètres :

Tableau 20-2 Paramètres Tenable SecurityCenter

Paramètre	Description
Server Address	Entrez l'adresse IP ou le nom d'hôte du dispositif Tenable SecurityCenter.
API Location	Entrez le chemin d'accès au fichier request.php pour votre version de Tenable SecurityCenter. Par défaut, le chemin d'accès à l'interface de programme d'application est **`sc4/request.php`**. Si vous rencontrez des problèmes en vous connectant à votre Tenable SecurityCenter depuis QRadar, vous pouvez vérifier le chemin d'accès vers votre fichier request.php, puis mettre cette zone 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 plages du routage CIDR que ce scanner doit prendre en compte :

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

b Cliquez sur **Add**.

Etape 8 Cliquez sur **Save**.

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

Modification d'un scanner 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 Mettez à jour les paramètres, si nécessaire. Voir **Tableau 20-2**.

Etape 7 Cliquez sur **Save**.

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

Suppression d'un scanner Tenable SecurityCenter

Pour supprimer un 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 Dans l'onglet **Admin**, cliquez sur **Deploy Changes**.

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 QRadar Console ou votre collecteur d'événement.

Installation de Java Cryptography Extension

Java™ Cryptography Extension (JCE) est une infrastructure Java™ requise pour que QRadar puisse décrypter les algorithmes de cryptographie avancée pour AES192 ou AES256.

Les informations suivantes décrivent l'installation de Oracle JCE sur QRadar. En fonction de votre configuration, vous pourriez avoir besoin de JCE pour communiquer avec QRadar

Pour installer Unrestricted JCE Policy Files sur QRadar.

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

https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk

Il est possible que plusieurs versions de JCE soient disponibles pour téléchargement. La version que vous téléchargez doit correspondre à la version de Java™ installée 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 à votre console QRadar ou à votre hôte géré en tant que superutilisateur.

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

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

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

`/opt/ibm/java-x86_64-60/jre/lib/security/US_export_policy.jar`

`/opt/ibm/java-x86_64-60/jre/lib/security/local_policy.jar`

Les fichiers jar sont copiés sur le système recevant les fichiers chiffrés en AES192 ou AE256. Selon votre configuration, il peut s'agir de votre QRadar Console ou d'un hôte géré.

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

21 GESTION DES PLANNINGS D'ANALYSE

Après avoir configuré chaque scanner pour permettre à IBM Security QRadar d'accéder aux données de vulnérabilité du client ou du dispositif, vous devez créer une planification afin que QRadar récupère les données de vulnérabilité.

Un planning d'analyse peut être exécuté une seule fois ou être configuré afin de récupérer régulièrement les données de vulnérabilité. Lorsqu'un planning d'analyse est terminé, QRadar est mis à jour avec les données de vulnérabilité les plus récentes.

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

Affichage des analyses planifiées

La fenêtre Scan Scheduling s'affiche lorsqu'il est planifié que QRadar collecte des données d'évaluation de la vulnérabilité à partir des dispositifs de vulnérabilité sur votre réseau. Le nom de chaque analyse s'affiche, accompagné de la plage du routage CIDR, du port ou de la plage de ports, de la priorité, de la puissance, du 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**.

La fenêtre Scan Scheduling s'affiche.

Les informations suivantes sont fournies pour chaque analyse planifiée :

Tableau 21-1 Paramètres d'analyse planifiée

Paramètre	Description
VA Scanner	Affiche le nom de l'analyse planifiée.
CIDR	Affiche les adresses IP à inclure dans cette analyse.

Tableau 21-1 Paramètres d’analyse planifiée (suite)

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

Tableau 21-1 Paramètres d'analyse planifiée (suite)

Paramètre	Description
Status	Affiche le statut de l'analyse. Un message de statut descriptif s'affiche en maintenant la souris sur le message de statut : • **New** - Indique que l'entrée de l'analyse planifiée a récemment été créée. Lorsque le statut est New, vous pouvez modifier l'entrée de l'analyse. Lorsque l'heure de début initiale pour l'analyse a été atteinte, le statut change à Pending et vous ne pouvez plus modifier l'entrée de l'analyse. • **Pending** - Indique que l'analyse a été placée dans la file d'attente de travaux. Le statut reste Pending jusqu'à ce qu'elle soit supprimée de la file d'attente par le module de scanner, ou que le statut indique un pourcentage (%) d'avancement ou un échec. Le scanner VA soumet un résultat d'analyse pour chaque adresse IP analysée. • **Percentage Complete** - Chaque fois qu'une adresse IP est analysée, le scanner VA calcule l'avancement de l'analyse. Percentage Complete indique le statut d'avancement en pourcentage (%) pour l'analyse sous la forme d'une valeur numérique. • **Complete** - Lorsque la zone Percentage Complete atteint les 100%, le statut de l'analyse devient 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 les informations détaillées sur les erreurs ou les analyses opérationnelles qui peuvent être en cours.*
Concurrency Mask	Affiche la taille du sous-réseau analysé lors d'une analyse VA (Vulnerability Assessment).
Next Run Time	Affiche un compte à rebours pour indiquer l'intervalle avant l'exécution de la prochaine analyse de vulnérabilité planifiée. Si l'analyse est planifiée avec un intervalle de 0, cela indique que la répétition de l'analyse n'est pas planifiée. Les analyses qui ne se répètent pas indiquent N/A pour la prochaine exécution. Le paramètre Next Run Time est mis à jour au moment de l'actualisation de la fenêtre Scan Scheduling.

Planification d'une analyse

Après avoir configuré les scanners de vulnérabilité dans QRadar, vous pouvez 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 analyse Vulnerability Assessment :

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

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

Le panneau Data Sources s'affiche.

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

La fenêtre Scan Scheduling s'affiche.

Etape 4 Cliquez sur **Add**.

La fenêtre Add Schedule s'affiche.

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

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 21-2 Paramètres de planification de l’analyse

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

Tableau 21-2 Paramètres de planification de l’analyse (suite)

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

Tableau 21-2 Paramètres de planification de l’analyse (suite)

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

Etape 6 Cliquez sur **Save**.

Modification d'un planning d'analyse

Après avoir créé un nouveau planning d'analyse, vous pouvez modifier ses paramètres.

Remarque : La modification d'un planning d'analyse n'est possible qu'après le déploiement de la configuration dans QRadar. Après le déploiement des modifications de configuration dans QRadar, le bouton de modification n'est pas 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 le planning que vous souhaitez modifier.

Etape 5 Cliquez sur **Edit**.

La fenêtre Edit Schedule s'affiche.

Etape 6 Mettez à jour les valeurs, si nécessaire. Voir **Tableau 21-2**.

Etape 7 Cliquez sur **Save**.

Suppression d'un planning d'analyse

Pour supprimer un planning d'analyse Vulnerability Assessment :

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

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

Le panneau Data Sources s'affiche.

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

la fenêtre VA Scanners s'affiche.

Etape 4 Sélectionnez l'analyse que vous souhaitez supprimer.

Etape 5 Cliquez sur **Delete**.

Une fenêtre de confirmation s'affiche.

Etape 6 Cliquez sur **OK**.

22 SCANNERS PRIS EN CHARGE

Tableau 22-1 fournit des informations sur les prises en charge de scanners pour l'évaluation de la vulnérabilité IBM Security QRadar.

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

Tableau 22-1 Scanners pour l'évaluation de vulnérabilité prise en charge

Fabricant	Scanner	Version	Option dans QRadar	Type de connexion
Beyond Security	AVDS	AVDS Management v12 (version prise en charge 129) et plus	Beyond Security AVDS Scanner	Importation des fichiers de données de vulnérabilité via SFTP
eEye Digital Security	eEye REM ou Retina CS eEye	REM v3.5.6 ou Retina CS v3.0 to v4.0	eEye REM Scanner	Alerte SNMP
Générique	AXIS	N/A	Axis Scanner	Importation des fichiers de données de vulnérabilité via SFTP
IBM	InfoSphere Guardium	v9.0 et supérieure	IBM Guardium SCAP Scanner	Importation des fichiers de données de vulnérabilité via SFTP
IBM	IBM Security AppScan Enterprise	AppScan Enterprise 8.6	IBM AppScan Scanner	Service Web IBM REST via HTTP ou HTTPS
IBM	SiteProtector	SiteProtector v2.9.x	IBM SiteProtector Scanner	Interrogation JDBC
IBM	Tivoli EndPoint Manager	IBM Tivoli EndPoint Manager v8.2.x	IBM Tivoli EndPoint Manager	Interface API basée sur le protocole SOAP via HTTP ou HTTPS
Juniper	NSM Profiler	2007.1r2, 2007.2r2, 2008.1r2, 2009r1.1 et 2010.x	Juniper NSM Profiler Scanner	Interrogation JDBC
Lumenison	Patchlink	6.4.4 et supérieure	Lumenison Patchlink Scanner	Interface API basée sur le protocole SOAP via HTTPS

Tableau 22-1 Scanners pour l'évaluation de vulnérabilité prise en charge (suite)

Fabricant	Scanner	Version	Option dans QRadar	Type de connexion
McAfee	Foundstone	5.0 à 6.5	Scanner Foundscan	Interface API basée sur le protocole SOAP via HTTPS
	Vulnerability Manager	Version 6.8 ou 7.0.	McAfee Vulnerability Manager	Interface API basée sur le protocole SOAP via HTTPS
nCircle	ip360	VnE Manager version 6.5.2 à 6.8.28	nCircle ip360 Scanner	Importation des fichiers de données de vulnérabilité via SFTP
Nessus	Nessus	Linux version 4.0.2 à 4.4.x, Windows version 4.2 à 4.4.x	Nessus Scanner	Importation de fichiers via SFTP et exécution de la commande SSH
	Nessus	Linux version 4.2 à 5.x, Windows version 4.2 à 5.x	Nessus Scanner	Interface API Nessus XMLRPC via HTTPS
netVigilance	SecureScout	2.6	SecureScout Scanner	Interrogation JDBC
Open Source	NMap	Version 3.7 à 5.50	NMap Scanner	Importation de données de vulnérabilité via SFTP et exécution de la commande SSH
Qualys	QualysGuard	Version 4.7 à 7.2	Qualys Scanner	Interface APIv2 via HTTPS
	QualysGuard	Version 4.7 à 7.2	Qualys Detection Scanner	Liste de détection d'hôte API via HTTPS
Rapid7	NeXpose	4.x à v5.4	Rapid7 NeXpose Scanner	Appel de procédure à distance via HTTPS
				Importation de fichiers locaux à partir d'un répertoire QRadar
Saint Corporation	SAINT	7.4.x	Saint Scanner	Importation de données de vulnérabilité via SFTP et exécution de la commande SSH
Tenable	SecurityCenter	version 4.6.0	Tenable SecurityCenter	Demande JSON via HTTPS

A AVIS ET MARQUES

Dans cette annexe :

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

Avis

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

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

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

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

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

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

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

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

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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

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

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via

d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Tous les prix IBM indiqués sont des prix de détail suggérés par IBM, sont à jour et peuvent être modifiés sans préavis. Les prix distributeurs peuvent donc varier.

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

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

Marques

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

Les noms suivants sont des marques ou des marques déposées d'autres sociétés :

Java et toutes les marques et tous les logos Java sont des marques ou des marques déposées d'Oracle et/ou de ses filiales.

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

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

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

INDEX