IBM Security QRadar
Version 7.2.4

Vulnerability Assessment Configuration Guide

Note

Before using this information and the product that it supports, read the information in “Notices” on page 93.

Product information

This document applies to IBM QRadar Security Intelligence Platform V7.2.4 and subsequent releases unless superseded by an updated version of this document.

Contents

Introduction to QRadar vulnerability assessment configurations v

Chapter 1. Vulnerability assessment scanner overview 1

Chapter 2. Beyond Security Automatic Vulnerability Detection System scanner overview 3
Adding a Beyond Security AVDS vulnerability scanner 3

Chapter 3. Adding a Digital Defense Inc AVS scanner 7

Chapter 4. eEye scanner overview 9
Adding an eEye REM SNMP scan 9
Adding an eEye REM JDBC scan 10
Installing the unrestricted Java Cryptography Extension 11

Chapter 5. IBM Security AppScan Enterprise scanner overview 13
Creating a customer user type for IBM AppScan 13
Enabling integration with IBM Security AppScan Enterprise 14
Creating an application deployment map in IBM Security AppScan Enterprise 14
Publishing completed reports in IBM AppScan 15
Adding an IBM AppScan vulnerability scanner 15

Chapter 6. IBM Security Guardium scanner overview. 17
Adding an IBM Security Guardium vulnerability scanner 17

Chapter 7. IBM Security SiteProtector scanner overview 21
Adding an IBM SiteProtector vulnerability scanner 21

Chapter 8. IBM Security Tivoli Endpoint Manager scanner overview 23
Adding an IBM Security Tivoli Endpoint Manager vulnerability scanner 23

Chapter 9. Foundstone FoundScan scanner overview 25
Adding a Foundstone FoundScan scanner 25
Importing certificates for Foundstone FoundScan. 26

Chapter 10. Microsoft SCCM scanner overview 29

Chapter 11. WMI enablement on scanner host. 31

Chapter 12. Adding a Microsoft SCCM scanner 33

Chapter 13. nCircle IP360 scanner overview. 35
Exporting nCircle IP360 scan results to an SSH server 35
Adding a nCircle IP360 scanner 35

Chapter 14. Nessus scanner overview 37
Adding a Nessus scheduled live scan. 37
Adding a Nessus live scan with the XMLRPC API 39
Adding a Nessus scheduled result import 40
Adding a Nessus completed report import with the XMLRPC API 42

Chapter 15. Nmap scanner overview . . . 45
Adding a Nmap remote result import . . . 45
Adding a Nmap remote live scan . . . 47

Chapter 16. Qualys scanner overview . . . 51
Adding a Qualys detection scanner . . . 51
Adding a Qualys scheduled live scan. . . . 53
Adding a Qualys scheduled import asset data report . . . 54
Adding a Qualys scheduled import scan report . . . 55

Chapter 17. Juniper Profiler NSM scanner overview . . . 59
Adding a Juniper NSM Profiler scanner . . . 59

Chapter 18. Rapid7 NeXpose scanners overview. . . . 61
Adding a Rapid7 NeXpose scanner API site import . . . 61
Adding a Rapid7 NeXpose scanner local file import . . . 62

Chapter 19. netVigilance SecureScout scanner overview . . . 65
Adding a netVigilance SecureScout scan . . . 65

Chapter 20. McAfee Vulnerability Manager scanner overview . . . 67
Adding a remote XML import scan . . . 67
Adding a McAfee Vulnerability Manager SOAP API scan . . . 68
Creating certificates for McAfee Vulnerability Manager . . . 69
Processing certificates for McAfee Vulnerability Manager . . . 70
Importing certificates for McAfee Vulnerability Manager . . . 71

Chapter 21. Outpost24 Vulnerability Scanner overview . . . 73
Creating an Outpost24 API authentication token for QRadar . . . 74

Chapter 22. SAINT scanner overview. . . . 75
Configuring a SAINTwriter template . . . 75
Adding a SAINT vulnerability scan . . . 76

Chapter 23. Tenable SecurityCenter scanner overview . . . 79
Adding a Tenable SecurityCenter scan . . . 79

Chapter 24. AXIS scanner . . . 81
Adding an AXIS vulnerability scan . . . 81

Chapter 25. Positive Technologies MaxPatrol . . . 83
Integrating Positive Technologies MaxPatrol with QRadar . . . 83
Adding a Positive Technologies MaxPatrol scanner . . . 83

Chapter 26. Scheduling a vulnerability scan. . . . 87

Chapter 27. Viewing the status of a vulnerability scan . . . 89

Chapter 28. Supported vulnerability scanners . . . 91

Notices . . . 93
Trademarks . . . 94
Privacy policy considerations . . . 95

Index . . . 97

Introduction to QRadar vulnerability assessment configurations

Integration with vulnerability assessment scanners provides administrators and security professionals information to build vulnerability assessment profiles for network assets.

Intended audience

Administrators must have QRadar® access and a knowledge of the corporate network and networking technologies.

Technical documentation

For information about how to access more technical documentation, technical notes, and release notes, see Accessing IBM® Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. Vulnerability assessment scanner overview

Integrate vulnerability assessment scanners with IBM Security QRadar to provide vulnerability assessment profiles for network assets.

References to QRadar apply to all products capable of collecting vulnerability assessment information.

Asset profiles for servers and hosts in your network provide information that can help you to resolve security issues. Using asset profiles, you can connect offenses that occur on your system to the physical or virtual assets as part of your security investigation. Asset data is helpful to identify threats, to identify vulnerabilities, services, ports, and monitor asset usage in your network.

The **Assets** tab provides a unified view of the information that is known about your assets. As more information is provided to the system through vulnerability assessment, the system updates the asset profile. Vulnerability assessment profiles use correlated event data, network activity, and behavioral changes to determine the threat level and vulnerabilities present on critical business assets in your network. You can schedule scans and ensure that vulnerability information is relevant for assets in the network.

Chapter 2. Beyond Security Automatic Vulnerability Detection System scanner overview

Vulnerability assessment is the evaluation of assets in the network to identify and prioritize potential security issues. QRadar products that support Vulnerability Assessment can import vulnerability data from external scanner products to identify vulnerabilities profiles for assets.

Vulnerability assessment profiles use correlated event data, network activity, and behavioral changes to determine the threat level and vulnerabilities present on critical business assets in your network. As external scanners generate scan data, QRadar can retrieve the vulnerability data with a scan schedule.

To configure a Beyond Security AVDS scanner, see "Adding a Beyond Security AVDS vulnerability scanner."

Adding a Beyond Security AVDS vulnerability scanner

Beyond Security Automated Vulnerability Detection System (AVDS) appliances create vulnerability data in Asset Export Information Source (AXIS) format. AXIS formatted files can be imported by XML files that can be imported.

About this task

To successfully integrate Beyond Security AVDS vulnerabilities with QRadar, you must configure your Beyond Security AVDS appliance to publish vulnerability data to an AXIS formatted XML results file. The XML vulnerability data must be published to a remote server that is accessible by using Secure File Transfer Protocol (SFTP). The term remote server refers to any appliance, third-party host, or network storage location that can host the published XML scan result files.

The most recent XML results that contain Beyond Security AVDS vulnerabilities are imported to when a scan schedule starts. Scan schedules determine the frequency with which vulnerability data created by Beyond Security AVDS is imported. After you add your Beyond Security AVDS appliance to QRadar, create a scan schedule to import the scan result files. Vulnerabilities from the scan schedule updates the **Assets** tab after the scan schedule completes.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your Beyond Security AVDS scanner.
5. From the **Managed Host** list, select the managed host from your QRadar deployment that manages the scanner import.
6. From the **Type** list, select **Beyond Security AVDS**.
7. In the **Remote Hostname** field, type the IP address or host name of the system that contains the published scan results from your Beyond Security AVDS scanner.
8. Choose one of the following authentication options:

Option	Description
Login Username	To authenticate with a user name and password: 1. In the **Login Username** field, type a username that has access to retrieve the scan results from the remote host. 2. In the **Login Password** field, type the password that is associated with the user name.
Enable Key Authorization	To authenticate with a key-based authentication file: 1. Select the **Enable Key Authentication** check box. 2. In the **Private Key File** field, type the directory path to the key file. The default directory for the key file is`/opt/qradar/conf/vis.ssh.key`. If a key file does not exist, you must create the vis.ssh.key file.

9. In the **Remote Directory** field, type the directory location of the scan result files.
10. In the **File Name Pattern** field, type a regular expression (regex) to filter the list of files that are specified in the Remote Directory. All matching files are included in the processing.

    The default value is `.*\.xml`. The `.*\.xml` pattern imports all xml files in the remote directory.
11. In the **Max Reports Age (Days)** field, type the maximum file age for your scan results file. Files that are older than the specified days and timestamp on the report file are excluded when the schedule scan starts. The default value is 7 days.
12. To configure the **Ignore Duplicates** option:
    - Select this check box to track files that are already processed by a scan schedule. This option prevents a scan result file from being processed a second time.
    - Clear this check box to import vulnerability scan results each time the scan schedule starts. This option can lead to multiple vulnerabilities associated with one asset.

    If a result file is not scanned within 10 days, the file is removed from the tracking list and is processed the next time the scan schedule starts.
13. To configure a CIDR range for your scanner:
    a. Type the CIDR range for the scan or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
14. Click **Save**.
15. On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to create a scan schedule. See Chapter 26, “Scheduling a vulnerability scan,” on page 87.

Chapter 3. Adding a Digital Defense Inc AVS scanner

You can add a Digital Defense Inc AVS scanner to your IBM Security QRadar deployment.

Before you begin

Before you add this scanner, a server certificate is required to support HTTPS connections. QRadar supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

About this task

At intervals that are determined by a scan schedule, QRadar imports the most recent XML results that contain Digital Defense Inc AVS vulnerabilities. To enable communication with the Digital Defense Inc AVS scanner, QRadar uses the credentials that you specify in the scanner configuration.

The following list provides more information about Digital Defense Inc AVS scanner parameters:

Remote Hostname
The host name of the remote server that hosts the Digital Defense Inc AVS scanner.

Remote Port
The port number of the remote server that hosts the Digital Defense Inc AVS scanner.

Remote URL
The URL of the remote server that hosts the Digital Defense Inc AVS scanner.

Client ID
The master client ID that uses to connect to the Digital Defense Inc AVS scanner.

Host Scope
When set to Internal, retrieves the active view for the internal hosts of the Digital Defense Inc AVS scanner. When set to External, retrieves the external active view of the Digital Defense Inc AVS scanner.

Retrieve Data For Account
The **Default** option indicates that the data is included from only the specified **Client ID**. If you want to include data from the Client ID and all its sub accounts, select **All Sub Accounts**. If you want to specify a single, alternate client ID, select **Alternate Client ID**.

Correlation Method

Specifies the method by which vulnerabilities are correlated.

- The **All Available** option queries the Digital Defense Inc vulnerability catalog and attempts to correlate vulnerabilities that are based on all the references that are returned for that specific vulnerability. References might include CVE, Bugtraq, Microsoft Security Bulletin, and OSVDB. Multiple references often correlate to the same vulnerability, but returns more results and take longer to process than the **CVE** option.
- The **CVE** option correlates vulnerabilities that are based only on the CVE-ID.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **VA Scanners** icon.
4. Click **Add**.
5. From the **Type** list box, select **Digital Defense Inc AVS**.
6. Configure the parameters.
7. To configure the CIDR ranges you want this scanner to consider, type the CIDR range, or click **Browse** to select the CIDR range from the network list.
8. Click **Add**.
9. Click **Save**.
10. On the **Admin** tab, click **Deploy Changes**.

What to do next

After you add your Digital Defense Inc AVS scanner, you can add a scan schedule to retrieve your vulnerability information.

Chapter 4. eEye scanner overview

QRadar can collect vulnerability data from eEye REM Security Management Console or eEye Retina CS scanners.

The following protocol options are available to collect vulnerability information from eEye scanners:

- Add an SNMP protocol eEye scanner. See "Adding an eEye REM SNMP scan."
- Add a JDBC protocol eEye scanner. See "Adding an eEye REM JDBC scan" on page 10

Adding an eEye REM SNMP scan

You can add a scanner to collect vulnerability data over SNMP from eEye REM or CS Retina scanners.

Before you begin

To use CVE identifiers and descriptions, you must copy the `audits.xml` file from your eEye REM scanner to the managed host responsible for listening for SNMP data. If your managed host is in a distributed deployment, you must copy the `audits.xml` to the Console first and SSH the file to `/opt/qradar/conf/audits.xml` on the managed host. The default location of `audits.xml` on the eEye scanner is `%ProgramFiles(x86)%\eEye Digital Security\Retina CS\Applications\RetinaManager\Database\audits.xml`.

To receive the most up-to-date CVE information, periodically update QRadar with the latest `audits.xml` file.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your SecureScout server.
5. From the **Managed Host** list, select the managed host from your QRadar deployment that manages the scanner import.
6. From the **Type** list, select **eEye REM Scanner**.
7. From the **Import Type** list, select **SNMP**.
8. In the **Base Directory** field, type a location to store the temporary files that contain the eEye REM scan data. The default directory is `/store/tmp/vis/eEye/`.
9. In the **Cache Size** field, type the number of transactions you want to store in the cache before the SNMP data is written to the temporary file. The default is 40. The default value is 40 transactions.
10. In the **Retention Period** field, type the time period, in days, that the system stores scan information. If a scan schedule did not import data before the retention period expires, the scan information from the cache is deleted.
11. Select the **Use Vulnerability Data** check box to correlate eEye vulnerabilities to Common Vulnerabilities and Exposures (CVE) identifiers and description information. .

12. In the **Vulnerability Data File** field, type the directory path to the eEye `audits.xml` file.
13. In the **Listen Port** field, type the port number that is used to monitor for incoming SNMP vulnerability information from your eEye REM scanner. The default port is 1162.
14. In the **Source Host** field, type the IP address of the eEye scanner.
15. From the **SNMP Version** list, select the SNMP protocol version. The default protocol is SNMPv2.
16. In the **Community String** field, type the SNMP community string for the SNMPv2 protocol, for example, `Public`.
17. From the **Authentication Protocol** list, select the algorithm to authenticate SNMPv3 traps.
18. In the **Authentication Password** field, type the password that you want to use to authenticate SNMPv3 communication. The password must include a minimum of 8 characters.
19. From the **Encryption Protocol** list, select the SNMPv3 decryption algorithm.
20. In the **Encryption Password** field, type the password to decrypt SNMPv3 traps.
21. To configure a CIDR range for your scanner:
    a. Type the CIDR range for the scan or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
22. Click **Save**.
23. On the **Admin** tab, click **Deploy Changes**.

What to do next

Select one of the following options:

- If you do not use SNMPv3 or use low-level SNMP encryption, you are now ready to create a scan schedule. See Chapter 26, “Scheduling a vulnerability scan,” on page 87.
- If your SNMPv3 configuration uses AES192 or AES256 encryption, you must install the unrestricted Java™ cryptography extension on each Console or managed host that receives SNMPv3 traps. See “Installing the unrestricted Java Cryptography Extension” on page 11.

Adding an eEye REM JDBC scan

You can add a scanner to collect vulnerability data over JDBC from eEye REM or CS Retina scanners.

Before you begin

Before you configure QRadar to poll for vulnerability data, we suggest you create a database user account and password for QRadar. If you assign the user account read-only permission to the RetinaCSDatabase, you can restrict access to the database that contains the eEye vulnerabilities. The JDBC protocol enables QRadar to log in and poll for events from the MSDE database. Ensure that no firewall rules block communication between the eEye scanner and the Console or managed host responsible for polling with the JDBC protocol. If you use database instances, you must verify port 1433 is available for the SQL Server Browser Service to resolve the instance name.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify the eEye scanner.
5. From the **Managed Host** list, select the managed host from the QRadar deployment that manages the scanner import.
6. From the **Type** list, select **eEye REM Scanner**.
7. From the **Import Type** list, select **JDBC**.
8. In the **Hostname** field, type the IP address or the host name of the eEye database.
9. In the **Port** field, type `1433`.
10. Optional. In the **Database Instance** field, type the database instance for the eEye database.

    If a database instance is not used, leave this field blank.
11. In the **Username** field, type the username required to query the eEye database.
12. In the **Password** field, type the password required to query the eEye database.
13. In the **Domain** field, type the domain required, if required, to connect to the eEye database.

    If the database is configured for Windows and inside a domain, you must specify the domain name.
14. In the **Database Name** field, type `RetinaCSDatabase` as the database name.
15. Select the **Use Named Pipe Communication** check box if named pipes are required to communicate to the eEye database. By default, this check box is clear.
16. Select the **Use NTLMv2** check box if the eEye scanner uses NTLMv2 as an authentication protocol. By default, this check box is clear.

    The Use NTLMv2 check box forces MSDE connections to use the NTLMv2 protocol when communicating with SQL servers that require NTLMv2 authentication. The Use NTLMv2 check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.
17. To configure a CIDR range for the scanner:
    a. In the text field, type the CIDR range you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
18. Click **Save**.
19. On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to create a scan schedule. See Chapter 26, “Scheduling a vulnerability scan,” on page 87.

Installing the unrestricted Java Cryptography Extension

The Java Cryptography Extension (JCE) is a Java framework that is required to decrypt advanced cryptography algorithms for AES 192-bit or AES 256-bit SNMPv3 traps.

Before you begin

Each managed host that receives SNMPv3 high-level traps requires the unrestricted JCE. If you require advanced cryptography algorithms for SNMP communication, you must update the existing cryptography extension on your managed host with an unrestricted JCE.

Procedure

1. Using SSH, log in to your QRadar Console.
2. To verify the version of Java on the Console, type the following command: `java -version`.

   The JCE file must match the version of the Java installed on the Console.
3. Download the latest version of the Java Cryptography Extension from the IBM website.

   https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk
4. Secure copy (SCP) the `local.policy.jar` and `US_export_policy.jar` file to the following directory of the Console: `/opt/ibm/java-[version]/jre/lib/security/`.
5. Optional. Distributed deployments require administrators to copy the `local.policy.jar` and `US_export_policy.jar` files from the Console appliance to the managed host.

What to do next

You are now ready to create a scan schedule. See Chapter 26, “Scheduling a vulnerability scan,” on page 87.

Chapter 5. IBM Security AppScan Enterprise scanner overview

QRadar retrieves AppScan Enterprise reports with the Representational State Transfer (REST) web service to import vulnerability data and generate offenses for your security team.

You can import scan results from IBM Security AppScan Enterprise report data, providing you a centralized security environment for advanced application scanning and security compliance reporting. You can import IBM Security AppScan Enterprise scan results to collect asset vulnerability information for malware, web applications, and web services in your deployment.

To integrate AppScan Enterprise with QRadar, you must complete the following tasks:

1. Generate scan reports in IBM AppScan Enterprise.

   Report configuration information can be found in your IBM Security AppScan Enterprise documentation.
2. Configure AppScan Enterprise to grant QRadar access to report data.
3. Configure your AppScan Enterprise scanner in QRadar.
4. Create a schedule in QRadar to import AppScan Enterprise results.

To configure IBM AppScan Enterprise to grant permission to report data, your AppScan administrator must determine which users have permissions to publish reports to QRadar. After AppScan Enterprise users configure reports, the reports that are generated by AppScan Enterprise can be published to QRadar, making them available for download.

To configure AppScan Enterprise to grant access to scan report data, see “Creating a customer user type for IBM AppScan.”

Creating a customer user type for IBM AppScan

You can create custom user types to assign permissions for limited and specific administrative tasks to administrators.

Procedure

1. Log in to your IBM AppScan® Enterprise appliance.
2. Click the **Administration** tab.
3. On the User Types page, click **Create** .
4. Select all of the following user permissions:
   - **Configure QRadar Integration** - Select this check box to allow users to access the QRadar integration options for AppScan Enterprise.
   - **Publish to QRadar** - Select this check box to allow QRadar access to published scan report data.
   - **QRadar Service Account** - Select this check box to add access to the REST API for the user account. This permission does not provide access the user interface.
5. Click **Save**.

What to do next

You are now ready to enable integration permissions. See “Enabling integration with IBM Security AppScan Enterprise”

Enabling integration with IBM Security AppScan Enterprise

IBM Security AppScan Enterprise must be configured to enable integration with QRadar.

Before you begin

To complete these steps, you must be logged in with a custom user type.

Procedure

1. Click the **Administration** tab.
2. On the **Navigation** menu, select **Network Security Systems**.
3. On the QRadar Integration Setting pane, click **Edit**.
4. Select the **Enable QRadar Integration** check box. Any reports that are previously published to QRadar are displayed. If any of the reports that are displayed are no longer required, you can remove them from the list. As you publish more reports to QRadar, the reports are displayed in this list.

What to do next

You are now ready to configure the Application Deployment Mapping in AppScan Enterprise. See “Creating an application deployment map in IBM Security AppScan Enterprise.”

Creating an application deployment map in IBM Security AppScan Enterprise

The Application Deployment Map allows AppScan Enterprise to determine the locations that host the application in your production environment.

About this task

As vulnerabilities are discovered, AppScan Enterprise knows the locations of the hosts and the IP addresses affected by the vulnerability. If an application is deployed to several hosts, then AppScan Enterprise generates a vulnerability for each host in the scan results.

Procedure

1. Click the **Administration** tab.
2. On the navigation menu, select **Network Security Systems**.
3. On the QRadar Integration Setting pane, click **Edit**.
4. In the **Application test location (host or pattern)** field, type the test location of your application.
5. In the **Application production location (host)** field, type the IP address of your production environment. To add vulnerability information to QRadar, your Application Deployment Mapping must include an IP address. If the IP address is not available in the AppScan Enterprise scan results, vulnerability data without an IP address is excluded from QRadar.

6. Click **Add**.
7. Repeat this procedure to map any more production environments in AppScan Enterprise.
8. Click **Done**.

What to do next

You are now ready to publish completed reports. See "Publishing completed reports in IBM AppScan."

Publishing completed reports in IBM AppScan

Completed vulnerability reports that are generated by AppScan Enterprise must be made accessible to QRadar by publishing the report.

Procedure

1. Click the **Jobs & Reports** tab.
2. Navigate to the security report you want to make available to QRadar.
3. On the menu bar of any security report, select **Publish** > **Grant** to provide report access to QRadar.
4. Click **Save**.

What to do next

You are now ready to enable integration permissions. See "Adding an IBM AppScan vulnerability scanner."

Adding an IBM AppScan vulnerability scanner

You can add a scanner to define which scan reports in IBM Security AppScan are collected by QRadar.

Before you begin

If your AppScan installation is set up to use HTPS, a server certificate is required. QRadar supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh` *`<IP or Hostname> <optional port - 443 default>`*. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

About this task

You can add multiple IBM AppScan scanners to QRadar, each with a different configuration. Multiple configurations provide QRadar the ability to import AppScan data for specific results. The scan schedule determines the frequency with which scan results are imported from the REST web service in IBM AppScan Enterprise.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your IBM AppScan Enterprise scanner.
5. From the **Managed Host** list, select the managed host from your QRadar deployment that manages the scanner import.
6. From the **Type** list, select **IBM AppScan Scanner**.
7. In the **ASE Instance Base URL** field, type the full base URL of the AppScan Enterprise instance. This field supports HTTP and HTTPS addresses, for example, `http://myasehostname/ase/`.
8. From the **Authentication Type** list, select one of the following options:
   - **Windows Authentication** - Select this option to use Windows Authentication with the REST web service.
   - **Jazz Authentication** - Select this option to use Jazz™ Authentication with the REST web service.
9. In the **Username** field, type the user name to retrieve scan results from AppScan Enterprise.
10. In the **Password** field, type the password to retrieve scan results from AppScan Enterprise.
11. In the **Report Name Pattern** field, type a regular expression (regex) to filter the list of vulnerability reports available from AppScan Enterprise. By default, the **Report Name Pattern** field contains **`.*`** as the regex pattern. The **`.*`** pattern imports all scan reports that are published to QRadar. All matching files from the file pattern are processed by QRadar. You can specify a group of vulnerability reports or an individual report by using a regex pattern.
12. To configure a CIDR range for your scanner:
    a. Type the CIDR range for the scanner or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
13. Click **Save**.
14. On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to create a scan schedule for IBM Security AppScan Enterprise. See Chapter 26, “Scheduling a vulnerability scan,” on page 87

Chapter 6. IBM Security Guardium scanner overview

IBM InfoSphere® Guardium® appliances are capable of exporting database vulnerability information that can be critical to protecting customer data.

IBM Guardium audit processes export the results of tests that fail the Common Vulnerability and Exposures (CVE) tests generated when running security assessment tests on your IBM Guardium appliance. The vulnerability data from IBM Guardium must be exported to a remote server or staging server in Security Content Automation Protocol (SCAP) format. QRadar can then retrieve the scan results from the remote server storing the vulnerability using SFTP.

IBM Guardium only exports vulnerability from databases containing failed CVE test results. If there are no failed CVE tests, IBM Guardium may not export a file at the end of the security assessment. For information on configuring security assessment tests and creating an audit process to export vulnerability data in SCAP format, see your IBM InfoSphere Guardium documentation.

After you have configured your IBM Guardium appliance, you are ready to configure QRadar to import the results from the remote server hosting the vulnerability data. You must add an IBM Guardium scanner to QRadar and configure the scanner to retrieve data from your remote server. The most recent vulnerabilities are imported by QRadar when you create a scan schedule. Scan schedules allow you to determine the frequency with which QRadar requests data from the remote server host your IBM Guardium vulnerability data.

Integration overview for IBM InfoSphere Guardium and QRadar.

1. On your IBM InfoSphere Guardium appliance, create an SCAP file with your vulnerability information. See your IBM Security InfoSphere Guardium documentation.
2. On your QRadar Console, add an IBM Guardium scanner. See "Adding an IBM Security Guardium vulnerability scanner"
3. On your QRadar Console, create a scan schedule to import scan result data. SeeChapter 26, "Scheduling a vulnerability scan," on page 87

Adding an IBM Security Guardium vulnerability scanner

Adding a scanner allows QRadar to collect SCAP vulnerability files from IBM InfoSphere Guardium.

About this task

Administrators can add multiple IBM Guardium scanners to QRadar, each with a different configuration. Multiple configurations provide QRadar the ability to import vulnerability data for specific results. The scan schedule determines the frequency with which the SCAP scan results are imported from IBM InfoSphere Guardium.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.

4. In the **Scanner Name** field, type a name to identify your IBM Guardium scanner.
5. From the **Managed Host** list, select the managed host from your QRadar deployment that manages the scanner import.
6. From the **Type** list, select **IBM Guardium SCAP Scanner**.
7. Choose one of the following authentication options:

Option	Description
Login Username	To authenticate with a user name and password: 1. In the **Login Username** field, type a username that has access to retrieve the scan results from the remote host. 2. In the **Login Password** field, type the password associated with the user name.
Enable Key Authorization	To authenticate with a key-based authentication file: 1. Select the **Enable Key Authentication** check box. 2. In the **Private Key File** field, type the directory path to the key file. The default is directory for the key file is`/opt/qradar/conf/vis.ssh`. If a key file does not exist, you must create the vis.ssh key file.

8. In the **Remote Directory** field, type the directory location of the scan result files.
9. In the **File Name Pattern** field, type a regular expression (regex) required to filter the list of SCAP vulnerability files specified in the **Remote Directory** field. All matching files are included in the processing. By default, the Report Name Pattern field contains `.*\.xml` as the regex pattern. The `.*\.xml` pattern imports all xml files in the remote directory.
10. In the **Max Reports Age (Days)** field, type the maximum file age for your scan results file. Files that are older than the specified days and timestamp on the report file are excluded when the schedule scan starts. The default value is 7 days.
11. To configure the **Ignore Duplicates** option:
    - Select this check box to track files that have already been processed by a scan schedule. This option prevents a scan result file from being processed a second time.
    - Clear this check box to import vulnerability scan results each time the scan schedule starts. This option can lead to multiple vulnerabilities being associated with an asset.

    If a result file is not scanned within 10 days, the file is removed from the tracking list and is processed the next time the scan schedule starts.
12. To configure a CIDR range for your scanner:
    a. In the text field, type the CIDR range you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
13. Click **Save**.

14. On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to create a scan schedule for IBM InfoSphere Guardium. See Chapter 26, “Scheduling a vulnerability scan,” on page 87

Chapter 7. IBM Security SiteProtector scanner overview

The IBM SiteProtector scanner module for QRadar accesses vulnerability data from IBM SiteProtector™ scanners through Java Database Connectivity (JDBC) queries.

The IBM SiteProtector scanner retrieves vulnerability data from the RealSecureDB table and polls for new vulnerabilities each time a scan schedule starts. The **Compare** field enables the query to retrieve any new vulnerabilities from the RealSecureDB table to ensure that duplicate vulnerabilities are not imported. When the IBM SiteProtector scanner is configured, the administrator can create a SiteProtector user account specifically for polling vulnerability data. After the user account is created, the administrator can verify that there are no firewalls that reject queries on the port configured to poll the database.

To configure an IBM Security SiteProtector scanner, see "Adding an IBM SiteProtector vulnerability scanner."

Adding an IBM SiteProtector vulnerability scanner

QRadar can poll IBM InfoSphere SiteProtector appliances for vulnerability data with JDBC.

About this task

Administrators can add multiple IBM SiteProtector scanners to QRadar, each with a different configuration. Multiple configurations provide QRadar with the ability to query SiteProtector and only import results from specific CIDR ranges. The scan schedule determines the frequency with which the database on the SiteProtector scanner is queried for vulnerability data.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify the IBM SiteProtector scanner.
5. From the **Managed Host** list, select the managed host from the QRadar deployment that manages the scanner import.
6. From the **Type** list, select **IBM SiteProtector Scanner**.
7. In the **Hostname** field, type the IP address or host name of the IBM SiteProtector that contains vulnerabilities to import.
8. In the **Port** field, type `1433` as the port for the IBM SiteProtector database.
9. In the **Username** field, type the username required to query the IBM SiteProtector database.
10. In the **Password** field, type the password required to query the IBM SiteProtector database.
11. In the **Domain** field, type the domain required, if required, to connect to the IBM SiteProtector database.

    If the database is configured for Windows and inside a domain, you must specify the domain name.

12. In the **Database Name** field, type `RealSecureDB` as the database name.
13. In the **Database Instance** field, type the database instance for the IBM SiteProtector database. If you are not using a database instance, you can leave this field blank.
14. Select the **Use Named Pipe Communication** if named pipes are required to communicate to the IBM SiteProtector database. By default, this check box is clear.
15. Select the **Use NTLMv2** check box if the IBM SiteProtector uses NTLMv2 as an authentication protocol. By default, this check box is clear.

    The Use NTLMv2 check box forces MSDE connections to use the NTLMv2 protocol when communicating with SQL servers that require NTLMv2 authentication. The Use NTLMv2 check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.
16. To configure a CIDR range for the scanner:
    a. In the text field, type the CIDR range for the scan or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
17. Click **Save**.
18. On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to create a scan schedule. See Chapter 26, “Scheduling a vulnerability scan,” on page 87

Chapter 8. IBM Security Tivoli Endpoint Manager scanner overview

The IBM Tivoli® Endpoint Manager scanner module accesses vulnerability data from IBM Tivoli Endpoint Manager using the SOAP API installed with the Web Reports application.

The Web Reports application for Tivoli Endpoint Manager is required to retrieve vulnerability data from Tivoli Endpoint Manager for QRadar. Administrators can create a user in IBM Tivoli Endpoint Manager for QRadar to use when the system collects vulnerabilities.

Note: QRadar is compatible with IBM Tivoli Endpoint Manager versions 8.2.x. However, administrators can use the latest version of IBM Tivoli Endpoint Manager that is available.

To add an IBM Tivoli Endpoint Manager scanner, see “Adding an IBM Security Tivoli Endpoint Manager vulnerability scanner”

Adding an IBM Security Tivoli Endpoint Manager vulnerability scanner

QRadar accesses vulnerability data from IBM Tivoli Endpoint Manager by using the SOAP API installed with the Web Reports application.

About this task

You can add multiple IBM Tivoli Endpoint Manager scanners in QRadar. Each scanner requires a different configuration to determine which CIDR ranges you want the scanner to consider.

Use multiple configurations for a single IBM Tivoli Endpoint Manager scanner to create individual scanners that collect specific result data from specific locations or vulnerabilities for specific types of operating systems.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your IBM Tivoli Endpoint Manager.
5. From the **Managed Host** list, select the managed host from your QRadar deployment that manages the scanner import.
6. From the **Type** list, select **IBM Tivoli Endpoint Manager**.
7. In the **Hostname** field, type the IP address or host name of the IBM Tivoli Endpoint Manager containing the vulnerabilities that you want to retrieve with the SOAP API.
8. In the **Port** field, type the port number that is used to connect to the IBM Tivoli Endpoint Manager by using the SOAP API. By default, port 80 is the port number for communicating with IBM Tivoli Endpoint Manager. If you use HTTPS, you must update this field with the HTTPS port number. For most configuration, use port 443.

9. Select the **Use HTTPS** check box to connect securely with the HTTPS protocol.

   If you select this check box, the host name or IP address that you specify uses HTTPS to connect to your IBM Tivoli Endpoint Manager. When you use HTTPS, a server certificate is required. Certificates must be placed in `/opt/qradar/conf/trusted_certificates` folder. QRadar supports certificates with the following file extensions: .crt, .cert, or .der. You can either use SCP or SFTP to manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory. Alternatively, you can download a copy of the certificate directly from the QRadar host. To do this, use SSH to connect the host and type the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into the `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.
10. In the **Username** field, type the user name access IBM Tivoli Endpoint Manager.
11. In the **Password** field, type the password that is required to access IBM Tivoli Endpoint Manager.
12. To configure a CIDR range for your scanner:
    a. In the text field, type the CIDR range that you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
13. Click **Save**.
14. On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to create a scan schedule for IBM Security Tivoli Endpoint Manager. See Chapter 26, “Scheduling a vulnerability scan,” on page 87

Chapter 9. Foundstone FoundScan scanner overview

The Foundstone FoundScan scanner queries the FoundScan Engine for host and vulnerability information from the FoundScan OpenAPI.

QRadar supports Foundstone FoundScan versions 5.0 to 6.5.

The FoundScan appliance must include a scan configuration that runs regularly to keep the host and vulnerability results current. To ensure that the FoundScan scanner is able to retrieve scan information, make sure the FoundScan system meets the following requirements:

- The FoundScan application must be active. Since the API provides access to the FoundScan application, administrators can verify that the FoundScan application runs continuously on the FoundScan server.
- The scan data to import must be complete and visible in the FoundScan user interface to retrieve scan results. If the scan is scheduled to be removed after completion, the results must be imported by the scan schedule before the scan is removed from FoundScan.
- The appropriate user privileges must be configured in the FoundScan application to enable communication between QRadar and FoundScan. The FoundScan OpenAPI provides host and vulnerability information. All vulnerabilities for a host assigned are assigned to port 0.

To connect to FoundScan, the FoundScan Engine requires authentication with client-side certificates. FoundScan includes a default certificate authority and client certificates that are the same for all scanner installations. The FoundScan plug-in also includes certificates for use with FoundScan 5.0. If the FoundScan Server uses custom certificates, administrators must import the appropriate certificates and keys. Instructions on how to import certificates is provided in this configuration documentation.

To add a FounScan API vulnerability scan, see “Adding a Foundstone FoundScan scanner.”

Adding a Foundstone FoundScan scanner

Administrators can add a Foundstone FoundScan scanner to collect host and vulnerability information through the FoundScan OpenAPI.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your FoundScan server.
5. From the **Managed Host** list, select the managed host from your QRadar deployment that manages the scanner import. Certificates for your FoundScan scanner must reside on the managed host selected in the Managed Host list box.
6. From the **Type** list, select **FoundScan Scanner**.
7. In the **SOAP API URL** field, type the IP address or hostname of the Foundstone FoundScan that contains the vulnerabilities you want to retrieve

with the SOAP API. For example, `https://foundstone IP address:SOAP port` The default value is `https://localhost:3800.`

8. In the **Customer Name** field, type the name of the customer that belongs to the user name.
9. In the **User Name** field, type the username required to access the Foundstone FoundScan server.
10. Optional. In the **Client IP Address** field, type the IP address of the server that you want to perform the scan. By default, this value is not used; however, is necessary when administrators validate some scan environments.
11. Optional. In the **Password** field, type the password required to access the Foundstone FoundScan server.
12. In the **Portal Name** field, type the portal name. This field can be left blank for QRadar. See your FoundScan administrator for more information.
13. In the **Configuration Name** field, type the scan configuration name that exists in FoundScan and to which the user has access. Make sure this scan configuration is active or runs frequently.
14. In the **CA Truststore** field, type the directory path and filename for the CA truststore file. The default path is `/opt/qradar/conf/foundscan.keystore`.
15. In the **CA Keystore** field, type the directory path and filename for the client keystore. The default path is `/opt/qradar/conf/foundscan.truststore`.
16. To configure a CIDR range for the scanner:
    a. In the text field, type the CIDR range for the scanner to consider or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
17. Click **Save**.
18. On the **Admin** tab, click **Deploy Changes**.

What to do next

Administrators can now import certificates from your FoundScan server to enable communication. See "Importing certificates for Foundstone FoundScan."

Importing certificates for Foundstone FoundScan

Administrators that use custom certificates or a version of Foundstone FoundScan lower than V5.0 must import the appropriate certificates to the managed host from the scanner configuration.

Before you begin

The scanner must be add to a managed host in the scan configuration before certificates are imported from the FoundScan server. The certificates must be imported to the correct managed host to collect vulnerability and host scan data.

Procedure

1. Obtain the two certificate files and the pass phrase from your FoundScan administrator.
   - The `TrustedCA.pem` file is the CA certificate for the FoundScan engine.
   - The `Portal.pem`file certificate is the private key that includes the certificate chain for the client.

2. Using SSH, copy the two pem files to the managed host assigned in your FoundScan configuration. If you have a distributed deployment, you must copy the files to the Console and SSH the files from the Console appliance to the managed host.
3. Navigate to the directory location of the pem files.
4. To remove the previous keystore certificate from the managed host, type the following command: `rm -f /opt/qradar/conf/foundscan.keystore`
5. To remove the previous truststore certificate from the managed host, type the following command: `rm -f /opt/qradar/conf/foundscan.truststore`
6. To import the pem files to your managed host, type the following command: `/opt/qradar/bin/foundstone-cert-import.sh [TrustedCA.pem] [Portal.pem]`
7. Repeat the certificate import for any more managed hosts in your deployment that connect to the Foundstone FoundScan appliance.

What to do next

You are now ready to create a scan schedule. See Chapter 26, “Scheduling a vulnerability scan,” on page 87.

Chapter 10. Microsoft SCCM scanner overview

IBM Security QRadar can import scan reports from Microsoft System Center Configuration Manager (SCCM) scanners.

To integrate an Microsoft SCCM scanner, perform the following steps:

1. On your Microsoft SCCM scanner, configure WMI. See Chapter 11, “WMI enablement on scanner host,” on page 31.
2. If automatic updates are not enabled on your QRadar Console, download and install the Microsoft SCCM RPM.
3. On yourQRadar Console, add an Microsoft SCCM scanner. See Chapter 12, “Adding a Microsoft SCCM scanner,” on page 33.
4. On your QRadar Console, create a scan schedule to import scan result data. See Chapter 26, “Scheduling a vulnerability scan,” on page 87.

Chapter 11. WMI enablement on scanner host

Before you can configure a Microsoft SCCM scanner, you must configure your system DCOM settings for each host you want to monitor.

Ensure that the scanner host meets the following conditions:

- You are a member of the Administrators group on that host.
- One the following operating systems is installed:
  - Windows 2000
  - Windows 2003
  - Windows 2008
  - XP
  - Vista software
  - Windows 7

  Note: 32-bit and 64-bit operating systems are supported.
- DCOM is configured and enabled.

  If a firewall is installed on the host or is located between the host and QRadar (such as a hardware or other intermediary firewall), the firewall must be configured to allow DCOM communication. Configure the firewall to allow port 135 to be accessible on the host and allow DCOM ports (random ports above 1024). Depending on the version of Windows that you use, you might also need to configure specific ports to be accessible to DCOM. For more information, see your Windows documentation.
- Windows Management Instrumentation (WMI) is enabled.
- The remote registry service is activated.

For specific instructions about how to configure DCOM and WMI on Windows 2008 and Windows 7, see the documents on the IBM support website:

- Windows 2008 (http://www-01.ibm.com/support/docview.wss?uid=swg21681046)
- Windows 7 (http://www-01.ibm.com/support/docview.wss?uid=swg21678809)

Chapter 12. Adding a Microsoft SCCM scanner

Before you begin

Ensure that WMI is enabled on your scanner host.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. Configure the following Microsoft SCCM parameters:

Parameter	Description
Scanner Name	The name to identify your scanner instance.
Managed Host	The managed host from your QRadar deployment that manages the scanner import.
Type	Microsoft SCCM
Host Name	The IP address or host name of the remote server that hosts the scan result files.
Domain	The domain used to connect to the remote server.

5. Configure the remaining parameters.
6. To configure a CIDR range for your scanner:
   a. Type the CIDR range that you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
   b. Click **Add**.
7. Click **Save**.

Chapter 13. nCircle IP360 scanner overview

QRadar can import XML2 scan reports from SSH servers that contain nCircle IP360 vulnerability information.

QRadar cannot connect directly with nCircle devices. You can configure an nCircle IP360 scanner device to export scan results in XML2 format to a remote SSH server. To import the most recent scan results from the remote server to QRadar, you can schedule a scan or poll the remote server for updates to the scan results.

The scan results contain identification information about the scan configuration from which it was produced. The most recent scan results are used when QRadar imports a scan. QRadar supports exported scan results only from the IP360 scanner in XML2 format.

To integrate an nCircle IP360 scanner, perform the following steps:

1. On your nCircle IP360 scanner, configure your nCircle scanner to export scan reports. See "Exporting nCircle IP360 scan results to an SSH server."
2. On yourQRadar Console, add an nCircle IP360 scanner. See "Adding a nCircle IP360 scanner"
3. On your QRadar Console, create a scan schedule to import scan result data. SeeChapter 26, "Scheduling a vulnerability scan," on page 87

Exporting nCircle IP360 scan results to an SSH server

QRadar uses an automated export function to publish XML2 scan data from nCircle IP360 appliances. QRadar supports VnE Manager version IP360-6.5.2 to 6.8.2.8.

Before you begin

Ensure that the remote server is a UNIX system with SSH enabled.

Procedure

1. Log in to the IP360 VNE Manager user interface.
2. From the navigation menu, select **Administer** > **System** > **VNE Manager** > **Automated Export**.
3. Click the **Export to File** tab.
4. Configure the export settings. The export must be configured to use the XML2 format.
5. Record the target settings that are displayed in the user interface for the scan export. These settings are necessary to configure QRadar to integrate with your nCircle IP360 device.

Adding a nCircle IP360 scanner

QRadar uses a Secure Shell (SSH) to access a remote server (SSH export server) to retrieve and interpret the scan data from nCircle IP360 appliances. QRadar supports VnE Manager version IP360-6.5.2 to 6.8.2.8.

Before you begin

This configuration requires the target settings that you recorded when you exported the XML2 scan data to the remote server.

About this task

If the scanner is configured to use a password, the SSH scanner server to which QRadar connects must support password authentication. If it does not, SSH authentication for the scanner fails. Make sure the following line is displayed in your `sshd_config` file, which is typically found in the `/etc/ssh directory` on the SSH server: `PasswordAuthentication yes`. If your scanner server does not use OpenSSH, the configuration can differ. For more information, see the vendor documentation for your scanner.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. Configure the following nCircle IP360 parameters:

Parameter	Description
Scanner Name	The name to identify your nCircle IP360 instance.
Managed Host	The managed host from your QRadar deployment that manages the scanner import.
Type	nCircle IP360
SSH Server Host Name	The IP address or host name of the remote server that hosts the scan result files.
SSH Port	The port number to connect to the remote server.
Remote Directory	The location of the scan result files.
File Pattern	The regular expression (regex) to filter the list of files that are specified in the **Remote Directory** field. To list all XML2 format files that end with XML, use the following entry: `XML2.*\.xml`

5. Configure the remaining parameters.
6. To configure a CIDR range for your scanner:
   a. Type the CIDR range that you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
   b. Click **Add**.
7. Click **Save**.
8. On the **Admin** tab, click **Deploy Changes**.

Chapter 14. Nessus scanner overview

QRadar can retrieve vulnerability scan reports about your network assets by leveraging the Nessus client and server relationship or by using the Nessus XMLRPC API to access scan data directly from Nessus.

When you configure your Nessus client, administrators can create a Nessus user account for your QRadar system. A unique user account ensures that QRadar possesses the credentials required to log in and communicate with the Nessus server. After the administrator creates the user account, a test of the connection from QRadar to your Nessus client with SSH can verify the user credentials and remote access. This ensures that each system can communicate before an attempt is made to collect scan data or start a live scan. The Nessus XMLRPC API is only available on Nessus servers and clients with software V4.2 and higher.

Note: Administrators should not install Nessus software on a critical system due to the CPU requirements when scans are active.

The following options are available for data collection of vulnerability information from Nessus scanners:

- Scheduled live scan. Live scans enable predefined scans to be started remotely over SSH in Nessus and the data imported at the completion of the scan. See "Adding a Nessus scheduled live scan."
- Live Scan API imports. The XMLRPC API enables predefined scans to be started remotely and actively collected. See"Adding a Nessus live scan with the XMLRPC API" on page 39
- Scheduled result imports. Static result files from completed scans are imported from a repository over SSH that contains the Nessus scan results. See "Adding a Nessus scheduled result import" on page 40
- Scheduled completed report API import. The XMLPRC API enables completed reports to be imported from the Nessus server. See "Adding a Nessus completed report import with the XMLRPC API" on page 42.

Adding a Nessus scheduled live scan

A live scan runs on your Nessus server and imports the result data from a temporary directory on the Nessus client that contains the scan report data.

Before you begin

Before you add this scanner, a server certificate is required to support HTTPS connections. QRadar supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your Nessus scanner.
5. From the **Managed Host** list, select the managed host from your QRadar deployment that manages the scanner import.
6. From the **Type** list, select **Nessus Scanner**.
7. From the **Collection Type** list, select **Scheduled Live Scan - XMLRPC API**.
8. In the **Hostname** field, type the IP address or hostname of the Nessus server.
9. In the **Port** field, type the port number the Nessus server. The default API port value is 8843.
10. In the **Server Username** field, type the user name to access Nessus server.
11. In the **Server Password** field, type the password to access Nessus server. Your Nessus server password must not contain the exclamation mark (!) character or authentication failures can occur over SSH.
12. In the **Client Temp Dir** field, type the directory path of the Nessus client that QRadar can use to store temporary files. QRadar uses the temporary directory of the Nessus client as a read and write location to upload scan targets and read scan results. Temporary files are removed from the client's temporary directory when the scan completes and the scan report is downloaded. The default directory path on the Nessus client is `/tmp`.
13. In the **Nessus Executable** field, type the directory path to the executable file on the Nessus server. By default, the directory path to the executable file is `/usr/bin/nessus`.
14. In the **Nessus Configuration File** field, type the directory path to the Nessus configuration file on the Nessus client.
15. In the **Client Hostname** field, type the hostname or IP address of the Nessus client.
16. In the **Client SSH Port** field, type the number of the SSH port on the Nessus server that can be used to retrieve scan result files. The default value is port 22.
17. In the **Client Username** field, type the user name to authenticate the SSH connection.
18. In the **Client Password** field, type the password that corresponds to the **Client Username** field. If the **Enable Key Authentication** field is enabled, the password is ignored. If the scanner is configured to use a password, the SSH scanner server to that connects to QRadar must support password authentication. If it does not, SSH authentication for the scanner fails. Ensure the following line is displayed in your `/etc/ssh/sshd_config` file: `PasswordAuthentication yes`. If your scanner server does not use OpenSSH, see the vendor documentation for the scanner configuration information.
19. If your system uses key authentication, select the **Enable Key Authentication** check box.
20. For key authentication systems: in the **Private Key File** field, type the directory path to the key file. The default directory for the key file `is/opt/qradar/conf/vis.ssh.key`. If a key file does not exist, you must create the vis.ssh.key file.

21. In the **CIDR Mask** field, type the size of the subnet scanned. The value that is specified for the mask represents the largest portion of the subnet the scanner can scan at one time. The mask segments the scan to optimize the scan performance.
22. To configure a CIDR range for your scanner:
    a. In the text field, type the CIDR range that you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
23. Click **Save**.
24. On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to create a scan schedule for your Nessus scanner. See Chapter 26, "Scheduling a vulnerability scan," on page 87

Adding a Nessus live scan with the XMLRPC API

The XMLRPC API enables QRadar to start a pre-configured scan that is based on a scan name and optional policy name on the Nessus server.

Before you begin

Before you add this scanner, a server certificate is required to support HTTPS connections. QRadar supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

About this task

To start a live scan from QRadar, you must specify the scan name and the policy name for the live scan data you want to retrieve. As the live scan progresses, you can place your mouse over your Nessus scanner in the Scan Scheduling window to view the percentage of the live scan that is complete. After the live scan reaches completion, QRadar uses the XMLRPC API to retrieve the scan data and update the vulnerability information for your assets.

The Nessus XMLRPC API is only available on Nessus servers and clients with software v4.2 and higher.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your Nessus scanner.

5. From the **Managed Host** list, select the managed host from your QRadar deployment that manages the scanner import.
6. From the **Type** list, select **Nessus Scanner**.
7. From the **Collection Type** list, select **Scheduled Live Scan - XMLRPC API**.
8. In the **Hostname** field, type the IP address or hostname of the Nessus server.
9. In the **Port** field, Type the port number the Nessus server. The default API port value is 8843.
10. In the **Username** field, type the user name to access Nessus server.
11. In the **Password** field, type the password to access Nessus server. Your Nessus server password must not contain the exclamation mark (!) character or authentication failures can occur over SSH.
12. Optional: In the **Scan Name** field, type the name of the scan you want displayed when the live scan runs on the Nessus server. If this field is clear, the API attempts to start a live scan for QRadar Scan. This field does not support by using the ampersand (&) character in this field.
13. In the **Policy Name** field, type the name of a policy on your Nessus server to start a live scan. The policy must exist on the Nessus server when the system attempts to start the scan. If the policy does not exist, then an error is displayed in the Status column. It is common for systems to have custom policy names, but several default policy names are included. `External Network Scan`, `Internal Network Scan`, `Web App Tests`, `Prepare for PCI DSS audits` are default policy names.
14. To configure a CIDR range for your scanner:
    a. In the text field, type the CIDR range that you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
15. Click **Save**.
16. On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to create a scan schedule for your Nessus scanner. See Chapter 26, “Scheduling a vulnerability scan,” on page 87

Adding a Nessus scheduled result import

A scheduled results import retrieves completed Nessus scan reports from an external location.

Before you begin

Before you add this scanner, a server certificate is required to support HTTPS connections. QRadar supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

About this task

The external location can be a Nessus server or a file repository that contains a completed scan report. QRadar connects to the location of your scan reports by using SSH and imports completed scan report files from the remote directory by using a regular expression or maximum report age to filter for your reports. QRadar supports imports of Nessus scan reports in `.nessus` format or scan reports that are exported to a Nessus output format, such as XML2.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your Nessus scanner.
5. From the **Managed Host** list, select the managed host from your QRadar deployment that manages the scanner import.
6. From the **Type** list, select **Nessus Scanner**.
7. From the **Collection Type** list, select **Scheduled Results Import**.
8. In the **Remote Results Hostname** field, type the IP address or hostname of the Nessus client or server that hostsyour Nessus or XML2 scan result files.
9. Choose one of the following authentication options:

Option	Description
Login Username	To authenticate with a user name and password: 1. In the **SSH Username** field, type the user name to access the Nessus scanner or the repository that hosts the scan result files. 2. In the **SSH Password** field, type the password that is associated with the user name. The password must not contain the exclamation mark (!) character. This character might cause authentication failures over SSH.
Enable Key Authorization	To authenticate with a key-based authentication file: 1. Select the **Enable Key Authentication** check box. 2. In the **Private Key File** field, type the directory path to the key file. The default directory for the key file is`/opt/qradar/conf/vis.ssh.key`. If a key file does not exist, you must create the vis.ssh.key file.

10. In the **Remote Results Directory** field, type the directory location of the scan result files. The default directory path is `./`.
11. In the **File Name Pattern** field, type a regular expression (regex) to filter the list of files that are specified in the Remote Directory. All matching files are included in the processing. By default, the **Report Name Pattern** field contains

`.*\.nessus` as the regex pattern. The `.*\.nessus` pattern imports all Nessus formatted result files in the remote directory.

12. In the **Max Reports Age (Days)** field, type the maximum file age for your scan results file. Files that are older than the specified days and time stamp on the report file are excluded when the schedule scan starts. The default value is 7 days.
13. To configure a CIDR range for your scanner:
    a. In the text field, type the CIDR range that you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
14. Click **Save**.
15. On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to create a scan schedule for IBM Security Tivoli Endpoint Manager. See Chapter 26, "Scheduling a vulnerability scan," on page 87

Adding a Nessus completed report import with the XMLRPC API

A scheduled results import using the XMLRPC API enables completed vulnerability reports to be downloaded from the Nessus server.

Before you begin

Before you add this scanner, a server certificate is required to support HTTPS connections. QRadar supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

About this task

QRadar connects to your Nessus server and downloads data from any completed reports matching the report name and maximum report age filter. The Nessus XMLRPC API is available on Nessus servers and clients using software v4.2 and higher.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your Nessus server.
5. From the **Managed Host** list, select the managed host from your QRadar deployment that manages the scanner import.

6. From the **Type** list, select **Scheduled Completed Report Import - XMLRPC AP**.
7. In the **Hostname** field, type the IP address or hostname of the IBM Tivoli Endpoint Manager containing the vulnerabilities you want to retrieve with the SOAP API.
8. In the **Port** field, type the port number the Nessus server. The default API port value is 8843.
9. In the **Username** field, type the username required to access the Nessus server.
10. In the **Password** field, type the password required to access the Nessus server.
11. In the **Report Name Pattern** field, type a regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing. By default, the Report Name Pattern field contains `.*` as the regex pattern. The `.*` pattern imports all nessus formatted result files in the remote directory.
12. In the **Max Reports Age (Days)** field, type the maximum file age for your scan results file. Files that are older than the specified days and timestamp on the report file are excluded when the schedule scan starts. The default value is 7 days.
13. To configure a CIDR range for your scanner:
    a. In the text field, type the CIDR range you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
14. Click **Save**.
15. On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to create a scan schedule. See Chapter 26, “Scheduling a vulnerability scan,” on page 87

Chapter 15. Nmap scanner overview

QRadar uses SSH to communicate with the Nmap server to either start remote Nmap scans or download the completed Nmap scan results.

When administrators configure an Nmap scan, a specific Nmap user account can be created for the QRadar system. A unique user account ensures that QRadar possesses the credentials required to log in and communicate with the Nmap server. After the user account creation is complete, administrators can test the connection from QRadar to the Nmap client with SSH to verify the user credentials. This ensures that each system can communicate before the system attempt to download vulnerability scan data or start a live scan.

The following options are available for data collection of vulnerability information from Nmap scanners:

- Remote live scan. Live scans use the Nmap binary file to remotely start scans. After the live scan completes, the data is imported over SSH. See "Adding a Nmap remote live scan" on page 47.
- Remote results import. The result data from a previously completed scan is imported over SSH. See "Adding a Nmap remote result import"

Adding a Nmap remote result import

A remote results import retrieves completed Nmap scan reports over SSH.

About this task

Scans must be generated in XML format using the `-oX` option on your Nmap scanner. After you add your Nmap scanner, you must assign a scan schedule to specify the frequency that the vulnerability data is imported from scanner.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your Nmap scanner.
5. From the **Managed Host** list, select the managed host from your QRadar deployment that manages the scanner import.
6. From the **Type** list, select **Nessus Scanner**.
7. From the **Collection Type** list, select **Remote Results Import**.
8. In the **Server Hostname** field, type the hostname or IP address of the remote system that hosts the Nmap client. We suggest that administrators host Nmap on a UNIX-based system with SSH enabled.
9. Choose one of the following authentication options:

Option	Description
Login Username	To authenticate with a user name and password: 1. In the **Server Username** field, type the username required to access the remote system hosting the Nmap client. 2. In the **Login Password** field, type the password associated with the user name. The password must not contain the ! character. This character could cause authentication failures over SSH. If the scanner is configured to use a password, the SSH scanner server to that connects to QRadar must support password authentication. If it does not, SSH authentication for the scanner fails. Ensure the following line is displayed in your `/etc/ssh/sshd_config` file: `PasswordAuthentication yes`. If your scanner server does not use OpenSSH, see the vendor documentation for the scanner configuration information.
Enable Key Authorization	To authenticate with a key-based authentication file: 1. Select the **Enable Key Authentication** check box. 2. In the **Private Key File** field, type the directory path to the key file. The default is directory for the key file is`/opt/qradar/conf/vis.ssh.key`. If a key file does not exist, you must create the vis.ssh.key file.

10. In the **Remote Folder** field, type the directory location of the scan result files.
11. In the **Remote File Pattern** field, type a regular expression (regex) required to filter the list of files specified in the remote folder. All matching files are included in the processing. The default regex pattern to retrieve Nmap results is `.*\.xml`. The `.*\.xml` pattern imports all xml result files in the remote folder. Scan reports imported and processed are not deleted from the remote folder. We suggest that you schedule a cron job to delete previously processed scan reports.
12. To configure a CIDR range for your scanner:
    a. In the text field, type the CIDR range you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
13. Click **Save**.
14. On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to create a scan schedule. See Chapter 26, “Scheduling a vulnerability scan,” on page 87

Adding a Nmap remote live scan

monitors the status of the live scan in progress and waits for the Nmap server to complete the scan. After the scan completes, the vulnerability results are downloaded over SSH.

About this task

Several types of Nmap port scans require Nmap to run as a root user. Therefore, QRadar must have access as root or you must clear the **OS Detection** check box. To run Nmap scans with OS Detection enabled, you must provide root access credentials to QRadar when you add the scanner. Alternately, you can have your administrator configure the Nmap binary with setuid root. See your Nmap administrator for more information.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your Nmap scanner.
5. From the **Managed Host** list, select the managed host from your QRadar deployment that manages the scanner import.
6. From the **Type** list, select **Nmap Scanner**.
7. From the **Scan Type** list, select **Remote Live Scan**.
8. In the **Server Hostname** field, type the IP address or hostname of the Nmap server.
9. Choose one of the following authentication options:

Option	Description
Server Username	To authenticate with a user name and password: 1. In the **Server Username** field, type the username required to access the remote system hosting the Nmap client using SSH. 2. In the **Login Password** field, type the password associated with the user name. If the **OS Detection** check box is selected, the username must have root privileges.

Option	Description
Enable Key Authorization	To authenticate with a key-based authentication file: 1. Select the **Enable Key Authentication** check box. 2. In the **Private Key File** field, type the directory path to the key file. The default is directory for the key file is`/opt/qradar/conf/vis.ssh.key`. If a key file does not exist, you must create the vis.ssh.key file. If the scanner is configured to use a password, the SSH scanner server to that connects to QRadar must support password authentication. If it does not, SSH authentication for the scanner fails. Ensure the following line is displayed in your `/etc/ssh/sshd_config` file: `PasswordAuthentication yes`. If your scanner server does not use OpenSSH, see the vendor documentation for the scanner configuration information.

10. In the **Nmap Executable** field, type the full directory path and filename of the Nmap binary file. The default directory path to the binary file is `/usr/bin/Nmap`.
11. Select an option for the **Disable Ping** check box. In some networks, the ICMP protocol is partially or completely disabled. In situations where ICMP is not enabled, you can select this check box to enable ICMP pings to enhance the accuracy of the scan. By default, the check box is clear.
12. Select an option for the **OS Detection** check box:
    - Select this check box to enable operating system detection in Nmap. You must provide the scanner with root privileges to use this option.
    - Clear this check box to receive Nmap results without operating system detection.
13. From the **Max RTT Timeout** list, select a timeout value. The timeout value determines if a scan should be stopped or reissued due to latency between the scanner and the scan target. The default value is 300 milliseconds (ms). If you specify a timeout period of 50 milliseconds, then we suggest that the devices that are scanned be in the local network. Devices in remote networks can use a timeout value of 1 second.
14. Select an option from the **Timing Template** list. The options include:
    - Paranoid - This option produces a slow, non-intrusive assessment.
    - Sneaky - This option produces a slow, non-intrusive assessment, but waits 15 seconds between scans.
    - Polite - This option is slower than normal and intended to ease the load on the network.
    - Normal - This option is the standard scan behavior.
    - Aggressive - This option is faster than a normal scan and more resource intensive.

- Insane - This option is not as accurate as slower scans and only suitable for very fast networks.
-

15. In the **CIDR Mask** field, type the size of the subnet scanned. The value specified for the mask represents the largest portion of the subnet the scanner can scan at one time. The mask segments the scan to optimize the scan performance.
16. To configure a CIDR range for your scanner:
    a. In the text field, type the CIDR range you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
17. Click **Save**.
18. On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to create a scan schedule. See Chapter 26, “Scheduling a vulnerability scan,” on page 87

Chapter 16. Qualys scanner overview

QRadar can retrieve vulnerability information from the QualysGuard Host Detection List API or download scan reports directly from a QualysGuard appliance. QRadar supports integration with QualysGuard appliances that use software version 4.7 through 7.10.

Qualys Detection Scanners

Add a Qualys Detection Scanner if you want to use the QualysGuard Host Detection List API to query multiple scan reports to collect vulnerability data for assets. The data that the query returns contains the vulnerabilities as identification numbers, which QRadar compares against the most recent Qualys Vulnerability Knowledge Base. The Qualys Detection Scanner does not support live scans, but enables the Qualys Detection Scanner to retrieve vulnerability information aggregated across multiple scan reports. QRadar supports key search parameters to filter for the information that you want to collect. You can also configure how frequently QRadar retrieves and caches the Qualys Vulnerability Knowledge Base.

Qualys Scanners

Add a Qualys scanner if you want to import specific live or imported reports that include scan or asset data. When you add a Qualys scanner, you can choose from the following collection types:

- Scheduled live - Scan Report
- Scheduled Import - Asset Data Report
- Scheduled Import - Scan Report

Adding a Qualys detection scanner

Add a Qualys detection scanner to use an API to query across multiple scan reports to collect vulnerability data for assets. The Qualys detection scanner uses the QualysGuard Host Detection List API.

Before you begin

Before you add this scanner, a server certificate is required to support HTTPS connections. QRadar supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.

3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your Qualys detection scanner.
5. From the **Managed Host** list, select the managed host that manages the scanner import.
6. From the **Type** list, select **Qualys Detection Scanner**.
7. Configure the following parameters:

Parameter	Description
Qualys Server Host Name	The Fully Qualified Domain Name (FQDN) or IP address of the QualysGuard management console. If you type the FQDN, use the host name and not the URL, for example, type `qualysapi.qualys.com` or `qualysapi.qualys.eu`.
Qualys Username	The user name that you specify must have access to download the Qualys Vulnerability Knowledge Base. For more information about how to update Qualys user accounts, see your Qualys documentation.
Operating System Filter	The regular expression (regex) to filter the scan data by the operating system.
Asset Group Names	A comma-separated list to query IP addresses by the asset group name.
Host Scan Time Filter (Days)	Host scan times that are older than the specified number of days are excluded from the results that Qualys returns.
Qualys Vulnerability Retention Period (Days)	The number of days that you want QRadar to store the Qualys Vulnerability Knowledge Base. If a scan is scheduled and the retention period expires, the system downloads an update. **Attention:** After you create this scanner for the first time, subsequent updates to this retention period might not take effect. For this change to take effect after the initial creation, you might need to delete or clear the cache.
Force Qualys Vulnerability Update	Forces the system to update to the Qualys Vulnerability Knowledge Base for each scheduled scan.

8. Optional: To configure a proxy, select the **Use Proxy** check box and configure the credentials for the proxy server.
9. Optional: To configure a client certificate, select the **Use Client Certificate** check box and configure the **Certificate File Path** field and **Certificate Password** fields.
10. Optional: To configure a CIDR range for your scanner, configure the CIDR range parameters and click **Add**.

    Restriction: The QualysGuard Host Detection List API accepts only CIDR ranges to a maximum of a single class A or /8 and does not accept the local host IP address (127.0.0.1).

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**. Changes to the proxy configuration require a **Deploy Full Configuration**.

Adding a Qualys scheduled live scan

Add a scheduled live scan to start preconfigured scans on the Qualys Scanner and then collect the completed scan results.

Before you begin

Before you add this scanner, a server certificate is required to support HTTPS connections. QRadar supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your Qualys scanner.
5. From the **Managed Host** list, select the managed host that manages the scanner import.
6. From the **Type** list, select **Qualys Scanner**.
7. Configure the following parameters:

Parameter	Description
Qualys Server Host Name	The Fully Qualified Domain Name (FQDN) or IP address of the QualysGuard management console. If you type the FQDN, use the host name and not the URL, for example, type `qualysapi.qualys.com` or `qualysapi.qualys.eu`.
Qualys Username	The user name that you specify must have access to download the Qualys Vulnerability Knowledge Base. For more information about how to update Qualys user accounts, see your Qualys documentation.

8. Optional: To configure a proxy, select the **Use Proxy** check box and configure the credentials for the proxy server.
9. Optional: To configure a client certificate, select the **Use Client Certificate** check box and configure the **Certificate File Path** field and **Certificate Password** fields.
10. From the **Collection Type** list, select **Scheduled Live - Scan Report**.
11. Configure the following parameters:

Parameter	Description
Scanner Name	To obtain the scanner name, contact your network administrator. Public scanning appliance must clear the name from this field.
Option Profiles	The name of the option profile that determines which live scan is started. Live scans support only one option profile name for each scanner configuration.

12. Optional: To configure a CIDR range for your scanner, configure the CIDR range parameters and click **Add**.
13. Click **Save**.
14. On the **Admin** tab, click **Deploy Changes**. Changes to the proxy configuration require a **Deploy Full Configuration**.

Adding a Qualys scheduled import asset data report

Add an asset report data import to schedule QRadar to retrieve a single asset report from your Qualys scanner.

Before you begin

Before you add this scanner, a server certificate is required to support HTTPS connections. QRadar supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your Qualys scanner.
5. From the **Managed Host** list, select the managed host that manages the scanner import.
6. From the **Type** list, select **Qualys Scanner**.
7. Configure the following parameters:

Parameter	Description
Qualys Server Host Name	The Fully Qualified Domain Name (FQDN) or IP address of the QualysGuard management console. If you type the FQDN, use the host name and not the URL, for example, type `qualysapi.qualys.com` or `qualysapi.qualys.eu`.

Parameter	Description
Qualys Username	The user name that you specify must have access to download the Qualys Vulnerability Knowledge Base. For more information about how to update Qualys user accounts, see your Qualys documentation.

8. Optional: To configure a proxy, select the **Use Proxy** check box and configure the credentials for the proxy server.
9. Optional: To configure a client certificate, select the **Use Client Certificate** check box and configure the **Certificate File Path** field and **Certificate Password** fields.
10. From the **Collection Type** list, select **Scheduled Import - Asset Data Report**.
11. Configure the following parameters:

Parameter	Description
Report Template Title	The report template title to replace the default asset data report title.
Max Reports Age (Days)	Files that are older than the specified days and time stamp on the report file are excluded when the schedule scan starts.
Import File	The directory path to download and import a single asset report from Qualys. If you specify an import file location, QRadar downloads the contents of the asset report from Qualys to a local directory and imports the file. If you leave this field blank or if the file or directory cannot be found, the Qualys scanner uses the API to retrieve the asset report by using the value in the **Report Template Title** field.

12. Optional: To configure a CIDR range for your scanner, configure the CIDR range parameters and click **Add**.
13. Optional: To enable QRadar to create custom vulnerabilities from the live scan data, select the **Enable Custom Vulnerability Creation** check box and select options that you want to include.
14. Click **Save**.
15. On the **Admin** tab, click **Deploy Changes**. Changes to the proxy configuration require a **Deploy Full Configuration**.

Adding a Qualys scheduled import scan report

Add a scan report data import to schedule QRadar to retrieve scan reports from your Qualys scanner.

Before you begin

Before you add this scanner, a server certificate is required to support HTTPS connections. QRadar supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.

- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your Qualys scanner.
5. From the **Managed Host** list, select the managed host that manages the scanner import.
6. From the **Type** list, select **Qualys Scanner**.
7. Configure the following parameters:

Parameter	Description
Qualys Server Host Name	The Fully Qualified Domain Name (FQDN) or IP address of the QualysGuard management console. If you type the FQDN, use the host name and not the URL, for example, type `qualysapi.qualys.com` or `qualysapi.qualys.eu`.
Qualys Username	The user name that you specify must have access to download the Qualys Vulnerability Knowledge Base. For more information about how to update Qualys user accounts, see your Qualys documentation.

8. Optional: To configure a proxy, select the **Use Proxy** check box and configure the credentials for the proxy server.
9. Optional: To configure a client certificate, select the **Use Client Certificate** check box and configure the **Certificate File Path** field and **Certificate Password** fields.
10. From the **Collection Type** list, select **Scheduled Import - Scan Report**.
11. Configure the following parameters:

Parameter	Description
Option Profiles	The name of the option profile to determine which scan to start. QRadar retrieves the completed live scan data after the live scan completes. Live scans support only one option profile name per scanner configuration.
Scan Report Name Pattern	The regular expression (regex) to filter the list of scan reports.
Max Reports Age (Days)	Files that are older than the specified days and time stamp on the report file are excluded when the schedule scan starts.

Parameter	Description
Import File	The directory path to download and import a single scan report from Qualys, for example, `/qualys_logs/test_report.xml`. If you specify an import file location, QRadar downloads the contents of the scan report from Qualys to a local directory and imports the file. If you leave this field blank or if the file or directory cannot be found, the Qualys scanner uses the API to retrieve the scan report by using the value in the **Options Profile** field.

12. Optional: To configure a CIDR range for your scanner, configure the CIDR range parameters and click **Add**.
13. Optional: To enable QRadar to create custom vulnerabilities from the live scan data, select the **Enable Custom Vulnerability Creation** check box and select options that you want to include.
14. Click **Save**.
15. On the **Admin** tab, click **Deploy Changes**. Any changes to the proxy configuration requires a **Deploy Full Configuration**.

What to do next

You are now ready to create a scan schedule. See Chapter 26, "Scheduling a vulnerability scan," on page 87.

Chapter 17. Juniper Profiler NSM scanner overview

QRadar can collect vulnerability data from the PostgreSQL database on the Juniper Profiler NSM scanner by polling for data with JDBC.

The Juniper Networks Netscreen Security Manager (NSM) console passively collects valuable asset information from your network through deployed Juniper Networks IDP sensors. QRadar connects to the Profiler database stored on the NSM server to retrieve these records. The QRadar server must have access to the Profiler database. QRadar supports NSM versions 2007.1r2, 2007.2r2, 2008.1r2, 2009r1.1, and 2010.x. For more information, see your vendor documentation. To collect data from the PostgreSQL database, QRadar must have access to the Postgres database port through TCP port 5432. Access is provided in the `pg_hba.conf` file, which is located in `/var/netscreen/DevSvr/pgsql/data/pg_hba.conf` on the system that hosts the Juniper NSM Profiler.

To add a Juniper NSM Profiler scanner, see"Adding a Juniper NSM Profiler scanner."

Adding a Juniper NSM Profiler scanner

Administrators can add a Juniper NSM Profiler scanner to poll for vulnerability data with JDBC.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your FoundScan server.
5. From the **Managed Host** list, select the managed host from your QRadar deployment that manages the scanner import. Certificates for your FoundScan scanner must reside on the managed host selected in the Managed Host list box.
6. From the **Type** list, select **Juniper NSM Profiler Scanner**.
7. In the **SOAP API URL** field, type the IP address or hostname of the Foundstone FoundScan that contains the vulnerabilities you want to retrieve with the SOAP API. For example, `https://foundstone IP address:SOAP port` The default value is `https://localhost:3800.`
8. In the **Customer Name** field, type the name of the customer that belongs to the user name.
9. In the **User Name** field, type the username required to access the Foundstone FoundScan server.
10. Optional. In the **Client IP Address** field, type the IP address of the server that you want to perform the scan. By default, this value is not used; however, is necessary when administrators validate some scan environments.
11. Optional. In the **Password** field, type the password required to access the Foundstone FoundScan server.
12. In the **Portal Name** field, type the portal name. This field can be left blank for QRadar. See your FoundScan administrator for more information.

13. In the **Configuration Name** field, type the scan configuration name that exists in FoundScan and to which the user has access. Make sure this scan configuration is active or runs frequently.
14. In the **CA Truststore** field, type the directory path and filename for the CA truststore file. The default path is `/opt/qradar/conf/foundscan.keystore`.
15. In the **CA Keystore** field, type the directory path and filename for the client keystore. The default path is `/opt/qradar/conf/foundscan.truststore`.
16. To configure a CIDR range for your scanner:
    a. In the text field, type the CIDR range for the scanner or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
17. Click **Save**.
18. On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to import certificates from your FoundScan server. See "Importing certificates for Foundstone FoundScan" on page 26.

Chapter 18. Rapid7 NeXpose scanners overview

Rapid7 NeXpose scanners can provide site data reports to QRadar to import vulnerabilities known about your network.

The following options are available to collect vulnerability information from Rapid7 NeXpose scanners:

- Site import of an adhoc reports through the Rapid7 API. See "Adding a Rapid7 NeXpose scanner API site import."
- Site import of a local file. See "Adding a Rapid7 NeXpose scanner local file import" on page 62

Adding a Rapid7 NeXpose scanner API site import

API imports enable QRadar to import ad hoc report data for vulnerabilities on your sites from Rapid7 NeXpose scanners. The site data the scan schedule imports depends on the site name.

Before you begin

Before you add this scanner, a server certificate is required to support HTTPS connections. QRadar supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your Rapid7 NeXpose scanner.
5. From the **Managed Host** list, select the managed host from your QRadar deployment that manages the scanner import.
6. From the **Type** list, select **Rapid7 Nexpose Scanner**.
7. From the **Import Type** list, select **Import Site Data - Adhoc Report via API**.
8. In the **Remote Hostname** field, type the IP address or host name of the Rapid7 NeXpose scanner.
9. In the **Login Userame** field, type the user name that to access the Rapid7 NeXpose scanner. The login must be a valid user. The user name can be obtained from the Rapid7 NeXpose user interface or from the Rapid7 NeXpose administrator.
10. In the **Login Password** field, type the password to access the Rapid7 NeXpose scanner.

11. In the **Port** field, type the port that is used to connect to the Rapid7 NeXpose Security Console. The port number is the same port to connect to the Rapid7 NeXpose user interface.
12. In the **Site Name Pattern** field, type the regular expression (regex) to determine which Rapid7 NeXpose sites to include in the scan. All sites that match the pattern are included when the scan schedule starts. The default value regular expression is `.*` to import all site names.
13. In the **Port** field, type the port that is used to connect to the Rapid7 NeXpose Security Console.
14. In the **Cache Timout (Minutes)** field, type the length of time the data from the last generated scan report is stored in the cache. If the cache timeout limit expires, new vulnerability data is requested from the API when the scheduled scan starts.
15. To configure a CIDR range for the scanner:
    a. In the text field, type the CIDR range for the scan or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
16. Click **Save**.
17. On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to create a scan schedule. See Chapter 26, “Scheduling a vulnerability scan,” on page 87.

Adding a Rapid7 NeXpose scanner local file import

Importing site vulnerability data using the local files allows QRadar to import completed vulnerability scans based on completed scan reports copied from your Rapid7 NeXpose scanner to QRadar.

Before you begin

Before you add this scanner, a server certificate is required to support HTTPS connections. QRadar supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

About this task

Local file imports collect vulnerabilities for a site from a local file that is downloaded. The Rapid7 NeXpose XML file that contains the site and vulnerability information must be copied from your Rapid7 NeXpose appliance to the Console or managed host you specify when the scanner is added to QRadar. The directory on the managed host must exist before the system can copy site reports to the managed host. Administrators can configure the site files to copy to the managed host files can be copied using Secure Copy (SCP) or Secure File Transfer Protocol (SFTP).

Note: Site files that are imported are not deleted from the import folder, but renamed to `.processed0`. Administrators can create a cron job to delete previously processed site files, if required.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your Rapid7 NeXpose scanner.
5. From the **Managed Host** list, select the managed host from your QRadar deployment that manages the scanner import.
6. From the **Type** list, select **Rapid7 Nexpose Scanner**.
7. From the **Import Type** list, select **Import Site Data - Local File**.
8. In the **Import Folder** field, type the directory path to the XML vulnerability data. If you specify an import folder, you must move the vulnerability data from your Rapid7 NeXpose scanner to QRadar.
9. In the **Import Name Pattern** field, type a regular expression (regex) pattern to determine which Rapid7 NeXpose XML files to include in the scan report. All file names matching the regex pattern are included when importing the vulnerability scan report. You must use a valid regex pattern in this field. The default value `.*\.xml` imports all files from the import folder.
10. To configure a CIDR range for your scanner:
    a. In the text field, type the CIDR range you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to create a scan schedule. See Chapter 26, “Scheduling a vulnerability scan,” on page 87.

Chapter 19. netVigilance SecureScout scanner overview

QRadar can collect vulnerability data from an SQL database on the SecureScout scanner by polling for data with JDBC.

netVigilance SecureScout NX and SecureScout SP store scan results in an SQL database. This database can be a Microsoft MSDE or SQL Server database. To collect vulnerabilities, QRadar connects to the remote database to locate the latest scan results for a given IP address. The data returned updates the asset profile in QRadar with the asset IP address, discovered services, and vulnerabilities. QRadar supports SecureScout scanner software version 2.6.

We suggest that administrators create a special user in your SecureScout database for QRadar to poll for vulnerability data.

The database user you create must have select permissions to the following tables:

- HOST
- JOB
- JOB_HOST
- SERVICE
- TCRESULT
- TESTCASE
- PROPERTY
- PROP_VALUE
- WKS
- IPSORT - The database user must have execute permission for this table.

To add a scanner configuration, see“Adding a netVigilance SecureScout scan.”

Adding a netVigilance SecureScout scan

Administrators can add a SecureScout scanner to query for vulnerability data with JDBC.

Before you begin

To query for vulnerability data, QRadar you must have appropriate administrative access to poll the SecureScout scanner with JDBC. Administrators must also ensure that firewalls, including the firewall on the SecureScout host permits a connection from the managed host responsible for the scan to the SecureScout scanner.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your SecureScout server.
5. From the **Managed Host** list, select the managed host from your QRadar deployment that manages the scanner import.
6. From the **Type** list, select **SecureScout Scanner**.

7. In the **Database Hostname** field, type the IP address or hostname of the SecureScout database server that contains the SQL server.
8. In the **Login Name** field, type the username required to access the SQL database of the SecureScout scanner.
9. Optional. In the **Login Password** field, type the password required to access the SQL database of the SecureScout scanner.
10. In the **Database Name** field, type `SCE`.
11. In the **Database Port** field, type the TCP port you want the SQL server to monitor for connections. The default value is 1433.
12. To configure a CIDR range for your scanner:
    a. In the text field, type the CIDR range you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
13. Click **Save**.
14. On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to create a scan schedule. See Chapter 26, “Scheduling a vulnerability scan,” on page 87.

Chapter 20. McAfee Vulnerability Manager scanner overview

The McAfee Vulnerability Manager scanner enables QRadar to import vulnerabilities from an XML file or query for a results file from the McAfee OpenAPI.

QRadar can collect vulnerability data from McAfee Vulnerability Manager appliances. The following software versions are supported

- v6.8 and v7.0 for the McAfee Vulnerability Manager SOAP API
- v6.8, v7.0, and v7.5 for remote XML imports

The following import options are available to collect vulnerability information from McAfee Vulnerability Manager:

- To add a remote XML import for vulnerability data, see "Adding a remote XML import scan."
- To retrieve vulnerabilities from the SOAP API, see "Adding a McAfee Vulnerability Manager SOAP API scan" on page 68

Adding a remote XML import scan

Remote XML imports enable QRadar to connect to a remote server and import the HostData XML vulnerability data that is created by your McAfee Vulnerability Manager appliance.

About this task

Remote XML file imports enable you to configure the McAfee Vulnerability Manager to export scan results to a remote server. QRadar connects to the remote repository over SFTP and imports completed XML scan reports from a remote directory. You can use the file import collection method to import completed scan reports from McAfee Vulnerability Manager V7.0 and V7.5.

Attention: The import might contain HostData and RiskData XML files. Only HostData XML files are supported as they contain the required host and vulnerability information. Ensure that only HostData XML files are placed in the remote directory or that the file name pattern that you configure matches only HostData reports.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify McAfee Vulnerability Manager.
5. From the **Managed Host** list, select the managed host from your QRadar deployment that manages the scanner import.
6. From the **Type** list, select **McAfee Vulnerability Manager**.
7. From the **Import Type** list, select **Remote XML Import**.
8. In the **Remote Hostname** field, type the IP address or host name of the remote server that hosts your McAfee Vulnerability Manager XML data.

9. In the **Remote Port** field, type the port to retrieve the XML vulnerability data.
10. Choose one of the following authentication options:

Option	Description
Login Username	Authenticates with a user name and password. The password must not contain the ! character. This character might cause authentication failures over SFTP.
Enable Key Authorization	Authenticate with a key-based authentication file. If a key file does not exist, you must create the vis.ssh.key file and place it in the `/opt/qradar/conf/vis.ssh.key` directory.

11. In the **Remote Directory** field, type the directory path to the XML vulnerability data.
12. In the **File Name Pattern** field, type a regular expression (regex) to filter the list of files that are specified in the Remote Directory. All matching files are included in the processing. Ensure that this pattern matches only HostData XML reports.
13. In the **Max Reports Age (days)** field, type the maximum file age for your scan results file.
14. To configure a CIDR range for the scanner:
    a. In the text field, type the CIDR range for the scan or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
15. Click **Save**.
16. On the **Admin** tab, click **Deploy Changes**.

Adding a McAfee Vulnerability Manager SOAP API scan

You can add a McAfee Vulnerability Manager scanner to enable QRadar to collect host and vulnerability information through the McAfee OpenAPI.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify the scanner.
5. From the **Managed Host** list, select the managed host that manages the scanner import. Certificates for the scanner must be on the managed host that is selected in the **Managed Host** list.
6. From the **Type** list, select **McAfee Vulnerability Manager**.
7. In the **SOAP API URL** field, type the IP address or hostname of the McAfee Vulnerability Manager that contains the vulnerabilities you want to retrieve with the SOAP API. For example, `https://foundstone IP address:SOAP port`. The default value is `https://localhost:3800.`
8. In the **Customer Name** field, type the name of the customer that belongs to the user name.
9. In the **User Name** field, type the user name to access McAfee Vulnerability Manager.

10. Optional: In the **Client IP Address** field, type the IP address of the server that you want to perform the scan.

    Tip: This field is typically not used; however, it may be required for you to validate some scan environments.
11. In the **Password** field, type the password to access McAfee Vulnerability Manager.
12. In the **Configuration Name** field, type the scan configuration name that exists in McAfee Vulnerability Manager and to which the user has access. Make sure that this scan configuration is active or runs frequently.
13. In the **CA Truststore** field, type the directory path and filename for the CA truststore file.

    The default path is `/opt/qradar/conf/mvm.keystore`.
14. In the **CA Keystore** field, type the directory path and filename for the client keystore.

    The default path is `/opt/qradar/conf/mvm.truststore`.
15. From the **McAfee Vulnerability Manager Version** list, select the software version of your McAfee Vulnerability Manager.
16. To remove previously detected vulnerabilities that were not detected by the most recent scan, select the **Vulnerability Cleanup** check box.
17. To configure a CIDR range for the scanner:
    a. Type the CIDR range for the scan or click **Browse** to select a CIDR range from the network list.

       The McAfee Vulnerability Manager accepts only CIDR addresses ranges to a 0/0 subnet that are added as 0.0.0.0/0.
    b. Click **Add**.
18. Click **Save**.
19. On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to create certificates from McAfee Vulnerability Manager. See "Creating certificates for McAfee Vulnerability Manager."

Creating certificates for McAfee Vulnerability Manager

To connect through the Foundstone Open API, configure third-party certificates with the McAfee Certificate Manager Tool.

Before you begin

If the Certificate Manager Tool is not installed on the McAfee Foundstone Enterprise Manager server, contact McAfee Technical Support.

About this task

You must process client-side certificates into valid keystore and truststore files for QRadar on the McAfee Foundstone Enterprise Manager server.

The McAfee Foundstone Enterprise Manager server must be compatible with the version of the FIPS-Capable OpenSSL used by the Foundstone Certificate Manager to correctly create the certificates. A Java Software Development Kit (Java SDK) must be present on this server for this processing. To obtain the most recentJava SDK go to the following website:

http://java.sun.com.

Procedure

1. Log in to the McAfee Foundstone Enterprise Manager server.
2. Run the Foundstone Certificate Manager.
3. Click the **Create SSL Certificates** tab.
4. Type the host address for QRadar.

   The certificate must be created with the host address for the QRadar appliance that retrieves vulnerability data from the McAfee Vulnerability Manager.
5. Optional: Click **Resolve**.

   If an error occurs when the Foundstone Certificate Manager attempts to resolve the host, type the IP address in the **Host Address** field . If the host cannot resolve, see Step 7.
6. Click **Create Certificate Using Common Name**.
7. Click **Create Certificate Using Host Address**.
8. Save the compressed file that contains the certificate files to a directory on your McAfee Vulnerability Manager.
9. Copy the pass phrase that is provided to a text file.
10. Repeat this process to generate any more certificates for managed hosts in your deployment.

What to do next

You are now ready to process the certificates to create the required keystore and truststore files. See “Processing certificates for McAfee Vulnerability Manager.”

Processing certificates for McAfee Vulnerability Manager

To create the keystore and truststore files required by QRadar, process the certificates that Foundstone Certificate Manager created.

Before you begin

You must have access to the support portal to download the files that are required to create the truststore and keystore files. The batch files require the path to the Java home directory on the McAfee Vulnerability Manager.

Procedure

1. Log in to the support portal to download the following files:
   - `VulnerabilityManager-Cert.bat.gz`
   - `q1labs_vis_mvm_cert.jar`
2. Extract the compressed files and copy the certificates and the downloaded files to the same directory on your McAfee Vulnerability Manager.
3. Open the command-line interface on the McAfee Vulnerability manager.
4. Go to the directory location of the files.
5. To run the batch file, type the following command: `VulnerabilityManager-Cert.bat "C:\Program Files\Java\jdk1.6.0_20"`.

The quotation marks in the command specify the Java home directory.

6. Repeat this process to create keystore and truststore files for any more managed hosts in your deployment.

Results

The keystore and truststore files are created. If an error is displayed, administrators can verify the path to the Java home directory.

What to do next

You are now ready to import the certificates for your QRadar appliance. See "Importing certificates for McAfee Vulnerability Manager"

Importing certificates for McAfee Vulnerability Manager

The keystore and truststore files must be imported to the managed host responsible for the scan.

Before you begin

You must add the scanner to a managed host in the scan configuration before you import the certificates. For security purposes, a secure file transfer protocol to copy a certificate file.

Procedure

1. To import the certificates, secure copy the mvm.keystore and mvm.truststore files to the following directories in QRadar:
   - `/opt/qradar/conf/`
   - `/opt/qradar/conf/trusted_certificates/`

     Note: If the `/opt/qradar/conf/trusted_certificates/` directory does not exist, do not create the directory. If the directory does not exist, administrators can ignore the file copy for the missing directory.

   If you have a distributed deployment, you must copy the files to the Console and SSH the files from the Console appliance to the managed host.
2. Log in to QRadar.
3. Click the **Admin** tab.
4. On the **Admin** tab, select **Advanced** > **Deploy Full Configuration**.

   Note: When you click **Deploy Full Configuration**, QRadar restarts all services. Service restart results in a gap in data collection for events and flows until the deployment process completes.
5. Repeat the certificate import for any more managed hosts in your deployment that collect vulnerabilities from McAfee Vulnerability Manager.

Chapter 21. Outpost24 Vulnerability Scanner overview

IBM Security QRadar uses HTTPS to communicate with the Outpost24 vulnerability scanner API to download asset and vulnerability data from previously completed scans.

The following table lists the specifications for the Outpost24 vulnerability scanner:

Table 1. Outpost24 Vulnerability Scanner specifications

Specification	Value
Scanner name	Outpost24 Vulnerability Scanner
Supported versions	HIAB V4.1 OutScan V4.1
Connection type	HTTPS
More information	Outpost24 website (http://www.outpost24.com/)

To configure QRadar to download asset and vulnerability data from an Outpost24 vulnerability scanner, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Outpost24 Vulnerability Scanner RPM on your QRadar system.
2. On the Outpost24 vulnerability scanner, create an application token for QRadar.
3. On the QRadar Console, add the Outpost24 vulnerability scanner. Configure all required parameters and use the following table to identify specific Outpost24 values:

Table 2. Outpost24 Vulnerability Scanner parameters

Parameter	Value
Type	Outpost24 Vulnerability Scanner
Server Hostname	The host name or IP address of the Outpost24 vulnerability scanner device.
Port	443
API token	Must use the API token that you created on the Outpost24 vulnerability scanner device.

4. Schedule a scan.

Related tasks:

"Creating an Outpost24 API authentication token for QRadar" on page 74
To enable IBM Security QRadar to use the Outpost24 API to download asset and vulnerability data, create an Application Access Token on the Outpost24 vulnerability scanner.

Chapter 26, "Scheduling a vulnerability scan," on page 87
Scan schedules are intervals assigned to scanners that determine when vulnerability assessment data is imported from external scanning appliances in your network. Scan schedules can also define CIDR ranges or subnets that are included in the data import when the vulnerability data import occurs.

Creating an Outpost24 API authentication token for QRadar

To enable IBM Security QRadar to use the Outpost24 API to download asset and vulnerability data, create an Application Access Token on the Outpost24 vulnerability scanner.

Procedure

1. Log in to Outpost24 vulnerability scanner.
2. Select **Settings > Account**.
3. Click the **Security Policy** tab.
4. In the Application Access Tokens pane, click **New**.
5. In the Maintaining App Access Token window, ensure that the **Active** check box is selected.
6. Type a name for the application, for example, QRadar.
7. Configure the IP restrictions and user access rights.
8. Click **Save**.
9. Copy the 64 character authentication token to a file.

What to do next

On your QRadar system, add the Outpost24 vulnerability scanner.

Chapter 22. SAINT scanner overview

Administrators can integrate their Security Administrator's Integrated Network Tool (SAINT) vulnerability scanners with QRadar for SAINT appliances with V7.4.x software.

Administrators can add SAINT scanners to QRadar to collect SAINT vulnerability data for hosts, including Mac addresses, ports, and service information. The SAINT scanner identifies vulnerabilities based on the specified scan level and uses SAINTwriter to generate custom reports. Therefore, your SAINT system must include a custom SAINTwriter report template and scans that runs regularly to ensure the results are current.

The following data collection types are supported for SAINT scanner configurations:

- Live scan - Start a remote scans on the SAINT scanner. The live scan generates vulnerability report based on the session name, which is imported after the scan completes.
- Report only - Import completed reports from the SAINT scanner based on the session name.

To configure a template for your report, see “Configuring a SAINTwriter template.”

Configuring a SAINTwriter template

Before administrators can add and import vulnerabilities from a SAINT scanner, a template must be configured in SAINTwriter.

Procedure

1. Log in to the SAINT user interface.
2. From the navigation menu, select **Data** > **SAINTwriter**.
3. Click **Report Type**.
4. From the **Type** list, select **Custom**.
5. In the **File Name** field, type a configuration file name.

   The configuration file name that is created must be used when you add the SAINT scanner to QRadar.
6. From the **Template Type** list, select **Technical Details**.
7. Click **Continue**.
8. Select **Lists**.
9. From the **Columns to include in host** list, change a None column to **MAC address**.
10. From the **Columns to include in vulnerability** list, change a None column to **Port**.
11. From the **Columns to include in vulnerability** list, change a None column to **Service**.
12. Click **Save**.

What to do next

You are now ready to add a scan configuration to QRadar for the SAINT scanner. See “Adding a SAINT vulnerability scan.”

Adding a SAINT vulnerability scan

Administrators can add a SAINT scanner configuration to collect specific reports or start scans on the remote scanner.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your SAINT scanner.
5. From the **Managed Host** list, select the managed host from your QRadar deployment that manages the scanner import.
6. From the **Type** list, select **SAINT Scanner**.
7. In the **Remote Hostname** field, type the IP address or host name of the SAINT scanner.
8. Choose one of the following authentication options:

Option	Description
Login Username	To authenticate with a user name and password: 1. In the **Login Username** field, type a username that has access to access the remote host. 2. In the **Login Password** field, type the password associated with the user name.
Enable Key Authorization	To authenticate with a key-based authentication file: 1. Select the **Enable Key Authentication** check box. 2. In the **Private Key File** field, type the directory path to the key file. The default is directory for the key file is`/opt/qradar/conf/vis.ssh.key`. If a key file does not exist, you must create the vis.ssh.key file.

9. In the **SAINT Base Directory** field, type the path to the installation directory of the SAINT scanner.
10. From the **Scan Type** list, select one of the following options:
    - Live Scan - Starts a vulnerability scan to generate report data based on the session name.
    - Report Only - Generates a scan report based on the session name.
11. For **Live Scan** configurations, select an option for the **Ignore Existing Data** check box.

- Select this check box to force the live scan to gather new vulnerability data from the network. This option removes any data from the session folder before the live scan starts.
- Clear this check box to enable the live scan to use existing data in the session folder.

12. From **Scan Level** list, select a scan level. The options include:
    - Vulnerability Scan - Scan for all vulnerabilities.
    - Port Scan - Scan for TCP or UDP services listening on the network.
    - PCI Compliance Scan - Scan ports and services with emphasis on DSS PCI compliance.
    - SANS Top 20 Scan - Scan for the top 20 most critical security vulnerabilities.
    - FISMA Scan - Scan for all vulnerabilities and including all custom scans and PCI levels.
13. In the **Session Name** field, type the session name for the SAINT scanner configuration.
14. In the **SAINT Writer Config** field, type the name of the SAINTwriter configuration file.
15. To configure a CIDR range for the scanner:
    a. In the text field, type the CIDR range for the scan or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
16. Click **Save**.
17. On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to create a scan schedule. See Chapter 26, “Scheduling a vulnerability scan,” on page 87.

Chapter 23. Tenable SecurityCenter scanner overview

A Tenable SecurityCenter scanner can be used to schedule and retrieve any open vulnerability scan report records from Nessus vulnerability scanners on your network. .

To configure a Tenable SecurityCenter scanner, see “Adding a Tenable SecurityCenter scan.”

Adding a Tenable SecurityCenter scan

You can add a Tenable SecurityCenter scanner to enable QRadar to collect host and vulnerability information through the Tenable API.

Before you begin

Verify the location of the `request.php` file on their Tenable SecurityCenter before a scanner is added to QRadar.

Before you add this scanner, a server certificate is required to support HTTPS connections. QRadar supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify the scanner.
5. From the **Managed Host** list, select the managed host from your QRadar deployment that manages the scanner import.
6. From the **Type** list, select **Tenable SecurityCenter**.
7. In the **Server Address** field, type the IP address of the Tenable SecurityCenter.
8. In the **API Location** field, type the path to the `request.php` file on the Tenable SecurityCenter.

   The default path to the API file is `sc4/request.php`.
9. In the **User Name** field, type the user name to access the Tenable SecurityCenter API.
10. In the **Password** field, type the password to access the Tenable SecurityCenter API.
11. To configure a CIDR range for the scanner:

    a. In the text field, type the CIDR range for the scan or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
12. Click **Save**.
13. On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to create a scan schedule. See Chapter 26, “Scheduling a vulnerability scan,” on page 87.

Chapter 24. AXIS scanner

You can import vulnerability data from any scanner that outputs data in Asset Export Information Source (AXIS) format. Axis is an XML data format that was created specifically for asset and vulnerability compatibility with IBM Security QRadar products.

AXIS is a standard format for scan result imports of vulnerability data. Vulnerability data for Axis scanners must comply with the AXIS format schema to be imported successfully. To successfully integrate an AXIS scanner with QRadar, XML result files must be available on a *remote server* or a scanner that supports SFTP or SMB Share communication. A remote server is a system or third-party appliance that can host the XML scan results.

Adding an AXIS vulnerability scan

Add an AXIS scanner configuration to collect specific reports or start scans on the remote scanner.

About this task

The following table describes AXIS scanner parameters when you select SFTP as the import method:

Table 3. AXIS scanner - SFTP properties

Parameter	**Description**
Remote Hostname	The IP address or host name of the server that has the scan results files.
Login Username	The user name that QRadar uses to log in to the server.
Enable Key Authentication	Specifies that QRadar authenticates with a key-based authentication file.
Remote directory	The location of the scan result files.
Private Key File	The full path to the file that contains the private key. If a key file does not exist, you must create the `vis.ssh.key` file.
File Name Pattern	The regular expression (regex) required to filter the list of files that are in the *Remote Directory*. The `.*\.xml` pattern imports all XML files from the remote directory.

The following table describes AXIS scanner parameters when you select *SMB Share* as the import method:

Table 4. AXIS scanner - SMB Share properties

Parameter	**Description**
Hostname	The IP address or host name of the SMB Share.
Login Username	The user name that QRadar uses to log in to SMB Share.

Table 4. AXIS scanner - SMB Share properties (continued)

Parameter	Description
Domain	The domain that is used to connect to the SMB Share.
SMB Folder Path	The full path to the share from the root of the SMB host. Use forward slashes, for example, `/share/logs/`.
File Name Pattern	The regular expression (regex) required to filter the list of files in the Remote Directory. The `.*\.xml` pattern imports all xml files in the remote directory.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify the AXIS scanner.
5. From the **Managed Host** list, select the managed host that manages the scanner import.
6. From the **Type** list, select **Axis Scanner**.
7. From the **Import Method** list, select **SFTP** or **SMB Share**.
8. Configure the parameters.
9. Configure a CIDR range for the scanner.
10. Click **Save**.
11. On the **Admin** tab, click **Deploy Changes**.

What to do next

For more information about how to create a scan schedule, see Chapter 26, “Scheduling a vulnerability scan,” on page 87.

Chapter 25. Positive Technologies MaxPatrol

You can add a Positive Technologies MaxPatrol scanner to your IBM Security QRadar deployment.

At intervals that are determined by a scan schedule, QRadar imports XML file results that contain MaxPatrol vulnerabilities. The MaxPatrol scanner imports files from a remote server that contains the exported scan data.

The following table provides Positive Technologies MaxPatrol scanner details:

Table 5. Positive Technologies MaxPatrol Scanner details

Vendor	Positive Technologies
Scanner name	MaxPatrol
Supported versions	V8.24.4 and later

Use the following procedures to integrate Positive Technologies MaxPatrol with QRadar

1. Configure your Positive Technologies MaxPatrol scanner to export scan reports. Enable the QRadar compatible XML file vulnerability exports. To obtain the necessary files and configuration procedures, contact Positive Technologies Customer Support.
2. On your QRadar Console, add a Positive Technologies MaxPatrol scanner.
3. On your QRadar Console, create a scan schedule to import scan result data.

Integrating Positive Technologies MaxPatrol with QRadar

Procedures that are required to integrate Positive Technologies MaxPatrol with QRadar.

Procedure

1. Configure your Positive Technologies MaxPatrol scanner to export scan reports. Enable the QRadar compatible XML file vulnerability exports. To obtain the necessary files and configuration procedures, contact Positive Technologies Customer Support.
2. On your QRadar Console, add a Positive Technologies MaxPatrol scanner.
3. On your QRadar Console, create a scan schedule to import scan result data.

Adding a Positive Technologies MaxPatrol scanner

Add a Positive Technologies MaxPatrol scanner to your IBM Security QRadar deployment.

Before you begin

Ensure that the following prerequisites are met: .

- The Positive Technologies MaxPatrol system is configured to export QRadar compatible XML vulnerability reports.

- An SFTP or SMB share is set up and contains the exported XML vulnerability reports.

About this task

The following table describes Positive Technologies MaxPatrol scanner parameters when you select SFTP as the import method:

Table 6. Positive Technologies MaxPatrol scanner SFTP properties

Parameter	Description
Remote Hostname	The IP address or host name of the server that has the scan results file.
Login Username	The user name that QRadar uses to log in to the server.
Enable Key Authentication	Specifies that QRadar authenticates with a key-based authentication file.
Remote directory	The location of the scan result files.
Private Key File	The full path to the file that contains the private key. If a key file does not exist, you must create the `vis.ssh.key` file.
File Name Pattern	The regular expression (regex) required to filter the list of files in the Remote Directory. The `.*\.xml` pattern imports all XML files in the remote directory.

The following table describes Positive Technologies MaxPatrol scanner parameters when you select SMB Share as the import method:

Table 7. Positive Technologies MaxPatrol scanner SMB Share properties

Parameter	Description
Hostname	The IP address or host name of the SMB Share.
Login Username	The user name that QRadar uses to log in to SMB Share.
Domain	The domain that is used to connect to the SMB Share.
SMB Folder Path	The full path to the share from the root of the SMB host. Use forward slashes, for example, `/share/logs/`.
File Name Pattern	The regular expression (regex) required to filter the list of files in the Remote Directory. The `.*\.xml` pattern imports all xml files in the remote directory.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify the Positive Technologies MaxPatrol scanner.

5. From the **Managed Host** list, select the managed host that manages the scanner import.
6. From the **Type** list, select **Positive Technologies MaxPatrol Scanner**.
7. Configure the parameters.
8. Configure a CIDR range for the scanner.
9. Click **Save**.
10. On the **Admin** tab, click **Deploy Changes**.

What to do next

For more information about how to create a scan schedule, see Chapter 26, “Scheduling a vulnerability scan,” on page 87.

Chapter 26. Scheduling a vulnerability scan

Scan schedules are intervals assigned to scanners that determine when vulnerability assessment data is imported from external scanning appliances in your network. Scan schedules can also define CIDR ranges or subnets that are included in the data import when the vulnerability data import occurs.

About this task

Scan schedules are created for each scanner product in your network and are used to retrieve vulnerability data. There is no limit to the number of scan schedules you can create. It is often helpful to create multiple scans in your network for vulnerabilities in your network. Large vulnerability imports can take a long time to complete and are often very system resource intensive. A scan cannot be scheduled until after the scanner has been added.

Procedure

1. Click the **Admin** tab.
2. Click the **Schedule VA Scanners** icon.
3. Click **Add**.
4. From the **VA Scanners** list, select the scanner that requires a scan schedule.
5. Choose one of the following options:

Option	Description
Network CIDR	Select this option to define a CIDR range for the data import. If a scanner includes multiple CIDR configurations, then the CIDR range can be selected from the list.
Subnet/CIDR	Select this option to define a subnet or CIDR range for the data import. The subnet/CIDR value that is defined by the administrator must be a Network CIDR that is available to the scanner.

6. From the **Priority** list, select the priority level to assign to the scan.

Option	Description
Low	Indicates the scan is of normal priority. Low priority is the default scan value.
High	Indicates the scan is high priority. High priority scans are always placed above low priority scans in the scan queue.

7. In the **Ports** field, type the ports that are included in the scan schedule. Any ports that are not in the schedule are not imported from the vulnerability data. Administrators can specify any port values from 1 - 65536. Individual port values can be included as comma-separate values, along with port ranges. For example, 21,443, 445, 1024-2048.

8. Select the start time for the schedule.
9. In the **Interval** field, type a time interval to indicate how often you want this scan to repeat. Scans schedules can contain intervals by the hour, day, week, or month.
10. Click **Save**.

Chapter 27. Viewing the status of a vulnerability scan

The Scan Schedule window provides administrators a status view for when each scanner is scheduled to collect vulnerability assessment data for asset in the network.

About this task

The name of each scan is displayed, along with the CIDR range, port or port range, priority, status, and next run time.

Table 8. Scan schedule status

Column name	Description
VA Scanner	Displays the name of the schedule scan.
CIDR	Displays the CIDR address ranges that are included in the vulnerability data import when the scan schedule starts.
Ports	Displays the port ranges that are included in the vulnerability data import when the scan schedule starts. Scan schedules are capable of starting a remote scan on a remote vulnerability appliance for specific vendors. For example, NMap or Nessus, or Nessus Scan Results Importer, then the ports listed in the Ports column are the ports contained in the scan. For most scanners, the port range is not considered when requesting asset information from a scanner. For example, nCircle IP360 and Qualys scanners report vulnerabilities on all ports, but require you to specify what port information to pull from the full report for display in the user interface.
Priority	Displays the priority of the scan. Scans schedules with a high priority are queued above in priority and run before low priority scans.
Status	Displays the current status of the scan. Each status field contains unique information about the scan status. • New scans can be edited until the state changes. • Pending scans must wait for another scan to complete. • In progress scans provide a percentage complete with tooltip information about the data import. • Completed scans provide a summary of the vulnerabilities imported or any partial imports of data that occurred. • Failed scans provide an error message on why the vulnerabilities failed to import.
Last Finish Time	Displays the last time the scan successfully imported vulnerability records for the schedule.
Next Run Time	Displays the next time the scan is scheduled to import vulnerability data. Scan schedules that display *Never* in the user interface are one time scans.

Procedure

1. Click the **Admin** tab.
2. Click the **Schedule VA Scanners** icon.
3. Review the Status column to determine the status of your log sources.

   The status column for each scanner provides a status message about each successful vulnerability import or failure.

Chapter 28. Supported vulnerability scanners

Vulnerability data can be collected from several manufacturers and vendors of security products. If the scanner deployed in your network is not listed in this document, you can contact your sales representative to review support for your appliance.

Table 9. Supported vulnerability scanners

Vendor	Scanner name	Supported versions	Configuration name	Connection type
Beyond Security	Automated Vulnerability Detection System (AVDS)	AVDS Management V12 (minor version 129) and above	Beyond Security AVDS Scanner	File import of vulnerability data with SFTP
eEye Digital Security	eEye REM	REM V3.5.6	eEye REM Scanner	SNMP trap listener
	eEye Retina CS	Retina CS V3.0 - V4.0		Database queries over JDBC
Generic	Axis	N/A	Axis Scanner	File import of vulnerability data with SFTP
IBM	InfoSphere Guardium	v9.0 and above	IBM Guardium SCAP Scanner	File import of vulnerability data with SFTP
IBM	IBM Security AppScan Enterprise	V8.6	IBM AppScan Scanner	IBM REST web service with HTTP or HTTPS
IBM	InfoSphere SiteProtector	V2.9.x	IBM SiteProtector Scanner	Database queries over JDBC
IBM	Tivoli Endpoint Manager	V8.2.x	IBM Tivoli Endpoint Manager	SOAP-based API with HTTP or HTTPS
Juniper Networks	NetScreen Security Manager (NSM) Profiler	2007.1r2	Juniper NSM Profiler Scanner	Database queries over JDBC
		2007.2r2		
		2008.1r2		
		2009r1.1		
		2010.x		
McAfee	Foundstone	V5.0 - V6.5	Foundscan Scanner	SOAP-based API with HTTPS
McAfee	Vulnerability Manager	V6.8	McAfee Vulnerability Manager	SOAP-based API with HTTPS
		V7.0		XML file import
		V7.5		
nCircle	ip360	VnE Manager V6.5.2 - V6.8.28	nCircle ip360 Scanner	File import of vulnerability data with SFTP
Nessus	Nessus	Linux V4.0.2 - V4.4.x	Nessus Scanner	File import over SFTP with SSH command execution
		Microsoft Windows V4.2 - V4.4.x		
Nessus	Nessus	Linux V4.2 - V5.x	Nessus Scanner	Nessus XMLRPC API over HTTPS
		Microsoft Windows V4.2 - V5.x		
netVigilance	SecureScout	V2.6	SecureScout Scanner	Database queries over JDBC
Open source	NMap	V3.7 - V6.0	NMap Scanner	File import of vulnerability data over SFTP with SSH command execution
Qualys	QualysGuard	V4.7 -V7.10	Qualys Scanner	APIv2 over HTTPS
Qualys	QualysGuard	V4.7 -V7.10	Qualys Detection Scanner	API Host Detection List over HTTPS
Rapid7	NeXpose	V4.x - V5.5	Rapid7 NeXpose Scanner	Remote Procedure Call (RPC) over HTTPS
				Local file import of XML file over SCP or SFTP to a local directory
Saint Corporation	SAINT	V7.4.x	Saint Scanner	File import of vulnerability data over SFTP with SSH command execution
Tenable	SecurityCenter	V4.6.0	Tenable SecurityCenter	JSON request over HTTPS

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

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

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

The following terms are trademarks or registered trademarks of other companies:

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Index

A

adding 7
adding a MaxPatrol scanner 83
Axis
  add 81
AXISscanner 81

C

connection type 91

D

Digital Defense AVS scanner 7

E

eEye CS Retina
  add JDBC scans 10
  add SNMP scans 9
  overview 9
eEye REM
  add JDBC scans 10
  add SNMP scans 9
  overview 9

F

Foundstone Foundscan 25
Foundstone FoundScan
  add 25
  importing certificates 26

I

IBM AppScan Enterprise
  adding 15
  create user type 13
  publish reports 15
IBM InfoSphere Guardium 17
  adding 17
IBM InfoSphere SiteProtector
  adding 21
IBM Security AppScan Enterprise 13
IBM Security SiteProtector 21
IBM Security Tivoli Endpoint Manager 23
integrating
  Positive Technologies MaxPatrol 83
introduction v

J

Java Cryptography Extension 12
Juniper NSM Profiler 59

L

log sources 3

M

MaxPatrol 83
McAfee Vulnerability Manager 67
  create certificate 69
  import certificates 71
  process certificates 70
Microsoft SCCM 29
  adding 33

N

nCircle IP360 35
  adding 23, 36
  exporting data 35
Nessus 37
  adding a live scan 37, 39
  adding a schedule result import 40, 45
  completed report import XMLRPC API 42
netVigilance SecureScout 65
network administrator v
Nmap 45
  adding a remote live scan 47

O

overview 3, 13, 17, 21, 23, 25, 29, 35, 37, 45, 51, 59, 61, 65, 67, 75, 79, 81

P

Positive Technologies MaxPatrol 83
  adding 83

Q

Qualys Detection 51

R

Rapid7 NeXpose scanner 61

S

SAINT
  add 76
  configure SAINTwriter 75
SAINT scanner 75
scan schedule
  status 89
  view 89
scan schedules 87
scanner
  Beyond Security AVDS 3
  IBM Security AppScan 14
  Juniper NSM Profiler 59
  McAfee Vulnerability Manager 67, 68
  Qualys Detection 51, 53
  Qualys scheduled import asset report 54
  Qualys scheduled import scan report 55
  Rapid7 NeXpose 61, 62
  Tenable SecurityCenter 79
SecureScout scanner
  adding 65
Supported vulnerability scanners 91

T

Tenable SecurityCenter scanner 79

V

vulnerability assessment overview 1