McAfee Vulnerability Manager scanner overview

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

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

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

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

- To add a remote XML import for vulnerability data, see "Adding a remote XML import scan."
- To retrieve vulnerabilities from the SOAP API, see "Adding a McAfee Vulnerability Manager SOAP API scan" on page 2

Adding a remote XML import scan

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

About this task

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

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

Procedure

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

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

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

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

Adding a McAfee Vulnerability Manager SOAP API scan

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

Procedure

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

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

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

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

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

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

What to do next

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

Creating certificates for McAfee Vulnerability Manager

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

Before you begin

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

About this task

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

The McAfee Foundstone Enterprise Manager server must be compatible with the version of the FIPS-Capable OpenSSL used by the Foundstone Certificate Manager

to correctly create the certificates. A Java™ Software Development Kit (Java SDK) must be present on this server for this processing. To obtain the most recentJava SDK go to the following website:

http://java.sun.com.

Procedure

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

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

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

What to do next

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

Processing certificates for McAfee Vulnerability Manager

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

Before you begin

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

Procedure

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

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

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

Results

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

What to do next

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

Importing certificates for McAfee Vulnerability Manager

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

Before you begin

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

Procedure

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

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

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

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

Index

M

O

S