

Manage AXIS scanners

IBM

Contents

AXIS scanner 1-1
Adding an AXIS vulnerability scan 1-1

Index X-1

AXIS scanner

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

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

Adding an AXIS vulnerability scan

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

About this task

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

Table 1-1. 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 QRadar uses to log in to the server.
Enable Key Authentication	Specifies that QRadar authenticates with a key-based authentication file.
Remote directory	The location of the scan result files.
Private Key File	The full path to the file that contains the private key. If a key file does not exist, you must create the <code>vis.ssh.key</code> file.
File Name Pattern	The regular expression (regex) required to filter the list of files that are in the <i>Remote Directory</i> . The <code>.*\.xml</code> 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 1-2. AXIS scanner - SMB Share properties

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

Table 1-2. AXIS scanner - SMB Share properties (continued)

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

Procedure

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

What to do next

For more information about how to create a scan schedule, see [Scheduling a vulnerability scan](#).

Index

A

Axis

 add 1-1

AXISscanner 1-1

O

overview 1-1