JUNIPER NETWORKS | Engineering Simplicity

Juniper Secure Analytics Managing Vulnerability Assessment Guide

Published
2022-05-13

RELEASE
7.5.0

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Secure Analytics Managing Vulnerability Assessment Guide
7.5.0

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

Use this guide to understand how you can enable vulnerability assessment and use that data to build profiles of attackers and targets.

1
CHAPTER

Vulnerability Assessment Scanner Overview

Vulnerability Assessment Scanner Overview

Integrate vulnerability assessment scanners with JSA to provide vulnerability assessment profiles for network assets.

References to JSA 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.

Installing the Java Cryptography Extension on JSA

The Java Cryptography Extension (JCE) is a Java framework that is required to decrypt advanced cryptography algorithms for AES192 or AES256. The following information describes how to install Oracle JCE on your JSA appliance.

1. Download the latest version of the Java Cryptography Extension.

   The Java Cryptography Extension version must match the version of the Java that is installed on JSA.
2. Extract the JCE file.

   The following Java archive (JAR) files are included in the JCE download:

   - **local_policy.jar**
   - **US_export_policy.jar**
3. Log in to your JSA Console or JSA Event Collector as a root user.
4. Copy the JCE JAR files to the following directory on your JSA Console or Event Collector:

   /opt/ibm/java-x86_64/jre/lib/security/

NOTE: The JCE JAR files are only copied to the system that receives the AES192 or AE256 encrypted files.

5. Restart the JSA services by typing one of the following commands:
   - If you are using JSA 2014.x, type **service ecs-ec restart**.
   - If you are using JSA 7.3.0, type **systemctl restart ecs-ec.service**.
   - If you are using JSA 7.3.1, type **systemctl restart ecs-ec-ingress.service**.

2
CHAPTER

Troubleshooting Scanners

Troubleshooting Scanners

IN THIS SECTION

Problem

Description

If you come across a problem with your scanner, you can troubleshoot the following issues:

Solution

What do you do if the product version or device you have is not listed in the *JSA Vulnerability Assessment Configuration Guide*?

Sometimes a version of a vendor product or a device is not listed as supported. If the product or device is not listed, follow these guidelines:

- **Version not listed** - If the scanner is for a product that is officially supported by JSA, but the version that is listed in the *JSA Vulnerability Assessment Configuration Guide* appears to be out-of-date, try the scanner to see whether it works. The product versions that are listed in the guide are versions that are tested by Juniper, but newer untested versions might also work. In most cases, no changes are necessary, or at most a minor update might be all that is required. Software updates by vendors might on rare occasions add or change event formats that break the scanner, requiring an RFE for the development of a new integration. This scenario is the only case where an RFE is required. In either event, open a support ticket for a review of the log source to troubleshoot and rule out any potential issues that are not related to the software version.
- **Device not listed** - When a device is not officially supported, open a request for enhancement (RFE) to have your device become officially supported by following these steps:

  1. Log in to JSA.

2. Log in to the support portal page.
3. Click the **Submit** tab and type the necessary information.

> **NOTE**: If you have vulnerability data from a scanner, attach it to the RFE and include the product version of the scanner that generated the vulnerability data.

3

CHAPTER

AXIS Scanner

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 JSA 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 JSA, 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.

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

Table 1: 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 JSA uses to log in to the server.
Enable Key Authentication	Specifies that JSA authenticates with a key-based authentication file.
Remote directory	The location of the scan result files.

Table 1: AXIS Scanner - SFTP Properties *(Continued)*

Parameter	Description

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.
	
	NOTE: The `vis.ssh.key` file must have `vis qradar` ownership.
	For example:
	
	`# ls -al /opt/qradar/conf/vis.ssh.key`
	`-rw------- 1 vis qradar 1679 Aug 7`
	`06:24 /opt/qradar/conf/vis.ssh.key`

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 2: AXIS Scanner - SMB Share Properties

Parameter	Description
Hostname	The IP address or host name of the SMB Share.
Login Username	The user name that JSA 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/**.

Table 2: AXIS Scanner - SMB Share Properties *(Continued)*

Parameter	Description
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.

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 an option that is based on one of the following platforms:
   - On the JSA Console, select the managed host that is responsible for communicating with the scanner device.
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**.

For more information about how to create a scan schedule, see "Scheduling a Vulnerability Scan" on page 112.

RELATED DOCUMENTATION

AXIS Scanner | 8

4

CHAPTER

Beyond Security Automatic Vulnerability Detection System Scanner Overview

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. JSA 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, JSA can retrieve the vulnerability data with a scan schedule.

To configure a Beyond Security AVDS scanner, see "Adding a Beyond Security AVDS Vulnerability Scanner" on page 12.

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.

To successfully integrate Beyond Security AVDS vulnerabilities with JSA, 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 JSA, create a scan schedule to import the scan result files. Vulnerabilities from the scan schedule updates the **Assets** tab after the scan schedule completes.

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 an option that is based on one of the following platforms:
   - On the JSA Console, select the managed host that is responsible for communicating with the scanner device.
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: **a.** In the **Login Username** field, type a username that has access to retrieve the scan results from the remote host. **b.** 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:
	a. Select the **Enable Key Authentication** check box.
	b. 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.
	NOTE: The `vis.ssh.key` file must have `vis qradar` ownership.
	For example:
	`# ls -al /opt/qradar/conf/vis.ssh.key`
	`-rw------- 1 vis qradar 1679 Aug 7 06:24 /opt/qradar/conf/vis.ssh.key`

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**.

You are now ready to create a scan schedule. See "Scheduling a Vulnerability Scan" on page 112.

RELATED DOCUMENTATION

Beyond Security Automatic Vulnerability Detection System Scanner Overview | 12

5
CHAPTER

Digital Defense Inc AVS Scanner Overview

Digital Defense Inc AVS Scanner Overview

The Digital Defense, Inc. AVS scanner module accesses vulnerability data from the Digital Defense, Inc. Frontline Vulnerability Manager (Frontline VM) by using the Frontline Connect API.

The Frontline Connect API works with JSA to collect vulnerability information.

JSA users can activate the Digital Defense vulnerability feeds in JSA to gather more information about security events by correlating vulnerability and threat data. Greater visibility is provided about the risk posture of hosts so that the user can make better, more informed decisions, and then take appropriate security action.

Before JSA can collect Digital Defense Frontline VM vulnerability data, you must complete the following steps:

1. "Install the Frontline Vulnerability Manager SSL Certificate" on page 16
2. "Creating an API Key in Frontline Vulnerability Manager" on page 17
3. "Adding a Digital Defense AVS Scanner" on page 18

RELATED DOCUMENTATION

Install the Frontline Vulnerability Manager SSL Certificate | 16
Creating an API Key in Frontline Vulnerability Manager | 17
Adding a Digital Defense AVS Scanner | 18

Install the Frontline Vulnerability Manager SSL Certificate

Before JSA can collect Digital Defense VM vulnerability data, you must download an SSL certificate.

The certificate must have a .crt, .cert, or .der file extension.

Copy the SSL certificate to the **/opt/qradar/conf/trusted_certificates** directory in JSA, by using one of the following options:

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

- SSH into your JSA Console or managed host and then type the following command:

  /opt/qradar/bin/getcert.sh ***<IP or hostname of Frontline VM device>***

When you use this command, the certificate for your Frontline VM is downloaded and placed into the **/opt/qradar/conf/trusted_certificates** directory in the appropriate format.

RELATED DOCUMENTATION

Creating an API Key in Frontline Vulnerability Manager | 17

Adding a Digital Defense AVS Scanner | 18

Creating an API Key in Frontline Vulnerability Manager

Before JSA can collect Digital Defense Frontline VM vulnerability data, you must create an API key in Frontline Vulnerability Manager.

1. Log in to the Frontline VM interface.
2. In the upper right side of the window, click your name, and then select **My Profile**.
3. Click **API Tokens > Create New Token**.
4. In the **Add New Token** field, type a name of your choosing for the token.
5. Select **Click to show key** to display the API key. Copy and record the API key. You need the API key when you add a scanner in JSA.

> **NOTE**: An API key is equivalent to the password of the user that created the API key. Do not use an API Key for more than one integration. If you believe an API Key is compromised, delete the token from the Frontline VM interface to disable it.

RELATED DOCUMENTATION

Adding a Digital Defense AVS Scanner | 18

Install the Frontline Vulnerability Manager SSL Certificate | 16

Adding a Digital Defense AVS Scanner

JSA accesses vulnerability data from the Digital Defense, Inc. Frontline Vulnerability Manager by using the Frontline Connect API that is installed with the Frontline Vulnerability Manager.

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. From the **Type** list, select **Digital Defense Inc AVS**.
5. In the **Scanner Name** field, type a name to identify your Digital Defense Inc AVS scanner.
6. In the **Description** field, type a description for your Digital Defense Inc AVS scanner.
7. Configure the parameters.

   The following table describes the parameters that require specific values for the Digital Defense Inc AVS scanner:

Parameter	Description
Remote Host	The host name of the remote server for the Digital Defense, Inc. AVS scanner. The host name must be `vm.frontline.cloud`.
Remote Port	The port number of the remote server for the Digital Defense, Inc. AVS scanner. The **Remote Port** value must be 443.
Remote URL	The URL of the remote server for the Digital Defense, Inc. AVS scanner. The Remote URL value must be **/nsas/blGateway.php**.
Client ID	A client ID is no longer used for this value. You might want to type the email address of the user who requested the API key.

(Continued)

Parameter	Description
Username	The email address of the user who requested the API key.
Password	The API key that you created when you completed the "Creating an API Key in Frontline Vulnerability Manager" on page 17.
Host Scope	Collects host data from internal or external hosts for the Frontline VM. Select one of the following options: • Internal • External
Retrieve Data for Account	From the list, select **Default**.
Correlation Method	Specifies the method by which vulnerabilities are correlated. Select one the following options: **All Available** - Queries the Frontline VM vulnerability catalog and correlates vulnerabilities that are based on all of the references that are returned for that specific vulnerability. References might include CVE, Bugtraq, Microsoft Security Bulletin, and OSVDB. Multiple references sometimes correlate to the same vulnerability. More results are returned, but processing takes longer than the CVE option. **CVE** - Queries the Frontline VM vulnerability and correlates vulnerabilities that are based only on the CVE-ID.

8. Configure the CIDR ranges that you want this scanner to retrieve by typing the CIDR range, or click **Browse** to select the CIDR range from the network list.
9. Click **Add > Save**.

TIP: Repeat 4 to 9 to create more import parameters.

RELATED DOCUMENTATION

- Install the Frontline Vulnerability Manager SSL Certificate | **16**
- Creating an API Key in Frontline Vulnerability Manager | **17**
- Scheduling a Vulnerability Scan | **112**

6
CHAPTER

eEye Scanner Overview

eEye Scanner Overview

JSA 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" on page 22.
- Add a JDBC protocol eEye scanner. See "Adding an eEye REM JDBC Scan" on page 24.

RELATED DOCUMENTATION

Installing the Java Cryptography Extension on JSA | 2

Adding an eEye REM SNMP Scan

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 JSA with the latest **audits.xml** file.

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

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 an option that is based on one of the following platforms:
   - On the JSA Console, select the managed host that is responsible for communicating with the scanner device.
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**.

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 "Scheduling a Vulnerability Scan" on page 112.

- 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 Java Cryptography Extension on JSA" on page 2.

RELATED DOCUMENTATION

Adding an eEye REM JDBC Scan | 24

Adding an eEye REM JDBC Scan

Before you configure JSA to poll for vulnerability data, we suggest you create a database user account and password for JSA. 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 JSA 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.

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

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 an option that is based on one of the following platforms:
   - On the JSA Console, select the managed host that is responsible for communicating with the scanner device.
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**.

You are now ready to create a scan schedule. See "Scheduling a Vulnerability Scan" on page 112.

RELATED DOCUMENTATION

Adding an eEye REM SNMP Scan | 22

7

CHAPTER

IBM AppScan Enterprise Scanner Overview

IBM AppScan Enterprise Scanner Overview

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

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 JSA, you must complete the following tasks:

1. Generate scan reports in IBM AppScan Enterprise.

   Report configuration information can be found in your IBMAppScan Enterprise documentation.

2. Configure AppScan Enterprise to grant JSA access to report data.

3. Configure your AppScan Enterprise scanner in JSA.

4. Create a schedule in JSA 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 JSA. After AppScan Enterprise users configure reports, the reports that are generated by AppScan Enterprise can be published to JSA, 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 Enterprise" on page 28.

RELATED DOCUMENTATION

Creating a Customer User Type for IBM AppScan Enterprise

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

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 Juniper Secure Analytics (JSA) Integration**— Select this check box to allow users to access the JSA integration options for AppScan Enterprise.
   - **Publish to JSA**— Select this check box to allow JSA access to published scan report data.
   - **JSA 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**.

You are now ready to enable integration permissions. See "Enabling Integration with IBM AppScan Enterprise" on page 28

RELATED DOCUMENTATION

Enabling Integration with IBM AppScan Enterprise | 28

Creating an Application Deployment Map in IBM AppScan Enterprise | 29

Publishing Completed Reports in IBM AppScan Enterprise | 30

Enabling Integration with IBM AppScan Enterprise

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

IBM AppScan Enterprise must be configured to enable integration with JSA.

1. Click the **Administration** tab.
2. On the **Navigation** menu, select **Network Security Systems**.

3. On the JSA Integration Setting pane, click **Edit**.
4. Select the **Enable JSA Integration** check box.

   Any reports that are previously published to JSA 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 JSA, the reports are displayed in this list.

You are now ready to configure the Application Deployment Mapping in AppScan Enterprise. See "Creating an Application Deployment Map in IBM AppScan Enterprise" on page 29.

RELATED DOCUMENTATION

Creating an Application Deployment Map in IBM AppScan Enterprise

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

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.

1. Click the **Administration** tab.
2. On the navigation menu, select **Network Security Systems**.
3. On the JSA 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 JSA, 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 JSA.
6. Click **Add**.
7. Repeat this procedure to map any more production environments in AppScan Enterprise.

8. Click **Done**.

You are now ready to publish completed reports. See "Publishing Completed Reports in IBM AppScan Enterprise" on page 30.

RELATED DOCUMENTATION

Publishing Completed Reports in IBM AppScan Enterprise | 30
Adding an IBM AppScan Enterprise Vulnerability Scanner | 31
Enabling Integration with IBM AppScan Enterprise | 28

Publishing Completed Reports in IBM AppScan Enterprise

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

1. Click the **Scan** tab, and then navigate to the security report that you want to make available to JSA.
2. On the menu bar of any security report, select **Publish > grant reports to JSA** to provide report access to JSA.

You are now ready to enable integration permissions. See "Adding an IBM AppScan Enterprise Vulnerability Scanner" on page 31.

RELATED DOCUMENTATION

Adding an IBM AppScan Enterprise Vulnerability Scanner | 31
Enabling Integration with IBM AppScan Enterprise | 28
Creating an Application Deployment Map in IBM AppScan Enterprise | 29

Adding an IBM AppScan Enterprise Vulnerability Scanner

If your AppScan installation is set up to use HTTPS, a server certificate is required. JSA 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.

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

You can add multiple IBM AppScan scanners to JSA, each with a different configuration. Multiple configurations provide JSA 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.

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 an option that is based on one of the following platforms:
   - On the JSA Console, select the managed host that is responsible for communicating with the scanner device.
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. HTTP and HTTPS are supported in the URL address.

   Example: XML API - **http://myasehostname/ase**

   Example: JSON API - **http://myasehostname/ase/api**
8. From the **API Type** list, select one of the following options:
   - **XML (Before v9.02)**— If your version of AppScan Enterprise is earlier than v9.02, select this option. This API type uses the AppScan XML REST web service.

- **JSON (v9.0.2 and later)**— If your version of AppScan Enterprise is version 9.02 or later, select this option. This API type uses the AppScan JSON REST web service.

9. If you selected **XML (Before v9.02)** as the **API Type**, select one of the following options from the **Authentication Type** list:
   - **Windows Authentication (AppScan Enterprise 9.0 and previous)**— Select this option to use Windows Authentication with the REST web service.
   - **AppScan Enterprise Authentication**— Select this option to use AppScan Enterprise Authentication with the REST web service.
10. In the **Username** field, type the user name to retrieve scan results from AppScan Enterprise.
11. In the **Password** field, type the password to retrieve scan results from AppScan Enterprise.
12. 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 JSA. All matching files from the file pattern are processed by JSA. You can specify a group of vulnerability reports or an individual report by using a regex pattern.
13. 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**.
14. Click **Save**.
15. On the **Admin** tab, click **Deploy Changes**.

You are now ready to create a scan schedule for IBM AppScan Enterprise. See "Scheduling a Vulnerability Scan" on page 112.

RELATED DOCUMENTATION

Enabling Integration with IBM AppScan Enterprise | 28

Creating an Application Deployment Map in IBM AppScan Enterprise | 29

Publishing Completed Reports in IBM AppScan Enterprise | 30

8
CHAPTER

IBM Guardium Scanner Overview

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

Integration overview for IBM InfoSphere Guardium and JSA.

1. On your IBM InfoSphere Guardium appliance, create an SCAP file with your vulnerability information. See your IBM InfoSphere Guardium documentation.
2. On your JSA Console, add an IBM Guardium scanner. See "Adding an IBM Guardium Vulnerability Scanner" on page 34
3. On your JSA Console, create a scan schedule to import scan result data. See"Scheduling a Vulnerability Scan" on page 112

Adding an IBM Guardium Vulnerability Scanner

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

Administrators can add multiple IBM Guardium scanners to JSA, each with a different configuration. Multiple configurations provide JSA 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.

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 an option that is based on one of the following platforms:
   - On the JSA Console, select the managed host that is responsible for communicating with the scanner device.
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: **a.** In the **Login Username** field, type a username that has access to retrieve the scan results from the remote host. **b.** In the **Login Password** field, type the password associated with the user name.

Enable Key Authorization	To authenticate with a key-based authentication file:
	a. Select the **Enable Key Authentication** check box.
	b. 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.
	NOTE: The `vis.ssh.key` file must have `vis qradar` ownership.
	For example:
	`# ls -al /opt/qradar/conf/vis.ssh.key`
	`-rw------- 1 vis qradar 1679 Aug 7 06:24 /opt/qradar/conf/vis.ssh.key`

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**.

You are now ready to create a scan schedule for IBM InfoSphere Guardium. See "Scheduling a Vulnerability Scan" on page 112

RELATED DOCUMENTATION

Configuring Guardium to Produce Report in AXIS Format

You can integrate IBM InfoSphere Guardium with JSA by using the Asset Export Information Source (AXIS) scanner. However, you must ensure that the Guardium vulnerability assessment reports are exported as AXIS format.

1. Log in to the IBM InfoSphere Guardium.
2. Click the **Tools** tab.
3. From the **Tools** page, select **Security Assessment Builder**.
4. Click **New** to create a new assessment.
5. From the **Security Assessment Builder** page, Enter the **Description, Period From**, **To**, **Client Ip** (optional), and **Server Ip** (optional).
6. Click **Add Datasource** and add the data sources that you want to run the assessment tests on.
7. From the **Datasource Finder** page, select a data source, and click **Add**.
8. Click **Apply** to save the newly added data source.
9. Add tests to the assessment by clicking **Configure Test**.
10. Select tests from an inventory of available tests, and click **Add Selections** to add them to the assessment.
11. Click **Return**.
12. To run the assessment, click **Run Once Now**.
13. From the **Assessment Results** screen, click **Create AXIS Results** to generate an output file in axis format.

RELATED DOCUMENTATION

Adding an IBM Guardium Vulnerability Scanner | 34

9

CHAPTER

IBM SiteProtector Scanner Overview

IBM SiteProtector Scanner Overview

The IBM SiteProtector scanner module for JSA 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 SiteProtector scanner, see "Adding an IBM SiteProtector Vulnerability Scanner" on page 39.

RELATED DOCUMENTATION

Adding an IBM SiteProtector Vulnerability Scanner | 39

Adding an IBM SiteProtector Vulnerability Scanner

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

Administrators can add multiple IBM SiteProtector scanners to JSA, each with a different configuration. Multiple configurations provide JSA 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.

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 an option that is based on one of the following platforms:
   - On the JSA Console, select the managed host that is responsible for communicating with the scanner device.
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. If you are using SQL authentication, disable Named Pipe Communication. 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**.

You are now ready to create a scan schedule. See "Scheduling a Vulnerability Scan" on page 112

RELATED DOCUMENTATION

IBM SiteProtector Scanner Overview | 39

10
CHAPTER

Juniper Profiler NSM Scanner Overview

Juniper Profiler NSM Scanner Overview

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

The Network and Security Manager (NSM) console passively collects valuable asset information from your network through deployed Juniper Networks IDP sensors. JSA connects to the Profiler database stored on the NSM server to retrieve these records. The JSA server must have access to the Profiler database. JSA 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, JSA 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" on page 42.

Adding a Juniper NSM Profiler Scanner

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

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 Juniper NSM Profiler server.
5. From the **Managed Host** list, select an option that is based on one of the following platforms:
   - On the JSA Console, select the managed host that is responsible for communicating with the scanner device.

   Certificates for your Juniper NSM Profiler scanner must reside on the managed host selected in the Managed Host list.
6. From the **Type** list, select **Juniper NSM Profiler Scanner**, and then configure the parameters.

Parameter	Description
Server Host Name	The IP address or host name of the Juniper NSM Profiler scanner that contains the vulnerabilities you want to retrieve.

(Continued)

Parameter	Description
Database Username	The user name that is required to access the Juniper NSM Profiler scanner.
Database Password	The password that is required to access the Juniper NSM Profiler scanner.
Database Name	The name of the database on the above server that contains the Juniper NSM Profiler scanner data.

7. To configure a CIDR range for your scanner complete the following steps:
   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**.
8. Click **Save**.

RELATED DOCUMENTATION

Juniper Profiler NSM Scanner Overview | 42

11

CHAPTER

McAfee Vulnerability Manager Scanner Overview

McAfee Vulnerability Manager Scanner Overview

The McAfee Vulnerability Manager scanner for JSA is deprecated.

12

CHAPTER

Microsoft SCCM Scanner Overview

Microsoft SCCM Scanner Overview

JSA imports scan reports from Microsoft System Center Configuration Manager (SCCM) scanners.

The Microsoft SCCM scanner collects the following information:

- Asset information
  - name
  - NetBIOS name, OS and version
  - IP addresses
  - MAC addresses
- Installed patches
- Pending patches

> **NOTE**: Pending patches might or might not have a vulnerability reference.

To integrate a Microsoft SCCM scanner, complete the following steps:

1. On your Microsoft SCCM scanner, configure WMI enablement.
2. If automatic updates are not enabled on your JSA console, download and install the Microsoft SCCM RPM.
3. On your JSA console, add a Microsoft SCCM scanner.
4. On your JSA console, create a scan schedule to import scan result data.

RELATED DOCUMENTATION

Enable WMI for Microsoft SCCM Scanners | 48

Adding a Microsoft SCCM Scanner | 49

Scheduling a Vulnerability Scan | 112

Enable WMI for Microsoft SCCM Scanners

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

The scanner host must meet the following conditions:

- You are a member of the **Read-only Analyst Role** on that host.
- One of the following operating systems is installed:
  - Windows 7
  - Windows 2008
  - Windows 2008 R2
  - Windows 2012
  - Windows 2012 R2 (only 64 bit is supported)
  - Vista software

  NOTE: SCCM is not supported on versions of Windows that were moved to *End of Life* by Microsoft. If a software version date is beyond the *Extended Support End Date*, the product might not function as expected. Juniper does not make code or vulnerability fixes to resolve issues for older operating systems. For example, Microsoft Windows Server 2003 R2 and Microsoft Windows XP are operating systems that are beyond the *Extended Support End Date*. Any questions about this announcement can be discussed in the JSA forums. For more information about support lifecycles, see the Microsoft Support lifecycle website (https://support.microsoft.com//en-us/lifecycle/search)

- DCOM is configured and enabled.

  If a firewall is installed on the host or is located between the host and JSA, 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. DCOM ports are random ports above 1024. Depending on your version of Windows, you might 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.

RELATED DOCUMENTATION

Adding a Microsoft SCCM Scanner | 49

Adding a Microsoft SCCM Scanner

Ensure that WMI is enabled on your scanner host.

Before you can add a Microsoft SCCM scanner, WMI must be enabled on your scanner host.

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 Microsoft SCCM server.
5. From the **Managed Host** list, select an option that is based on one of the following platforms:
   - On the JSA Console, select the managed host that is responsible for communicating with the scanner device.
6. From the **Type** list, select **Microsoft SCCM**, and then configure the parameters.

Parameter	Description
Host Name	The IP address or host name of the remote server that hosts the scan result files.
Domain	The domain that is used to connect to the remote server.

7. Configure the remaining parameters.
8. To configure a CIDR range for your scanner, complete the following steps:
   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**.
9. Click **Save**.

RELATED DOCUMENTATION

Enable WMI for Microsoft SCCM Scanners | 48

13

CHAPTER

nCircle IP360 Scanner Overview

nCircle IP360 Scanner Overview

JSA supports both nCircle and Tripwire versions of the IP360 scanner. Administrators can import XML2 scan reports from SSH servers that contain IP360 vulnerability information.

JSA 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 JSA, 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 JSA imports a scan. JSA 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" on page 52.
2. On your JSA Console, add an nCircle IP360 scanner. See "Adding a nCircle IP360 Scanner" on page 53
3. On your JSA Console, create a scan schedule to import scan result data. See"Scheduling a Vulnerability Scan" on page 112

Exporting nCircle IP360 Scan Results to an SSH Server

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

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

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 JSA to integrate with your nCircle IP360 device.

RELATED DOCUMENTATION

Adding a nCircle IP360 Scanner | 53

Adding a nCircle IP360 Scanner

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

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

If the scanner is configured to use a password, the SSH scanner server to which JSA 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.

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	From the **Managed Host** list, select an option that is based on one of the following platforms: • On the JSA Console, select the managed host that is responsible for communicating with the scanner device.

(Continued)

Parameter	Description
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**.

RELATED DOCUMENTATION

Exporting nCircle IP360 Scan Results to an SSH Server | 52

14

CHAPTER

Nessus Scanner Overview

Nessus Scanner Overview

Tenable provides an integration with JSA by using its Tenable.sc and Tenable.io platforms to address the needs of enterprise customers. For more information about Nessus APIs, see the blog “A Clarfication about Nessus Professional” by Tenable.

As of December 2018, Tenable officially removed support for Nessus APIs. As a result, Tenable does not support direct integration between Nessus and JSA.

15

CHAPTER

netVigilance SecureScout Scanner Overview

netVigilance SecureScout Scanner Overview

JSA 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, JSA connects to the remote database to locate the latest scan results for a given IP address. The data returned updates the asset profile in JSA with the asset IP address, discovered services, and vulnerabilities. JSA supports SecureScout scanner software version 2.6.

We suggest that administrators create a special user in your SecureScout database for JSA 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" on page 58.

Adding a NetVigilance SecureScout Scan

To query for vulnerability data, JSA 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.

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

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 an option that is based on one of the following platforms:

   On the JSA Console, select the managed host that is responsible for communicating with the scanner device.
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**.

You are now ready to create a scan schedule. See "Scheduling a Vulnerability Scan" on page 112.

RELATED DOCUMENTATION

netVigilance SecureScout Scanner Overview | 58

16
CHAPTER

NMap Scanner Overview

NMap Scanner Overview

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

NOTE: Although there is an NMap binary on each JSA host, it is reserved for internal JSA use only. Configuring an NMap vulnerability scanner to use a JSA console or JSA managed host as the remote NMap scanner is not supported and can cause instabilities.

When administrators configure an NMap scan, a specific NMap user account can be created for the JSA system. A unique user account ensures that JSA possesses the credentials that are required to log in and communicate with the NMap server. After the user account creation is complete, administrators can test the connection from JSA to the NMap client with SSH to verify the user credentials. This test 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 64.
- Remote results import. The result data from a previously completed scan is imported over SSH. See "Adding a NMap Remote Result Import" on page 61.

Adding a NMap Remote Result Import

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

Scans must be generated in XML format by 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.

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 JSA 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 host name or IP address of the remote system that hosts the NMap client. Adminitrators should 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: a. In the **Server Username** field, type the user name that is required to access the remote system that hosts NMap client. b. In the **Login Password** field, type the password that is associated with the user name. The password must not contain the ! character. This character might cause authentication failures over SSH. If the scanner is configured to use a password, the SSH scanner server to that connects to JSA 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.

(Continued)

Option	Description

Enable Key Authorization	To authenticate with a key-based authentication file:
	a. Select the **Enable Key Authentication** check box.
	b. 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.
	NOTE: The `vis.ssh.key` file must have `vis qradar` ownership.
	For example:
	`# ls -al /opt/qradar/conf/vis.ssh.key`
	`-rw------- 1 vis qradar 1679 Aug 7 06:24 /opt/qradar/conf/vis.ssh.key`

10. In the **Remote Folder** field, type the directory location of the scan result files.

    Linux example: **/home/scans**

    Windows example: **/c:/zenmap**

11. In the **Remote File Pattern** field, type a regular expression (regex) that is required to filter the list of files that are 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. You should 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 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**.

You are now ready to create a scan schedule. See "Scheduling a Vulnerability Scan" on page 112

RELATED DOCUMENTATION

Adding a NMap Remote Live Scan | 64

Adding a NMap Remote Live Scan

JSA 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.

Several types of NMap port scans require NMap to run as a root user. Therefore, JSA 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 JSA 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.

NOTE: Although there is an NMap binary on each JSA host, it is reserved for internal JSA use only. Configuring an NMap vulnerability scanner to use a JSA console or JSA managed host as the remote NMap scanner is not supported and can cause instabilities.

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 JSA 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: **a.** In the **Server Username** field, type the username required to access the remote system hosting the NMap client using SSH. **b.** 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.

Enable Key Authorization	To authenticate with a key-based authentication file:
	a. Select the **Enable Key Authentication** check box.
	b. 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.
	NOTE: The `vis.ssh.key` file must have `vis qradar` ownership.
	For example:
	`# ls -al /opt/qradar/conf/vis.ssh.key`
	`-rw------- 1 vis qradar 1679 Aug 7 06:24 /opt/qradar/conf/vis.ssh.key`
	If the scanner is configured to use a password, the SSH scanner server to that connects to JSA 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 disable 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**.

You are now ready to create a scan schedule. See "Scheduling a Vulnerability Scan" on page 112

RELATED DOCUMENTATION

Adding a NMap Remote Result Import | **61**

CHAPTER 17

Outpost24 Vulnerability Scanner Overview

Outpost24 Vulnerability Scanner Overview

IN THIS SECTION

JSA 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 3: 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/)

Server Certificates

Before you add a scanner, a server certificate is required to support HTTPS connections. JSA 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 Secure Copy (SCP) or Secure File Transfer Protocol (SFTP).
- To automatically download the certificate to the**/opt/qradar/conf/trusted_certificates** directory, SSH into the Console or managed host and type the following command:

  /opt/qradar/bin/getcert.sh <*IP_or_Hostname*> <*optional_port_(443_default)*>

Install the Java Cryptography Extension

The default certificates that are used by OUTSCAN and HIAB use 2048-bit keys. As a result, you must modify the Java cryptography when you use these certificates. For more information, see "Installing the Java Cryptography Extension on JSA" on page 2.

Configuration Steps

To configure JSA 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 from the Juniper Downloads onto your JSA system.
2. On the Outpost24 vulnerability scanner, create an application token for JSA.
3. On the JSA Console, add the Outpost24 vulnerability scanner. Configure all required parameters and use the following table to identify specific Outpost24 values:

   Table 4: 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

Table 4: Outpost24 Vulnerability Scanner Parameters *(Continued)*

Parameter	Value
API token	Must use the API token that you created on the Outpost24 vulnerability scanner device.

4. Schedule a scan.

Creating an Outpost24 API Authentication Token for JSA

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

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, JSA.
7. Configure the IP restrictions and user access rights.
8. Click **Save**.
9. Copy the 64 character authentication token to a file.

On your JSA system, add the Outpost24 vulnerability scanner.

RELATED DOCUMENTATION

Outpost24 Vulnerability Scanner Overview | 69

18
CHAPTER

Qualys Scanner Overview

Qualys Scanner Overview

IN THIS SECTION

JSA can retrieve vulnerability information from the QualysGuard Host Detection List API or download scan reports directly from a QualysGuard appliance. You can integrate JSA with QualysGuard appliances that use software version 4.7 through 8.1.

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 JSA 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. JSA supports key search parameters to filter for the information that you want to collect. You can also configure how frequently JSA 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

RELATED DOCUMENTATION

Installing the Qualys Certificate | 74
Adding a Qualys Detection Scanner | 74
Adding a Qualys Scheduled Live Scan | 76

Installing the Qualys Certificate

Before you can log in to Qualys, you must download the Qualys certificate into JSA.

A server certificate is required to support HTTPS connections. JSA supports certificates with the following file extensions: .crt, .cert, or .der. Certificates can be manually copied to the **/opt/qradar/conf/trusted_certificates** directory on JSA by using SCP or SFTP. However, you can also download the Qualys certificate from a customer URL.

1. Contact Qualys for a customer URL and your login credentials. For more information about Qualys login, see www.qualys.com/support (https://www.qualys.com/support/faq/login/).
2. Download the certificate by typing the following command:

   /opt/qradar/bin/getcert.sh <*customer_URL*>
3. Copy the downloaded certificate to the **/opt/qradar/conf/trusted_certificates** directory.

RELATED DOCUMENTATION

Adding a Qualys Detection Scanner | 74
Adding a Qualys Scheduled Live Scan | 76
Adding a Qualys Scheduled Import Asset Report | 78

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 .

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 an option that is based on one of the following platforms:
   - On the JSA Console, select the managed host that is responsible for communicating with the scanner device.
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, 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 KnowledgeBase. For more information about how to update Qualys subscription, see your Qualys documentation.
Qualys Password	The password for your Qualys login.
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 JSA to store the Qualys Vulnerability Knowledge Base. If a scan is scheduled and the retention period is expired, the system downloads an update.

(Continued)

Parameter	Description
Force Qualys Vulnerability Update	Forces the system to update to the Qualys Vulnerability Knowledge Base for each scheduled scan.

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

> **NOTE**: The QualysGuard Host Detection List API accepts only CIDR ranges to a maximum of a single class A or /8 and must not encompass the local host IP address (127.0.0.1) or 0.0.0.0.

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

RELATED DOCUMENTATION

Adding a Qualys Scheduled Live Scan | 76

Adding a Qualys Scheduled Import Asset Report | 78

Adding a Qualys Scheduled Import Scan Report | 80

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.

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 an option that is based on one of the following platforms:
   - On the JSA Console, select the managed host that is responsible for communicating with the scanner device.
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, 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 KnowledgeBase. For more information about how to update Qualys subscription, see your Qualys documentation.
Qualys Password	The password for your Qualys login.

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. Optional: To enable JSA 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**.

RELATED DOCUMENTATION

Adding a Qualys Scheduled Import Asset Report | 78

Adding a Qualys Scheduled Import Scan Report | 80

Adding a Qualys Detection Scanner | 74

Adding a Qualys Scheduled Import Asset Report

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

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 an option that is based on one of the following platforms:
   - On the JSA Console, select the managed host that is responsible for communicating with the scanner device.
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, 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 KnowledgeBase. For more information about how to update Qualys subscription, see your Qualys documentation.
Qualys Password	The password for your Qualys login.

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, JSA 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 JSA 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**.

RELATED DOCUMENTATION

Adding a Qualys Scheduled Import Scan Report | 80
Adding a Qualys Detection Scanner | 74
Adding a Qualys Scheduled Live Scan | 76

Adding a Qualys Scheduled Import Scan Report

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

1. On the **Admin** tab, click the **VA Scanners** icon, and then click **Add**.
2. In the **Scanner Name** field, type a name to identify your Qualys scanner.
3. Give your Qualys scanner a name and description.
4. From the **Type** list, select **Qualys Scanner**.
5. 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, the host name and not the URL, use the following syntax **qualysapi.qualys.com** or **qualysapi.qualys.eu**.
Qualys username	The user name that you specify must have access to download the Qualys KnowledgeBase. For more information about how to update Qualys subscription, see your Qualys documentation.

(Continued)

Parameter	Description
Qualys password	The password for your Qualys login.

6. If you use a proxy server, select the **Use Proxy** check box and configure the credentials for the proxy server.
7. If a client certificate is required for your Qualys account, select the **Use Client Certificate** check box and configure the **Certificate File Path** field and **Certificate Password** fields.
8. From the **Collection Type** list, select **Scheduled Import - Scan Report**. This option pulls in the scan results from the Scans tab of the Qualys Enterprise console.
9. Configure the following parameters:

Parameter	Description
Option Profiles	The name of the option profile to determine which scan to start. JSA 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.
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, JSA 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 **Options Profile** field.

10. To create custom vulnerabilities from the live scan data, select the **Enable Custom Vulnerability Creation** check box, and then select options that you want to include.

11. To configure a CIDR range for your scanner, configure the CIDR range parameters and click **Add**.
12. Click **Save**.

You are now ready to create a scan schedule. See "Scheduling a Vulnerability Scan" on page 112.

RELATED DOCUMENTATION

- Adding a Qualys Detection Scanner | **74**
- Adding a Qualys Scheduled Live Scan | **76**
- Adding a Qualys Scheduled Import Asset Report | **78**

19
CHAPTER

Rapid7 NeXpose Scanners Overview

Rapid7 NeXpose Scanners Overview

Rapid7 NeXpose scanners can provide site data reports to JSA 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" on page 86.
- Site import of a local file. See "Adding a Rapid7 NeXpose Scanner Local File Import" on page 84
- Site import of a remote file. See "Adding a Rapid7 Nexpose Scanner Remote File Import" on page 88

Adding a Rapid7 NeXpose Scanner Local File Import

Before you add this scanner, a server certificate is required to support HTTPS connections. JSA 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.

JSA uses local files to import site vulnerability data from your Rapid7 Nexpose scanner.

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 JSA. The destination directory on the managed host must exist before the Rapid7 NeXpose appliance can copy site reports to the managed host. The site files can be copied to the managed host using Secure Copy (SCP) or Secure File Transfer Protocol (SFTP).

The import directory created on the managed host or JSA console must have the appropriate owner and permission set on it for the vis user within JSA. For example, **chown -R vis:qradar** ***<import_directory_path>*** and **chmod 755** ***<import_directory_path>*** set the owner of the import directory path to vis user with adequate read-write-execute permissions.

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.

You must use the **XML Export** or **XML Export 2.0** report format for the XML export to JSA.

XML Export is also known as **raw XML**. The XML export contains an extensive set of scan data with the smallest amount of structure. The XML export scan data must be parsed so that other systems can use the information.

XML Export 2.0 is similar to **XML Export**, but has more attributes:

- Asset Risk
- Exploit Title
- Site Name
- Exploit IDs
- Malware Kit Name(s)
- Site Importance
- Exploit Skill Needed
- PCI Compliance Status
- Vulnerability Risk
- Exploit Source Link
- Scan ID
- Vulnerability Since
- Exploit Type
- Scan Template.

1. Click **Admin** > **System Configuration**.
2. Click the **VA Scanners** icon, and then click **Add**.
3. Type a **Scanner Name** to identify your Rapid7 NeXpose scanner.
4. From the **Managed Host** list, select an option that is based on one of the following platforms:
    - On the JSA Console, select the managed host that is responsible for communicating with the scanner device.

5. From the **Type** list, select **Rapid7 Nexpose Scanner**.
6. From the **Import Type** list, select **Import Site Data - Local File**.
7. Type the directory path to the XML vulnerability data in the Import Folder field. If you specify an import folder, you must move the vulnerability data from your Rapid7 Nexpose scanner to JSA.
8. 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 that match the regex pattern are included when the vulnerability scan report is imported. You must use a valid regex pattern in this field. The default value **..*\.xml** imports all files from the import folder.
9. Enter the CIDR range that you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
10. Click **Save**.
11. On the **Admin** tab, click **Deploy Changes**.

You are now ready to create a scan schedule. See "Scheduling a Vulnerability Scan" on page 112.

RELATED DOCUMENTATION

Adding a Rapid7 NeXpose Scanner API Site Import | 86

Adding a Rapid7 NeXpose Scanner API Site Import

Before you add this scanner, a server certificate is required to support HTTPS connections. JSA 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.

API imports enable JSA 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.

1. Click **Admin** > **System Configuration**.
2. Click the **VA Scanners** icon, and then click **Add**.
3. Type a **Scanner Name** to identify your Rapid7 NeXpose scanner.

4. From the **Managed Host** list, select an option that is based on one of the following platforms:
   - On the JSA Console, select the managed host that is responsible for communicating with the scanner device.
5. Select **Rapid7 Nexpose Scanner** from the **Type** list.
6. From the **Import Type** list, select **Import Site Data - Local File**.
   - **Import Site Data** - **Asset and Vulnerability data via SQL API** - Default and suggested option for importing results.
   - **Import Site Data** - **Adhoc Report via API**
7. In the **Remote Hostname** field, type the IP address or host name of the Rapid7 NeXpose scanner.
8. In the **Login Username** field, type the user name that is used 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.
9. In the **Login Password** field, type the password to access the Rapid7 NeXpose scanner.
10. 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.
11. 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.
12. 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.
13. Enter the path to the local directory to store downloaded XML reports.
14. To configure a CIDR range for the scanner complete the following steps:
    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**.

You are now ready to create a scan schedule. See "Scheduling a Vulnerability Scan" on page 112.

RELATED DOCUMENTATION

Adding a Rapid7 NeXpose Scanner Local File Import | 84

Adding a Rapid7 Nexpose Scanner Remote File Import

Before you add this scanner, make sure that you have a server certificate that supports HTTPS connections. JSA 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.
- Use SSH to log in to 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.

JSA uses remote files to import site vulnerability data from your Rapid7 Nexpose scanner.

Remote file imports collect vulnerabilities for a site from a remote 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 JSA. The destination directory on the managed host or Console must exist before the Rapid7 Nexpose appliance can copy site reports. The site files can be copied to the managed host or Console by using Secure Copy (SCP) or Secure File Transfer Protocol (SFTP).

The import directory that is created on the managed host or JSA Console must have the appropriate owner and permission set on it for the VIS user within JSA. For example, chown -R vis:qradar *<import_directory_path>* and chmod 755 *<import_directory_path>* set the owner of the import directory path to VIS user with adequate read-write-execute permissions.

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.

1. Click **Admin** > **System Configuration**.
2. Click the **VA Scanners** icon, and then click **Add**.
3. Type a **Scanner Name** to identify your Rapid7 NeXpose scanner.
4. From the **Managed Host** list, select an option that is based on one of the following platforms:
   - On the JSA Console, select the managed host that is responsible for communicating with the scanner device.
5. From the **Type**, select **Rapid7 Nexpose Scanner**.

6. From the **Import Type** list, select **Import Site Data - Remote File**.
7. Enter the **Remote Hostname** of the server that has the scan result files and the **Remote Port** of the remote SSH server.
8. Enter the user name and password for the remote SSH server.
9. Optional: Enable key authentication, and then enter the full local path to the SSH private key file.
10. Indicate the location of the remote directory that contains the scan results on the remote SSH server.
11. In the **File 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 that match the regex pattern are included when the vulnerability scan report is imported. You must use a valid regex pattern in this field. The default value **.*\.xml** imports all files from the import folder.
12. Enter the maximum number of days to use the report file. Files older than this number of days aren't processed. Set the number to 0 if you want to disable report age checking.
13. Configure a CIDR range for your scanner:
    a. In the 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**.

You are now ready to create a scan schedule. See "Scheduling a Vulnerability Scan" on page 112.

RELATED DOCUMENTATION

Rapid7 NeXpose Scanners Overview | 84

Adding a Rapid7 NeXpose Scanner Local File Import | 84

Adding a Rapid7 NeXpose Scanner API Site Import | 86

20

CHAPTER

SAINT Security Suite Overview

SAINT Security Suite Scanner

JSA collects and imports scan reports from Security Administrator's Integrated Network Tool (SAINT) Security Suite vulnerability appliances by JSA using the SAINT API. SAINT Security Suite scan reports include vulnerability data, MAC addresses, port information, and service information.

To integrate SAINT Security Suite with JSA, complete the following steps:

1. From your SAINT Security Suite appliance, obtain and record the SAINT API port number. You need this information when you add a scanner in JSA. See"Obtaining the SAINT API Port Number" on page 92.

2. From your SAINT Security Suite appliance, obtain and record the SAINT API token. You need this information when you add a scanner in JSA. See "Obtaining the SAINT API Token" on page 93.

3. From your SAINT Security Suite appliance, configure the SAINT API to send scan reports to JSA. See "Adding a JSA Host to the Allowed API Clients List" on page 93.

4. Copy the server certificate to support HTTPS connections. See "Copy the Server Certificate" on page 94.

5. From your JSA Console, add a SAINT Security Suite vulnerability scanner. See "Adding a SAINT Security Suite Vulnerability Scanner in JSA" on page 95.

   The SAINT Security Suite vulnerability scanner supports the **Live Scan** and **Report Only** scan options in JSA.

   - **Live scan** - If you select this option when you add a SAINT Security Suite scanner in JSA, JSA starts a live remote vulnerability scan on the SAINT Scanner. When the scan is complete, JSA collects and imports the vulnerability scan report. You might want to select this option if you don't have any existing scans on the SAINT Security Suite appliance.

   - **Report only** - If you select this option when you add a SAINT Security Suite scanner in JSA, JSA imports only scan reports for scans that exist on the SAINT Security Suite appliance. You might want to select this option if the SAINT Security Suite appliance has scans that are scheduled to run regularly.

6. From your JSA Console, create a scan schedule for the scanner that you added. See "Scheduling a Vulnerability Scan" on page 112.

RELATED DOCUMENTATION

Copy the Server Certificate | 94

Obtaining the SAINT API Port Number

You must be a SAINT user with the necessary permissions and have the web address for the SAINT web console. These items are supplied by your scanner administrator.

Before you can add a SAINT Security Suite scanner in JSA, you must obtain and record the SAINT API port number from the SAINT web console.

The SAINT API port is the port on the SAINT Security Suite appliance that the SAINT API uses for listening. JSA uses the SAINT API port to send API requests to the SAINT Security Suite scanner.

1. Log in to the SAINT web console by using the web address that you use to access the SAINT Security Suite appliance. The web address is provided by your SAINT Security Suite scanner administrator.
2. Click **Configuration > System Options**.
3. Click the **API** tab, and then record the SAINT API port number that is displayed in the **API Port** field.

Use the SAINT API port number when you add the SAINT Security Suite scanner in JSA.

RELATED DOCUMENTATION

Obtaining the SAINT API Token

You must be a SAINT user with the necessary permissions and have the web address for the SAINT web console. These items are supplied by your scanner administrator.

Before you can add a SAINT Security Suite scanner in JSA, you must obtain the SAINT API token from the SAINT web console. The SAINT API token is a unique identifier that is used by JSA to authenticate API requests to the SAINT Security Suite scanner.

1. Log in to the SAINT web console by using the web address that you use to access the SAINT appliance. The web address is provided by your SAINT Security Suite scanner administrator.
2. From the menu bar, select **Profile**.
3. In the User Profile window, record the value in the **API Token** field.

Use the API token that you recorded when you add the SAINT Security Suite scanner in JSA.

RELATED DOCUMENTATION

- SAINT Security Suite Scanner | 91
- Copy the Server Certificate | 94
- Obtaining the SAINT API Port Number | 92
- Adding a JSA Host to the Allowed API Clients List | 93
- Adding a SAINT Security Suite Vulnerability Scanner in JSA | 95
- Scheduling a Vulnerability Scan | 112

Adding a JSA Host to the Allowed API Clients List

You must be a SAINT user with the necessary permissions and have the web address for the SAINT web console. These items are supplied by your scanner administrator.

Before you can add a SAINT Security Suite scanner in JSA, you must add the IP address for your JSA Console to the list of allowed API clients on the SAINT web console.

1. Log in to the SAINT web console by using the web address that you use to access the SAINT Security Suite appliance.
2. Click **Configuration > System Options**.
3. Click the **API** tab.

4. In the **Allowed API Clients** field, type the IP address of your JSA host. If you want to specify more than one JSA host, you can type multiple IP addresses in a comma-separated list.
5. Click **Save**.

RELATED DOCUMENTATION

- SAINT Security Suite Scanner | 91
- Copy the Server Certificate | 94
- Obtaining the SAINT API Port Number | 92
- Obtaining the SAINT API Token | 93
- Adding a SAINT Security Suite Vulnerability Scanner in JSA | 95
- Scheduling a Vulnerability Scan | 112

Copy the Server Certificate

You need a server certificate to support HTTPS connections. JSA supports certificates with the `.crt, .cert, or .der` file extensions.

To copy a certificate to the **/opt/qradar/conf/trusted_certificates directory**, choose one of the following options:

1. Manually copy the certificate to the **/opt/qradar/conf/trusted_certificates directory** by using SCP or SFTP.
2. Use SSH to log in to the JSA Console or managed host and retrieve the certificate by typing the following command:

   /opt/qradar/bin/getcert.sh <IP or Hostname of the SAINT API><Port of the SAINT API>

   A certificate is downloaded from the specified host name or IP address and placed into the **/opt/qradar/conf/trusted_certificates directory** in the appropriate format.

RELATED DOCUMENTATION

- SAINT Security Suite Scanner | 91
- Obtaining the SAINT API Port Number | 92
- Obtaining the SAINT API Token | 93
- Adding a JSA Host to the Allowed API Clients List | 93

Adding a SAINT Security Suite Vulnerability Scanner in JSA

Before you can add the SAINT Security Suite vulnerability scanner in JSA, you need to complete the following steps:

1. "Obtaining the SAINT API Port Number" on page 92.
2. "Adding a JSA Host to the Allowed API Clients List" on page 93.
3. "Obtaining the SAINT API Token" on page 93.
4. "Copy the Server Certificate" on page 94.

JSA uses the SAINT API to collect and import scan reports from your SAINT Security Suite appliance.

1. Log in to the JSA Console.
2. Click the **Admin** tab.
3. Click the **VA Scanners** icon, and then click **Add**.
4. In the **Scanner Name** field, type a name to identify your SAINT Security Suite scanner.
5. From the **Managed Host** list, selectan option that is based on one of the following platforms:
   - On the JSA Console, select the managed host that is responsible for communicating with the scanner device.
6. From the **Type** list, select **SAINT Security Suite Scanner**.
7. In the **Remote API Hostname** field, type the IP address or the host name for the SAINT API.
8. In the **API Port** field, type the SAINT API port number. For more information about the API port, go to "Obtaining the SAINT API Port Number" on page 92.
9. In the **API Token** field, type the SAINT API token. For more information about the SAINT API token, go to "Obtaining the SAINT API Token" on page 93.
10. From the **Scan Type** list, select one of the following scan type options:

Option	Description
Live Scan	JSA creates and runs a new scan on the SAINT Security Suite appliance. After the scan completes, JSA collects and imports a scan report from the SAINT Security Suite appliance.
Report Only	JSA collects and imports scan reports for all scans that are already on the SAINT Security Suite appliance that match the following requirements. • The scan is not older than the age specified in the **Max Report Age** field. • The scan level of the scan matches the specified **Scan Level**. • The target map of the scan has at least one IP address in common with the CIDR range. This option does not start new scans on the SAINT Security Suite appliance. To collect accurate results, ensure that relevant, regularly run scans are scheduled on the SAINT Security Suite appliance.

11. From the Scan Level list, select a scan level that you want to use from the following options.

> **NOTE**: On the SAINT Security Suite appliance and in SAINT Security Suite documentation, scan levels are referred to as scan policies. For more information OVAL/SCAP scans, go to the SAINT Security Suite documentation website . From the navigation pane, click **User Guide > SCAP**.

Scan level	Description
Normal	SAINT collects information to get the general character of a host and establishes the operating system type and, if possible, the software release version.

(Continued)

Scan level	Description
Heavy/Vulnerability Scan	The **Heavy/Vulnerability Scan** level is also known as the heavy policy. SAINT looks for services that are listening on TCP or UDP ports. Any services that are detected are scanned for any known vulnerabilities. This scan includes SAINT's entire set of vulnerability checks, and is the scan policy that SAINT suggests you use in most situations.
Discovery	SAINT scans the targets and determines which targets have live hosts. This scan level only completes the minimum scanning that is required to identify live hosts. Therefore, the **Discovery** scan is not very intrusive.
Port Scan	SAINT identifies services that are listening on TCP or UDP ports.
Web Crawl	SAINT detects web directories on the targets by scanning ports for web services, and then finds directories by following HTML links, starting from the home page.
SQL/XSS	SAINT looks for SQL injection and cross-site scripting vulnerabilities on web servers. Both generic tests are included. SAINT finds HTML forms and tests all parameters for SQL injection and cross-site scripting, and then checks for known SQL injection and cross-site scripting vulnerabilities.
Windows Patch	SAINT looks for missing Windows patches. Most of the checks for Windows patches require Windows domain authentication.

(Continued)

Scan level	Description
Content Search	SAINT searches files on Windows and Linux/Mac targets for credit card numbers, social security numbers, or any other patterns that are specified. Authentication is needed. If you are scanning a Linux/Mac target, SSH must be enabled.
PCI	SAINT scans the targets by using all vulnerability checks that are relevant for Payment Card Industry and Data Security Standard (PCI DSS) compliance.
Anti-virus Information	Information is collected about installed AV software, such as last scan date, enabled, definition file dates, and other information that is useful for auditing requirement 5 of the PCI DSS. Information is also collected for Windows versions for many of the AV software products, such as McAfee, Symantec, AVG, F-Secure, MS Forefront, and Trend Micro. Authentication is needed. Facts that contain the string '(Master)' indicate that an anti-virus server, manager, or admin is installed on the target.
FISMA	SAINT scans the targets by using all vulnerability checks that are relevant for Federal Information Security Management Act (FISMA) compliance.
Authentication Test	SAINT authenticates against the targets by using the credentials that are specified when adding a vulnerability scanner.
Win Password Guess	Completes password guess checks against Windows targets by using the password guess and password dictionary configuration options. Authentication is suggested for SAINT to enumerate accounts.

(Continued)

Scan level	Description
Microsoft Patch Tuesday	Checks for the last published Microsoft patch Tuesday vulnerabilities on the second Tuesday of each month. This scan level and associated content are usually updated by SAINTexpress by noon on Wednesday.
Web Scan (OWASP Top 10)	Checks for vulnerabilities in web servers and web applications, such as SQL injection, cross-site scripting, unpatched web server software, weak SSL ciphers, and other OWASP Top 10 vulnerabilities. It also enables file content checks. Authentication might be necessary for some of the checks that are included.
IAVA (Maps CVEs to IAVA codes)	SAINT scans the targets by using all vulnerability checks that are relevant for Information Assurance Vulnerability Alert (IAVA) compliance.
OS Password Guess	Includes all SAINT password guess features that are designed to guess the operating system password. This policy includes checks for default FTP passwords, and dictionary-based password guesses through Telnet, SSH, and FTP. Authentication is suggested to ensure user account enumeration.
NERC CIP	SAINT scans the targets by using all vulnerability checks that are relevant for North American Electric Reliability Corporation and Critical Infrastructure Protection (NERC CIP) compliance.

(Continued)

Scan level	Description
Software Inventory	Generates a list of software that is installed on Windows targets. Authentication is needed. The software list is generated by enumerating the uninstall key in the Windows registry. Only software that was registered with the operating system during installation is included. Software that was placed on the system without running an installer program is usually omitted. Registered software that was incorrectly removed from the system might be included in the list after removal.
HIPAA	SAINT scans the targets by using all vulnerability checks that are relevant for Health Insurance Portability and Accountability Act (HIPAA) compliance.
SOX	SAINT scans the targets by using all vulnerability checks that are relevant for Sarbanes-Oxley Act (SOX) compliance.

(Continued)

Scan level	Description
Mobile Device	The **Mobile Device** scan level queries Active Directory servers for information about mobile devices that use Exchange ActiveSync, and then uses that information to suggest vulnerabilities on those devices. The devices are listed in the scan results as separate targets even though those targets are not scanned. For this scan level to succeed, OpenLDAP must be installed on the scanning host, and the scan must run with Windows domain administrator credentials. For more information about Authentication, go to the SAINT Security Suite documentation website - Step 4 – Authentication. The target list must include at least one Active Directory server, and the SSL certificate for that Active Directory server is installed and configured on the scanning host. For more information about Windows Targets, go to the SAINT Security Suite documentatin website - Authenticating to Windows Targets.
Network Device	Checks for vulnerabilities in routers, switches, and other networking devices.
OVAL Scan	Runs an OVAL/SCAP scan. For more information about OVAL/SCAP scans, go to the SAINT Security Suite documentation website. From the navigation pane, click **User Guide > Using SAINT > SCAP**.

For more information about SAINT scan parameters, go to the SAINT Security Suite documentation website and complete the following steps. From the navigation pane, click **User Guide > Using SAINT > Jobs Tab**.

12. If you selected **OVAL Scan** from the **Scan Level** list, type the name of the scan policy that you want to use in the **OVAL Scan Policy Name** field. OVAL/SCAP scans are types of scans that are based on benchmarks that are collected from authoritative sources.

13. If you selected **Live Scan** for the scan type, provide the scan target credentials that are used to authenticate targets during scans. From the **Scan Target Credentials Type** list, select one of the following options for the credentials that you want to use:

> **NOTE**: Scan Target credentials are ignored when **Report Only** is selected for the scan type.

Option	Description
None	Do not use any credentials.
HTTP Basic	Use credentials for basic HTTP credentials.
Linux/Unix/Mac (SSH)	Use credentials for connecting to a Linux, UNIX, or Mac server through SSH.
Microsoft SQL Server	Use credentials for connecting to a Microsoft SQL Server database.
Oracle	Uses credentials for connecting to an Oracle database.
Windows Admin	Use credentials of an administrator account on a Windows server.
Windows non-Admin	Use credentials of a non-administrator account on a Windows server.
MySQL	Use credentials for connecting to a MySQL database.
SNMPv3	Use SNMPv3 credentials.

14. If you selected any of the options, except for the **None** option from the **Scan Target Credentials Type** list, configure the following parameters for the **Scan Target Credentials** that you selected:

Parameter	Value
Scan Target Credentials Username	The user name for the scan target credential that you selected.
Scan Target Credentials Password	The password for the scan target credential that you selected.

15. Optional: If you selected **Linux/Unix/Mac (SSH)** from the **Scan Target Credentials Type** list, specify the **SSH Private Key**.
16. Optional: If you selected **Oracle** from the **Scan Target Credentials Type** list, you can specify an Oracle Service ID (SID) of an Oracle database instance by typing it in the **Oracle SID** field.
17. Optional: If you selected **SNMPv3** from the **Scan Target Credentials Type** list, complete the following steps:
    a. Select one of the following checksum algorithm options from the **SNMP Password Protocol** list:

Option	Description
SHA	Select this option for the password that you typed in the **Scan Target Credentials Password** field to use the SHA protocol.
MD5	Select this option for the password that you typed in the **Scan Target Credentials Password** field to use the MD5 protocol

    b. Optional: You can specify an **SNMP passphrase** by typing it in the **SNMP Passphrase** field. If you specified an **SNMP Passphrase**, select one of the following options from the **SNMP Passphrase Protocol** list:

Option	Description
DES	Select this option for the passphrase that you typed in the **SNMP passphrase** field to use the DES protocol.

(Continued)

Option	Description
AES	Select this option for the password that you typed in the **SNMP passphrase** field to use the AES protocol.

18. If you selected **Report Only** from the **Scan Type** list, type the maximum age of scan reports that you want to import in the **Max Report Age** field.
19. Configure CIDR ranges for the scanner:
    a. In the **CIDR Ranges** field, type the CIDR range for the scan or click **Browse** to select a CIDR range from the network list.
    b. Click Add.
20. Click **Save**.

RELATED DOCUMENTATION

SAINT Security Suite Scanner | 91

Copy the Server Certificate | 94

Obtaining the SAINT API Port Number | 92

Obtaining the SAINT API Token | 93

Adding a JSA Host to the Allowed API Clients List | 93

Scheduling a Vulnerability Scan | 112

21
CHAPTER

Tenable.io Scanner Overview

Tenable.io Scanner Overview

JSA collects and imports scan reports from Tenable.io by using the Tenable.io API. Tenable.io scan reports include vulnerability data, MAC addresses, port information, and service information.

To integrate Tenable.io with JSA, complete these steps:

- Obtain and record the Tenable.io API Access key and Secret key from Tenable.io. You need this information when you add a scanner in JSA.
- From your JSA Console, add a Tenable.io scanner.
- From your JSA Console, schedule a vulnerability scan.

RELATED DOCUMENTATION

Obtaining the Tenable.io API Access key and Secret key | 106

Adding a Tenable.io Scanner to JSA | 107

Scheduling a Vulnerability Scan | 112

Obtaining the Tenable.io API Access key and Secret key

You must obtain the Tenable.io API Access and Secret keys from Tenable.io before you can add a Tenable.io scanner in JSA. JSA collects vulnerability information by using the Tenable.io API.

1. Log in to Tenable.io as Administrator.
2. Click the **API Keys** tab.
3. Click **Generate**, and then record the **Access key** and **Secret key** values. These keys are used to authenticate with the Tenable.io REST API. You will need these values when you add a Tenable.io scanner in JSA.

> **NOTE**: Existing API keys are replaced. You must update the applications where previous API keys were used.

You are now ready to add a scanner in JSA. See "Adding a Tenable.io Scanner to JSA" on page 107.

RELATED DOCUMENTATION

Tenable.io Scanner Overview | 106

Adding a Tenable.io Scanner to JSA | 107

Adding a Tenable.io Scanner to JSA

You must be a Tenable.io user, and you must have the Tenable.io API Public key and Secret key. For more information, see "Obtaining the Tenable.io API Access key and Secret key" on page 106.

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

1. Click the **Admin** tab, click the **VA Scanners** icon in the Data Sources section, and then click **Add**.
2. In the **Scanner Name** field, type a name to identify your Tenable.io scanner.
3. From the **Managed Host** list, select an option that is based on one of the following platforms:
   - On the JSA Console, select the managed host that is responsible for communicating with the scanner device.
4. From the **Type** list, select **Tenable.io**.
5. In the **API End point** field, type **cloud.tenable.com**.
6. In the **Access Key** field, type the Tenable.io **Access key** value that you recorded when you completed the "Obtaining the Tenable.io API Access key and Secret key" on page 106.
7. In the **Secret Key** field, type the Tenable.io **Secret key** value that you recorded when you completed the "Obtaining the Tenable.io API Access key and Secret key" on page 106.
8. Select the **Severity level(s)** for which you want to filter the results.
9. Configure a CIDR range for the Tenable.io scanner. In the **CIDR range** field, type the CIDR range for the scan, or click **Browse** to select a CIDR range from the network list.
10. Click **Add**, and then click **Save**.
11. On the **Admin** tab, click **Deploy Changes**.

You are now ready to create a scan schedule. See "Scheduling a Vulnerability Scan" on page 112.

RELATED DOCUMENTATION

Tenable.io Scanner Overview | 106

Obtaining the Tenable.io API Access key and Secret key | 106

22

CHAPTER

Tenable SecurityCenter Scanner Overview

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" on page 109.

Adding a Tenable SecurityCenter Scan

Verify the location of the API on your Tenable SecurityCenter.

A server certificate is required to support HTTPS connections. JSA 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 hostname or IP and placed into **/opt/qradar/conf/trusted_certificates** directory in the appropriate format.

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

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 an option that is based on one of the following platforms:
   - On the JSA Console, select the managed host that is responsible for communicating with the scanner device.
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 API on the Tenable SecurityCenter.

   The default path to the API file for SecurityCenter Version 4 is **sc4/request.php**.

The default path to the API file for SecurityCenter Version 5 is **rest**.

9. From the **API Version** list, select the version for your SecurityCenter.

> **TIP**: Support for Tenable SecurityCenter (Tenable.sc) on JSA is limited to the versions supported by Tenable. For more information, see Tenable Software Release Lifecycle Matrix.

10. In the **User Name** field, type the username to access the Tenable SecurityCenter API.
11. In the **Password** field, type the password to access the Tenable SecurityCenter API.
12. Enable or disable the **Allow Untrusted Certificates** parameter, which is based on the certificate type you use.

    If you enable the **Allow Untrusted Certificates** parameter, the scanner can accept selfsigned and otherwise untrusted certificates that are located within the **/opt/qradar/conf/trusted_certificates/** directory. If you disable the parameter, the scanner trusts only certificates that are signed by a trusted signer.

> **TIP**: By default, this parameter is enabled for existing scanners and disabled for new scanners.

13. Configure a CIDR range for the scanner.
    a. In the CIDR ranges field, 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**.

You are now ready to create a scan schedule. See "Scheduling a Vulnerability Scan" on page 112.

RELATED DOCUMENTATION

Tenable SecurityCenter Scanner Overview | 109

23
CHAPTER

Scheduling a Vulnerability Scan

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.

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.

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.

(Continued)

Option	Description
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. Select **Clean Vulnerability Ports** to delete all vulnerabilities found on each asset, and replace with data reported in the next scan run.
11. Click **Save**.

CHAPTER 24

Viewing the Status Of a Vulnerability Scan

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.

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

Table 5: 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.

Table 5: Scan Schedule Status *(Continued)*

Column name	Description
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.

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.

25

CHAPTER

Supported Vulnerability Scanners

Supported Vulnerability Scanners

Vulnerability data can be collected from several manufacturers and vendors of security products as shown in Table 6 on page 118. 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 6: 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
Digital Defense Inc	AVS	N/A	Digital Defense Inc AVS	HTTPS
eEye Digital Security	eEye REM	REM V3.5.6	eEye REM Scanner	SNMP trap listener
	eEye Retina CS	Retina CS V3.0 to V4.0		Database queries over JDBC
Generic	Axis	N/A	Axis Scanner	File import of vulnerability data with SFTP
IBM	IBMAppScan Enterprise	V8.6 to V9.0.3.10	IBMAppScan Scanner	IBM REST web service with HTTP or HTTPS
IBM	InfoSphereGuardium	v9.0 and above	IBMGuardium SCAP Scanner	File import of vulnerability data with SFTP
IBM	Bigfix	V8.2x to V9.5.2	IBM BigFix Scanner	SOAP-based API with HTTP or HTTPS

Table 6: Supported Vulnerability Scanners *(Continued)*

Vendor	Scanner name	Supported versions	Configuration name	Connection type
IBM	InfoSphereSite Protector	V2.9.x	IBMSiteProtector Scanner	Database queries over JDBC
IBM	Tivoli Endpoint Manager Now known as IBM BigFix			
Juniper Networks	Network and Security Manager (NSM) Profiler	2007.1r2	Juniper NSM Profiler Scanner	Database queries over JDBC
		2007.2r2		
		2008.1r2		
		2009r1.1		
		2010.x		
McAfee	Vulnerability Manager **NOTE**: The McAfee Vulnerability Manager scanner for JSA is deprecated.			
Microsoft	Microsoft System Center Configuration Manager (SCCM)	MicrosoftWindows	Microsoft SCCM	DCOM must be configured and enabled

Table 6: Supported Vulnerability Scanners *(Continued)*

Vendor	Scanner name	Supported versions	Configuration name	Connection type
nCircle or Tripwire	IP360	VnE Manager V6.5.2 to V6.8.28	nCircle ip360 Scanner	File import of vulnerability data with SFTP
net Vigilance	SecureScout	V2.6	SecureScout Scanner	Database queries over JDBC
Open source	NMap	V3.7 to V6.0	NMap Scanner	File import of vulnerability data over SFTP with SSH command execution
Outpost 24	Outpost24	HIAB V4.1 OutScan V4.1	Outpost24	API over HTTPS
Qualys	QualysGuard	V4.7 to V8.1	Qualys Scanner	APIv2 over HTTPS
Qualys	QualysGuard	V4.7 to V8.1	Qualys Detection Scanner	API Host Detection List over HTTPS
Rapid7	NeXpose	V4.x to V6.5	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	Security Administrator's Integrated Network Tool (SAINT)	V7.4.x	Saint Scanner	File import of vulnerability data over SFTP with SSH command execution

Table 6: Supported Vulnerability Scanners *(Continued)*

Vendor	Scanner name	Supported versions	Configuration name	Connection type
Tenable	SecurityCenter	V4 and V5	Tenable SecurityCenter	JSON request over HTTPS
Tenable	Nessus Tenable provides an integration with JSA by using its Tenable.sc and Tenable.io platforms to address the needs of enterprise customers. For more information about Nessus APIs, see the blog “A Clarfication about Nessus Professional” by Tenable. As of December 2018, Tenable officially removed support for Nessus APIs. As a result, Tenable does not support direct integration between Nessus and JSA.			