IBM QRadar Vulnerability Manager 7.4.0

User Guide

Note

Before you use this information and the product that it supports, read the information in “Notices” on page 131.

© Copyright International Business Machines Corporation 2012, 2020.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Introduction to IBM QRadar Vulnerability Manager

This information is intended for use with IBM QRadar Vulnerability Manager. QRadar Vulnerability Manager is a scanning platform that is used to identify, manage, and prioritize the vulnerabilities on your network assets.

This guide contains instructions for configuring and using QRadar Vulnerability Manager on an IBM QRadar SIEM or IBM QRadar Log Manager console.

Intended audience

System administrators responsible for configuring IBM QRadar Vulnerability Manager must have administrative access to IBM QRadar SIEM and to your network devices and firewalls. The system administrator must have knowledge of your corporate network and networking technologies.

Technical documentation

For information about how to access more technical documentation, technical notes, and release notes, see Accessing IBM Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacting customer support

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

Statement of good security practices

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

© Copyright IBM Corp. 2012, 2020

Chapter 1. What's new for users in QRadar Vulnerability Manager 7.4.0

QRadar Vulnerability Manager 7.4.0 introduces a new search parameter to identify controversial vulnerabilities, and enhancements to vulnerability exceptions.

Controversial vulnerabilities search parameters

QRadar Vulnerability Manager 7.4.0 includes new search parameters that leverage vulnerability data that is retrieved from multiple scanners. The **Found by Scanner** and **Not Found by Scanner** parameters provide the following benefits:

- Reduce data set redundancy through the removal of duplicate vulnerabilities.
- Improve quality of results by reducing potential false positives.
- Compare vulnerabilities discovered by multiple scanners to improve scanning techniques and identify shortcomings.

Enhancement to vulnerability exceptions

QRadar Vulnerability Manager 7.4.0 removes a limitation that allowed users to create exceptions for only one vulnerability instance in an exception rule. You can now create rules that include exceptions for multiple vulnerabilities.

For more information, see the *IBM QRadar Vulnerability Manager User Guide*.

© Copyright IBM Corp. 2012, 2020

Chapter 2. Installations and deployments

Depending on the product that you install and whether you upgrade IBM QRadar or install a new system, the **Vulnerabilities** tab might not be displayed.

You access IBM® Security QRadar Vulnerability Manager by using the Vulnerabilities tab:

- If you install QRadar SIEM, the **Vulnerabilities** tab is enabled by default with a temporary license key.
- If you install QRadar Log Manager, the **Vulnerabilities** tab is not enabled. You can purchase the license for QRadar Vulnerability Manager separately and enable it by using a license key.

For more information about upgrading, see the *IBM QRadar Upgrade Guide*.

QRadar Vulnerability Manager license

To use QRadar Vulnerability Manager after an install or upgrade, you must upload and allocate a valid license key. For more information, see the *Administration Guide*. The license for QRadar Vulnerability Manager license is applied and processed in real time to QRadar Vulnerability Manager scanned assets that have at least one IP address. The QRadar Vulnerability Manager scan must fall within the configured retention time for the IP address of the asset.

1. From the **Admin** tab, click the **Asset Profiler Configuration**
2. Find the **Asset IP Retention (In Days)** row to edit the asset IP retention value.
3. Change the retention value or check that it is suitable for your needs. The default asset IP retention value is 120 days.

QRadar Vulnerability Manager and QRadar Risk Manager licenses

IBM QRadar Vulnerability Manager and IBM QRadar Risk Manager are combined into one offering and both are enabled through a single base license. The combined offering provides an integrated network scanning and vulnerability management workflow. With the base license, you are entitled to use QRadar Vulnerability Manager to scan up to 256 assets. You can integrate QRadar Risk Manager with up to 50 standard configuration sources. If you are entitled to either QRadar Vulnerability Manager or QRadar Risk Manager, you are automatically entitled to the base license allowance for the other product. You require extra licenses to scan more than 256 assets or to integrate with more than 50 configuration sources.

Vulnerability processing and scanning deployments

When you install and license QRadar Vulnerability Manager, a vulnerability processor is automatically deployed on your QRadar console. A processor is not automatically deployed if you use a software activation key on your QRadar console.

The vulnerability processor provides a scanning component by default. If required, you can deploy more scanners, either on dedicated QRadar Vulnerability Manager managed host scanner appliances or QRadar managed hosts. For example, you can deploy a vulnerability scanner on an Event Collector or QRadar QFlow Collector.

If required, you can move the vulnerability processor to a different managed host in your deployment. You might move the processor to preserve disk space on your QRadar console.

Restriction: You can have only one vulnerability processor in your deployment. You can move the vulnerability processor only to a dedicated QRadar Vulnerability Manager processor appliance. You can't add a vulnerability processor to the QRadar Flow Processor 1728 appliance.

You can add the vulnerability processor to the following QRadar appliances: 600, 700, 8099, 8024, 8000, 3124, 8026, 2100, 3199, 3126, 8021, and 3100.

© Copyright IBM Corp. 2012, 2020

Auto updates and vulnerability information

When you run the auto update, you get the most recent vulnerability metadata and scan tools that are available. Configure your auto updates through an internet connection or from a local offline server. Typically, vulnerability metadata and scan tools are updated weekly.

As a best practice, ensure that you run auto updates after you install a QRadar software update. Run auto update from the **Admin** tab, by clicking the **Auto Update** icon.

For more information about installing QRadar auto updates, see the *IBM QRadar Administration Guide*.

Related concepts

Options for adding scanners to your QRadar Vulnerability Manager deployment

Options for moving the vulnerability processor in your QRadar Vulnerability Manager deployment

Vulnerability processor and scanner appliance activation keys

You can scan and process your vulnerabilities by using dedicated QRadar Vulnerability Manager managed host appliances.

When you install a processor or scanner managed host appliance, you must type a valid activation key.

For more information about installing a managed host appliance, see the *Installation Guide* for your product.

The activation key is a 24-digit, four part, alphanumeric string that you receive from IBM. The activation key specifies which software modules apply for each appliance type:

- The QRadar Vulnerability Manager processor appliance includes vulnerability processing and scanning components.
- The QRadar Vulnerability Manager scanner appliance includes only a vulnerability scanning component.

You can obtain the activation key from the following locations:

- If you purchased a QRadar Vulnerability Manager software or virtual appliance download, a list of activation keys are included in the *Getting Started* document that is attached in a confirmation email. You can use this document to cross-reference the part number for the appliance that you are supplied with.
- If you purchased an appliance that is preinstalled with QRadar Vulnerability Manager software, the activation key is included in your shipping box or CD.

Vulnerability backup and recovery

You can use the backup and recovery capabilities in IBM QRadar SIEM to back up and restore IBM QRadar Vulnerability Manager vulnerability and configuration data.

When you install QRadar Vulnerability Manager, the QRadar SIEM nightly or on-demand backups include QRadar Vulnerability Manager scan profiles, scan results, and configuration information.

You can configure data or configuration backups and recovery by using the **Admin** tab.

For more information about backup and recovery, see the *IBM QRadar Administration Guide*.

Ports used for communication between QRadar and QRadar Vulnerability Manager managed hosts

QRadar Vulnerability Manager uses secure ports to connect to managed hosts.

Ports used for communication

The following table describes the ports that are used for secure communication between QRadar and QRadar Vulnerability Manager managed hosts.

Table 1. QRadar Vulnerability Manager communication ports

Communication	Port	Protocol
QRadar Console to QRadar Vulnerability Manager processor	22, 9999, 8989, 8844	TCP
QRadar Console to QRadar Vulnerability Manager scanner	22	TCP
QRadar Vulnerability Manager processor to QRadar Console	443	TCP
QRadar Vulnerability Manager scanner to QRadar Vulnerability Manager processor	9999	TCP

Options for moving the vulnerability processor in your QRadar Vulnerability Manager deployment

If required, you can move the vulnerability processor from your QRadar console to a dedicated QRadar Vulnerability Manager managed host appliance.

For example, you might move your vulnerability processing capability to a managed host to minimize disk space impact on your QRadar console.

Restriction: You can have only one vulnerability processor in your deployment. Also, you must deploy the vulnerability processor only on a QRadar console or QRadar Vulnerability Manager managed host processor appliance.

To move the vulnerability processor, choose one of the following options:

Option 1: Deploy a dedicated QRadar Vulnerability Manager processor appliance

To deploy a processor appliance you must complete the followings tasks:

1. Install a dedicated QRadar Vulnerability Manager processor appliance.
2. Add the managed host processor appliance to your QRadar Console by using the **System and License Management** tool on the **Admin** tab.

   When you select the managed host option, the processor is automatically removed from the QRadar console.

Option 2: Move the vulnerability processor from your console to your managed host

If the vulnerability processor is on your QRadar console, then later you can move your vulnerability processor to a previously installed QRadar Vulnerability Manager managed host processor appliance.

At any time, you can move the vulnerability processor back to your QRadar console.

Deploying a dedicated QRadar Vulnerability Manager processor appliance

You can deploy a dedicated QRadar Vulnerability Manager processor appliance as a managed host.

When you deploy your vulnerability processor to a managed host, all vulnerabilities are processed on the managed host.

Restriction: After you deploy processing to a dedicated QRadar Vulnerability Manager managed host, any scan profiles or scan results that are associated with a QRadar console processor are not displayed. You can continue to search and view vulnerability data on the **Manage Vulnerabilities** pages.

Before you begin

Ensure that a dedicated QRadar Vulnerability Manager managed host is installed and a valid processor appliance activation key is applied. For more information, see the *Installation Guide* for your product.

Procedure

1. Log in to QRadar Console as an administrator:

   `https://`*`IP_Address_QRadar`*

   The default user name is `admin`. The password is the password of the root user account that was entered during the installation.
2. On the navigation menu (☰), click **Admin**.
3. In the **System Configuration** pane, click **System and License Management**.
4. From the host table, click the QRadar Console host, and click **Deployment Actions** > **Add Host**.
5. Enter the IP address and password for the host.
6. To create an SSH tunnel on port 22, select **Encrypt Host Connections**.

   Important: Do not select **Remote Tunnel Initiation** for encryption on managed hosts.
7. To enable encryption compression for communications with a host, select **Encryption Compression**.
8. To enable NAT for a managed host, select **Network Address Translation** and add the following information:

   Table 2. NAT configuration

Field	Description
NAT Group	If the managed host is on the same subnet as the QRadar Console, select the QRadar Console that is on the NATed network. If the managed host is not on the same subnet as the QRadar Console, select the managed host that is on NATed network.
Public IP	The managed host uses this IP address to communicate with other managed hosts in different networks that use NAT.

   The NATed network must use static NAT.
9. Click **Add**.

   Note: Don't close the window until the process for adding the host completes.
10. Close the **System and License Management** window.
11. On the **Admin** tab toolbar, click **Advanced** > **Deploy Full Configuration**.
12. Click **OK**.

Related concepts

Vulnerability processor and scanner appliance activation keys

Related tasks

Verifying that a vulnerability processor is deployed

Moving your vulnerability processor to a managed host or console

If required, you can move your vulnerability processor between a QRadar Vulnerability Manager managed host appliance and your QRadar console.

Before you begin

Ensure that a dedicated QRadar Vulnerability Manager managed host is installed and a valid processor appliance activation key is applied.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click **System and License Management** > **Deployment Actions** > **Manage Vulnerability Deployment**.
3. Click **Enable Processor**.
4. Select the managed host or console from the **Processor** list.

   If your processor is on the managed host, you can select only the QRadar console.
5. Click **Save**.
6. On the **Admin** tab toolbar, select **Advanced** > **Deploy Full Configuration**.
7. Click **OK**.

   After you change your vulnerability processor deployment, you must wait for your deployment to fully configure. In the **Scan Profiles** page, the following message is displayed: **QVM is in the process of being deployed.**

Related concepts

Vulnerability processor and scanner appliance activation keys

Verifying that a vulnerability processor is deployed

In IBM QRadar Vulnerability Manager, you can verify that your vulnerability processor is deployed on a QRadar console or QRadar Vulnerability Manager managed host.

Procedure

1. Log in to the QRadar console.
2. On the navigation menu (☰), click **Admin**.
3. Click **System and License Management** > **Deployment Actions** > **Manage Vulnerability Deployment**.
4. Verify that the processor is displayed on **Processor** list.

Removing a vulnerability processor from your console or managed host

If required, you can remove the vulnerability processor from a QRadar console or QRadar Vulnerability Manager managed host.

Procedure

1. Log in to the QRadar console.
2. On the navigation menu (☰), click **Admin**.

3. Click **System and License Management** > **Deployment Actions** > **Vulnerability Deployment Management**.
4. Click the **Enable Processor** check box to deselect it.
5. Click **Remove**.
6. Click **Save**.
7. Close the **System and License Management** window.
8. On the **Admin** tab toolbar, select **Advanced** > **Deploy Full Configuration**.
9. Click **OK**.

Options for adding scanners to your QRadar Vulnerability Manager deployment

If you have a large network and require flexible scanning options, you can add more scanners to your IBM QRadar Vulnerability Manager deployment.

Your QRadar Vulnerability Manager processor is automatically deployed with a scanning component. By deploying more scanners you can increase the flexibility of your scanning operations. For example, you can scan specific areas of your network with different scanners and at different scheduled times.

Dynamic vulnerability scans

The vulnerability scanners that you deploy might not have access to all areas of your network. In QRadar Vulnerability Manager you can assign different scanners to network CIDR ranges. During a scan, each asset in the CIDR range that you want to scan is dynamically associated with the correct scanner.

To add more vulnerability scanners, choose any of the following options:

Deploy a dedicated QRadar Vulnerability Manager managed host scanner appliance
You can scan for vulnerabilities by using a dedicated QRadar Vulnerability Manager managed host scanner appliance.

Important: Do not select **Remote Tunnel Initiation** for encryption on managed hosts.

To deploy a scanner appliance, you must complete the followings tasks:

1. Install a dedicated QRadar Vulnerability Manager managed host scanner appliance.
2. Add the managed host scanner appliance to your QRadar Console by using the **System and License Management** tool on the **Admin** tab.

Deploy a QRadar Vulnerability Manager scanner to your QRadar console or managed host
If you move your vulnerability processor from your QRadar console to a QRadar Vulnerability Manager managed host, you can add a scanner to your console.

You can also add a vulnerability scanner to any of the following QRadar managed hosts: QRadar Console, Event Processor, Flow Processor, Combo Processor, Event Collector, QFlow Collector, and Data Node.

Note: The vulnerability scanner cannot be added to the App Host, App Node, and QRadar Network Insights.

Run an automatic update when you add a scanner or other managed host with scanning capabilities. For more information about automatic updates, see the *IBM Security QRadar Administration Guide*.

Configure access to an IBM hosted scanner and scan your DMZ
You can configure access to an IBM hosted scanner and scan the assets in your DMZ.

Related concepts
Dynamic vulnerability scans

In IBM QRadar Vulnerability Manager, you can configure a scan to use certain vulnerability scanners for specific CIDR ranges in your network. For example, your scanners might have access only to certain areas of your network.

Related tasks

Associating vulnerability scanners with CIDR ranges
In IBM QRadar Vulnerability Manager, to do dynamic scanning, you must associate vulnerability scanners with different segments of your network.

Scanning CIDR ranges with different vulnerability scanners
In IBM QRadar Vulnerability Manager, you can scan areas of your network with different vulnerability scanners.

Deploying a dedicated QRadar Vulnerability Manager scanner appliance

You can deploy a dedicated QRadar Vulnerability Manager managed host scanner appliance.

Before you begin

Ensure that a dedicated QRadar Vulnerability Manager managed host scanner appliance is installed and a valid appliance activation key is applied.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click **System and License Management** > **Deployment Actions** > **Add Managed Host**.
3. Enter the Host IP address and password of the QRadar Vulnerability Manager managed host scanner appliance.
4. Click **Add**.

   You must wait several minutes while the managed host is added.
5. Close the **System and License Management** window.
6. On the **Admin** tab toolbar, select **Advanced** > **Deploy Full Configuration**.
7. Click **OK**.

Related concepts

Vulnerability processor and scanner appliance activation keys

Deploying a vulnerability scanner to a QRadar console or managed host

You can deploy a QRadar Vulnerability Manager scanner to a QRadar console or QRadar managed host. For example, you can deploy a scanner to a flow collector, flow processor, event collector, event processor, or data node.

Before you begin

In an All-in-One deployment the controller is used as a built-in scanner. You cannot add a separate scanner appliance to a QRadar Console when the QRadar Vulnerability Manager processor is on the QRadar Console. In a non-All-in-One deployment it's a good practice to move the QRadar Vulnerability Manager processor to a dedicated appliance when you're scanning more than 50k assets.

To deploy a scanner on your QRadar console, ensure that the vulnerability processor is moved to a dedicated QRadar Vulnerability Manager managed host appliance.

To deploy scanners on QRadar managed hosts, ensure that you have existing managed hosts in your deployment. For more information, see the *Installation Guide* for your product.

Procedure

1. On the navigation menu ( ), click **Admin**.
2. Click **System and License Management** > **Deployment Actions** > **Manage Vulnerability Deployment**.
3. Click **Add Additional Vulnerability Scanners**.
4. Click the **+** icon.
5. From the **Host** list, select the QRadar managed host or console.

   Restriction: You cannot add a scanner to a QRadar console when the vulnerability processor is on the console. You must move the vulnerability processor to a QRadar Vulnerability Manager managed host.
6. Click **Save**.
7. Close the **System and License Management** window.
8. On the **Admin** tab toolbar, select **Advanced** > **Deploy Full Configuration.**.
9. Click **OK**.
10. Check the **Scan Server** list on the **Scan Profiles Configuration** page to ensure that the scanner is added.

    For more information, see "Creating a scan profile" on page 37.

What to do next

Run an automatic update after you add the scanner or other managed host with scanning capabilities. Alternatively, you can scan after the default daily scheduled automatic update runs. If the automatic updates for other scanners are run earlier, then the automatic updates for all the scanners might not be fully synchronized until the next daily update.

Related tasks

Moving your vulnerability processor to a managed host or console

Scanning the assets in your DMZ

In IBM QRadar Vulnerability Manager, you can connect to an external scanner and scan the assets in your DMZ for vulnerabilities.

If you want to scan the assets in the DMZ for vulnerabilities, you do not need to deploy a scanner in your DMZ. You must configure QRadar Vulnerability Manager with a hosted IBM scanner that is located outside your network.

Detected vulnerabilities are processed by the processor on either your QRadar console or QRadar Vulnerability Manager managed host.

Procedure

1. Configure your network and assets for external scans.
2. Configure QRadar Vulnerability Manager to scan your external assets.

Related information

QRadar Vulnerability Manager - New External Scan / DMZ Scan Addresses

Configuring your network and assets for external scans

To scan the assets in a DMZ network, you must configure your network and inform IBM of the assets that you want to scan.

About this task

To scan assets in a DMZ network, you must complete the following steps:

1. Configure the network.
2. Send required network specifics to the External Scanner Team.

Configuring the network for external scans

To scan the assets in a DMZ network, you must first configure your network for external scans.

Procedure

1. Ensure that the QRadar Vulnerability Manager processor has internet access to allow communication with the DMZ scanner.

   Note: A static IP address is required.
2. Ensure each asset that is to be scanned by the DMZ scanner has internet access.
3. Configure an outbound firewall rule for port 443 to allow a connection to the DMZ scanner.

   Tip: Incoming connections are not required.
4. Allowlist `external-scanner.qradar.ibmcloud.com` on network intrusion detection systems to enable end-to-end certificate transparency between the QRadar Vulnerability Manager processor and the DMZ scanner.

Sending network specifics to the External Scanner Team

After you configure your network for external scans, you must inform IBM of the assets that you want to scan.

Procedure

Send the following network specifics to the External Scanner Team at QRadar-QVM-Hosted-Scanner@hursley.ibm.com.

Option	Description
Gateway IP address	The External/Public IP of the QRadar Vulnerability Manager processor (where the scan originates from). If you use a proxy server, provide the IP of the proxy server instead.
Load balancers (optional)	If you employ load balancers, an explicit list or range of all load balancers is required.
IP address list/range	The explicit list/range of all the assets to be scanned.

Restriction: DMZ/External scans do not complete successfully until the requested information is sent to QRadar-QVM-Hosted-Scanner@hursley.ibm.com and a confirmation email is received.

Related information

QRadar Vulnerability Manager - New External Scan / DMZ Scan Addresses

Configuring QRadar Vulnerability Manager to scan your external assets

To scan the assets in your DMZ, you must configure IBM QRadar Vulnerability Manager, by using the **System and License Management** tool on the **Admin** tab.

Procedure

1. From the **Admin** tab, click **System and License Management**.
2. From the **Display** menu, select **Systems**.
3. Click **Deployment Actions** > **Manage Vulnerability Deployment**.
4. Click **Use External Scanner**.
5. In the **Gateway IP** field, enter an external IP address.

Restriction: You cannot scan external assets until your external IP address is configured. Ensure that you email details of your external IP address to IBM.

6. If your network is configured to use a proxy server, click **Enable Proxy Server** and enter the details of your server.
7. Click **Save** and then click **Close**.
8. On the **Admin** tab toolbar, click **Advanced** > **Deploy Full Configuration**.
9. Click **OK**.

   A scanner that is called **IbmExternalScanner** is added to your deployment. You can either associate your DMZ CIDR ranges with this scanner or use this scanner as a scan server in scan profiles.

   Important: Authenticated scans are not conducted from the external scanner.

Related information

QRadar Vulnerability Manager - New External Scan / DMZ Scan Addresses

Supported web browsers

For the features in IBM QRadar products to work properly, you must use a supported web browser.

The following table lists the supported versions of web browsers.

Table 3. Supported web browsers for QRadar products

Web browser	Supported versions
64-bit Mozilla Firefox	60 Extended Support Release and later
64-bit Microsoft Edge	38.14393 and later
64-bit Google Chrome	Latest

The Microsoft Internet Explorer web browser is no longer supported on QRadar 7.4.0 or later.

Security exceptions and certificates

If you are using the Mozilla Firefox web browser, you must add an exception to Mozilla Firefox to log in to QRadar. For more information, see your Mozilla Firefox web browser documentation.

Navigate the web-based application

When you use QRadar, use the navigation options available in the QRadar Console instead of your web browser **Back** button.

QRadar Vulnerability Manager high-availability scans

Use a QRadar high-availability (HA) deployment to maintain your vulnerability scanning schedule, if your primary QRadar deployment fails.

High-availability (HA) version 2 is supported in QRadar Vulnerability Manager.

You must use identical appliances with identical software configurations in your high-availability (HA) setup. For information about setting up a high-availability (HA) deployment, see the *IBM QRadar High Availability Guide*.

High availability (HA) scans

The following appliances are supported in a QRadar Vulnerability Manager high-availability (HA) deployment:

- Console
- Scanner appliance (610)
- Processor appliance (600)

Important notes

Take note of the following information when you deploy high availability (HA) vulnerability scanning:

- Cancel and restart any in-progress scans after a failover if the scans were in progress during the failover.
- If you replace an appliance in your HA scanning environment, it might not appear in the deployment. You must re-add the appliance to the HA deployment, and then deploy changes.
- Use identical appliances and configurations in your high availability (HA) setup.
- Auto updates do not resume after a failover. You must run an auto update in an uninterrupted active setup.

Extending the QRadar Vulnerability Manager temporary license period

By default, when you install IBM QRadar SIEM, you can see the **Vulnerabilities** tab because a temporary license key is also installed. When the temporary license expires, you can extend it for an extra four weeks.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click the **Vulnerability Manager** icon in the **Try it out** area.
3. To accept the end-user license agreement, click **OK**.

   When the extended license period is finished, you must wait six months before you can activate the temporary license again. To have permanent access to QRadar Vulnerability Manager, you must purchase a license.

QRadar Vulnerability Manager high-availability scans

Use a QRadar high-availability (HA) deployment to maintain your vulnerability scanning schedule, if your primary QRadar deployment fails.

High-availability (HA) version 2 is supported in QRadar Vulnerability Manager.

You must use identical appliances with identical software configurations in your high-availability (HA) setup. For information about setting up a high-availability (HA) deployment, see the *IBM QRadar High Availability Guide*.

High availability (HA) scans

The following appliances are supported in a QRadar Vulnerability Manager high-availability (HA) deployment:

- Console
- Scanner appliance (610)
- Processor appliance (600)

Important notes

Take note of the following information when you deploy high availability (HA) vulnerability scanning:

- Cancel and restart any in-progress scans after a failover if the scans were in progress during the failover.

- If you replace an appliance in your HA scanning environment, it might not appear in the deployment. You must re-add the appliance to the HA deployment, and then deploy changes.
- Use identical appliances and configurations in your high availability (HA) setup.
- Auto updates do not resume after a failover. You must run an auto update in an uninterrupted active setup.

Chapter 3. Overview of QRadar Vulnerability Manager

IBM QRadar Vulnerability Manager is a network scanning platform that detects vulnerabilities within the applications, systems, and devices on your network or within your DMZ.

QRadar Vulnerability Manager uses security intelligence to help you manage and prioritize your network vulnerabilities. For example, you can use QRadar Vulnerability Manager to continuously monitor vulnerabilities, improve resource configuration, and identify software patches. You can also, prioritize security gaps by correlating vulnerability data with network flows, log data, firewall, and intrusion prevention system (IPS) data.

You can maintain real-time visibility of the vulnerabilities that are detected by the built-in QRadar Vulnerability Manager scanner and other third-party scanners. Third-party scanners are integrated with QRadar and include HCL BigFix®, Guardium®, AppScan®, Nessus, nCircle, and Rapid 7.

Note:

Upon deployment, the QRadar Vulnerability Manager automatically updates the default **BB:Host Definition: VA Scanner Source IP** building block to include the locations of all QVM processors. This behavior is by design.

To manually add to this building block, add a new source IP Test Group with new IP addresses.

Unless otherwise noted, all references to QRadar Vulnerability Manager refer to IBM QRadar Vulnerability Manager. All references to QRadar refer to IBM QRadar SIEM and IBM QRadar Log Manager and all references to SiteProtector refer to IBM Security SiteProtector.

Vulnerability scanning

In IBM QRadar Vulnerability Manager, vulnerability scanning is controlled by configuring scan profiles. Each scan profile specifies the assets that you want to scan and the scan schedule.

Vulnerability processor

When you license QRadar Vulnerability Manager, a vulnerability processor is automatically deployed on your QRadar console. The processor contains a QRadar Vulnerability Manager scanning component.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Deployment options

Vulnerability scanning can be deployed in different ways. For example, you can deploy your scanning capability to a QRadar Vulnerability Manager managed host scanner appliance or a QRadar managed host.

Configuration options

Administrators can configure scans in the following ways:

- Schedule scans to run at times convenient for your network assets.
- Specify the times during which scans are not allowed to run.
- Specify the assets that you want to exclude from scans, either globally or for each scan.
- Configure authenticated patch scans for Linux®, UNIX, or Windows operating systems.
- Configure different scanning protocols or specify the port ranges that you want to scan.

© Copyright IBM Corp. 2012, 2020

Categories of QRadar Vulnerability Manager vulnerability checks

IBM QRadar Vulnerability Manager checks for multiple types of vulnerabilities in your network.

Vulnerabilities are categorized into the following broad categories:

- Risky default settings
- Software features
- Misconfiguration
- Vendor flaws

Risky default settings

By leaving some default settings in place, you can make your network vulnerable to attacks. The following situations are examples that can make your network vulnerable:

- Leaving sample pages or scripts on an IIS installation
- Not changing the default password on a 3Com Hub/Switch
- Leaving "public" or "private" as an SNMP community name on an SNMP enabled device
- Not setting the sa login password on an MS-SQL server

Software features

Some software settings for systems or applications are designed to aid usability but these settings can introduce risk to your network. For example, the Microsoft NetBIOS protocol is useful in internal networks, but if it is exposed to the Internet or an untrusted network segment it introduces risk to your network.

The following examples are software features or commands that can expose your network to risk:

- ICMP time stamp or netmask requests
- Sendmail expand or verify commands
- Ident protocol services that identify the owner of a running process.

Misconfiguration

In addition to identifying misconfigurations in default settings, QRadar Vulnerability Manager can identify a broader range of misconfigurations such as in the following cases:

- SMTP Relay
- Unrestricted NetBios file sharing
- DNS zone transfers
- FTP World writable directories
- Default administration accounts that have no passwords
- NFS World exportable directories

Vendor flaws

Vendor flaws is a broad category that includes events such as buffer overflows, string format issues, directory transversals, and cross-site scripting. Vulnerabilities that require a patch or an upgrade fix are included in this category.

Checks made by QRadar Vulnerability Manager

QRadar Vulnerability Manager uses a combination of active checks that involves sending packets and remote probes, and passive correlation checks. The QRadar Vulnerability Manager database covers approximately 70,000 Network, OS, and Application layer vulnerabilities.

You can search the complete scanning library by CVE, date range, vendor name, product name, product version, and exposure name from the **Research** window on the **Vulnerabilities** tab.

QRadar Vulnerability Manager tests

The following examples are some of the categories that QRadar Vulnerability Manager tests:

- Database checks
- Web server checks
- Web application server checks
- Common web scripts checks
- Custom web application checks
- DNS server checks
- Mail server checks
- Application server checks
- Wireless access point checks
- Common service checks
- Obsolete software and systems

The following table describes some checks that are made by QRadar Vulnerability Manager.

Table 4. Types of QRadar Vulnerability Manager checks

Type of Check	Description
Port scan	Scans for active hosts and the ports and services that are open on each active host. Returns MAC if the host is on the same subnet as the scanner. Returns OS information.

Table 4. Types of QRadar Vulnerability Manager checks (continued)	
Type of Check	**Description**
Web application scanning	Checks each web application and web page on a web server by using the following checks: File upload HTTP directory browsing CWE-22 - Improper limitation of a path name to a restricted directory (path traversal) Interesting file / seen in logs Auto complete password in Browser Misconfiguration in default files Information disclosure Unencrypted login form Directory index-able: checks if the server directories can be browsed HTTP PUT allowed: checks if the PUT option is enabled on server directories Existence of obsolete files CGI scanning: common web page checks Injection (XSS/script/HTML) Remote file retrieval (server wide) Command execution from remote shell SQL injection, including authentication bypass, software identification, and remote source Reverse tuning options, except for specified options. **Note:** Authenticated web app scanning is not supported. For example, if authentication is required to access the site, you can't run web app tests.
OS	User name and password disclosure Access to file systems Default user names and passwords Privilege escalation Denial of service Remote command execution Cross site scripting (Microsoft)
Database	Exploits and open access to databases. Default passwords Compromised user names and passwords Denial of service Admin rights

Table 4. Types of QRadar Vulnerability Manager checks (continued)	
Type of Check	**Description**
Web server	Known vulnerabilities, exploits, and configuration issues on web servers. Denial of service Default admin passwords File system view ability Cross site scripting
Common web scripts	Commonly found web scripts such as CGI E-commerce-related scripts ASP PHP
DNS server	Weak password encryption Denial of service Determine account names Send emails Read arbitrary emails and sensitive account information Get admin access
Wireless access point	Default admin account passwords Default SNMP community names Plain text password storage Denial of service
Common services	Domain name system (DNS) File transfer protocol (FTP) Simple mail transfer protocol (SMTP)
Application server	Authentication bypass Denial of service Information disclosure Default user names and passwords Weak file permissions Cross site scripting
Oval	Client-side vulnerabilities on IE, Chrome, Skype, and others.
Password testing	Default password testing
Windows patch scanning	Collects registry key entries, windows services, installed windows applications, and patched Microsoft bugs.
UNIX patch scanning	Collects details of installed RPMs

Web application scanning

QRadar Vulnerability Manager uses unauthenticated scanning for core web application scanning. The following list describes QRadar Vulnerability Manager web vulnerability checks:

- SQL Injection Vulnerabilities

  SQL injection vulnerabilities occur when poorly written programs accept user-provided data in a database query without validating the input, which is found on web pages that have dynamic content. By testing for SQL injection vulnerabilities, QRadar Vulnerability Manager assures that the required authorization is in place to prevent these exploits from occurring.

- Cross-Site Scripting (XSS) Vulnerabilities

  Cross-Site Scripting vulnerabilities can allow malicious users to inject code into web pages that are viewed by other users. HTML and client-side scripts are examples of code that might be injected into web pages. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy. QRadar Vulnerability Manager tests for varieties of persistent and non-persistent cross-site scripting vulnerabilities to ensure that the web application is not susceptible to this threat.

- Web Application Infrastructure

  QRadar Vulnerability Manager includes thousands of checks that check default configurations, cgi scripts, installed and supporting application, underlying operating systems and devices.

- Web page errors

For in-depth web application scanning, QRadar Vulnerability Manager integrates with IBM Security AppScan to provide greater web application visibility to your vulnerabilities.

Network device scanning

QRadar Vulnerability Manager includes the SNMP plug-in that supports scanning of network devices. QRadar Vulnerability Manager supports SNMP V1 and SNMP V2. SNMP V3 is not supported. QRadar Vulnerability Manager uses a dictionary of known community defaults for various SNMP-enabled devices. You can customize the dictionary.

External scanner checks

The external scanner scans the following OWASP (Open Web Application Security Project) CWEs (Common Weakness Enumerations):

- Directory Listing
- Path Traversal, Windows File Parameter Alteration, UNIX File Parameter Alteration, Poison Null Byte Windows Files Retrieval, Poison Null Byte UNIX Files Retrieval
- Cross-Site Scripting, DOM-Based Cross-Site Scripting
- SQL Injection, Blind SQL Injection, Blind SQL Injection (Time Based)
- Autocomplete HTML Attribute Not Disabled for Password Field
- Unencrypted Login Request, Unencrypted Password Parameter
- Remote Code Execution, Parameter System Call Code Injection, File Parameter Shell Command Injection, Format String Remote Command Execution

Database scanning

QRadar Vulnerability Manager detects vulnerabilities on major databases by using unauthenticated scanning of target hosts. In addition, QRadar Vulnerability Manager targets several databases by using plug-ins.

Operating system checks

Table 5. Operating system checks

Operating system	Vulnerability scanning	Patch scanning	Configuration
Windows	Yes	Yes	Yes
AIX® UNIX	Yes	Yes	No
CentOS Linux	Yes	Yes	No
Debian Linux	Yes	Yes	No
Fedora Linux	Yes	Yes	No
Red Hat Linux	Yes	Yes	No
Sun Solaris	Yes	Yes	No
HP-UX	Yes	Yes	No
Suse Linux	Yes	Yes	No
Ubuntu Linux	Yes	Yes	No
CISCO	No	No	No
AS/400® / iSeries	No	No	No

OVALs and operating systems

OVAL definitions are supported on the following operating systems:

- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7
- Microsoft Windows Vista
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003
- CentOS versions 3 - 7
- IBM AIX versions 4-7
- RHEL versions 3 - 7
- SUSE versions 10 - 11
- Ubuntu versions 6-14
- Red Hat 9
- Solaris versions 2.6, 7 - 10

Vulnerability management dashboard

You can display vulnerability information on your QRadar dashboard.

IBM QRadar Vulnerability Manager is distributed with a default vulnerability dashboard so that you can quickly review the risk to your organization.

You can create a new dashboard, manage your existing dashboards, and modify the display settings of each vulnerability dashboard item.

For more information about dashboards, see the *Users Guide* for your product.

Reviewing vulnerability data on the default vulnerability management dashboard

You can display default vulnerability management information on the QRadar dashboard.

The default vulnerability management dashboard contains risk, vulnerability, and scanning information.

You can configure your own dashboard to contain different elements like saved searches.

Procedure

1. Click the **Dashboard** tab.
2. On the toolbar, in the **Show Dashboard** list, select **Vulnerability Management**.

Creating a customized vulnerability management dashboard

In QRadar you can create a vulnerability management dashboard that is customized to your requirements.

Procedure

1. Click the **Dashboard** tab.
2. On the toolbar, click **New Dashboard**.
3. Type a name and description for your vulnerability dashboard.
4. Click **OK**.
5. On the toolbar select **Add Item** > **Vulnerability Management** and choose from the following options:
   - If you want to show default saved searches on your dashboard, select **Vulnerability Searches**.
   - If you want to show website links to security and vulnerability information, select **Security News**, **Security Advisories**, or **Latest Published Vulnerabilities**.
   - If you want show information that is about completed or running scans, select **Scans Completed** or **Scans In Progress**.

Creating a dashboard for patch compliance

Create a dashboard that shows the most effective patch to use to remediate vulnerabilities that are found on the network.

Procedure

1. Click the **Dashboard** tab.
2. On the toolbar, click **New Dashboard**.
3. Type a name and description for your vulnerability dashboard.
4. Click **OK**.
5. On the toolbar, select **Add Item** > **Vulnerability Management** > **Vulnerability Searches** and choose the default saved search that you want to show on your dashboard.
6. On the header of the new dashboard item, click the yellow **Settings** icon.

7. Select **Patch** from the **Group By** list and then select one of the following options from the **Graph By** list:
   - If you want to see how many assets need to a have the patch applied, select **Asset Count**.
   - If you want to see the cumulative risk score by patch, select **Risk Score**.
   - If you want to see the number of vulnerabilities that are covered by a patch, select **Vulnerability Count**.
8. Click **Save**.
9. To view vulnerability details on the **Manage Vulnerabilities** > **By Vulnerability** page on the **Vulnerabilities** tab, click the **View in By Vulnerability** link at the bottom of the dashboard item.

Chapter 4. Vulnerability scanning strategy and best practices

Good planning is essential for the setup of a stable and efficient IBM QRadar Vulnerability Manager scanning system in your network.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Analyze your network structure, and determine the best scanning configuration for your network, from both a hardware and a scanning performance perspective.

Consider the following information, which includes best practices for setting up your QRadar Vulnerability Manager scanning deployment:

- Scan policy types

  Choose the scan policy type that meets your scanning requirements and consider the time and resources that are required to complete the scan.
- Scan duration and ports to scan

  Decide whether you need to scan all TCP and UDP ports. UDP ports take longer to scan than TCP ports.
- Tune your asset discovery.

  Tune your asset discovery to manage your asset discovery times and effectiveness.
- Tune your asset discovery performance.

  Adjust and optimize the speed and accuracy at which assets are discovered in your network.
- Scanner placement in your network

  Place scanners close to the assets that you are scanning, and be aware of the impact of network latency on your scan times.
- Web application scanning

  This scan can take a long time and be resource-intensive. If you don't need to run this scan as part of a full scan, you can exclude this scan.
- Dynamic scanning

  You might save time by implementing dynamic scanning.
- Network bandwidth setting

  Adjust the network bandwidth setting according to your network bandwidth and the number of assets that you can scan concurrently.
- Network interface cards on scanners

  Use network interface cards to segment your network scanning.
- Vulnerability management for asset owners

  Assign owners to your assets.
- Notification of asset owners on the timing of scans.

  Ensure that asset owners are aware of scan times.
- Triggering scans of new assets

  Trigger scans of new assets when they are added to the asset database.
- Configure environmental risk for an asset

  Use the CVSS Environmental Score to manipulate and prioritize the risk score on selected assets.

© Copyright IBM Corp. 2012, 2020

- External scanning FAQs

  What you need to know about setting up an external scan.

Scan policy types

IBM QRadar Vulnerability Manager provides several default scan policy types. You can also define your own scans from the scan templates.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

The following scan templates are the most commonly used templates:

Discovery scan policy

Discovers network assets, and then scans ports to identify key asset characteristics, such as operating system, device type, and services. Vulnerabilities are not scanned.

A lightweight uncredentialed scan that searches an address space for active IP addresses, and then scans their ports. It runs DNS and NetBIOS lookups to discover the operating system, open services, and network names.

If possible, run this uncredentialed scan weekly to provide good network visibility. This scan is most helpful for identifying new assets and changes to previously scanned assets.

Note: Use the **assets seen in last 14 days but not scanned** saved search from the **Assets** tab, to identify new assets that QRadar passively discovered the last 14 days.

Full scan policy

Discovers network assets by using a fast scan port range. Runs a user-configurable port scan and unauthenticated scan of discovered services like FTP, web, SSH, and database. An authenticated scan is run when credentials are provided.

Runs the full suite of QRadar Vulnerability Manager tests.

A full scan has these phases:

1. Discovery scan.
2. Uncredentialed scan.

   Checks services that do not require credentials, for example, reading banners and responses for version information, SSL certificate expiry, testing default accounts, and testing responses for vulnerabilities.
3. Credentialed scan.

   QRadar Vulnerability Manager logs on to the asset and gathers information about the installed application inventory and required configuration, and raises or suppresses vulnerabilities. Credential scans are preferable to uncredentialed scans. Uncredentialed scans provide a useful overview of the vulnerability posture of the network. However, credentialed scanning is essential for a comprehensive and effective vulnerability management program.

   You can't edit the build-in policies but you can copy them to create your own custom scan policy.

   Tip: Full scans can sometimes lock some administration accounts, for example, SQL Server, when QRadar Vulnerability Manager tests multiple default credentials on accounts. Turn off these logon tests by taking the following steps:

   a. Click the **Vulnerabilities** tab.
   b. From the **Scan Policy** window, click **Scan Policies**.
   c. Click the **Full Scan** policy, then click **Edit**.
   d. Click the **Tools** tab.

      By default, the **Included** list is displayed.

e. From the **Filter** menu, select **Default Logons (Dos Risk)**.

f. Click **Exclude All** to remove the check marks next to the items in the list.

g. Click **Save**.

h. Verify that the **Default Logons (Dos Risk)** tools are in the **Excluded** list.

Run a full scan every 2-3 months for a detailed and accurate assessment of vulnerabilities in your network. The full scan is resource-intensive so the scheduling and resource allocation is important for optimal performance.

Patch scan policy

Scouts the network to discover assets, and then runs a fast port scan and credentialed scan of the assets.

You use patch scans to determine which patches and products are installed or missing on the network.

A patch scan has two main phases:

1. Discovery scan
2. Credentialed scan

Run this credentialed scan every 1-4 weeks to determine what patches and products are installed or missing on your network. The patch scan places only a minimal load on your network and active testing is kept to a low level.

PCI scan policy

Scans all TCP and UDP ports 0-65535.

You are not required to scan all UDP ports for PCI compliance. Typically you scan the most common UDP ports for PCI compliance but the list of ports might change slightly over time in accordance with PCI security standards.

If you scan all UDP ports, the scan might take a long time and not complete within the timeout period on larger network segments, resulting in some `Scan Interference Detected - Scan Potentially Incomplete` vulnerability instances.

You can create your own custom PCI scan policy by copying this policy, renaming the policy, and modifying the UDP scan ports according to your requirements.

Database scan policy

Scans database ports, 523, 1433, 1521, and 3306 for popular database services.

Use the uncredentialed database scan to scan ports DB2 (523), Microsoft SQL (1433), MySQL (3306), Oracle (1521), and Informix (1526), for popular database services.

Run this scan regularly if you have high database activity.

Related concepts

Scan policies

Scan duration and ports scanning

How you manage your network scanning configuration is influenced by the number of assets in your network, your network infrastructure, and the scan completion times.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

It can take a long time to scan large network, so you need a scanning strategy that optimizes your scanning resources.

Tip: It is always good practice to use operational windows to perform scans at times that don't overlap with nightly backups or automatic updates.

Port scanning strategy

Your scanning strategy is influenced by the number of hosts that you want to scan, whether it's a class C network of 256 hosts, or a class B network of 65,536 hosts. Your overall scan time can be significantly impacted by increasing the number of hosts that you want to scan. To get the overall scan time to an acceptable range, and you can reduce the scan time per host.

For example, if you do a network discovery scan on a class B network and it takes 1 second for TCP port discovery, the following statements are true:

- Scanning one port on 65536 hosts at 1 second per host takes 18 hours.
- If you scan one extra port on each of the 65536 hosts and allow 1 second per host, it takes an extra 18 hours to scan that extra port.

From the example, you can see the impact of adding one extra scanning port on a large network. If you're scanning a large number of hosts, understand what services are important and are prone to high-risk vulnerabilities so that you can configure your scan policies appropriately at the discovery scan stage. Before you implement your scan policies, run test scans by using different scan polices, and estimate the timing and the resources that are required to complete these scans.

Tip: The default QRadar discovery-scan policy runs a Nmap fast scan of TCP and UDP ports, and you can use it to scan a smaller number of hosts.

UDP port scanning takes longer that TCP port scanning because it's a connectionless protocol. Scanning all UDP ports can take a long time and is resource-intensive. Consider whether you need to scan all UDP ports or whether you scan these ports less frequently than TCP ports.

The following ports are some of the highest priority UDP ports that you need to consider scanning regularly:

- Authentication services such as RADIUS and Kerberos
- Back doors and remote access applications
- Backup applications
- Database servers
- DNS (Domain Name System)
- NetBIOS and Common Internet File System (CIFS)
- NFS (Network File System)
- NTP (Network Time Protocol)
- P2P (peer-to-peer) and chat applications
- Routing protocols, including RIP (Routing Information Protocol)
- RPC (Remote Procedure Call) and RPC endpoint mapping
- SNMP (Simple Network Management Protocol) and SNMP trap
- Syslog
- TFTP (Trivial File Transfer Protocol)
- VPNs, including Internet Security Association and Key Management Protocol (ISAKMP), Layer Two Tunneling Protocol (L2TP), and (NAT Traversal) NAT-T.
- Ports that are known to be associated with malicious activity.

Typical scan times

The following table gives information about scanning times.

Table 6. Scanning times for QRadar appliances	
QRadar appliance	**Scan times**
QRadar 2100/3100 All-in-One	A default full scan of 2000-4000 assets takes 2-3 days.
QRadar Vulnerability Manager on the following managed hosts: 610 1200 1300 1400 1500	A default full scan of 2000-4000 assets takes 2-3 days. An offboard QRadar Vulnerability Manager processor on a managed host (600) is required when more than 50,000 assets are being scanned regularly or when scans are running for long periods of time on the QRadar Console.

Tune your asset discovery configuration

Tune your asset discovery to manage your asset discovery times and effectiveness.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Tune your asset discovery from the **Asset Discovery** tab of your scan policy. You can use the default configuration as a fast and efficient way to discover your assets. ICMP pings and TCP SYN packets are enabled by default.

Use the following options to tune your asset discovery:

- Send ICMP pings.

  Pings are sent to the IP addresses that are configured in the scan profile that uses this scan policy.
- Send TCP SYN packets to ports.

  This option is a reliable quick option that is enabled for preconfigured ports.
- Send UDP packets to ports.

  Select this option to send UDP packets to preconfigured ports. UDP is slower than TCP. If you send a UDP packet to an inactive IP address it might take several seconds to complete because of retries.
- Enable traceroute detection.

  Traceroute detection requires more resources and scan times increase.
- Enable ICMP detection.

  ICMP detection requires more resources and scan times increase.
- OS and service fingerprinting

  Probe ports for OS and service information. If you select this option, scan times increase.

You can configure custom discovery options. The options that you choose depend on your requirements and your network structure. Test various options to discover an optimum discovery configuration that matches your needs.

Tune your asset discovery performance

Adjust and optimize the speed and accuracy at which services are discovered on your assets.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Tune your discovery performance from the **Discovery Performance** tab of your scan policy. You can use the default configuration as a fast and efficient way to discover your assets.

Use the following options to tune your asset discovery performance:

- **Maximum retries**

  Scan times can increase when you increase Maximum retries number but when you set this number too low, the accuracy of your scan results might be impacted.
- **Minimum timeout interval**

  The scan timeout interval is reduced to the minimum level that is configured when the network is reliable.
- **Initial timeout interval**

  Nmap adjusts the timeout value in response to previous probes. If latency increases, the timeout value is increased. If you decrease both the initial timeout and the maximum timeout intervals too low, the scan times might be faster, but you risk having to retransmit.
- **Scan delay**

  Use this setting to adjust the delay between scan probes. If your devices use rate limiting, then you can synchronize the scan delay with the rate-limiting value to achieve the optimum scan times.
- **Minimum packets per second**

  Nmap sends packets at the highest possible rate that your network tolerates, between the **Minimum packets per second** rate and the **Maximum packets per second rate**.
- **Maximum packets per second**

  By default, this field is empty because Nmap dynamically sets an appropriate packet speed for your network. If you want, you can configure your own rate.

Web application scanning

Web scans can be slow when you have complex web applications. All ports that run HTTP or HTTPS services, including Microsoft HTTP RPC ports, are scanned.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Part of a full scan or a web scan includes a phase that uses resource-intensive techniques that is similar to web crawling or spidering. If the scanner must crawl multiple web pages that have multiple links, the scan can be slow and demanding on your resources. Web scans look for web vulnerabilities, such as determining whether an HTTP server version has vulnerabilities, expired SSL certificates or weak SSL ciphers. The web scan also looks for Open Web Application Security Project (OWASP) vulnerabilities such as SQL injection, cross-site scripting (XSS), security misconfigurations.

If you don't need to scan your web applications, create a custom full scan policy, and exclude the **http – CGI scanner** scan tool that is on the **Tools** tab of your scan policy.

Scanner placement in your network

Scan operations are more efficient when scanners have good connectivity to the assets that are scanned and are not obstructed by firewalls, or other devices that impact the flow of the scan data. You can deploy

an unlimited number of scanners in your network, but you must have a software license for every QRadar managed host that you deploy as a scanner.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Consider the following factors before you place scanners in your network:

- Avoid scanning assets through firewalls for the following reasons:
  - Firewalls slows the scan, and block some ports that are required to complete the scan.
  - When you scan assets through a firewall, events are created in IBM QRadar and the EPS numbers (events per second) are increased, which can impact your EPS license.
  - Stateful firewalls can cause QRadar to create assets erroneously. Stateful firewalls respond to out-of-sequence TCP packets and that can make the scanner think that a host exists.
- Do not scan over low-bandwidth WAN connections.
- If the ping time from the scanner to the asset is over 40 ms, place the scanner closer to the asset.
- Don't scan through a load balancer because it's more difficult for the scanner to manage the scan when the network traffic is load balanced to different servers.
- Avoid configuring your scanner to scan IP address ranges that you know are not used. During the discovery phase of a scan, it takes longer for a scanner to determine that an IP address is not in use than it does to determine whether an IP address is active.
- Deploy more scanners rather than run several concurrent scans from the same scanner. As you add more concurrent scans to the same scanner, resources become stretched and each scan takes much longer.

Dynamic scanning

Use dynamic scanning in IBM QRadar Vulnerability Manager to associate individual scanners with an IP address, CIDR ranges, IP address ranges, or a domain that you specify in the scan profile. Dynamic scanning is most beneficial when you deploy several scanners. For example, if you deploy more than 5 scanners, you might save time by using dynamic scanning.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

The benefits of implementing dynamic scanning depend on your network infrastructure and the number of scanners that are available. For example, if you have 10 QRadar Vulnerability Manager scanners and you don't use dynamic scanning, you must configure 10 individual scan jobs. QRadar Vulnerability Manager selects the appropriate scanner for each IP address that is scanned.

If dynamic scanning is used in your scan profile and you associate 2 scanners with one asset, the scanner that includes the asset in the smallest matching subnet is prioritized to scan the asset first.

For example, your asset IP address is 10.2.2.3, and scanner A is assigned to the 10.2.2.0/24 CIDR address range, and scanner B is assigned to the 10.2.2.3/32 CIDR address. Scanner B is prioritized to scan the asset before scanner A because the subnet (/32) is a precise match for the asset.

Before you enable dynamic scanning, run test scans and then assess the impact on your network resources, scan performance, and the scan times.

Related tasks

Creating a scan profile

Network bandwidth for simultaneous asset scans

By adjusting the network bandwidth setting, you change the number of assets that can be scanned concurrently and the number of vulnerability tools that can be used concurrently to scan the assets. Some

scans use more vulnerability tools to scan, which impacts the number of assets that can be scanned concurrently.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

The network bandwidth setting ranges from a low setting of 200 Kbps to full setting of 5000 Kbps. Configure the bandwidth setting from the details tab of a scan profile. The default network bandwidth setting is medium, which is 1000 Kbps.

Adjust the bandwidth, according to the following scenarios:

- Adjust the network bandwidth to 5000 Kbps (full) to patch scan up to 50 assets concurrently or keep at 1000 Kbps (medium) to patch scan up to 10 assets concurrently.
- Use the 5000 Kbps (full) setting if your network has good bandwidth.
- Do not use the 5000 Kbps setting over a slow WAN connection.
- If you scan through a firewall and it's a log source, the scan traffic creates events, and you might have to lower the network bandwidth to avoid exceeding your EPS (events per second) license threshold.

Related tasks

Creating a scan profile

Network interface cards on scanners

In IBM QRadar Vulnerability Manager scanning is not dependent on the network interface cards (NICs) that are configured on the scanner appliance.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

You can configure many NICs, although 4-5 is a typical configuration. QRadar Vulnerability Manager uses standard TCP/IP protocols to scan any device that has an IP address. If multiple NICs are defined, scanning follows the standard networking configuration on an appliance.

If the target assets that you're scanning are in different networks, configure individual NICs to connect to the different networks.

This segmentation of the networks by using NICs makes it possible for the scanner to connect directly to different networks. For example, one Ethernet interface might be configured to connect to the 10.100.85.0/24 network and a second Ethernet interface might be configured to connect to the 192.168.0.0/24 network.

Vulnerability management for asset owners

Assign owners to your assets so that your discovered vulnerabilities are assigned to the asset owners. The assigned vulnerabilities are assigned with a due date, which is calculated based on the risk level of the vulnerability.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Configure the remediation reports that you want to send to asset owners, by highlighting the following information:

- The patches that they need to install.
- The steps that are required to remediate the vulnerability.
- The assets that have overdue vulnerabilities.
- New vulnerabilities that were discovered since the last scan.

The standard remediation reports are available on the **Email** tab of the **Scan Profile Configuration** page. You can create extra customer reports by using QRadar Vulnerability Manager searches.

From the **Reports** tab, you can create a vulnerabilities report, and assign this report to a scan reports group. You can configure recipients for this report in a scan profile, which can be seen in the **Available Reports** window of the **What to Email** tab on the **Scan Profile Configuration** screen.

Use search criteria to ensure that your reports focus on the vulnerability remediation activities that you require to meet your specific business and compliance needs.

To make remediation report creation easier, use QRadar Vulnerability Manager to automatically create asset vulnerabilities and vulnerability reports for each asset owner from a single report definition.

When assets are rescanned, any remediated vulnerabilities are automatically detected and flagged as fixed. They are removed from reports and views, unless they are explicitly configured otherwise. Any vulnerabilities that were previously fixed and are detected again are automatically reopened.

Related tasks

Assigning a technical user as the owner of asset groups

Emailing asset owners when vulnerability scans start and stop

Email the configured asset technical owners to alert them of the scan schedule. You can also email reports to asset owners.

Searching vulnerability data

Vulnerability scan notifications

To avoid false alarms when scan activity is high, notify asset owners of the timing of scans.

Some QRadar Vulnerability Manager scan tools, such as web tools, can generate a large amount of traffic. For example, a web scan might send 500 HTTP requests per second to HTTP servers. If asset owners see an unusual amount of traffic, they might think that the asset that is being scanned is subject to a DOS attack or similar attack.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Configure scan profiles to send emails to asset owners and other interested parties before and after a scan so that asset owners are aware that a larger than usual amount of network traffic or load might occur in their network. Another way to make asset owners aware of asset scan times, is to agree to a scanning schedule with the asset owners.

Configure email notification from the **Email** tab of the scan profile.

Triggering scans of new assets

Use events that are processed by the custom rules engine (CRE) to trigger scans on new assets when they are assigned new IP addresses.

Before you begin

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Create a scan profile with the **On Demand Scanning** enabled.

Procedure

1. From the **Log Activity** tab, click **Rules** > **Rules**.
   You can also get to the rules menu from the **Offenses** and **Network Activity** tabs.

2. From the **Actions** menu, click **New Event Rule**.
3. Click **Events**, and then click **Next** to continue.
4. Add tests to your rule list.
   a) Click the add icon (**+**) icon beside **when the events were detected by one or more of these log sources** test.
   b) Click the add icon (**+**) beside **when the event QID is one of the following QIDs** test.
   c) Click the add icon (**+**) beside **and when the source IP is one of the following IP addresses** test.
5. In the **Rule** pane, edit each rule value.
   a) For the first rule, click **these log sources** and add the Asset Profiler item from the list.
   b) For the second rule, click **QIDs**, then search for QIDs that are described in the following table, and add these QIDs to your rule.

Table 7. QID names and descriptions to add to rule

QID	Name	Description
68750030	**IP Address Created**	This event occurs when a new IP address record is created for an asset.
68750013	**Asset Created**	This event occurs when a new asset is created.

   c) For the third rule, click **and** so it changes to **and NOT**, then click **IP addresses** and add 127.0.0.1

      The following example is the output of this rule configuration:

      and NOT when the source IP is one of the following 127.0.0.1
6. In the **Apply** text box, type a unique name for this rule, and leave **Local** as the default system setting, and then click **Next**.
7. In the **Rule Response** section, click **Trigger Scan**.
   a) From the **Scan Profile to be used as a template** menu, select the scan profile that you want to use.

      You must select the **On Demand Scanning** option in the scan profile that you want to use with this rule.
   b) Click **Source** for the **Local IPs to Scan** option.
   c) Enter values for the **Response Limiter** setting.

      Configure appropriate intervals to avoid a potential overload on your system.
   d) If you don't want to start watching events right away, clear the **Enable Rule** option and then click **Finish**.

Configuring environmental risk for an asset

Use the CVSS Environmental Score to manipulate and prioritize the risk score on selected assets. If you configure the **CVSS, Weight & Compliance** parameters for an asset, you can apply higher risk scores to assets that are more important or critical.

About this task

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

If you have important or critical assets and less important assets with the same vulnerabilities, you can configure the CVSS Environmental Score on the important assets or critical assets to have a higher risk score than the less important assets. By applying a higher risk score to your most important assets, you highlight these important assets in your scan results.

Procedure

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Double-click the asset that you want to edit, and then click **Edit Asset**.
4. Click **CVSS, Weight & Compliance** in the **Edit Asset Profile** window.
5. Configure the parameters in the **CVSS, Weight & Compliance** pane.
   The following table lists the parameters for the **CVSS, Weight & Compliance** pane.

Parameter	Description
Collateral Damage Potential	The potential for loss of life or physical assets through damage or theft of this asset, or economic loss of productivity or revenue. If you raise the **Collateral Damage Potential**, for example, from **Low** to **High**, the calculated value for the **CVSS Score** increases. The **Collateral Damage Potential** parameter is directly linked with the **Weight** parameter. If you change one parameter the other parameter is impacted.
Confidentiality Requirement	The impact to confidentiality for this asset when a vulnerability is exploited. If you raise the confidentiality requirement, for example, from **Low** to **High**, the calculated value for the **CVSS Score** increases.
Availability Requirement	The impact to the asset's availability when a vulnerability is successfully exploited. Attacks that consume network bandwidth, processor cycles, or disk space impact the availability of an asset. If you raise the availability requirement setting, for example, from **Low** to **High**, the calculated value for the **CVSS Score** increases.
Integrity Requirement	The impact to the asset's integrity when a vulnerability is successfully exploited. Integrity refers to the trustworthiness and guaranteed veracity of information. If you raise the integrity requirement, for example, from **Low** to **High**, the calculated value for the **CVSS Score** increases.
Weight	The **Weight** is linked with the **Collateral Damage Potential** setting. If you select 10 for the **Weight** parameter the **Collateral Damage Potential** changes to **High**.

6. Click **Save**.

External scanning FAQ

Scan the assets in your DMZ or network perimeter from the cloud by using an IBM hosted external scanner. Run uncredentialed scans from outside your network to give you an added defense in protecting your assets from an external attack.

- “What information do you need to provide?” on page 36

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

What information do you need to provide?

You must email `QRadar-QVM-Hosted-Scanner@hursley.ibm.com` with the following information:

- Your organization's external IP address.
- If you use load balancers, you must provide the IP addresses that are used by the load balancers.
- The IP address range of the assets in your DMZ.

Note: You must have a local installation of QRadar Vulnerability Manager.

Does the QRadar team verify the CIDR range that is provided?

The CIDR range is checked and ownership is verified before any scanning starts.

What is the impact of the external scan on servers such as web servers?

The scan is not intrusive but it places some load on your systems. Run the scan when the servers are not highly active.

How are the scan results from the cloud sent to the QRadar Vulnerability Manager processor?

The external scanner sends scan results from the cloud to the QRadar Vulnerability Manager processor over a secure connection.

Do your need to use an internal scanner to scan the DMZ in addition to the external scanner?

Most network attacks come from the outside, so the external scanner targets all external attack surfaces from the perspective of an outsider.

It is good practice to run external scanning and internally-authenticated scanning in your DMZ because firewalls might restrict access to certain vulnerabilities, ports, services, and hosts.

If you use a load balancer for inbound traffic, the external scanner might have access to only one of the servers that are connected to the load balancer. In this case, you might need to configure an access route so that the external scanner can scan all of the servers. Alternatively, you can use an internal scanner to scan these servers in your DMZ.

(Back to top)

Chapter 5. Scan configuration

In IBM QRadar Vulnerability Manager, all network scanning is controlled by the scan profiles that you create. You can create multiple scan profiles and configure each profile differently depending on the specific requirements of your network.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Scan profiles

Use scan profiles to do the following tasks:

- Specify the network nodes, domains, or virtual domains that you want to scan.
- Specify the network assets that you want to exclude from scans.
- Create operational windows, which define the times at which scans can run.
- Manually run scan profiles or schedule a scan to run at a future date.
- Run, pause, resume, cancel, or delete a single or multiple scans.
- Use centralized credentials to run Windows, UNIX, or Linux operating systems.
- Scan the assets from a saved asset search.

Related concepts
Centralized credential sets

Creating a scan profile

In IBM QRadar Vulnerability Manager, you configure scan profiles to specify how and when your network assets are scanned for vulnerabilities.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Administrative** > **Scan Profiles**.
3. On the toolbar, click **Add**.

   When you create a scan profile, the only mandatory fields are **Name** and **IP Addresses** on the **Details** tab of the **Scan Profile Configuration** page. In addition, you can also configure the following optional settings.

   - If you added more scanners to your QRadar Vulnerability Manager deployment, select a scanner from the **Scan Server** list. This step is unnecessary if you want to use dynamic scanning.
   - To enable this profile for on-demand scanning, click the **On Demand Scanning Enabled** check box.

     By selecting this option, you make the profile available to use if you want to trigger a scan in response to a custom rule event. It also enables on-demand vulnerability scanning by using the right-click menu on the **Assets** page.
   - By selecting the **Dynamic Server Selection** check box, you can choose the most appropriate scanner that is available. Ensure that you define the scanners in the **Administrative** > **Scanners** page.

© Copyright IBM Corp. 2012, 2020

Security profiles must be updated with an associated domain. Domain-level restrictions are not applied until the security profiles are updated, and the changes are deployed.

- To scan your network by using a predefined set of scanning criteria, select a scan type from the **Scan Policies** list.
- If you configured centralized credentials for assets, click the **Use Centralized Credentials** check box. For more information, see the *IBM QRadar Administration Guide*.

4. Click **Save**.

Related concepts

Network bandwidth for simultaneous asset scans
By adjusting the network bandwidth setting, you change the number of assets that can be scanned concurrently and the number of vulnerability tools that can be used concurrently to scan the assets. Some scans use more vulnerability tools to scan, which impacts the number of assets that can be scanned concurrently.

Dynamic scanning
Use dynamic scanning in IBM QRadar Vulnerability Manager to associate individual scanners with an IP address, CIDR ranges, IP address ranges, or a domain that you specify in the scan profile. Dynamic scanning is most beneficial when you deploy several scanners. For example, if you deploy more than 5 scanners, you might save time by using dynamic scanning.

Options for adding scanners to your QRadar Vulnerability Manager deployment

Scan policies

Dynamic vulnerability scans
In IBM QRadar Vulnerability Manager, you can configure a scan to use certain vulnerability scanners for specific CIDR ranges in your network. For example, your scanners might have access only to certain areas of your network.

Related tasks

Associating vulnerability scanners with CIDR ranges
In IBM QRadar Vulnerability Manager, to do dynamic scanning, you must associate vulnerability scanners with different segments of your network.

Rescanning an asset by using the right-click menu option

Configuring a scan policy
In IBM QRadar Vulnerability Manager, you can configure a scan policy to meet any specific requirements for your vulnerability scans. You can copy and rename a preconfigured scan policy or you can add a new scan policy. You can't edit a preconfigured scan policy.

Creating an external scanner scan profile

In IBM QRadar Vulnerability Manager, you can configure scan profiles to use a hosted scanner to scan assets in your DMZ.

Before you begin

QRadar Vulnerability Manager must be configured with a hosted scanner. For more information, see “Scanning the assets in your DMZ” on page 10.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Administrative** > **Scan Profiles**.
3. On the toolbar, click **Add**.

   When you create a scan profile, the only mandatory fields are **Name** and **IP Addresses** on the **Details** tab of the **Scan Profile Configuration** page. To create an external scanner profile, you must also follow the remaining steps in this procedure.
4. To create an external scanner profile, use the following procedure.

a) From the **Scan Server** list, select **IbmExternalScanner**.

b) From the **Scan Policies** list, select **Full Scan** or **Web Scan**.

c) Click the **Domain and Web App** tab. In the **Virtual Webs** pane, enter the domain and IP address information for the websites and applications that you want to scan.

d) Click **Save**.

Important: Authenticated scans are not conducted from the external scanner.

Creating a benchmark profile

To create Center for Internet Security compliance scans, you must configure benchmark profiles. You use CIS compliance scans to test for Windows and Red Hat Enterprise Linux CIS benchmark compliance.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Administrative** > **Scan Profiles**.
3. On the toolbar, click **Add Benchmark**.
4. If you want to use pre-defined centralized credentials, select the **Use Centralized Credentials** checkbox .

   Credentials that are used to scan Linux operating systems must have root privileges. Credentials that are used to scan Windows operating systems must have administrator privileges.
5. If you are not using dynamic scanning, select a QRadar Vulnerability Manager scanner from the **Scan Server** list.
6. To enable dynamic scanning, click the **Dynamic server selection** checkbox.

   If you configured domains in the **Domain Management** window in the **Admin** tab, you can select a domain from the **Domain** list. Only assets within the CIDR ranges and domains that are configured for your scanners are scanned.
7. In the **When To Scan** tab, set the run schedule, scan start time, and any pre-defined operational windows.
8. In the **Email** tab, define what information to send about this scan and to whom to send it.
9. If you are not using centralized credentials, add the credentials that the scan requires in the **Additional Credentials** tab.

   Credentials that are used to scan Linux operating systems must have root privileges. Credentials that are used to scan Windows operating systems must have administrator privileges.
10. Click **Save**.

What to do next

t_qrm_ug_create_assetcompq.dita

Related concepts

Centralized credential sets

Running scan profiles manually

In IBM QRadar Vulnerability Manager you can run one or more scan profile manually.

You can also schedule scans to run at a future date and time. For more information, see “Scan scheduling” on page 42.

Before you begin

Ensure that a vulnerability processor is deployed. For more information, see “Verifying that a vulnerability processor is deployed” on page 7.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Profiles**.
3. On the **Scan Profiles** page, select the check box on the row assigned to the scan profiles that you want to run.

   Note: To find the scan profiles you want to run, use the toolbar **Name** field to filter scan profiles by name.
4. On the toolbar, click **Run**.

   By default, scans complete a fast scan by using the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) protocol. A fast scan includes most ports in the range 1 - 1024.

Related concepts
Scan profile details
Related tasks
Managing scan results

Rescanning an asset by using the right-click menu option

In IBM QRadar Vulnerability Manager, you can quickly rescan an asset by using the right-click option.

The right-click scan option is also available on the QRadar **Offenses** tab, and the QRadar Risk Manager sub-net asset view.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Manage Vulnerabilities** > **By Asset**.
3. On the **By Asset** page, identify the asset that you want to rescan.
4. Right-click the **IP Address** and select **Run Vulnerability Scan**.
5. In the **Run Vulnerability Scan** window, select the scan profile that you want use when the asset is rescanned.

   The scanning process requires a scan profile. The scan profile determines the scanning configuration options that are used when the scan runs.

   To view a scan profile in the **Run Vulnerability Scan** window, you must select the **On Demand Scanning Enabled** check box in the **Details** tab on the **Scan Profile Configuration** page.

   Important: The scan profile that you select might be associated with multiple scan targets or IP address ranges. However, when you use the right-click option, only the asset that you select is scanned.
6. Click **Scan Now**.
7. Click **Close Window**.
8. To review the progress of your right-click scan, in the navigation pane, click **Scan Results**.

   Right-click scans are identified by the prefix **RC:**.

Related concepts
Asset vulnerabilities

Scan profile details

In IBM QRadar Vulnerability Manager, you can describe your scan, select the scanner that you want to use, and choose from a number of scan policy options.

Scan profile details are specified in the **Details** tab, in the **Scan Profile Configuration** page.

See especially the following options:

Table 8. Scan profile details configuration options	
Options	**Description**
Use Centralized Credentials	Specifies that the profile uses pre-defined credentials. Centralized credentials are defined in the **Admin** > **System Configuration** > **Centralized Credentials** window.
Scan Server	The scanner that you select depends on your network configuration. For example, to scan DMZ assets, then select a scanner that has access to that area of your network. The **Controller** scan server is deployed with the vulnerability processor on your QRadar console or QRadar Vulnerability Manager managed host. **Restriction:** You can have only 1 vulnerability processor in your deployment. However, you can deploy multiple scanners either on dedicated QRadar Vulnerability Manager managed host scanner appliances or QRadar managed hosts.
On Demand Scanning	Enables on-demand asset scanning for the profile. Use the right-click menu on the **Assets** page to run on-demand vulnerability scanning. By selecting this option, you also make the profile available to use if you want to trigger a scan in response to a custom rule event. By enabling on-demand scanning, you also enable dynamic scanning.
Dynamic server selection	Specifies whether you want to use a separate vulnerability scanner for each CIDR range that you scan. During a scan, QRadar Vulnerability Manager automatically distributes the scanning activity to the correct scanner for each CIDR range that you specify. If you configured domains in the **Domain Management** window of the **Admin** tab, you can also select the domain that you want to scan.
Bandwidth Limit	The scanning bandwidth. The default setting is medium. **Important:** If you select a value greater than 1000 kbps, you can affect network performance.
Scan Policies	The pre-configured scanning criteria about ports and protocols. For more information, see “Scan policies” on page 51.

Related concepts

Dynamic vulnerability scans

In IBM QRadar Vulnerability Manager, you can configure a scan to use certain vulnerability scanners for specific CIDR ranges in your network. For example, your scanners might have access only to certain areas of your network.

Scan policies

Related tasks

Creating an on-demand scan profile

To trigger a scan in response to a custom rule event, configure an on-demand scan profile and enable dynamic scanning.

Scan scheduling

In IBM QRadar Vulnerability Manager, you can schedule the dates and times to scan your network assets for known vulnerabilities.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Scan scheduling is controlled by using the **When To Scan** pane, in the **Scan Profile Configuration** page. A scan profile that is configured with a manual setting must be run manually. However, scan profiles that are not configured as manual scans, can also be run manually. When you select a scan schedule, you can further refine your schedule by using operational windows to configure allowed scan times.

Choose one of the following scheduling options:

- Manual
- Run Once
- Daily
- Weekly
- Monthly
- Advanced

  Use cron expressions to create schedules, for example, 9:00 AM every Monday through Friday, or 3:30 AM the first Friday of every month. Cron expressions give you the ability to create irregular scan schedules. Schedule a maximum of one scan per day.

Be aware of the impact of changes in Daylight Saving Time on your **Run Once**, **Daily**, **Weekly**, and **Monthly** scan schedules. For example, on the 27th of March 2016, clocks in the UK go forward by 1 hour at 1:00 AM, so any scans that are configured to run between 1:00 AM and 1:59 AM on the 27th of March 2016 run between to 2:00 AM and 2:59 AM.

Advanced scan schedules that are configured to run between 1:00 AM and 1:59 AM on the 27th of March 2016 are skipped and do not run. All subsequent scans run at the scheduled times.

Related tasks

Configuring a permitted scan interval

Reviewing your scheduled scans in calendar format

Scanning domains monthly

In IBM QRadar Vulnerability Manager, you can configure a scan profile to scan the domains on your network each month.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Profiles**.
3. On the toolbar, click **Add**.

   When you create a scan profile, the only mandatory fields are **Name** and **IP Addresses** on the **Details** tab of the **Scan Profile Configuration** page. To set up monthly scans, you must also follow the remaining steps in this procedure.
4. Click the **When To Scan** pane.
5. In the **Run Schedule** list, select **Monthly**.
6. In the **Start Time** field, select a start date and time for your scan.

7. In the **Day of the month** field, select a day each month that your scan runs.
8. Click the **Domain and Web App** tab.
9. In the **Domains** field, type the URL of the asset that you want to scan and click (**>**).
10. Click **Save**.
11. During and after the scan, you can monitor scan progress and review completed scans.

Scheduling scans of new unscanned assets

In IBM QRadar Vulnerability Manager, you can configure scheduled scans of newly discovered, unscanned network assets.

Procedure

1. Click the **Assets** tab.
2. In the navigation pane, click **Asset Profiles**, then on the toolbar click **Search** > **New Search**.
3. To specify your newly discovered, unscanned assets, complete the following steps in the **Search Parameters** pane:
   a) Select **Days Since Asset Found**, **Less than 2** then click **Add Filter**.
   b) Select **Days Since Asset Scanned Greater than 2** then click **Add Filter**.
   c) Click **Search**.
4. On the toolbar, click **Save Criteria** and complete the following steps:
   a) In the **Enter the name of this search** field, type the name of your asset search.
   b) Click **Include in my Quick Searches**.
   c) Click **Share with Everyone**.
   d) Click **OK**.
5. Click the **Vulnerabilities** tab.
6. In the navigation pane, select **Administrative** > **Scan Profiles**.
7. On the toolbar, click **Add**.

   When you create a scan profile, the only mandatory fields are **Name** and **IP Addresses** on the **Details** tab of the **Scan Profile Configuration** page. To schedule scans for unscanned assets, you must also follow the remaining steps in this procedure.
8. In the **Include Saved Searches** pane, select your saved asset search from the **Available Saved Searches** list and click (**>**).
9. Click the **When To Scan** pane and in the **Run Schedule** list, select **Weekly**.
10. In the **Start Time** fields, type or select the date and time that you want your scan to run on each selected day of the week.
11. Select the check boxes for the days of the week that you want your scan to run.
12. Click **Save**.

    For more information about using the **Assets** tab and saving asset searches, see the *Users Guide* for your product.

Related tasks

Searching vulnerability data

Reviewing your scheduled scans in calendar format

In IBM QRadar Vulnerability Manager, the scheduled scan calendar provides a central location where you can review information about scheduled scans.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Administrative** > **Scheduled Scans**.
3. Hover your mouse on the scheduled scan to display information about the scheduled scan.

   For example, you can show the time that a scan took to complete.
4. Double-click a scheduled scan to edit the scan profile.

Network scan targets and exclusions

In IBM QRadar Vulnerability Manager, you can provide information about the assets, domains, or virtual webs on your network that you want to scan.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Use the **Details** tab on the **Scan Profile Configuration** page to specify the network assets that you want to scan.

You can exclude a specific host or range of hosts that must never be scanned. For example, you might restrict a scan from running on critical servers that are hosting your production applications. You might also want to configure your scan to target only specific areas of your network.

QRadar Vulnerability Manager integrates with QRadar by providing the option to scan the assets that form part of a saved asset search.

Scan targets

You can specify your scan targets by defining a CIDR range, IP address, IP address range, or a combination of all three.

Domain scanning

You can add domains to your scan profile to test for DNS zone transfers on each of the domains that you specify.

A host can use the DNS zone transfer to request and receive a full zone transfer for a domain. Zone transfer is a security issue because DNS data is used to decipher the topology of your network. The data that is contained in a DNS zone transfer is sensitive and therefore any exposure of the data might be perceived as a vulnerability. The information that is obtained might be used for malicious exploitation such as DNS poisoning or spoofing.

Scans that used saved asset searches

You can scan the assets and IP addresses that are associated with a QRadar saved asset search.

Any saved searches are displayed in the **Asset Saved Search** section of the **Details** tab.

For more information about saving an asset search, see the *Users Guide* for your product.

Exclude network scan targets

In **Excluded Assets** section of the **Domain and Web App** tab, you can specify the IP addresses, IP address ranges, or CIDR ranges for assets that must not be scanned. For example, if you want to avoid scanning a highly loaded, unstable, or sensitive server, exclude these assets.

When you configure a scan exclusion in a scan profile configuration, the exclusion applies only to the scan profile.

Virtual webs

You can configure a scan profile to scan different URLs that are hosted on the same IP address.

When you scan a virtual web, QRadar Vulnerability Manager checks each web page for SQL injection and cross site scripting vulnerabilities.

Related tasks

Scanning CIDR ranges with different vulnerability scanners
In IBM QRadar Vulnerability Manager, you can scan areas of your network with different vulnerability scanners.

Excluding assets from all scans
In IBM QRadar Vulnerability Manager, scan exclusions specify the assets in your network that are not scanned.

Scheduling scans of new unscanned assets

Scanning domains monthly

Excluding assets from all scans

In IBM QRadar Vulnerability Manager, scan exclusions specify the assets in your network that are not scanned.

About this task

Scan exclusions apply to all scan profile configurations and might be used to exclude scanning activity from unstable or sensitive servers. Use the **IP Addresses** field on the **Scan Exclusion** page to enter the IP addresses, IP address ranges, or CIDR ranges that you want to exclude from all scanning. To access the **Scan Exclusion** page:

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Administrative** > **Scan Exclusions**.
3. On the toolbar, select **Actions** > **Add**.

   Note: You can also use the **Excluded Assets** section of the **Vulnerabilities** > **Administrative** > **Scan Profiles** > **Add** > **Domain and Web App** tab to exclude assets from an individual scan profile.

Managing scan exclusions

In IBM QRadar Vulnerability Manager you can update, delete, or print scan exclusions.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Administrative** > **Scan Exclusions**.
3. From the list on the **Scan Exclusions** page, click the **Scan Exclusion** that you want to modify.
4. On the toolbar, select an option from the **Actions** menu.
5. Depending on your selection, follow the on-screen instructions to complete this task.

Scan protocols and ports

In IBM QRadar Vulnerability Manager, you can choose different scan protocols and scan various port ranges.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

You can configure your scan profile port protocols by using TCP and UDP scan options.

Configure scanning protocols and the ports that you want to scan on the **Port Scan** tab of an existing or new scan policy configuration window.

Note: You can also configure port scanning from the **How To Scan** tab in the **Scan Profile Configuration** window but this option is only enabled for backwards compatibility. Do not use the **How To Scan** tab to configure new port scans.

Scanning a full port range

In IBM QRadar Vulnerability Manager, you can scan the full port range on the assets that you specify.

About this task

Create a scan policy to specify the ports that you want to scan, and then add this scan policy to a scan profile, which you use to run the scan.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Policies**.
3. On the toolbar, click **Add** to create a new scan policy or **Edit** to edit an existing policy.
4. Click the **Settings** tab.
   a) Enter a name and description for the scan policy.
   b) Select the scan type.
5. Click the **Port Scan** tab.
6. In the **Protocol** field, select a protocol. The default values are **TCP & UDP**.

   Note: UDP port scans are much slower than TCP port scans because of the way that UDP works. A UDP port scan can take up to 24 hours to scan all ports (1-65535) on an asset.
7. In the **Range** field, type **1-65535**.

   Restriction: Port ranges must be configured in dash-separated, comma-delimited, consecutive, ascending, and non-overlapping order. Multiple port ranges must be separated by a comma. For example, the following examples show the delimiters that are used to enter port ranges:(1-1024, 1055, 2000-65535).
8. In the **Timeout (m)** field, type the time in minutes after which you want the scan to cancel if no scan results are discovered.

   Important: You can type any value in the range 1 - 500. Ensure that you do not enter too short a time, otherwise the port scan cannot detect all running ports. Scan results that are discovered before the timeout period are displayed.
9. Optional: Configure more options on the other tabs if you want to use the scan policy to complete more tasks.
10. Click **Save**.
11. From the **Scan Profiles** page, create a new scan profile.
    a) Add the scan policy that you saved.
    b) Configure the remaining parameters for the scan profile and save.
    c) From the **Scan Profiles** page, select the new scan profile, and then click **Run** on the toolbar to run the scan.

    For more information about creating a scan profile, see “Creating a scan profile” on page 37.

    Note: You can also configure port scanning from the **How To Scan** tab in the **Scan Profile Configuration** window but this option is only enabled for backwards compatibility. Do not use the **How To Scan** tab to configure new port scans.

Scanning assets with open ports

In IBM QRadar Vulnerability Manager, you can configure a scan profile to scan assets with open ports.

Procedure

1. Click the **Assets** tab.
2. In the navigation pane, click **Asset Profiles** then on the toolbar, click **Search** > **New Search**.
3. To specify assets with open ports, configure the following options in the **Search Parameters** pane:
   a) Select **Assets With Open Port**, **Equals any of 80** and click **Add Filter**.
   b) Select **Assets With Open Port**, **Equals any of 8080** and click **Add Filter**.
   c) Click **Search**.
4. On the toolbar, click **Save Criteria** and configure the following options:
   a) In the **Enter the name of this search** field, type the name of your asset search.
   b) Click **Include in my Quick Searches**.
   c) Click **Share with Everyone** and click **OK**.
5. Click the **Vulnerabilities** tab.
6. In the navigation pane, select **Administrative** > **Scan Profiles**.
7. On the toolbar, click **Add**.

   When you create a scan profile, the only mandatory fields are **Name** and **IP Addresses** on the **Details** tab of the **Scan Profile Configuration** page. To scan assets with open ports, you must also follow the remaining steps in this procedure.
8. On the **Details** tab, select your saved asset search from the **Available Saved Searches** list and click **>**.

   When you include a saved asset search in your scan profile, the assets and IP addresses associated with the saved search are scanned.
9. Click the **When To Scan** pane and in the **Run Schedule** list, select **Manual**.
10. Click the **What To Scan** pane.
11. Click **Save**.

    For more information about saving an asset search, see the *Users Guide* for your product.

What to do next

Perform the steps in the procedure, “Running scan profiles manually” on page 39.

Configuring a permitted scan interval

In IBM QRadar Vulnerability Manager, you can create an operational window to specify the times that a scan can run.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

About this task

If a scan does not complete within the operational window, it is paused and continues when the operational window reopens. To configure an operational window:

Procedure

1. Click the **Vulnerabilities** tab.

2. In the navigation pane, click **Administrative** > **Operational Window**.
3. On the toolbar, click **Actions** > **Add**.
4. Enter a name for the operational window in the **Name** field.
5. Choose an operational window schedule from the **Schedule** list.
6. Select the times when scanning is permitted.
7. Select your timezone.
8. If you selected **Weekly** from the **Schedule** list, then click the desired days of the week check boxes in the **Weekly** area.
9. If you selected **Monthly** from the **Schedule** list, then select a day from the **Day of the month** list.
10. Click **Save**.

    Operational windows can be associated with scan profiles by using the **When To Scan** tab on the **Scan Profile Configuration** page.

    If you assign two overlapping operational windows to a scan profile, the scan profile runs from the beginning of the earliest operational window to the end of the later operational window. For example, if you configure two daily operational windows for the periods 1 a.m. to 6 a.m. and 5 a.m. to 9 a.m., the scan runs between 1 a.m. and 9 a.m.

    For operational windows that do not overlap, the scan starts from the earliest operational window and pauses if there's a gap between the operational windows, and then resumes at the beginning of the next operational window.

Scanning during permitted times

In IBM QRadar Vulnerability Manager, you can schedule a scan of your network assets at permitted times, by using an operational window.

About this task

Tip: If you are applying the operational window to an authenticated patch scan, set the minimum window to 4 hours.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Operational Window**.
3. On the toolbar, select **Actions** > **Add**.
4. Type a name for your operational window, configure a permitted time interval and click **Save**.
5. In the navigation pane, select **Administrative** > **Scan Profiles**.
6. On the toolbar, click **Add**.

   When you create a scan profile, the only mandatory fields are **Name** and **IP Addresses** on the **Details** tab of the **Scan Profile Configuration** page. To configure scanning during permitted times, you must also follow the remaining steps in this procedure.
7. Click the **When To Scan** tab.
8. In the **Run Schedule** list, select **Daily**.
9. In the **Start Time** fields, type or select the date and time that you want your scan to run each day.
10. In the **Operational Windows** pane, select your operational window from the list and click (**>**).
11. Click **Save**.

Managing operational windows

In IBM QRadar Vulnerability Manager, you can edit, delete, and print operational windows.

Remember: You can edit an operational window while it is associated with a scan profile.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Operational Window**.
3. Select the operational window that you want to edit.
4. On the toolbar, select an option from the **Actions** menu.
5. Follow the instructions in the user interface.

   Restriction: You cannot delete an operational window that is associated with a scan profile. You must first disconnect the operational window from the scan profile.

Disconnecting an operational window

If you want to delete an operational window that is associated with a scan profile, you must disconnect the operational window from the scan profile.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Profiles**.
3. Select the scan profile that you want to edit.
4. On the toolbar, click **Edit**.
5. Click the **When To Scan** pane.
6. Select the relevant option from the **Run Schedule** list as required.
7. In the **Name** field, select the operational window that you want to disconnect and click (**<**).
8. Click **Save**.

Dynamic vulnerability scans

In IBM QRadar Vulnerability Manager, you can configure a scan to use certain vulnerability scanners for specific CIDR ranges in your network. For example, your scanners might have access only to certain areas of your network.

During a scan, QRadar Vulnerability Manager determines which scanner to use for each CIDR, IP address, or IP range that you specify in your scan profile.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Dynamic scanning and domains

If you configured domains in the **Domain Management** window on the **Admin** tab, you can associate scanners with the domains that you added.

For example, you might associate different scanners each with a different domain, or with different CIDR ranges within the same domain. QRadar dynamically scans the configured CIDR ranges that contain the IP addresses you specify on all domains that are associated with the scanners on your system. Assets with the same IP address on different domains are scanned individually if the CIDR range for each domain includes that IP address. If an IP address is not within a configured CIDR range for a scanner domain, QRadar scans the domain that is configured for the Controller scanner for the asset.

Setting up dynamic scanning

To use *dynamic scanning*, you must do the following actions:

1. Add vulnerability scanners to your QRadar Vulnerability Manager deployment. For more information, see “Options for adding scanners to your QRadar Vulnerability Manager deployment” on page 8.

2. Associate vulnerability scanners with CIDR ranges and domains.
3. Configure a scan of multiple CIDR ranges and enable **Dynamic server selection** in the **Details** tab of the **Scan Profile Configuration** page.

Related concepts

Options for adding scanners to your QRadar Vulnerability Manager deployment

Scan profile details

Related tasks

Creating an on-demand scan profile

To trigger a scan in response to a custom rule event, configure an on-demand scan profile and enable dynamic scanning.

Associating vulnerability scanners with CIDR ranges

In IBM QRadar Vulnerability Manager, to do dynamic scanning, you must associate vulnerability scanners with different segments of your network.

Before you begin

You must add extra vulnerability scanners to your deployment. For more information, see "Options for adding scanners to your QRadar Vulnerability Manager deployment" on page 8.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scanners**.

   Attention: By default, the Controller scanner is displayed. The Controller scanner is part of the QRadar Vulnerability Manager processor that is deployed on either your QRadar Console or on a dedicated QRadar Vulnerability Manager processing appliance. You can assign a CIDR range to the Controller scanner, but you must deploy extra scanners to use dynamic scanning.
3. Click a scanner on the **Scanners** page.
4. On the toolbar, click **Edit**.

   Restriction: You cannot edit the name of the scanner. To edit a scanner name, click **Admin** > **System and License Management** > **Deployment Actions** > **Manage Vulnerability Deployment**.
5. In the **CIDR** field, type a CIDR range or multiple CIDR ranges that are separated by commas.
6. Click **Save**.

Related concepts

Options for adding scanners to your QRadar Vulnerability Manager deployment

Related tasks

Creating an on-demand scan profile

To trigger a scan in response to a custom rule event, configure an on-demand scan profile and enable dynamic scanning.

Scanning CIDR ranges with different vulnerability scanners

In IBM QRadar Vulnerability Manager, you can scan areas of your network with different vulnerability scanners.

Before you begin

You must configure your network CIDR ranges to use the different vulnerability scanners in your QRadar Vulnerability Manager deployment. For more information, see "Options for adding scanners to your QRadar Vulnerability Manager deployment" on page 8.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Profiles**.
3. On the toolbar, click **Add**.
4. Click the **Dynamic server selection** check box.

   If you configured domains in the **Admin** > **Domain Management** window, you can select a domain from the **Domain** list. Only assets within the domain you selected are scanned.
5. Add more CIDR ranges.
6. Click **Save**.
7. Click the check box on the row that is assigned to your scan on the **Scan Profiles** page and click **Run**.

Related tasks

Creating an on-demand scan profile
To trigger a scan in response to a custom rule event, configure an on-demand scan profile and enable dynamic scanning.

Scan policies

A scan policy provides you with a central location to configure specific scanning requirements.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

You can use scan policies to specify scan types, ports to be scanned, vulnerabilities to scan for and scanning tools to use. In IBM QRadar Vulnerability Manager, a *scan policy* is associated with a scan profile and is used to control a vulnerability scan. You use the **Scan Policies** list on the **Details** tab of the **Scan Profile Configuration** page to associate a scan policy with a scan profile.

You can create a new scan policy or copy and modify a pre-configured policy that is distributed with QRadar Vulnerability Manager.

Pre-configured scan policies

The following pre-configured scan policies are distributed with QRadar Vulnerability Manager:

- Full scan
- Discovery scan
- Database scan
- Patch scan
- PCI scan
- Web scan

A description of each pre-configured scan policy is displayed on the **Scan Policies** page.

Related tasks

Modifying a pre-configured scan policy
In IBM QRadar Vulnerability Manager, you can copy a pre-configured scan policy and modify the policy to your exact scanning requirements.

Configuring a scan policy

In IBM QRadar Vulnerability Manager, you can configure a scan policy to meet any specific requirements for your vulnerability scans. You can copy and rename a preconfigured scan policy or you can add a new scan policy. You can't edit a preconfigured scan policy.

Scan policy automatic updates for critical vulnerabilities

As part of IBM QRadar Vulnerability Manager daily automatic updates, you receive new scan policies for tasks such as detecting zero-day vulnerabilities on your assets.

Use scan policies that are delivered by automatic update to create scan profiles to scan for specific vulnerabilities. To view all scan policies on your system, go to **Administrative** > **Scan Policies** on the **Vulnerabilities** tab.

You must not edit scan policies that are delivered by automatic update as your changes might be overwritten by later updates. You can create a copy and edit it.

If you delete a scan policy that is delivered by automatic update, it can be recovered only by QRadar customer support.

Modifying a pre-configured scan policy

In IBM QRadar Vulnerability Manager, you can copy a pre-configured scan policy and modify the policy to your exact scanning requirements.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Policies**.
3. On the **Scan Policies** page, click a pre-configured scan policy.
4. On the toolbar, click **Edit**.
5. Click **Copy**.
6. In the **Copy scan policy** window, type a new name in the **Name** field and click **OK**.
7. Click the copy of your scan policy and on the toolbar, click **Edit**.
8. In the **Description** field, type new information about the scan policy.

   Important: If you modify the new scan policy, you must update the information in the description.
9. To modify your scan policy, use the **Port Scan**, **Vulnerabilities**, **Tool Groups**, or **Tools** tabs.

   Restriction: Depending on the **Scan Type** that you select, you cannot use all the tabs on the **Scan Policy** window.

Configuring a scan policy

In IBM QRadar Vulnerability Manager, you can configure a scan policy to meet any specific requirements for your vulnerability scans. You can copy and rename a preconfigured scan policy or you can add a new scan policy. You can't edit a preconfigured scan policy.

Before you begin

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Policies**.
3. On the toolbar, click **Add**.

4. Type the name and description of your scan policy.

   To configure a scan policy, you must at least configure the mandatory fields in the **New Scan Policy** window, which are the **Name** and **Description** fields.
5. From the **Scan Type** list, select the scan type.
6. To manage and optimize the asset-discovery process, click the **Asset Discovery** tab.
7. To manage the ports and protocols that are used for a scan, click the **Port Scan** tab.
8. To include specific vulnerabilities in your patch scan policy, click the **Vulnerabilities** tab.

   Note: The **Vulnerabilities** tab is available only when you select a patch scan.
9. To include or exclude tool groups from your scan policy, click the **Tool Groups** tab.

   Note: The **Tool Groups** tab is available only when you select a zero-credentialed full-scan or full-scan plus policy.
10. To include or exclude tools from a scan policy, click the **Tools** tab.

    Note: The **Tools** tab is available only when you select a zero-credentialed Full Scan or Full Scan Plus policy.

    Important: If you do not modify the tools or tool groups, and you select the **Full** option as your scan type, then all the tools and tool groups that are associated with a full scan are included in your scan policy.
11. Click **Save**.

Chapter 6. False positives management

Commonly, false positives in vulnerability scanning occur when the scanner can access only a subset of the required information, which prevents it from accurately determining whether a vulnerability exists.

To help reduce the number of false positives, you must configure your scanners with the appropriate credentials. The scans need access to all of the asset information required information from assets so that you can accurately determine whether a vulnerability exists.

Why do false positives occur?

A false positive might occur when the scanner can read only the configuration information from service banners. For example, a scanner that reads an Apache banner can detect that only version 2.2.15 is installed from the HTTP banner, even when version 2.2.15-39 is also installed and that the version contains a software fix that was backported.

Another example is when the scanner reads the banner and detects the version of SSH that is installed, but can't detect the patch level or the operating system. If the scanner detects that SSH-2 is installed but can't determine the operating system, the scanner can't accurately determine whether a vulnerability exists in some instances. The vulnerability might be correctly identified on one asset but is a false positive on the other asset because SSH vulnerabilities on Red Hat SSH might not be the same for other Linux operating systems.

Why don't scanners retrieve all the required information

Vulnerability scanners can't always access the information that they need to accurately determine whether a vulnerability exists. This limitation commonly results in false positives.

Scanner can't authenticate

If the scanner can't authenticate on the end point, the scanner must rely on the limited information from anonymous network services probing such as the information retrieved from reading banners.

Banners might contain incorrect versions and outdated patch-level information, which results in false positives. However, if the scanner can authenticate, it can determine the full version of the operation system and patch-level information, and then suppress any false-positive vulnerabilities.

Best practices about banners

Use these best practices about banners when you set up vulnerability scanning in your network:

- Don't include detailed or sensitive information in a banner because a hacker can get crucial information about the applications and services that are running on an asset and then use known vulnerabilities to exploit them.
- Know the type of information that is available anonymously in banners. Assess the likely attempted attack vectors. This information is helpful for assessing your network security, and for gathering network information.
- Flag vulnerability information that is read from banners as false positives by tagging the vulnerability as an exception from tabs such as the **Vulnerability Instances** pane of the **Asset Details** window or the **Vulnerability History** window.
- Tune scans by enabling or disabling tools in scan policies that can prevent these scans from starting.

Authenticated Windows based scan techniques

Authenticated Windows based scanning uses the following two techniques to detect vulnerabilities:

- Registry scanning where the scanner needs access to the registry.
- OVAL scanning where WMI (Windows Management Instrumentation) must be configured correctly.

© Copyright IBM Corp. 2012, 2020

If either of these two techniques fail, then the scan result is prone to false positives.

You must enable the remote registry service for the scanner to access the registry.

Misconfiguration of WMI (Windows Management Instrumentation) can generate false positives.

Identify authentication failures

If a scan does not authenticate successfully, hover your cursor over the warning symbol see why the scan encountered issues. For example,

```
The last scan of this asset failed
STATUS_LOGON_FAILURE
Therefore the vulnerability may not be accurate
```

Other examples of warnings messages include, SSH `logon failure`, `remote registry service not started`, and `no WMI access`.

Related concepts

Scanning on Windows-based assets

QRadar Vulnerability Manager uses registry scanning and Open Vulnerability Assessment Language (OVAL) scanning to detect vulnerabilities on Windows-based assets. Use authenticated scans to detect all Windows vulnerabilities. Unauthenticated scans might not detect all Windows vulnerabilities.

Related tasks

Configuring an authenticated scan of the Windows operating system

Enabling permissions for Linux or UNIX patch scans

Applying a vulnerability exception rule

How is the vulnerability scan result detected?

Determine whether the vulnerability scan result is generated from an authenticated scan or from an anonymous reading of a banner. Scan results that are generated form an anonymous reading of a banner are more likely to be false positives.

Hover in the **Details** column of the vulnerability scan result for the asset to see how the vulnerability is detected.

1. Click the **Vulnerabilities** tab.
2. From the navigation menu, click **Scan Results**.
3. Double-click a scan profile in the **Name** column.
4. Click any row in the **Vulnerability Instances** column.
5. Hover over a result in the **Details** column to see more details.

   For example, the following details might be generated when the scanner reads a banner:

   ```
   SERVER: Apache/2.2.15(Red Hat)
   ```

Patch scans and false positives

Vulnerabilities that are detected from patch scans are unlikely to be false positives, except for Windows KB updates. Windows updates, which are prefixed by a knowledge base number (KB) can be false positives when the WMI (Windows Management Instrumentation) phase of the Windows authenticated scan fails.

Windows updates are superseded over time. For example, a current Windows KB supersedes the initial KB that addressed an original vulnerability fix. Superseding isn't an issue for recent Windows updates or when WMI or OVAL scanning is successful because the scan accounts for any newer updates.

Investigating a potential false positive from an authenticated scan

Sometimes, an authenticated scan generates a false positive because the scan fails.

About this task

Research the vulnerability.

Procedure

1. Click the **Vulnerabilities** tab.
2. From the navigation menu, click **Scan Results**.
3. In the **Scan results** window, click a row in the Vulnerabilities column.
4. Click the vulnerability that you want to investigate.
5. Click the **Plugin Details** link to open the patching window for the vulnerability.
6. Use the tabs to discover Oval Definition, Windows Knowledge Base, or UNIX advisory information about the vulnerability.
   - For vulnerabilities that are created from an Open Vulnerability and Assessment Language (OVAL) test, click the appropriate **OVAL** tab to see the criteria that QRadar Vulnerability Manager uses in the test.
   - For vulnerabilities that are created from an Windows KB registry scan, click the **Windows KB** tab to view the updates (KBs) that QRadar Vulnerability Manager associates with the vulnerability.
   - For vulnerabilities that are created because of a missing RPM Package Manager (RPM), click the **Unix** tab. The displayed packages and revisions are checked against the appropriate operating systems releases.

Chapter 7. Authenticated patch scans

In IBM QRadar Vulnerability Manager, you can scan for community names and run authenticated patch scans for Windows, Linux, and UNIX operating systems.

SNMP community names

You can scan your network assets by using SNMP community names. This function applies to SNMP V1 and V2c.

When you scan assets, QRadar Vulnerability Manager authenticates by using the SNMP services that are found and completes a more detailed vulnerability scan.

Windows patch scans

To scan Windows operating systems for missing patches, the remote registry access and Windows management instrumentation (WMI) must be enabled. If your Windows patch scan returns WMI connectivity issues, you must configure your Windows systems.

To read WMI data on a remote server, you must enable the connections between your QRadar console and the server that you are monitoring. If the server is using a Windows firewall, then you must configure the system to enable remote WMI requests.

If you are use a non-administrator account to monitor the Windows server, then you must enable the account to interact with Distributed Component Object Model (DCOM).

If the patch scan tool cannot connect to a Windows asset, a yellow triangular warning icon is displayed next to the asset in the scan results. The following vulnerability is raised: `Local Checks Error`.

Enabling some restrictions for unauthenticated RPC clients in your Windows Group Policy prevents QRadar Vulnerability Manager from running WMI queries when it scans a Windows server. When this authentication failure occurs, a yellow triangular warning icon is displayed next to the asset in the scan results. For example, if you enable **Restrict Unauthenticated RPC Client** in Windows 2012, you can select **None**, **Authenticated**, or **Authenticated without exceptions** from the menu. If you select **Authenticated without exceptions**, QRadar Vulnerability Manager cannot run WMI queries and is unable to complete the scan.

Secure Linux operating system authenticated scanning

To scan Linux operating systems by using secure authentication, you can configure public key encryption between your console or managed host and your scan targets.

When secure authentication is configured, you do not need to specify a Linux operating system password in your scan profile.

You must configure public key authentication on every Linux operating system that you scan.

If you move your vulnerability processor to a dedicated vulnerability processor appliance, you must reconfigure the secure authentication between the dedicated vulnerability processor appliance and the scan target.

If the patch scan tool cannot connect to a Linux asset, a yellow triangular warning icon is displayed next to the asset in the scan results. The following vulnerability is raised: `SSH Patch Scanning - Failed Logon`.

Related tasks

Configuring Linux operating system public key authentication

Configuring an authenticated scan of the Linux or UNIX operating systems

Configuring an authenticated scan of the Windows operating system

© Copyright IBM Corp. 2012, 2020

Centralized credential sets

When you run authenticated scans, you can use a central list that stores the login credentials for your Linux, UNIX, or Windows operating systems. Your system administrator must configure the list of credentials.

An administrator can specify credentials for SNMP network devices and Linux, UNIX, or Windows operating systems. Therefore, a user who is responsible for configuring a scan profile does not need to know the credentials of each asset that is scanned. Also, if the credentials of an asset change, the credentials can be modified centrally rather than updating the scan profile.

Related tasks

Configuring an authenticated scan of the Linux or UNIX operating systems

Configuring an authenticated scan of the Windows operating system

Creating a benchmark profile

To create Center for Internet Security compliance scans, you must configure benchmark profiles. You use CIS compliance scans to test for Windows and Red Hat Enterprise Linux CIS benchmark compliance.

Configuring a credential set

In IBM QRadar Vulnerability Manager, you can create a credential set for the assets in your network. During a scan, if a scan tool requires the credentials for a Linux, UNIX, or Windows operating system, the credentials are automatically passed to the scan tool from the credential set.

Procedure

1. On the navigation menu ( ), click **Admin**.
2. In the **System Configuration** pane, click **Centralized Credentials**.
3. In the **Centralized Credentials** window, on the toolbar, click **Add**.

   To configure a credential set, the only mandatory field in the **Credential Set** window is the **Name** field.
4. In the **Credential Set** window, click the **Assets** tab.
5. Type a CIDR range for the assets that you want to specify credentials for and click **Add**.

   Users must have network access permissions that are granted in their security profile for an IP address or CIDR address range that they use or create credentials for in **Centralized Credentials**.
6. Click the **Linux/Unix**, **Windows**, or **Network Devices (SNMP)** tabs, then type your credentials.
7. Click **Save**.

What to do next

t_qradar_ug_asset_savesearch.dita

Configuring Linux operating system public key authentication

To scan Linux operating systems by using secure public key authentication, you must configure your IBM QRadar console or managed host and the asset that you want to scan. When authentication is configured you can do authenticated scanning by specifying a Linux operating system user name, and not specifying a password. QRadar supports both `rsa` and `dsa` for SSH key generation.

Before you begin

You must install a public and private key on a QVM scanner, and install the public key on the scan target.

A QVM scanner is automatically installed on a QVM processor host, and might also be installed on other managed hosts.

The user account on the scan target must have a login shell and must be capable of running the commands that are required for a patch scan on the target. For more information, see "Enabling permissions for Linux or UNIX patch scans" on page 62.

This procedure describes how to configure a single public/private key pair and transfer them to a QVM scanner and scan target.

Procedure

1. Using SSH, log in to the QRadar console as the root user.
2. Generate a public key pair by typing the following command:

   ```
   su -m -c 'ssh-keygen -t <key_type>' qvmuser
   ```

   Note: *<key_type>* is either dsa or rsa.
3. Accept the default file by pressing **Enter**.
4. Accept the default passphrase for the public key by pressing **Enter**.
5. Press **Enter** again to confirm.
6. Copy the public and private keys to all managed hosts on which a QVM scanner is installed.

   ```
   cd /home/qvmuser/.ssh
   ```

   ```
   rsync -ogp id_<key_type> id_<key_type>.pub <IP address>:/home/qvmuser/.ssh
   ```

   - Replace *<key_type>* with dsa or rsa.
   - Replace *<IP address>* with the IP address of the scanner and enter the root password when prompted.

   Note: The QVM processor includes a scanner. If the processor is not running on the QRadar console, you must also transfer the keys to the QVM processor.
7. Copy the public key to the scan target by typing the following command:

   ```
   cd /home/qvmuser/.ssh
   ```

   ```
   ssh-copy-id -i id_<key_type>.pub <user>@<IP address>
   ```

   - *<key_type>* – dsa or rsa.
   - *<IP address>* – the IP address of the scan target.
   - *<user>* – the user on the scan target.
8. Type the user password for the scan target.
9. Check that the *qvmuser* account on the QVM scanner can SSH to the scan target without a password by typing the following command:

   ```
   su -m -c 'ssh -o StrictHostKeyChecking=no <user>@<IP address> ls' qvmuser
   ```

   - *<IP address>* – the IP address of the scan target.
   - *<user>* – the user on the scan target.

   A list of the files in the user's home directory on the scan target is displayed.

What to do next

Create a scan profile in QRadar Vulnerability Manager with user name of the user on the scan target without specifying a password and run a patch scan.

Related tasks

Configuring an authenticated scan of the Linux or UNIX operating systems

Configuring an authenticated scan of the Linux or UNIX operating systems

In IBM QRadar Vulnerability Manager, you can configure an authentication scan of the Linux or UNIX operating systems that are on your network. You can manually specify the credentials in the scan profile or use a credential set.

Before you begin

To scan by using a credential list, you must first define a central list of the credentials that are required by your operating systems. For more information, see "Configuring a credential set" on page 60.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Profiles**.
3. On the toolbar, click **Add**.

   When you create a scan profile, the only mandatory fields are **Name** and **IP Addresses** on the **Details** tab of the **Scan Profile Configuration** page. To configure an authenticated scan, you must also follow the remaining steps in this procedure.
4. Click **Use Centralized Credentials** to scan your Linux or UNIX operating systems.

   If a credential set is not configured and you do not manually specify the credentials, the scan tools run but no credentials are passed in.

   If QVM cannot find a centralized credential set for the hosts that you are scanning, it uses existing credentials that you manually specify in the **Additional Credentials** tab.
5. Click the **When To Scan** tab.
6. In the **Run Schedule** list, select **Manual**.
7. Click the **Additional Credentials** tab.
8. In the **Linux/Unix Patch Scanning** area, type the user name and password for the Linux or UNIX hosts that you want to scan and click **>**.

   A password is not required, if you configured secure public key authentication between your console and your scan target.
9. Click **Save**.
10. In the **Scan Profiles** page, click **Run**.

Related concepts

Centralized credential sets

Related tasks

Configuring a credential set

In IBM QRadar Vulnerability Manager, you can create a credential set for the assets in your network. During a scan, if a scan tool requires the credentials for a Linux, UNIX, or Windows operating system, the credentials are automatically passed to the scan tool from the credential set.

Configuring Linux operating system public key authentication

Enabling permissions for Linux or UNIX patch scans

Non-root user accounts must have the permissions to run the commands that QRadar Vulnerability Manager requires to scan for patches on Linux and UNIX computers.

About this task

Do the following tasks to verify that the user account that you use for scanning has the relevant permissions for Linux or UNIX patch scanning,

Procedure

1. SSH to the asset.
2. Run the following uname commands:

```
uname -m
uname -n
uname -s
uname -r
uname -v
uname -p
uname -a
```

3. Depending on your operating system, run the following commands:

Table 9. Commands to run on your Operating System

Operating System	Commands

Linux	The following files contain the relevant content for your distribution:
	/etc/redhat-release
	/etc/SuSE-release
	/etc/debian-version
	/etc/slackware-version
	/etc/mandrake-version
	/etc/gentoo-version
	For example, on Red Hat Enterprise Linux, use the commands:
	`ls /etc/redhat-release`
	`cat/etc/redhat-release`
	`rpm -qa --qf '%{NAME}--%{VERSION}---%{RELEASE}|%{EPOCH}--%{ARCH}---%{FILENAMES}--%{SIGPGP}---%{SIGGPG}\n'`
	`rpm -qa --qf '%{NAME}-%{VERSION}-%{RELEASE}|%{EPOCH}\n'`

Solaris	`/usr/bin/svcs -a/`
	`usr/bin/pkginfo -x | awk '{ if ( NR % 2 ) { prev = \$1 } else { print prev\" \"\$0 } }'`
	`/usr/bin/showrev -p`
	`/usr/sbin/patchadd -p`
	`/usr/bin/isainfo -b`
	`/usr/bin/isainfo -k`
	`/usr/bin/isainfo -n`
	`/usr/bin/isainfo -v`

HP-UX	`/usr/sbin/swlist -l fileset -a revision` `/usr/sbin/swlist -l patch`
AIX	`oslevel -r` `lslpp -Lc`

Table 9. Commands to run on your Operating System (continued)	
Operating System	**Commands**
ESX	`vmware -vesxupdate query --all` `. /etc/profile ;  /sbin/esxupdate query –all`

Tip:

As a best practice, turn off email notifications for the scan user account because email notification might interfere with the processing of scan results. View your operating system documentation for details about turning off email notifications for user accounts.

Chapter 8. Scanning on Windows-based assets

QRadar Vulnerability Manager uses registry scanning and Open Vulnerability Assessment Language (OVAL) scanning to detect vulnerabilities on Windows-based assets. Use authenticated scans to detect all Windows vulnerabilities. Unauthenticated scans might not detect all Windows vulnerabilities.

When are vulnerability data updates visible in QRadar?

Newly published vulnerabilities are visible on the QRadar Vulnerability Manager dashboard and in the research section of the **Vulnerability** tab in QRadar.

QRadar Vulnerability Manager gets daily vulnerability updates, which includes news, advisories, newly published vulnerabilities and their associated metadata, test data, and any new detection.

QRadar Vulnerability Manager systems are typically updated with the most recent vulnerabilities 2-3 days after they are announced.

What types of scanning methods are available?

The following list describes important points about scanning methods that are available to detect vulnerabilities on Windows-based assets:

Authenticated or unauthenticated scans
You must use authenticated scans to detect all Windows-based vulnerabilities. If you use an unauthenticated scan to detect Windows-based vulnerabilities, the results might not be complete and they are prone to false positives.

Registry scans
Registry scanning is used to detect vulnerabilities on the Windows operating system.

- QRadar Vulnerability Manager uses the remote registry service and Windows Management Instrumentation (WMI) to retrieve information about installed KB service packs, installed software, and enabled services from the endpoints that it scans, and this information is correlated with vulnerability definitions.
- Each Windows vulnerability definition includes the Bulletin, KB, product, OS, service pack, and required Windows service.

Open Vulnerability Assessment Language (OVAL) scans
OVAL (Open Vulnerability Assessment Language) scanning is used to detect vulnerabilities on the Windows operating system.

Open Vulnerability Assessment Language (OVAL) is a standard that is referenced when you do OVAL tests for vulnerabilities and configuration tests on assets. The following list describes information about vulnerabilities and OVAL tests.

- Tests can include any combination of registry keys, registry key values, `.dll` and `.exe` versions, running services, presence of files.
- Each vulnerability definition is an XML logical expression that determines whether the system is vulnerable.
- All `.exe` and `.dll` versions are tested.
- You can click the CVE link for a vulnerability to see whether it has an OVAL test, for example, CVE-2013-3910 (https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-3910)
- OVAL test definitions are available online at the Oval website, (https://oval.cisecurity.org/)
- The OVAL test can override a generated vulnerability.

Windows OS patch scans
Windows operating system *patch* scanning is an authenticated network-based method that is used to interrogate the target computer for missing security-related software fixes and updates.

© Copyright IBM Corp. 2012, 2020

Patch scans do a limited Nmap port scan of ports, 22, 139, and 445, to determine whether the asset is a Windows or an UNIX asset. If the port scan discovers NetBIOS ports 139 or 445, it knows that these ports are from a Windows-based asset. The enum vulnerability tool is used to scan a Windows asset.

Patch scans are not intrusive, and they don't do any active vulnerability tests.

Patch scans factor in superseded patches automatically.

It is possible to scan computers for Windows OS patches without configuring Windows Management Instrumentation (WMI) and Administrative Shares but the results are not complete and they are prone to false positives.

Configuration requirements for Windows-based asset scanning

The following list describes requirements that you must configure for Windows-based asset scanning:

- Configure remote registry access on the assets.
- Configure Windows management instrumentation (WMI) on the assets.
- To read WMI data on a remote server through a firewall, you must allow WMI requests through a Windows firewall.
- If you use a non-administrator account to monitor the Windows server, you must set minimum DCOM permissions and grant DCOM remote access permissions for that non-administrator account.
- Configure administrative shares on the assets.

Configuring an authenticated scan of the Windows operating system

In IBM QRadar Vulnerability Manager, you can configure a scan of the Windows operating systems that are installed on your network. You can manually specify the credentials in the scan profile or use a credential set.

If scanning is performed without administrative privileges, then QRadar Vulnerability Manager scans the remote registry for each installation on the Windows operating system.

Scanning without administrative privileges is incomplete, prone to false positives, and does not cover many third-party applications.

Before you begin

QRadar Vulnerability Manager uses standard Windows operating system remote access protocols that are enabled by default in most windows deployments.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Profiles**.
3. On the toolbar, click **Add**.

   When you create a scan profile, the only mandatory fields are **Name** and **IP Addresses** on the **Details** tab of the **Scan Profile Configuration** page. To configure an authenticated scan of the Windows operating system, you must also follow the remaining steps in this procedure.
4. Click **Use Centralized Credentials** to scan your Windows operating systems.

   You must configure a credential set or manually specify credentials for hosts before scan tools that require credentials can run.

   If QVM cannot find a centralized credential set for the hosts that you are scanning, it uses existing credentials that you manually specify in the **Additional Credentials** tab.
5. Click the **When To Scan** pane.

6. In the **Run Schedule** list, select **Manual**.

   If you want the scan to run at a later time, choose from one of the available **Run Schedule** options.
7. Click the **Additional Credentials** area.
8. In the **Windows Patch Scanning** area, type the **Domain**, **Username**, and **Password** for the Windows hosts that you want to scan and click (**>**).

   The domain name that you type is your Windows domain, not an internet domain.
9. Click **Save**.
10. In the **Scan Profiles** page, click **Run**.

Related concepts

Centralized credential sets

Authenticated patch scans

Remote Registry

The Remote Registry service must be enabled and started and accessible from both the QRadar Vulnerability Manager scanner appliance and the configured scanning user used in the scan profile.

If the remote registry cannot be accessed, windows patch scanning fails completely.

If QRadar Vulnerability Manager cannot access the remote registry, the scan results record the following error:

```
Local Checks Error – Remote Registry Service Not Running
```

In QRadar Vulnerability Manager version 7.2.3 and later, a yellow triangle icon is displayed next to the asset in the scan results.

The status of the remote registry service can be verified from the **Administrative Control Panel** under **Services**. Ensure that the following dependent services are started:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC EndPoint Mapper

QRadar Vulnerability Manager can access the remote registry over the classic NetBIOS (ports 135, 137, 139) or the newer NetBIOS over TCP (on port 445). Network or personal firewalls that block access to either of these protocols prevents access to Windows patch scans.

Administrative user accounts have access to the remote registry by default. Non-administrative user accounts do not have access to the remote registry. You must configure access.

Enabling remote registry access to assets on the Windows operating system

To scan Windows-based systems, you must configure your registry.

Procedure

1. Log in to your Windows-based system.
2. Click **Start**.
3. In the **Search programs and files** field, type **services** and press Enter.
4. In the **Services** window, locate the **Remote Registry** service.
5. Right-click the **Remote Registry** service and click **Start**.
6. Close the **Services** window.

Assigning minimum remote registry permissions

Administrative user accounts have access to the remote registry by default. Non-administrative user accounts do not have access to the remote registry. You must configure access.

Procedure

1. On the target Windows computer, create or designate a Local or Global User (example, "QVM_scan_user") and assign read-only Registry access to the non-administrative user account.
2. Log on to your Windows computer by using an account that has administrator privileges. Click **Start** > **Run**.
3. Type `regedit`.
4. Click **OK**.
5. Go to the key:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers \winreg.

   The permissions that are associated with this registry key control which users or group can access the registry remotely from the network.
6. Highlight the **winreg** key and do one of the following steps:
   - On Windows XP or later, click **Edit** > **Permissions**.
   - On Windows 2000, click **Security** > **Permissions**.
7. Give read-only access to the designated "QVM_scan_user" account.

   On Windows XP, the *ForceGuest* setting is enabled by default when in workgroup mode. This setting might cause access problems for WMI connections and shares access, other DCOM services, and RPC services. You cannot disable the *ForceGuest* setting on Windows XP Home computers.

Configuring WMI

QRadar Vulnerability Manager uses Windows Management Instrumentation (WMI) to locate and identify versions of the installed .exe and .dll files on the target assets that are scanned.

About this task

Without the information that is provided by Windows Management Instrumentation (WMI), many third-party applications are missed. False positives that are detected during registry scanning (by using the remote registry service) cannot be identified or removed by QRadar Vulnerability Manager.

WMI is installed on all of modern Windows operating systems, such as Windows Vista, Windows 2008, Windows 2012, Windows 7, Windows 8, and Windows 8.1).

Remote WMI requests must be enabled and accessible by the scanning user on assets that are scanned. If WMI is not available, the following error is reported in the scan results:

```
Local Checks Error – Unable to Query WMI serviceMount Remote Filesystem
```

In QRadar Vulnerability Manager version 7.2.3 and above, a yellow triangle warning icon appears next to the asset in the scan results.

To read WMI data on a remote server, a connection must be made from your management computer (where the monitoring software is installed) to the server that you are monitoring. If the target server is running the Windows Firewall (also called Internet Connection Firewall) which is installed on Windows XP and Windows 2003 computers, you must configure the firewall to allow remote WMI requests through. To configure Windows Firewall to allow remote WMI requests, open a shell prompt and enter the following command:

```
netsh firewall set service RemoteAdmin enable
```

If your patch scan is not successful, do the following steps.

Procedure

1. On the target server, go to **Control Panel** > **Administrative Tools** > **Computer Management**.
2. Expand **Services and Applications**.
3. Right-click **WMI Control** and click **Properties**.
4. Click the **Security** tab.
5. Click **Security**.
6. If necessary, add the monitoring user, and click the **Remote Enable** check box for the user or group that requests WMI data. To add a monitoring user or group:
   a) Click **Add**.
   b) In the **Enter the object names to select** field, type the name of your group or user name.
   c) Click **OK**.
7. Click **Advanced** and apply to the root and sub name spaces.

   Note: In some cases, you might also need to configure the Windows firewall and DCOM settings.

   If you experience WMI issues, you can install the WMI Administrative tools from the Microsoft website.

   The tools include a WMI browser that helps you connect to a remote machine and browse through the WMI information. These tools help you to isolate any connectivity issues in a more direct and simpler environment.

Setting minimum DCOM permissions

To connect to a remote computer by using WMI, you must ensure that the correct DCOM settings and WMI namespace security settings are enabled for the connection.

About this task

To grant DCOM remote launch and activation permissions for a user or group, do these steps.

Procedure

1. Click **Start** > **Run**, type `DCOMCNFG`, and then click **OK**.
2. In the **Component Services** dialog box, expand **Component Services**, expand **Computers**, and then right-click **My Computer** and click **Properties**.
3. In the **My Computer Properties** dialog box, click the **COM Security** tab.
4. Under **Launch and Activation Permissions**, click **Edit Limits**.
5. In the **Launch Permission** dialog box, if your name or your group does not appear in the **Groups or user names** list, follow these steps:
   a) In the **Launch Permission** dialog box, click **Add**.
   b) In the **Select Users, Computers, or Groups** dialog box, add your name and the group in the **Enter the object names to select** box, and then click **OK**.
6. In the **Launch Permission** dialog box, select your user and group in the **Group or user names** box.
7. In the **Allow** column under **Permissions for User**, select **Remote Launch** and select **Remote Activation**, and then click **OK**.

Setting DCOM remote access permissions

You must set up DCOM remote access permissions for certain users and groups.

About this task

If Computer A is connecting remotely to Computer B, you can set the remote access permissions on Computer B to allow a user or group that is not a member of the Administrators group on Computer B to connect remotely to Computer B.

Procedure

1. Click **Start** > **Run**, type `DCOMCNFG`, and then click **OK**.
2. In the **Component Services** dialog box, expand **Component Services**, expand **Computers**, and then right-click **My Computer** and click **Properties**.
3. In the **My Computer Properties** dialog box, click the **COM Security** tab.
4. In the **Access Permissions** section, click **Edit Limits**.
5. Configure one of the following users or groups to have remote access rights:
   - In the **Access Permission** dialog box, select the **ANONYMOUS LOGON** name in the **Group or user names** box. In the **Permissions for ANONYMOUS LOGON** area, select the **Allow** check box for **Remote Access**, and then click **OK**.
   - In the **Access Permission** dialog box, select the **Everyone** name in the **Group or user names** box. In the **Permissions for Everyone** area, select the **Allow** check box for **Remote Access**, and then click **OK**.
   - In the **Access Permission** dialog box, select the **<QVM scan user>** name in the **Group or user names** box. In the **Permissions for <QVM scan user>** area, select the **Allow** check box for **Remote Access**, and then click **OK**.

   Note: If you want to use the **<QVM scan user>** user account, you must create the user account before you grant DCOM remote access rights. You must also configure WMI access (step 6) for this user.

Administrative shares

All Windows computers have administrative shares, `\\machinename\driveletter$` enabled, especially when they are part of a domain.

QRadar Vulnerability Manager uses administrative shares to detect vulnerabilities on the following limited set of applications:

- Mozilla Firefox
- Mozilla Thunderbird
- Java™ FX
- Apache Archiva
- Apache Continuum
- Google ChromePreferences

Administrative shares are not visible to non-administrative users, and some organizations disable administrative shares or use non-administrative user accounts to scan. If administrative shares are not accessible, QRadar Vulnerability Manager might miss vulnerabilities in the products in the preceding list or produce false positives. In general, QRadar Vulnerability Manager vulnerability tests use only administrative shares as a last resort, and use registry scans and WMI.

Enabling administrative shares

On Windows Vista or later, administrative shares are disabled by default when in "workgroup" mode.

About this task

Enable administrative shares by using these steps:

Procedure

1. Click **Start** > **Run** and type `regedit`.
2. Go to the key:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
3. Right-click **WMI Control** and click **Properties**.
4. Add a new DWORD named: `LocalAccountTokenFilterPolicy`
5. Set the value to 1.

Disabling administrative shares

Some organizations do not want to enable administrative shares. However, when enable the remote registry service, the server service is started and administrative shares are enabled.

About this task

To disable administrative shares, modify the following registry key:

Procedure

1. Click **Start** > **Run** and type `regedit`.
2. Go to the key: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer**
3. Set the **`AutoShareWks`** parameter to `0`.

   Note: This action does not disable the IPC$ share. Although this share is not used to access files directly, ensure that anonymous access to this share is disabled. Alternatively, you can remove the IPC$ share completely by deleting it at start-up by using the following command:

   ```
   net share IPC$ /delete
   ```

   Use this method to remove the C$ and D$ shares also.

Manually configuring NTLMv2 authentication to prevent scan failures

You must manually configure the credentialed scans that you run against assets that use Microsoft New Technology LAN Manager version 2 (NTLMv2) so that you can prevent the scans from failing.

About this task

When you run a credentialed scan against a Windows asset that uses the LAN Manager Authentication Level of "`Send NTLMv2 response only. Refuse LM and NTLM`", some of the scan tools can fail authentication. A yellow warning triangle is displayed for the asset, and a local checks error vulnerability is raised. Running the scan multiple times can result in locking the user account out of the asset.

To prevent the scans that you run against assets that use NTMLv2 from failing, manually enable NTMLv2 authentication in the following files on the QVM Scanner:

- `/opt/qvm/etc/smb.conf`
- `/opt/qvm/etc/smb.conf.smbv1`

- `/opt/qvm/etc/smb.conf.smbv2`

Procedure

Open each of these files and add the following line: `client ntlmv2 auth = yes`

Chapter 9. Vulnerability exception rules

In IBM QRadar Vulnerability Manager, you can configure exception rules to minimize the number of false positive vulnerabilities.

When you apply exception rules to vulnerabilities, you reduce the number of vulnerabilities that are displayed in search results.

If you create a vulnerability exception, the vulnerability is not removed from QRadar Vulnerability Manager.

Viewing exception rules

To display vulnerability exceptions, you can search your vulnerability data by using search filters.

To view exception rules, click the **Vulnerabilities** tab, then click **Vulnerability Exception** in the navigation pane.

Tip: The **Exception Rules** table displays only the most recently entered comment. To view other comments, hover over the **Comment** column for the rule.

Related tasks

Reducing the number of false positive vulnerabilities

Applying a vulnerability exception rule

In IBM QRadar Vulnerability Manager, you can manually apply a vulnerability exception rule to a vulnerability that you decide does not pose a significant threat.

If you apply an exception rule, the vulnerability is no longer displayed in QRadar Vulnerability Manager search results. However, the vulnerability is not removed from QRadar Vulnerability Manager.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities** > **By Network**.
3. Search your vulnerability data. On the toolbar, click **Search** > **New Search**.
4. Click the **Vulnerability Instances** column link.
5. Select the vulnerability that you want to create an exception rule for.
6. On the toolbar, select **Actions** > **Exception**.
7. In the **Exception Rule** field, select an expiry option.
8. To provide a reason for the exception, select a reason from the **Reason** list.
9. In the **Assets** field, select your target assets for the exception rule by choosing from the following options:
   - To apply the exception to all assets, select **Exception vulnerability for all assets**.
   - To apply the exception to a specific asset, select **Exception for specific asset with current IP**.

     By default, the asset that is associated with the vulnerability that you selected in Step 5 is selected.
   - To apply the exception to a specific IP address, CIDR, or network, enter the details, select your domain and click **Add**.

     If you select a specific network from your network hierarchy, the exception applies only to the IP addresses in that network. For example, if an IP address is assigned to two networks in the network hierarchy, the exception does not apply to that same IP address in the second network, unless you specify it as an exception.

© Copyright IBM Corp. 2012, 2020

10. In the **Notes** field, enter comments in the **Comments** text box.
11. Click **Save** or **Cancel**.

Related concepts

False positives management

Commonly, false positives in vulnerability scanning occur when the scanner can access only a subset of the required information, which prevents it from accurately determining whether a vulnerability exists.

Related tasks

Searching vulnerability data

Managing a vulnerability exception rule

If you receive new information about a vulnerability, you can update or remove an existing vulnerability exception rule.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Vulnerability Exception**.
3. Click the vulnerability that you want to manage.
4. On the toolbar, select an option from the **Actions** menu.

   Important: If you delete a vulnerability exception rule, no warning is displayed. The vulnerability is immediately deleted.
5. Click **Save**.

Searching vulnerability exceptions

In IBM QRadar Vulnerability Manager, you can search your vulnerability data and filter the search results to display vulnerability exceptions.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Manage Vulnerabilities** > **By Asset**.
3. On the toolbar, select **Search** > **New Search**.
4. To filter your vulnerability data to include vulnerability exceptions, from the **Search Parameters** pane, select one of the following options:
   - Include vulnerability exceptions

     Displays all vulnerabilities, including vulnerabilities with an exception rule applied to them.
   - Only include vulnerability exceptions

     Displays vulnerabilities only with an exception rule applied to them.
5. Click **Add Filter**.
6. Click **Search**.

Chapter 10. Scan investigations

In IBM QRadar Vulnerability Manager, you can investigate summary asset and vulnerability data for each scan.

To investigate vulnerability scans, do the following tasks:

- Build and save complex vulnerability search criteria.
- Investigate exploitation risk levels at a network, asset, and vulnerability level.
- Prioritize your vulnerability remediation processes.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Scan results

You can use the **Scan Results** page to investigate the following information:

- The progress of a scan and the scanning tools that are queued and running.
- The status of a scan. For example, a scan with a status of **Stopped** indicates that the scan completed successfully or was canceled.
- The degree of risk that is associated with each completed scan profile. The **Score** column shows the Common Vulnerability Scoring System (CVSS) score for the completed scan profile. The CVSS base and temporal score are included in the calculation of this score but the CVSS environmental score is not included in this calculation. The CVSS environmental score is incorporated in the **Risk Score** column that you can view in the **Manage Vulnerabilities** window.
- The total number of assets that were found by the scan.
- The total number of vulnerabilities that were discovered by the completed scan profile.
- The total number of open services that were discovered by the completed scan profile.

Note: Scan progress can indicate that the scan is 100% complete while the results are still processing. To see if processing is complete, hover over the progress bar.

Vulnerability counts

The **Scan Results** page shows **Vulnerabilities** and **Vulnerabilities Instances**.

- The **Vulnerabilities** column shows the total number of unique vulnerabilities that were discovered on all the scanned assets.
- When you scan multiple assets, the same vulnerability might be present on different assets. Therefore, the **Vulnerability Instances** column shows the total number of vulnerabilities that were discovered on all the scanned assets.

Searching scan results

In IBM QRadar Vulnerability Manager, you can search and filter your scan results.

For example, you might want to identify recent scans, scans on a specific IP address, or scans that identified a specific vulnerability.

About this task

Use the **Name** field on the **Vulnerabilities** tab to search results by scan profile name. To use more advanced criteria in your search, do the following:

© Copyright IBM Corp. 2012, 2020

Domain-level restrictions are not applied until the security profiles are updated with an associated domain, and the changes are deployed.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Scan Results**.
3. On the toolbar, select **Search** > **New Search**.

   To search your scan results, there are no mandatory fields. All parameters are optional.
4. To show scan results for scans that completed within a recent number of days, type a value in the **Scan Run in the last days** field.
5. To show scan results for a specific vulnerability, click **Browse** in the **Contains Vulnerability** field.
6. To show scan results for scans that were only scheduled, click **Exclude on demand scan**.
7. Click **Search**.

Related concepts

Scan scheduling

In IBM QRadar Vulnerability Manager, you can schedule the dates and times to scan your network assets for known vulnerabilities.

Including column headings in asset searches

Limit asset searches with filters that include custom asset profiles, name, vulnerability count, and risk score.

Procedure

1. Click the **Assets** tab.
2. In the navigation pane, click **Asset Profiles**, then on the toolbar click **Search** > **New Search**.
3. In the field containing column names, in the field on the left, click the column headings you want to include in your search, and click the arrow button to move the selected headings to field on the right.
4. Click the up and down buttons to change the priority of the selected column headings.
5. When the field on the right contains all the column heading that you want to search on, click **Search**.

Managing scan results

In IBM QRadar Vulnerability Manager, on the **Scan Results** page, you can manage your scan results and manage the scans that are running.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Scan Results**.
3. If you want to rerun completed scans, select the check box in the rows assigned to the scans and click **Run**.

   A completed scan has a status of **Stopped**.
4. To delete completed scan results:
   a) On the **Scan Results** page, select the check box in the rows assigned to the scans results you want to delete.
   b) On the toolbar, click **Delete**.

      If you delete a set of scan results, no warning is displayed. The scan results are immediately deleted.

Remember: When you delete a set of scan results, neither the scan data in the QRadar asset model or the scan profile are deleted.

5. To cancel a scan that is running:
   a) On the **Scan Results** page, select the check box in the rows assigned to the scans you want to cancel.
   b) On the toolbar, click **Cancel**.

      You can cancel a scan that has a status of **Running** or **Paused**.

      After you cancel a scan, the status of the scan is **Stopped**.

Republishing scan results

If the asset model is not automatically updated with results from a completed scan, you can manually republish them from the **Scan Results** page.

About this task

If you did not select the **Update Asset Model** check box when you configured a scan profile, the scan results aren't automatically published to the asset model. You can update the asset model manually with scan results for that profile.

Procedure

1. Go to **Vulnerabilities** > **Scan Results**
2. Click the check box on the row that is assigned to the scan results that you want to republish.
3. Click **Republish** on the **Scan Results** page toolbar and then click **OK**.

   A red warning icon in the **Type** column indicates that the asset model is not updated with the selected scan results. The red warning icon disappears after the republishing process is complete.
4. Move the mouse pointer over the **Type** column to view confirmation in the tooltip that the asset model is updated for the selected scan results.

   Note: You can republish multiple scan results at the same time. However, if you republish two sets of scan results from the same profile, the asset model is updated with only the latest set of scan results.

   If you configured automatic report generation on the **Email** tab of the **Scan Profile Configuration** page, reports are generated and sent to the email addresses you configured when you republish scan results.

Asset risk levels and vulnerability categories

In IBM QRadar Vulnerability Manager, you can investigate the exploitation risk level of your scanned assets on the **Scan Results Assets** page.

The **Scan Results Assets** page provides a risk and vulnerability summary for each of the assets that you scanned by running a scan profile.

Risk score

Each vulnerability that is detected on your network has a risk score that is calculated by using the Common Vulnerability Scoring System (CVSS) base score. A high risk score provides an indication of the potential for a vulnerability exploitation.

On the **Scan Results Assets** page the **Score** column is an accumulation of the risk score for each vulnerability on an asset. The accumulated value provides an indication of the level of risk that is associated with each asset.

To quickly identify the assets that are most at risk to vulnerability exploitation, click the **Score** column heading to sort your assets by the risk level.

Vulnerability counts and categories

The **Scan Results Assets** page shows the total number of vulnerabilities and open services that were discovered on every scanned asset.

To identify the assets with the highest number of vulnerabilities, click the **Vulnerability Instances** column heading to order your assets.

The **High**, **Medium**, **Low**, and **Warning** columns group all vulnerabilities according to their risk.

The **Policy Check Passed %** and **Policy Check Failed %** columns display the percentage of policy checks that the asset passed or failed in the benchmark scan. Click the values in these columns to see more information on policy checks that passed or failed on the **Scan Results Policy Checks** page.

Asset, vulnerability, and open services data

In IBM QRadar Vulnerability Manager, the **Scan Results Asset Details** page shows asset, vulnerability, and open services data.

By using the options on the toolbar, you can switch between viewing vulnerabilities and open services.

The **Scan Results Asset Details** page provides the following information:

- Summary information about the asset that you scanned, including the operating system and network group.
- A list of the vulnerabilities or open services that were discovered on the scanned asset.
- Various ways of categorizing and ordering your list of vulnerabilities or open services for example, **Risk**, **Severity**, and **Score**.
- A quick way to view open service or vulnerability information. On the toolbar, click **Vulnerabilities** or **Open Services**.
- An easy way to view detailed information about the asset that you scanned. On the toolbar, click the **Asset Details**.
- An alternative method of creating a vulnerability exception. On the toolbar, click **Actions** > **Exception**.

The caution icon indicates that the scan failed. Hover over the icon for additional details.

For more information about the **Asset Details** window, see the *Users Guide* for your product.

Related concepts

Vulnerability exception rules

In IBM QRadar Vulnerability Manager, you can configure exception rules to minimize the number of false positive vulnerabilities.

Viewing the status of asset patch downloads

View whether an asset has a pending patch download. If there are no pending downloads, the asset has all available patches.

Procedure

1. Search for the asset that you want to confirm the patch status for.
2. Click the Asset IP address to open the **Asset Details** window.
3. Click **Details** > **Properties** to open the **Asset Properties** window.
4. Click the **Windows Patches** arrow.
5. View the patch status in the **Pending** column.
   - True - the asset has pending patches to download.
   - False - the asset has no pending patch downloads.

Vulnerability risk and PCI severity

In IBM QRadar Vulnerability Manager, you can review the risk and payment card industry (PCI) severity for each vulnerability that is found by a scan.

You can review the following information:

- The risk level that is associated with each vulnerability.
- The number of assets in your network on which the specific vulnerability was found.

To investigate a vulnerability, you can click a vulnerability link in the **Vulnerability** column.

Troubleshooting scan issues

Troubleshoot scanning issues in your network by investigating logs, error, and warning messages.

Slow response time from scanned host

Deploy the QRadar Vulnerability Manager scanning appliance relatively close to the assets that you are scanning. Use commands such as traceroute to ensure that packets are reaching the asset in less than 50 ms; otherwise scans might take a long time.

Check status of scan tools

If your scans are running for a long time, and you want to know what tools are running, hover over the scan progress percentage on the scan results page to display a popup window, which shows you the active tool.

Patch scan is not connecting to a Linux asset

If the patch-scan tool is not connecting to a Linux asset, a yellow triangular warning icon is displayed next to the asset in the scan results.

You might see the SSH `Patch Scanning - Failed Logon` error message.

Validate the user name and password. If you are using public key encryption, check the public key.

To scan Linux operating systems by using secure authentication, configure public key encryption between your console or managed host and your scan targets. Non-root user accounts must have the permissions to run the commands that QRadar Vulnerability Manager requires to scan for patches on Linux and UNIX computers. For more information, see Chapter 7, “Authenticated patch scans,” on page 59.

Local checks error

If the patch scan tool cannot connect to a Windows asset, a yellow triangular warning icon is displayed next to the asset in the scan results.

You might see the `Local Checks Error` error message, which means that the authenticated scan failed.

You can configure credentials in the scan profile or in centralized credentials. If the scanner is scanning Windows-based hosts, the following three windows services must be configured correctly:

- Remote registry
- Windows Management Instrumentation (WMI)
- Admin shares

For more information, see Chapter 8, “Scanning on Windows-based assets,” on page 65.

Same vulnerability titles for different KBs

If the KB for a bulletin is superseded by a KB in a future bulletin the vulnerability title does not change.

Stalled scan

If the scan is stalled or the scan is intermittent, an authorized user can log on to the scanner and verify the connectivity with the scan processor. Check the QRadar Vulnerability Manager error logs for connection errors.

UDP port scan takes a long time

If a scan policy is configured to scan all UDP ports, the scan might take a long time to complete, especially if the target host has several closed UDP ports. For PCI compliance scans, you are not required to scan all UDP ports. For more information, see “Scan duration and ports scanning” on page 27.

Number of assets scanned warning

If you see the following warning message on the **Scan Results** screen, your scan performance and scan results are not affected:

WARNING: You have scanned *<number>* assets but are only licensed to scan *<number>* assets. License Update Required!

Note: You might need to check your QRadar Vulnerability Manager license to verify how many assets your license permits you to scan.

Emailing asset owners when vulnerability scans start and stop

Email the configured asset technical owners to alert them of the scan schedule. You can also email reports to asset owners.

Before you begin

Configure the system mail server and technical owners for assets. For more information, see the *IBM QRadar Administration Guide*.

Procedure

1. Click the **Vulnerabilities** tab.
2. Click **Administrative** > **Scan Profiles**.
3. On the row assigned to the scan you want to edit, select the check box and click **Edit** on the toolbar.
4. In the **What To Email** area of the **Email** tab, select the appropriate check boxes.
5. If you selected the **Reports** check box, in the **Available Reports** field, select the reports that you want to email and click the arrow to move reports into the **Selected Reports** field.

   Reports can be large. Confirm that the sent reports are not rejected by the recipient's email provider.
6. In the **Who to Email** area, select the recipients that you want to receive the emails:
   - To email the configured technical owners of the scanned assets, select the **Technical Owners** check box. Technical owners receive emails about their assets only.
   - To enter or select email addresses in the field, select the **To Addresses** check box. Select emails and click **Add Me** to email the selected email recipients. Entered email addresses receive emails and reports regarding all scanned assets.
7. Click **Save**.

Chapter 11. Management of your vulnerabilities

In IBM QRadar Vulnerability Manager, you can manage, search, and filter your vulnerability data to help you focus on the vulnerabilities that pose the greatest risk to your organization.

The vulnerability data that is displayed is based on the vulnerability status information that is maintained in the QRadar asset model. This information includes vulnerabilities that are found by the QRadar Vulnerability Manager scanner and the vulnerabilities that are imported from external scanning products.

Manage your vulnerabilities to provide the following information:

- A network view of your current vulnerability posture.
- Identify vulnerabilities that pose the greatest risk to your organization and assign vulnerabilities to QRadar users for remediation.
- Establish how widely your network is impacted by vulnerabilities and display detailed information about the network assets that contain vulnerabilities.
- Decide which vulnerabilities pose less risk to your organization and create vulnerability exceptions.
- Display historical information about the vulnerabilities on your network.
- Display vulnerability data by network, asset, vulnerability, open service, or vulnerability instance.

Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) is used to rate the severity and risk of computer system security.

CVSS is an open framework that consists of the following metric groups:

- Base
- Temporal
- Environmental

Base

The base score severity range is 0 to 10 and represents the inherent characteristics of the vulnerability. The base score has the largest bearing on the final CVSS score, and can be further divided into the following sub-scores:

- Impact

  The impact sub-score represents metrics for confidentiality impact, integrity impact, and the availability impact of a successfully exploited vulnerability.

- Exploitability

  The exploitability sub-score represents metrics for Access Vector, Access Complexity, and Authentication, and measures how the vulnerability is accessed, the complexity of the attack, and the number of times an attacker must authenticate to successfully exploit a vulnerability.

Temporal

The temporal score represents the characteristics of a vulnerability threat that change over time, and consists of the following metrics:

- Exploitability

  The availability of techniques or code that can be used to exploit the vulnerability, which changes over time.

- Remediation Level

© Copyright IBM Corp. 2012, 2020

The level of remediation that is available for a vulnerability.

- Report Confidence

  The level of confidence in the existence of the vulnerability and the credibility of its technical details.

Environmental

The environmental score represents characteristics of the vulnerability that are impacted by the user's environment. Configure the following environmental metrics to highlight the vulnerabilities of important or critical assets by applying higher environmental metrics. Apply the highest scores to the most important assets because losses that are associated with these assets have greater consequences for the organization.

- Collateral Damage Potential (CDP)

  The potential for loss of life or physical assets through the damage or theft of this asset, or the economic loss of productivity or revenue.

- Target Distribution (TD)

  The proportion of vulnerable systems in your user's environment.

- Confidentiality Requirement (CR)

  The level of impact to the loss of confidentiality when a vulnerability is exploited on this asset.

- Integrity Requirement (IR)

  This metric indicates the level of impact to the loss of integrity when a vulnerability is successfully exploited on this asset.

- Availability Requirement (AR)

  The level of impact to the asset's availability when a vulnerability is successfully exploited on this asset.

Related tasks

Configuring environmental risk for an asset

Use the CVSS Environmental Score to manipulate and prioritize the risk score on selected assets. If you configure the **CVSS, Weight & Compliance** parameters for an asset, you can apply higher risk scores to assets that are more important or critical.

Investigating vulnerability risk scores

In IBM QRadar Vulnerability Manager, you can investigate vulnerability risk scores and understand how each score is calculated.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. Click the **Risk Score** column to sort your vulnerabilities by risk.
4. To investigate the risk score, hover you mouse on a vulnerability risk score.

Risk score details

In IBM QRadar Vulnerability Manager, vulnerability risk scores provide an indication of the risk that a vulnerability poses to your organization.

Using IBM QRadar Risk Manager, you can configure policies that adjust vulnerability risk scores and draw attention to important remediation tasks.

Risk Score

The **Risk Score** provides specific network context by using the Common Vulnerability Scoring System (CVSS) base, temporal, and environmental metrics.

When QRadar Risk Manager is not used to manage risk, the **Risk Score** column shows the CVSS environmental metric score with a maximum value of 10.

Risk adjustments

If IBM QRadar Risk Manager is installed and you configured vulnerability risk policies, then the risk adjustments are listed. The adjustments either increase or decrease the overall risk that is associated with a vulnerability.

Related concepts

Integration with QRadar Vulnerability Manager

Related tasks

Prioritizing high risk vulnerabilities by applying risk policies

Custom risk classification

Use custom risk scores in QRadar Vulnerability Manager to classify vulnerabilities that pose the most risk to your organization. Custom risk classification allows you to override a vulnerability's risk with your own risk classification.

Based on your individual requirements, you might want to override a vulnerability's risk with your own risk classification. A vulnerability that is classified as a high CVSS score by QRadar Vulnerability Manager may not actually pose a serious risk for numerous mitigating factors. For example, if a CVSS 9.5 IPv6 vulnerability is published, and an enterprise does not have any IPV6 infrastructure, then the high CVSS score is not justified.

Configuring custom risk scores for vulnerabilities

In IBM QRadar Vulnerability Manager, you can add an internal custom risk score to vulnerabilities that reflects the real risk to your organization. Assigned vulnerabilities have an associated remediation ticket with a due date that can be changed by adding a custom risk.

About this task

A nightly auto update job runs to update all the custom risk fields. For reporting and saved search purposes, your custom risk changes do not come into effect right away. You can run the auto update manually to populate the custom risk information that is entered. Run the auto update by clicking the **Auto Update** icon on the **Admin** tab.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Research** > **Vulnerabilities** or **Manage** > **Vulnerabilities**.
3. To assign a custom risk score to a vulnerability, use the following steps:
   a) Select a vulnerability and click **Edit/Triage**.
   b) Choose a custom risk type from the **Custom Risk Assignment** window.

      Tip: Removing the custom risk for assigned vulnerabilities reverts the vulnerability due date to the PCI severity value.
   c) To reflect the vulnerability assignment, you can add a note by using the RTF text box. For example, you can add a note to explain why you are changing the classification.
   d) Click **Save**.

e) When a custom risk is created on any vulnerability, a new column that is called **Custom Risk** displays in the **Research Vulnerabilities** or **Manage Vulnerabilities** screen.

4. To view the custom risk details and note related to a custom risk assignment, double-click the vulnerability.
5. To calculate the due date for an assigned vulnerability's remediation ticket, use the **Calculate Assigned Vulnerability Due Date** setting.
   a) On the **Admin** tab, click **QVM Configuration**.
   b) In the **QVM Configuration** window, set the **Calculate Assigned Vulnerability Due Date** option to **True**.
      This setting is enabled by default. When enabled, the assigned vulnerability due date is recalculated when a custom risk is applied, to correspond to the risk value's due days set in **Vulnerability Assignment** > **Remediation Settings**.

   The following table outlines sample scenarios where the custom risk might change the due date of a remediation ticket.

Scenario	Custom Risk	Existing Due Date	Updated Due Date
Custom risk used to increase ticket priority.	Increased from existing value	Later than the custom risk due date	Vulnerability takes the custom risk due date.
Custom risk used to decrease ticket priority.	Decreased from existing value	Earlier than custom risk due date	Vulnerability takes the custom risk due date.
Custom risk used to increase ticket priority.	Increased from existing value	Earlier than or equal to custom risk due date	Vulnerability keeps the existing due date.

   QRadar Vulnerability Manager adds the following note to the vulnerability details if any of these scenarios occur:

   ```
   Vulnerability Details Note: Custom risk set to ___. Due date has been
   changed from xxxxxx to xxxxxx.
   ```

   Tip: If you disable **Calculate Assigned Vulnerability Due Date**, the due date is not recalculated.
6. To search for vulnerabilities that are not triaged yet, use the following steps:
   a) In the navigation pane, click **Research** > **Vulnerabilities**.
   b) Click **Search** > **New Search**.
   c) In the **Custom Risk Level** section, select one of the following parameters to search:

Table 10. Custom risk search parameters.

Custom Risk Search Type	Description
All Vulnerabilities	Returns all vulnerabilities regardless of whether a custom risk is assigned.
All triaged vulnerabilities	Returns all vulnerabilities with a custom risk assigned.
All not yet triaged vulnerabilities	Returns all vulnerabilities that do not have a custom risk assigned.
All vulnerabilities with the specific custom risk level	Returns vulnerabilities that are filtered on the custom risk type that is selected, for example, critical, high, or medium.

   d) Click **Search**.
7. Export a list of vulnerabilities from the **Vulnerability List** screen for audit or compliance purposes, by using the following steps:
   a) In the navigation pane, click **Research** > **Vulnerabilities**.
   b) Select the CSV or XML export option.

Searching vulnerability data

In IBM QRadar Vulnerability Manager, you can identify important vulnerabilities by searching your vulnerability data.

QRadar Vulnerability Manager provides various methods to search your data. You can search by network, by asset, by open service, or by vulnerability.

Default saved searches provide a fast method of identifying the risk to your organization. Saved searches are displayed in the **Available Saved Searches** field on the **Vulnerability Manager Search** page.

Before you begin

You must create a scan profile and scan your network assets.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. On the toolbar, select **Search** > **New Search**.
4. If you want to load a saved search, do the following steps:
   a) Select a group from the **Group** list.
   b) In the **Type Saved Search** field, type the saved search that you want to load.
   c) From the **Available Saved Searches** list, select a saved search, and then click **Load**.
   d) Click **Search**.
5. If you want to create a new search, do the following steps in the **Search Parameters** pane:
   a) In the **first list**, select the parameter that you want to use.
   b) In the **second list**, select a search modifier. The modifiers that are available depend on the search parameter that you select.
   c) In the **third list**, type or select the specific information that is related to your search parameter.
   d) Click **Add Filter**.

   For example, to email the vulnerabilities that are assigned to a technical user, select **Technical Owner Contact** and provide an email address that is configured on the **Vulnerability Assignment** page.
6. Click **Search**.
7. On the toolbar, click **Save Search Criteria**.

   Important: Vulnerability reports use saved search information. If you want to create a report that emails a technical user, you must save your search criteria.

Related concepts

Vulnerability search parameters

In IBM QRadar Vulnerability Manager, you can search your vulnerability data and save the searches for later use.

Vulnerability quick searches

Search vulnerabilities by typing a text search string that uses simple words or phrases.

In IBM QRadar Vulnerability Manager, you can use quick searches to filter vulnerabilities on the **My Assigned Vulnerabilities** and **Manage Vulnerabilities** pages.

Use the **Quick Searches** list to do a pre-configured vulnerability search.

Use the **Quick Filter** field to create your own vulnerability filters. Click **Save Search Criteria** to add your vulnerability quick filters to the **Quick Searches** list.

Table 11. Vulnerability quick filter syntax guidelines	
Description	**Example**

Include any plain text that you expect to find in vulnerability title, description, solution, concern, reference ID type, or reference ID value.	`2012-3764`
	`MS203`
	`java`

To search only the text in the vulnerability title, add **:A** to the search text string	`PHP:A`
To search only the text in the vulnerability description, add **:B** to the search text string	`cross-site scripting:B`
To search only the text in the vulnerability external reference type, add **:C** to the search text string	`RedHat RHSA:C`
Include wildcard characters. The search term cannot start with a wildcard.	`SSLv*`

Group terms with logical operators: **AND**, **OR**, and **NOT** (or **!**). To be recognized as logical operators and not as search terms, the operators must be uppercase.	`PHP AND Traversal`
	`XSS:A OR cross-site scripting:A`
	`!MySQL`
	`NOT MySQL`

Related tasks

Saving your vulnerability search criteria

Vulnerability search parameters

In IBM QRadar Vulnerability Manager, you can search your vulnerability data and save the searches for later use.

The following table is not a complete list of vulnerability search parameters, but a subset of the available options.

Select any of the parameters to search and display vulnerability data.

Table 12. Vulnerability search parameters	
Option	**Description**
Access Complexity	The complexity of the attack that is required to exploit a vulnerability.
Access Vector	The network location from where a vulnerability can be exploited.
Asset saved search	The host, IP address, or range of IP addresses associated with a saved asset search. For more information about saving asset searches, see the *Users Guide* for your product.
Assets with Open Service	Assets that have specific open services. For example, HTTP, FTP, and SMTP.
Authentication	The number of times an attacker must authenticate against a target to exploit a vulnerability.

Table 12. Vulnerability search parameters (continued)

Option	Description
Availability Impact	The level that resource availability can be compromised if a vulnerability is exploited.
Confidentiality Impact	The level of confidential information that can be obtained if a vulnerability is exploited.
Days since asset found	The elapsed number of days since the asset with the vulnerability was discovered on your network. Assets can be discovered either by an active scan or passively by using log or flow analysis.
Days since associated vulnerability service traffic	Displays vulnerabilities on assets with associated layer 7 traffic to or from an asset, based on the elapsed number of days since the traffic was detected.
Domain	If you configured IBM QRadar for multi-domain systems, use this option to specify the domain you want to search for vulnerabilities.
By Open Service	Search for vulnerabilities that are associated with particular open services such as, HTTP, FTP, and SMTP.
External Reference of type	Vulnerabilities that have an associated HCL BigFix Fixlet. By using this parameter, you can show only those vulnerabilities without an available patch.
Impact	The potential impact to your organization. For example, access control loss, downtime, and reputation loss.
Include early warnings	Include newly published vulnerabilities that are detected in your network and are not present in any scan results.
Include vulnerability exceptions	Those vulnerabilities with an exception rule applied.
Integrity Impact	The level to which system integrity might be compromised if a vulnerability is exploited.
Only include assets with risk	Vulnerabilities that pass or fail specific risk policies that are defined and monitored in IBM QRadar Risk Manager. **Note:** You must monitor at least one question in the **Policy Monitor** page on the **Risks** tab to use this search parameter.
Only include assets with risk passed	Vulnerabilities that pass specific risk policies that are defined and monitored in QRadar Risk Manager.
Only include early warnings	Include only newly published vulnerabilities that are detected in your network and are not present in any scan results.

Table 12. Vulnerability search parameters (continued)	
Option	**Description**
Only include Vulnerability Exceptions	Include only vulnerabilities with an exception rule applied in your search.
Overdue by Days	Search for vulnerabilities that are overdue for remediation by a specified number of days.
Patch Status	Filter vulnerabilities by patch status. For more information, see “Identifying the patch status of your vulnerabilities” on page 93.
PCI Severity	Search for vulnerabilities by the PCI Severity level (High, Medium, or Low) assigned by the PCI compliance service. Vulnerabilities assigned a High or Medium PCI Severity level fail PCI compliance.
Quick Search	You can search for a vulnerabilities title, description, solution, and external reference ID. In the **Quick Search** field, you can use AND, OR, and NOT operators, and brackets.
Risk	Search for vulnerabilities by risk level (High, Medium, Low, Warning).
Unassigned	Search for vulnerabilities with no assigned user to remediate them.
Vulnerability External Reference	Vulnerabilities that are based on an imported list of vulnerability IDs, for example CVE ID. For more information about Reference Sets, see the *Administration Guide* for your product.
Vulnerability has a virtual patch from vendor	Vulnerabilities that can be patched by an intrusion prevention system.
Vulnerability state	The status of the vulnerability since the last scan of your network or specific network assets. For example, when you scan assets, the vulnerabilities that are discovered are either New, Pre-existing, Fixed, or Existing.
Vulnerability with risk	Filter vulnerabilities by risk policy results. You must monitor at least one question in the **Policy Monitor** page on the **Risks** tab to use this search parameter.

Saving your vulnerability search criteria

In IBM QRadar Vulnerability Manager, you can save your vulnerability search criteria for future use.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. On the toolbar, select **Search** > **New Search** and complete the search of your data.
4. On the toolbar, click **Save Search Criteria**.
5. In the **Save Search Criteria** window, type a recognizable name for your saved search.

6. To include your saved search in the **Quick Searches** list on the toolbar, then click **Include in my Quick Searches**.
7. To share your saved search criteria with all QRadar users, then click **Share with Everyone**.
8. To place your saved search is a group, then click a group or click **Manage Groups** to create a new group.

   For more information about managing search groups, see the *Administration Guide* for your product.
9. If you want to show the results of your saved search when you click any of the **Manage Vulnerabilities** pages in the navigation pane, then click **Set As Default**.
10. Click **OK**.

Deleting saved vulnerability search criteria

In IBM QRadar Vulnerability Manager, you can delete your saved vulnerability search criteria.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Manage Vulnerabilities** > **By Network**
3. On the toolbar, select **Search** > **New Search**.
4. On the **Vulnerability Manager Search** page, in the **Available Saved Searches** list, select the saved search that you want to delete.
5. Click **Delete**.
6. Click **OK**.

Vulnerability instances

In IBM QRadar Vulnerability Manager, you can display the vulnerabilities on each of the scanned assets in your network. Each vulnerability might be listed multiple times because the vulnerability exists on several of your assets.

If you configure third-party vulnerability assessment (VA) scanners, by using the QRadar **Admin** tab, then the vulnerabilities that are detected are automatically displayed in the **By Vulnerability Instances** page.

For more information about VA scanners, see the *Administration Guide* for your product.

The **By Vulnerability Instances** page provides the following information:

- A view of every vulnerability that was detected by scanning your network assets.
- The risk that each vulnerability poses to the Payment Card Industry (PCI).
- The risk that a vulnerability poses to your organization. Click the **Risk Score** column to identify the highest risk vulnerabilities.
- The name or email address of the user that is assigned to remediate the vulnerability.
- The numbers of days in which a vulnerability must be remediated.

Related concepts

Risk score details

Network vulnerabilities

In IBM QRadar Vulnerability Manager, you can review vulnerability data that is grouped by network.

The **By Network** page provides the following information:

- An accumulated risk score that is based on the vulnerabilities that are detected on each of your networks.
- The number of the assets, vulnerabilities, and open services for each network.

- The number of vulnerabilities that are assigned to a technical user and are overdue for remediation.

Asset vulnerabilities

In IBM QRadar Vulnerability Manager, you can display summary vulnerability data that is grouped by each scanned asset.

You can use the **By Asset** page to prioritize the remediation tasks for assets in your organization that pose the greatest risk.

The **By Asset** page provides the following information:

- An accumulated risk score that is based on the vulnerabilities that are detected on each of your assets.

  Click the **Risk Score** column to sort your assets by their risk.
- The number of asset vulnerabilities that are assigned to a technical user and are overdue for remediation.

Related information

How do vulnerabilities get mapped to specific Asset IDs? (Security Learning Academy course)

Open service vulnerabilities

In IBM QRadar Vulnerability Manager, you can display vulnerability data that is grouped by open service.

The **By Open Service** page shows an accumulated risk score and vulnerability count for each service in your entire network.

Investigating the history of a vulnerability

In IBM QRadar Vulnerability Manager, you can display useful information about the history of a vulnerability.

For example, you can investigate information about how the risk score of a vulnerability was calculated. You can also review information about when a vulnerability was first discovered and the scan that was used to discover the vulnerability.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. Search your vulnerability data.
4. Click the vulnerability that you want to investigate.
5. On the toolbar, select **Actions** > **History**.

Related tasks

Searching vulnerability data

Reducing the number of false positive vulnerabilities

In IBM QRadar Vulnerability Manager, you can automatically create exception rules for vulnerabilities that are associated with a specific type of server.

When you configure server types, QRadar Vulnerability Manager creates exception rules and automatically reduces the vulnerabilities that are returned by searching your data.

Procedure

1. Click the **Assets** tab.
2. In the navigation pane, select **Server Discovery**.

3. To automatically create false positive exception rules for vulnerabilities on specific server types, from the **Server Type** list, select one of the following options:
   - FTP Servers
   - DNS Servers
   - Mail Servers
   - Web Servers

   It might take a few minutes for the **Ports** field to refresh.
4. From the **Network** list, select the network for your servers.
5. Click **Discover Servers**.
6. In the **Matching Servers** pane, select the servers where the vulnerability exception rules are created.
7. Click **Approve Selected Servers**.

Results

Depending on your server type selection, the following vulnerabilities are automatically set as false positive exception rules:

Table 13. Server type vulnerabilities

Server Type	Vulnerability
FTP Servers	**FTP Server Present**
DNS Servers	**DNS Server is Running**
Mail Servers	**SMTP Server Detected**
Web Servers	**Web Service is Running**

Investigating high risk assets and vulnerabilities

In IBM QRadar Vulnerability Manager, you can investigate high risk vulnerabilities that might be susceptible to exploitation.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. On the **By Vulnerability Instances** page, click the **Risk Score** column heading to sort the vulnerabilities by risk score.
4. To investigate the CVSS metrics that are used to derive the risk score, hover your mouse on the **Risk Score** field.
5. Identify the vulnerability that has the highest score and click the **Vulnerability** link.
6. In the **Vulnerability Details** window, investigate the vulnerability:
   a) To view the IBM Security Systems website, click the **X-Force** link.
   b) To view the National Vulnerability Database website, click the **CVE** link.

      The IBM Security Systems website and National Vulnerability Database provide remediation information and details on how a vulnerability might affect your organization.
   c) To open the **Patching** window for the vulnerability, click the **Plugin Details** link. Use the tabs to discover Oval Definition, Windows Knowledge Base, or UNIX advisory information about the vulnerability. This feature provides information on how QRadar Vulnerability Manager checks for vulnerability details during a patch scan. You can use it to identify why a vulnerability was raised on an asset or why it was not.

d) The **Solution** text box contains detailed information about how to remediate a vulnerability.

Related concepts

Risk score details

Prioritizing high risk vulnerabilities by applying risk policies

In IBM QRadar Vulnerability Manager, you can alert administrators to high-risk vulnerabilities by applying risk policies to your vulnerabilities.

When you apply a risk policy, the risk score of a vulnerability is adjusted, which allows administrators to prioritize more accurately the vulnerabilities that require immediate attention.

In the following example, the vulnerability risk score is automatically increased by a percentage factor for any vulnerability that remains active on your network after 40 days.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. On the toolbar, click **Search** > **New Search**.
4. In the **Search Parameters** pane, configure the following filters:
   a) **Risk Equals High**
   b) **Days since vulnerabilities discovered Greater than or equal to 40**
5. Click **Search** and then on the toolbar click **Save Search Criteria**.

   Type a saved search name that is identifiable in QRadar Risk Manager.
6. Click the **Risks** tab.
7. In the navigation pane, click **Policy Monitor**.
8. On the toolbar, click **Actions** > **New**.
9. In the **What do you want to name this question** field, type a name.
10. In the **Which tests do you want to include in your question** field, click **are susceptible to vulnerabilities contained in vulnerability saved searches**.
11. In the **Find Assets that** field, click the underlined parameter on the **are susceptible to vulnerabilities contained in vulnerability saved searches**.
12. Identify your QRadar Vulnerability Manager high risk vulnerability saved search, click **Add**, then click **OK**.
13. Click **Save Question**.
14. In the **Questions** pane, select your question from the list and on the toolbar click **Monitor**.

    Restriction: The **Event Description** field is mandatory.
15. Click **Dispatch question passed events**.
16. In the **Vulnerability Score Adjustments** field, type a risk adjustment percentage value in the **Percentage vulnerability score adjustment on question fail** field.
17. Click **Apply adjustment to all vulnerabilities on an asset** then click **Save Monitor**.

What to do next

On the **Vulnerabilities** tab, you can search your high risk vulnerabilities and prioritize your vulnerabilities.

Related concepts

Integration with QRadar Vulnerability Manager

Related tasks

Saving your vulnerability search criteria

Configuring custom display colors for risk scores

Configure custom color coding for IBM QRadar Vulnerability Manager risk scores to view color-coded risk scores in QRadar Vulnerability Manager interfaces.

Procedure

1. In IBM QRadar, select **Vulnerabilities** > **Vulnerability Assignment** > **Risk Preferences**.
2. In the **Greater than or equal to** column, enter the minimum risk score value for High, Medium, Low, and Warning.
3. In the **Color** column, select or define a color to represent High, Medium, Low, and Warning risk scores.

   Note: The colors that you apply do not change the default risk colors on the **Scan Results** page. The **Score** column on the **Scan Results** page and the **Scan Results Asset Details** page uses default values and colors, which you cannot change.

Identifying vulnerabilities with a BigFix patch

In IBM QRadar Vulnerability Manager, you can identify the vulnerabilities that have an available fix.

After you identify your vulnerabilities that have an available fix, you can investigate detailed fix information in the **Vulnerability Details** window.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. On the toolbar, select **Search** > **New Search**
4. In the **Search Parameters** pane configure the following options:
   a) In the **first list** select **External Reference of type**.
   b) In the **second list** select **Equals**.
   c) In the **third list** select **IBM BigFix Patch**.
   d) Click **Add Filter**.
   e) Click **Search**.

   The **By Vulnerability Instances** page shows the vulnerabilities that have an available fix.
5. Order your vulnerabilities according to their importance by clicking the **Risk Score** column heading.
6. To investigate patch information for a vulnerability, click a vulnerability link in the **Vulnerability** column.
7. In the **Vulnerability Details** window, scroll to the bottom of the window to view the vulnerability patch information.

   The **Site ID** and **Fixlet ID** are unique identifiers that you use to apply vulnerability patches by using HCL BigFix.

   The **Base** column indicates a unique reference that you can use to access more information on a knowledge base.

Identifying the patch status of your vulnerabilities

In IBM QRadar Vulnerability Manager, you can identify the patch status of your vulnerabilities.

By filtering patched vulnerabilities, you can prioritize your remediation efforts on the most critical vulnerabilities in your organization.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. On the toolbar, select **Search** > **New Search**.
4. In the **first list** in the **Search Parameters** pane, select **Patch Status**.
5. In the **second list**, select a search modifier.
6. To filter your vulnerabilities according to their patch status, select one of the following options from the third list:

Option	Description
Pending Downloads	Select this option to show vulnerabilities that are scheduled to be patched
Pending Restart	Select this option to shows vulnerabilities that are patched after the scanned asset is restarted
Fixed	Select this option to show vulnerabilities that are patched by HCL BigFix

7. Click **Add Filter**.
8. Click **Search**.

Related concepts

HCL BigFix integration

Removing unwanted vulnerability data

Use QRadar Vulnerability Manager vulnerability cleansing functionality to remove stale vulnerability data from the asset model.

About this task

Any one of the following scenarios might leave you with unwanted vulnerability data:

- Change of scanner type
- Decommissioned assets
- Change of IP address
- Inaccurate or test scans

Important: After you remove vulnerability data for an asset or scanner type, it cannot be recovered.

Procedure

To remove unwanted vulnerability data, you have two options:

- Use the **Actions** > **Clean Vulnerabilities (All)** option on the **Assets** page to remove all vulnerability data for a selected scanner type.
- Use the **Actions** > **Clean Vulnerabilities (Asset)** option on the **Asset Details** page to remove all vulnerability data for a particular asset with a selected scanner type.

Configuring vulnerability data retention periods

You can set the retention period for vulnerability trend data and scan results in IBM QRadar Vulnerability Manager. Use configuration rules to change the default values.

Procedure

1. Click **Admin** > **QVM Configuration**.

2. In the **QVM Vulnerability Retention** section of the **QVM Configuration** window, enter a value in the following fields:

Rule	Description	Default Value
Vulnerability Trend Reporting Data (In Days)	Sets how many days QRadar Vulnerability Manager retains vulnerability trend data for use in daily vulnerabilities reports.	14 days
Vulnerability Trend Reporting Data (In Weeks)	Sets how many weeks QRadar Vulnerability Manager retains vulnerability trend data for use in weekly vulnerabilities reports.	14 weeks
Vulnerability Trend Reporting Data (In Months)	Sets how many months QRadar Vulnerability Manager retains vulnerability trend data for use in monthly vulnerabilities reports.	14 months
Purge Scan Results After Period (In Days)	Use this rule with **Purge Scan Results After Period (In Execution Cycles)** to set the retention limits for scan results data. Sets the number of days that QRadar Vulnerability Manager retains data after it applies the **Purge Scan Results After Period (In Execution Cycles)** limiting rule.	30 days
Purge Scan Results After Period (In Execution Cycles)	Use this rule with **Purge Scan Results After Period (In Days)** to set the retention limits for scan results data. Sets how many versions of scan result data that QRadar Vulnerability Manager retains. This rule has precedence over the value you set in **Purge Scan Results After Period (In Days)**. For the default values for the **Purge Scan Results After Period (In Days)** and **Purge Scan Results After Period (In Execution Cycles)** rules: • QRadar Vulnerability Manager retains scan results data for the three most recent execution cycles. It also retains any other versions of results for scans that you run within the 30 days limit. • If any of the three most recent execution cycles occurred beyond the 30 days limit, QRadar Vulnerability Manager retains scan results data for those execution cycles.	Three execution cycles

3. Click **Save**.

Chapter 12. Vulnerability remediation

In QRadar Vulnerability Manager, you can assign vulnerabilities to a technical user for remediation.

You can assign vulnerabilities to your technical user by using two methods.

- Assign individual vulnerabilities to a technical user for remediation.
- Assign a technical user as the owner of asset groups

Note: A ticket that is closed and manually reopened displays a status of **Reopened**, which can't be closed by automatic remediation. A ticket that is manually reopened must be closed manually. If a scan profile detects a vulnerability that has been closed, the ticket status is set to **Opened**. These tickets can be closed by automatic remediation after the vulnerability is no longer detected in the scan profile.

Related tasks

Configuring remediation times for the vulnerabilities on assigned assets

Assigning individual vulnerabilities to a technical user for remediation

When you assign a vulnerability for remediation in IBM QRadar Vulnerability Manager, you can set the due date and write a note about the reason for the assignment.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Manage Vulnerabilities**.
3. Search your vulnerability data.
4. Select the vulnerability that you want to assign for remediation.
5. On the toolbar, click **Actions** > **Assign/Edit**.
6. Select a technical user from the **Assigned User** list.
7. In the **Due Date** list, select a future date when the vulnerability must be remediated.

   If you do not select a date, the **Due Date** is set as the current date.
8. In the **Notes** field, type useful information about the reason for the vulnerability assignment.
9. Click **Save**.

Related tasks

“Assigning a technical user as the owner of asset groups” on page 97

Assigning a technical user as the owner of asset groups

In IBM QRadar Vulnerability Manager, you can configure groups of assets and automatically assign their vulnerabilities to technical users.

After you assign a technical user and scan the assets, all vulnerabilities on the assets are assigned to the technical user for remediation.

The remediation times for vulnerabilities can be configured using the **Remediation Times** option, depending on their risk or severity.

If you add a new asset to your network, and it is contained in a technical user's asset group, vulnerabilities on the asset are automatically assigned to the technical user.

You can automatically email reports to your technical users with the details of vulnerabilities that they are responsible for fixing.

© Copyright IBM Corp. 2012, 2020

The **Remediation Times**, **Schedule** and **Risk Preferences** options are enabled only for administrative users, and non-administrative users who have no associated domain.

Before you begin

If you want to configure a group of assets that are identified by a saved asset search, you must search your assets and save the results.

For more information about searching assets and saving the results, see the *User Guide* for your product.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Vulnerability Assignment**.
3. On the toolbar, click **Add**.
4. Type a name, email address, and CIDR range.

   To automatically assign a technical user in the **New Asset Owner** window, the only mandatory fields are **Name**, **Email**, and **CIDR**. If multi-domain environments are enabled, select a domain association for that particular asset owner.
5. If you configured IBM QRadar for multiple domains, select the relevant domain from the **Domain** list.
6. To filter the list of assets in your CIDR range by asset name, type a text string in the **Asset Name Filter** field.
7. To filter the list of assets in your CIDR range by operating system, type a text string in the **OS Filter** field.
8. To assign the technical user to the assets that are associated with a saved asset search, click **Asset Search**. The **Asset Search** option is disabled if domains have been configured in the **Domain Management** page.
9. Click **Save**.
10. On the toolbar, click **Remediation Times**.

    You can configure the remediation time for each type of vulnerability, depending on their risk and severity.

    For example, you might need high risk vulnerabilities to be fixed within 5 days.
11. On the toolbar, click **Schedule**.

    By default, the technical user contact for your assets is updated every 24 hours.

    New assets added to your deployment and falling within the CIDR range that you specified are automatically updated with the technical contact that you specified.

    Important: The schedule applies to the associations you made between technical users and groups of assets.
12. Click **Update Now**, to immediately set the owner of your assets.

    Depending on the size of your deployment, it might take an extended time to update your assets.
13. Click **Save**.

    Any vulnerabilities that are already assigned to a technical user for remediation are updated with the new technical user.
14. If vulnerabilities were not previously assigned to a technical user, you must scan the assets that you assigned to the technical user.

    Important: Scanning the assets ensures that any vulnerabilities assigned to a technical user exist on the asset.

Configuring remediation times for the vulnerabilities on assigned assets

In IBM QRadar Vulnerability Manager you can configure the remediation times for different types of vulnerabilities.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Vulnerability Assignment**.
3. Select an assignment from the **Asset Owners** list.
4. On the toolbar, click **Remediation Times**.
5. Update the remediation times for vulnerabilities that are based on their risk and severity.
6. Click **Save**.

Chapter 13. Vulnerability reports

In IBM QRadar Vulnerability Manager, you can generate or edit an existing report, or use the report wizard to create, schedule, and distribute a new report.

QRadar Vulnerability Manager contains several default reports.

The report wizard provides a step-by-step guide on how to design, schedule, and generate reports.

For more information, see the *IBM QRadar User Guide*.

Emailing technical users with their assigned vulnerabilities that require remediation

When you assign vulnerabilities to a technical user for remediation, you can generate a report that emails the technical user.

The email contains information about the vulnerabilities that the technical user must remediate.

Generating PCI compliance reports

You can generate a compliance report for your PCI (payment card industry) assets.

The compliance report demonstrates that you took all the security precautions necessary to protect your critical assets.

Running a default QRadar Vulnerability Manager report

In IBM QRadar Vulnerability Manager, you can run a default vulnerability management report.

Procedure

1. Click the **Reports** tab.
2. From the list of reports, click the report that you want to run.

   For example, you might want to show a report of your vulnerability overview for the last seven days.
3. On the toolbar, select **Actions** > **Run Report**, then click **OK**.
4. To view the completed report in a PDF format, click the icon in the **Formats** column.

Emailing assigned vulnerability reports to technical users

In IBM QRadar Vulnerability Manager, you can send an assigned vulnerabilities report to the technical contact for each asset.

An emailed report reminds your administrators that vulnerabilities are assigned to them and require remediation. Reports can be scheduled monthly, weekly, daily, or hourly.

Before you begin

You must complete the following tasks:

1. Assign a technical user as the owner of asset groups. For more information, see “Assigning a technical user as the owner of asset groups” on page 97
2. Scan the assets that you assigned the technical owner to.
3. Create and save a vulnerability search that uses the **Technical Owner Contact** parameter as an input. For more information, see “Searching vulnerability data” on page 85

© Copyright IBM Corp. 2012, 2020

Procedure

1. Click the **Reports** tab.
2. On the toolbar, select **Actions** > **Create**.
3. Click **Weekly** and then click **Next**.
4. Click the undivided report layout that is displayed on the upper left section of the report wizard and click **Next**.
5. Type a **Report Title**.
6. In the **Chart Type** list, select **Asset Vulnerabilities** and type a **Chart Title**.
7. If a technical contact owner is responsible for more than five assets and you want to email all asset information, increase the value in the **Limit Assets To Top** list.

   Remember: By using the **Assets** tab, you must ensure that the same technical contact owner is assigned to each asset that they are responsible for.
8. In the **Graph Type** field, select **AggregateTable**.

   If you select any value other than **AggregateTable**, the report does not generate a vulnerability sub-report.
9. In the **Graph Content** pane, click **Search to Use** and select your saved technical contact vulnerability search then click **Save Container Details**.
10. Click **Next** and select your report output type.
11. In the report distribution section of the report wizard, click **Multiple Reports**.
12. Click **All Asset Owners**.
13. Click **Load asset owners** to display all list of the technical users contact details.

    You can remove any technical users that you do not want to email with a list of assigned vulnerabilities.
14. On the Reports list, select the report that you created and on the toolbar, select **Actions** > **Run Report**.

Related tasks

Assigning a technical user as the owner of asset groups

Searching vulnerability data

Generating PCI compliance reports

In IBM QRadar Vulnerability Manager, you can generate a compliance report for your PCI (payment card industry) assets. For example, generate a report for assets that store credit card or other sensitive financial information.

The compliance report demonstrates that you took all the security precautions necessary to protect your assets.

Procedure

1. Run a PCI scan for the assets in your network that store or process PCI information.

   For more information, see “Creating a scan profile” on page 37.
2. Update your asset compliance plans and software declarations.

   Your compliance plan and software declarations are displayed in the special notes section of the executive summary.

   For more information, see the PCI security standards for approved software vendors.
3. Create and run a PCI compliance report for the assets that you scanned.

Related tasks

Creating a scan profile

Updating your asset compliance plans and software declarations

In IBM QRadar Vulnerability Manager, if you want to generate a PCI compliance report for your assets, you must complete your attestations for each asset.

Your attestation of compliance is displayed on your PCI compliance report.

Procedure

1. Click the **Assets** tab.
2. In the navigation pane, click **Asset Profiles**.
3. On the **Assets** page, select the asset that you want to provide an attestation for.
4. On the toolbar, click **Edit Asset**.
5. In the **Edit Asset Profile** window, click the **CVSS, Weight & Compliance** pane.
6. Complete the following fields. Use the hover help if you need assistance:
   - Compliance Plan
   - Compliance Notes
   - Compliance Notes Declaration
   - Compliance Notes Description
   - Compliance Out Of Scope Reason
7. Click **Save**.

Creating a PCI compliance report

In IBM QRadar Vulnerability Manager, you can create and run a PCI compliance report.

The PCI compliance report demonstrates that your assets involved in PCI activities comply with security precautions that prevent outside attack.

Before you begin

Ensure that you ran a PCI compliance scan.

Procedure

1. Click the **Reports** tab.
2. On the toolbar, select **Actions** > **Create**.
3. Click **Weekly** and then click **Next**.
4. Click the undivided report layout that is displayed on the upper left section of the report wizard and click **Next**.
5. Type a **Report Title**.
6. In the **Chart Type** list, select **Vulnerability Compliance** and type a **Chart Title**.
7. In the **Scan Profile** list, select the scan profile for the assets that you scanned.

   Attention: If no scan profile is displayed, you must create and run a PCI scan of the assets in your network that store or process PCI information.
8. In the **Scan Result** list, select the version of the scan profile that you want to use.

   Remember: To provide evidence of your compliance, you must select the **Latest** option in the **Scan Result** list. You can also generate a compliance report by using a scan profile that was run at an earlier date.
9. In the **Report Type** list, select a report type.

   If you select **Executive Summary**, **Vulnerability Details**, or a combination of both, the attestation is automatically attached to your PCI compliance report.

10. Complete the information in the **Scan Customer Information** and **Approved Scanning Vendor Information** panes.

    Important: You must add a name in the **Company** field for both panes, as this information is displayed in the attestation section of the report.
11. Click **Save Container Details** and then click **Next**.
12. Use the Report Wizard to complete your PCI compliance report.

Results

The report is displayed in the reports list and is automatically generated.

Note:

Some table columns in the resultant PDF document are not displayed when you create a PDF report with the following parameters:

- Chart type - Vulnerabilities
- Graph type - Table
- Data to use - Current
- Group by - Instance

The large number of table columns that cannot fit on a standard landscape US letter page causes this error to occur.

To avoid this issue, do not use PDF output for this type of report. View Vulnerabilities Reports that use Group by Instance in a spreadsheet or XML format. To export the report, select **XLS** or **XML** as the report format in the Report Wizard.

Including column headings in asset searches

Limit asset searches with filters that include custom asset profiles, name, vulnerability count, and risk score.

Procedure

1. Click the **Assets** tab.
2. In the navigation pane, click **Asset Profiles**, then on the toolbar click **Search** > **New Search**.
3. In the field containing column names, in the field on the left, click the column headings you want to include in your search, and click the arrow button to move the selected headings to field on the right.
4. Click the up and down buttons to change the priority of the selected column headings.
5. When the field on the right contains all the column heading that you want to search on, click **Search**.

Chapter 14. Scanning new assets that communicate with the Internet

Use IBM QRadar Risk Manager to create offenses when new assets communicate with the Internet, which triggers a QRadar Vulnerability Manager scan of the assets.

To trigger scans of new assets that communicate with the Internet, follow these steps:

1. Create a saved search for new assets.
2. Create an on-demand scan profile with dynamic scanning enabled.
3. Create a QRadar Risk Manager policy monitor question to target the new assets from the asset saved search.
4. Monitor the QRadar Risk Manager policy monitor question.
5. Edit the rule that is created by the offense.

Creating an asset saved search for new assets

Create a saved search to capture the new assets that were added to the database within the number of days that you specify.

Procedure

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Click **Search** > **New Search**.
4. Add your search criteria in the **Search Parameter(s)** pane.
5. Select **Days Since Asset Found**, **Less than or equal to**, and then enter the number of days.

   You can specify other criteria but the most important criteria is **Days Since Asset Found**.
6. Click **Add Filter**.
7. Click **Search**.
8. Click **Save Criteria**.
9. Enter a name for the search, and then click **OK** to save your search.

Creating an on-demand scan profile

To trigger a scan in response to a custom rule event, configure an on-demand scan profile and enable dynamic scanning.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Administrative** > **Scan Profiles**.
3. On the toolbar, click **Add**.
4. Add a **Name** and **IP Addresses** on the **Details** tab.

   You can use any IP address because this IP address is replaced when dynamic scanning is used.
5. Select the **On Demand Scanning Enabled** check box
6. Select the **Dynamic Server Selection** check box.

© Copyright IBM Corp. 2012, 2020

Use dynamic scanning in IBM QRadar Vulnerability Manager to associate individual scanners with an IP address, CIDR ranges, IP address ranges, or a domain that you specify in the scan profile. Dynamic scanning is most useful when you deploy several scanners.

7. Click **Save**.

Related concepts

Dynamic vulnerability scans
In IBM QRadar Vulnerability Manager, you can configure a scan to use certain vulnerability scanners for specific CIDR ranges in your network. For example, your scanners might have access only to certain areas of your network.

Scan profile details

Related tasks

Associating vulnerability scanners with CIDR ranges
In IBM QRadar Vulnerability Manager, to do dynamic scanning, you must associate vulnerability scanners with different segments of your network.

Scanning CIDR ranges with different vulnerability scanners
In IBM QRadar Vulnerability Manager, you can scan areas of your network with different vulnerability scanners.

Creating a policy monitor question to test for Internet communication

Create a QRadar Risk Manager policy monitor question to test for communication between new assets and the Internet. The new assets are defined in an asset saved search.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. From the **Actions** menu, click **New Asset Question**.
4. In the **What do you want to name this question** field, type a name for the question.
5. From the **Evaluate On** list, select **Actual Communication**.
6. From the **Importance Factor** list, select the level of importance you want to associate with this question.
7. Specify the time range for the question.
8. From the **Which tests do you want to include in your question** field, select the add (**+**) icon beside the following tests:
   - **have accepted communication to the internet**
   - **and include only the following asset saved searches**
9. Configure the parameters for your tests in the **Find Assets that** field.
   a) Change the test to **have accepted communication from the internet** by clicking **to**.
   b) Click **asset saved searches** and then select your saved search.
10. To assign membership to this question, in the groups area, select the relevant check boxes.
11. Click **Save Question**.

Monitoring communication between new assets and the Internet

Configure the policy monitor question to generate an offense when an asset from the asset saved search communicates with the Internet.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. Select the question that you want to monitor.
4. Click **Monitor**.
5. Select an interval from the **Policy evalutation interval**.
6. Enter a name in the **Event Name** field.

   If you select **Ensure the dispatched event is part of an offense**, the *Event Name* appears in the **Description** field for an offense when you select **All Offenses** on the **Offenses** tab.

   The name of the rule that is generated from an offense is **Risk Question Monitor:** <*Event Name*>. This format for the offense name appears on the **Offenses** tab when an offense is generated.
7. Enter an event name description.
8. In the **Event Details** section, select **Ensure the dispatched event is part of an offense** check box, and **(Correlate By: Asset)** from the menu.
9. In the **Additional Actions** section:
   - **Email**

     This option is helpful when you want to get a notification for the first event that is dispatched as an offense. You can edit the rule that is generated from that offense to trigger a scan. If you don't want to be notified about every event, after you configure the rule that is generated by the offense, you can turn off this notification.
   - **Send to SysLog**

     If you want the event to be logged, select this option.
   - **Notify**

     If you want the event to appear in the **System Notifications** alert on the dashboard, select this option.
10. Select **Enable the monitor results function for this question/simulation**.
11. Click **Save Monitor**.
12. Click **Submit Question**.

Configuring an offense rule to trigger a scan

To trigger a scan of any assets that are communicating with the Internet, configure the rule that is generated by the offense.

Before you begin

An offense must be generated. You can generate the offense manually or wait for an asset to communicate with the Internet. To generate the offense, you can do any of the following steps:

- Generate an offense manually by temporarily connecting any new asset from the asset saved search to the Internet.
- Search the rules on the **Offenses** tab and search for the rule after an offense is generated.
- Enable email notification for the dispatched event that creates an offense. You can edit the rule when you get this notification.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **Rules**.
3. Use the search box on the toolbar to search for the rule.

   The name of the rule is **Risk Question Monitor :** <*Event Name*>.

   You can search by the *Event Name*, which is from the **Monitor Question Results** window.

   The *Event Name* for an offense appears in the **Description** field when you select **All Offenses**.
4. Double-click the rule name to open the **Rule Wizard**.
5. Click **Next**.
6. Configure the following settings:
   a) Select the **Ensure the detected event is part of an offense** check box.
   b) Select **Destination IP** from the **Index offense based on** menu.
   c) Select the **Send to Local SysLog** check box.
   d) Select the **Trigger Scan** check box.
   e) Select the scan profile that you want to use from the **Scan Profile to be used as a template** menu.

      You must select the **On Demand Scanning** option in the scan profile that you want to use with this rule.
   f) Click the **Destination** radio button for the **Local IPs to Scan** field.
   g) Enter values for the **Response Limiter** setting.

      Configure appropriate intervals to avoid a potential overload on your system.
   h) If you don't want to activate this rule right away, clear the **Enable Rule** option and then click **Finish**.

Chapter 15. Security software integrations

IBM QRadar Vulnerability Manager integrates with other security products to help you manage and prioritize your security risks. Integrations with other software extends the capabilities of QRadar Vulnerability Manager.

Integration with QRadar Vulnerability Manager

IBM QRadar Vulnerability Manager integrates with IBM QRadar Risk Manager to help you prioritize the risks and vulnerabilities in your network.

You install QRadar Risk Manager as a separate appliance and then you add it to your QRadar SIEM console as a managed host by using the **System and License Management** tool on the **Admin** tab.

For more information about installing QRadar Risk Manager, see the *IBM QRadar Risk Manager Installation Guide*.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Risk policies and vulnerability prioritization

You can integrate QRadar Vulnerability Manager with QRadar Risk Manager by defining and monitoring asset or vulnerability risk policies.

When the risk policies that you define in QRadar Risk Manager either pass or fail, vulnerability risk scores in QRadar Vulnerability Manager are adjusted. The adjustment levels depend on the risk policies in your organization.

When the vulnerability risk scores are adjusted in QRadar Vulnerability Manager, administrators can do the following tasks:

- Gain immediate visibility of the vulnerabilities that failed a risk policy.

  For example, new information might be displayed on the QRadar dashboard or sent by email.
- Re-prioritize the vulnerabilities that require immediate attention.

  For example, an administrator can use the **Risk Score** to quickly identify high-risk vulnerabilities.

If you apply risk policies at an asset level in QRadar Risk Manager, then all the vulnerabilities on that asset have their risk scores adjusted.

For more information about creating and monitoring risk policies, see the *IBM QRadar Risk Manager User Guide*.

© Copyright IBM Corp. 2012, 2020

Chapter 16. HCL BigFix integration

IBM QRadar Vulnerability Manager integrates with HCL BigFix to help you filter and prioritize the vulnerabilities that can be fixed.

Why use BigFix capabilities with vulnerability management?

Previously known as IBM Security Endpoint Manager, BigFix provides shared visibility and control between IT operations and security. BigFix applies Fixlets to high priority vulnerabilities that are identified and sent by QRadar Vulnerability Manager to BigFix. Fixlets are packages that you deploy to your assets or endpoints to remediate specific vulnerabilities. You can simultaneously deploy Fixlets to many assets or endpoints from the **Manage Vulnerable Computers** dashboard on the BigFix console.

Use the **Manage Vulnerable Computers** on the BigFix console to manage and control a network of hundreds of thousands of assets or endpoints across a range of platforms and devices that are in any geographical location.

How to remediate vulnerabilities with BigFix?

BigFix provides a dashboard that is integrated with QRadar Vulnerability Manager. Use this dashboard on the BigFix console to view and remediate vulnerabilities that are detected and sent by QRadar Vulnerability Manager.

To see QRadar Vulnerability Manager vulnerability data in the BigFix console, configure QRadar Vulnerability Manager, and then configure BigFix to process the vulnerability data that is sent from QRadar Vulnerability Manager. For information about configuring BigFix, see the *IBM BigFix QRadar User Guide*.

How do QRadar Vulnerability Manager and BigFix work together?

QRadar Vulnerability Manager scans your assets or endpoints for vulnerabilities and assigns a risk score, which represents the risk level that a vulnerability poses to your organization. QRadar Vulnerability Manager uses the risk score parameter in the BigFix adapter to filter the high-risk vulnerabilities to send to BigFix for remediation. QRadar Vulnerability Manager assigns a CVE ID to each vulnerability that it sends to BigFix.

Learn more about how vulnerability data is identified and handled:

The following list describes how vulnerability data that is identified by CVEs (Common Vulnerabilities and Exposures) is handled by QRadar Vulnerability Manager and BigFix

- QRadar Vulnerability Manager sends only vulnerabilities that have CVE IDs to BigFix.
- QRadar Vulnerability Manager sends all CVE IDs that are associated with a single vulnerability to BigFix. Some vulnerabilities can have many CVE IDs.
- QRadar Vulnerability Manager sends only the CVE with the highest risk score to BigFix when that CVE shows two or more vulnerabilities.

  For example, the following CVE ID, 2016-0015 shows two different vulnerabilities. Only the CVE with the high-risk vulnerability is sent to BigFix.

```
{
Name: CVE-2016-0015
- MS16-007 - Microsoft - DirectShow - Code Execution Issue
Vulnerability ID: 169296
CVE: 2016-0015
Risk: High

Name: Microsoft Windows DirectShow code execution
Vulnerability ID: 169243
CVE: 2016-0015
```

© Copyright IBM Corp. 2012, 2020

```
Risk: Medium
}
```

BigFix receives the vulnerability data with risk scores and CVE IDs from QRadar Vulnerability Manager, which is visible on the BigFix **Manage Vulnerable Computers** dashboard. Use the **Manage Vulnerable Computers** dashboard on the BigFix console to view and manage the vulnerabilities that are sent by QRadar Vulnerability Manager. BigFix remediates the high-risk vulnerabilities that it has a Fixlet® for by applying a Fixlet directly to the asset or endpoint. QRadar Vulnerability Manager gets a vulnerability fix status update from BigFix Web Reports by using the SOAP API.

How to extend BigFix to QRadar Risk Manager?

If you have a QRadar Risk Manager installation, you can use risk policies in QRadar Risk Manager to further refine your asset risk scores. When the risk policies that you define in QRadar Risk Manager either pass or fail, vulnerability risk scores in QRadar Vulnerability Manager are adjusted. You can reprioritize the vulnerabilities that require immediate attention. If you apply risk policies to assets in QRadar Risk Manager, then the risk scores for all the vulnerabilities on that asset are adjusted. For more information, see the QRadar Risk Manager user guide.

Vulnerability remediation

Depending on whether you installed and integrated BigFix, QRadar Vulnerability Manager provides the following information about your vulnerabilities.

If BigFix is not installed

QRadar Vulnerability Manager provides daily updates about vulnerabilities for which a fix is available.

QRadar Vulnerability Manager maintains a list of vulnerability fix information. Fix information is correlated against the known vulnerability catalog.

Use search in QRadar Vulnerability Manager to identify vulnerabilities that have an available fix.

If BigFix is installed

QRadar Vulnerability Manager also provides specific details about the vulnerability fix process. For example, a fix might be scheduled, or an asset might be already fixed.

The BigFix server gathers fix information from each of the BigFix agents. QRadar Vulnerability Manager gets updates on vulnerability fix information from the BigFix server at preconfigured time intervals.

Use search in QRadar Vulnerability Manager to identify vulnerabilities that are scheduled to be fixed or are already fixed.

Integration components

A typical integrated deployment consists of the following components:

- IBM QRadar Console.
- QRadar Vulnerability Manager.
- BigFix server.
- BigFix agent on each scan target in your network.

Related tasks

Identifying the patch status of your vulnerabilities

Related information

Interactions between IBM QRadar and HCL BigFix

Before, you configure the integration between IBM QRadar and BigFix it's important to understand how they interact with each other.

The following diagram shows a high-level overview of some interactions between QRadar and BigFix from the initial scan of assets, to remediation of vulnerabilities on the scanned assets.

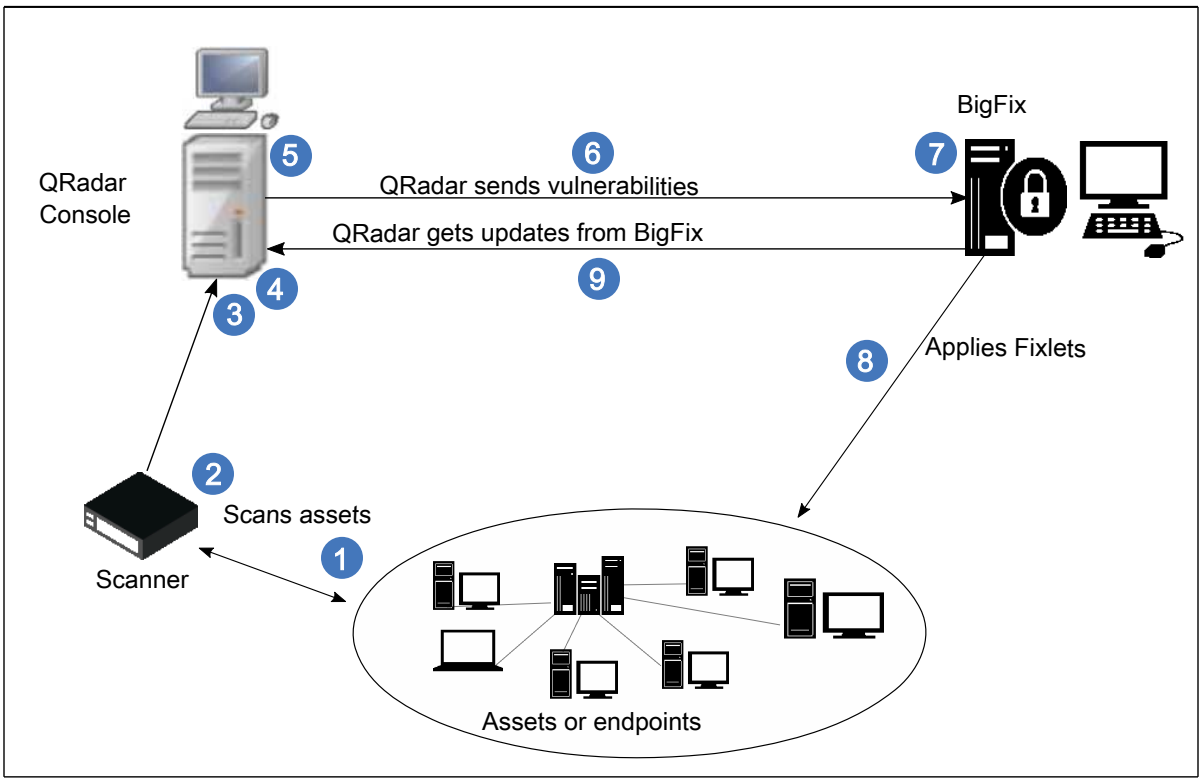

Figure 1. QRadar Vulnerability Manager and BigFix interactions

The following list describes a broad outline of interactions between QRadar and BigFix from the initial scan for vulnerabilities to the remediation of those vulnerabilities:

1. QRadar Vulnerability Manager scanner completes an authenticated scan of assets to discover vulnerabilities. Only the vulnerabilities from assets that are configured in scan profiles that use Full, Patch, or PCI scan policies are eligible for processing by BigFix.
2. If a BigFix agent is installed on an asset QRadar Vulnerability Manager retrieves the *BES agent ID* from the asset when it detects vulnerabilities on the asset. The *BES agent ID* is the unique identifier that is used by BigFix to identify the asset and to remediate vulnerabilities on that asset. BigFix refers to QRadar assets as computers.
3. The scan results are updated in the QRadar asset model, which includes the *BES agent ID* from any assets that have a BigFix agent. When the scan status in the scan profile displays a status of `progress=100%`, then the asset model is updated, and vulnerability data is sent to BigFix within 15 minutes by default.
4. When the asset model is updated with the scan data, the BigFix adapter that is installed on the QRadar Console receives the updated vulnerability data with risk scores from the asset model. The data contains the *BES agent ID*. The BigFix adapter processes only vulnerability information from assets when a *BES agent ID* is included.
5. The vulnerability data that is sent to BigFix is filtered on the risk-score parameters that are configured in the adapter properties file (`/opt/qvm/adaptor/config/adaptor.properties`) on the QRadar Console. The default risk score is 0.0, which means that all vulnerabilities are sent to BigFix.

6. The BigFix adapter uses the BigFix REST API to send the vulnerability information to BigFix and it correlates vulnerability CVEs with Fixlets. By default, data is sent to BigFix in 15-minute intervals.
7. The vulnerability information that is sent by the REST API is viewable on the BigFix **Manage Vulnerable Computers** dashboard. You can deploy Fixlets to the assets with high-risk vulnerabilities from the BigFix **Manage Vulnerable Computers** dashboard. BigFix uses the *BES agent ID* as the unique reference for the asset when it applies Fixlets directly to the asset.
8. BigFix applies Fixlets to the assets that have vulnerabilities.
9. The SOAP API (Web Reports) is used to get vulnerability patch status from BigFix. Use saved searches, and filters from the **Vulnerabilities** tab to view this updated vulnerability information.

   You must rescan the patched assets to update the asset model with the revised vulnerability status of your assets.

Configuring encrypted communication between HCL BigFix and QRadar

For IBM QRadar Vulnerability Manager to receive vulnerability fix status updates by using Web Reports from HCL BigFix configure Transport Layer Security (TLS).

When QRadar Vulnerability Manager receives Fixlet status updates from BigFix, it uses the SOAP API forBigFix Web Reports to request updates by using queries that use the BigFix Relevance language. The queries are used to extract data from the in-memory BigFix Web Reports database. QRadar parses and saves the data. You can use saved searches to view the BigFix updates in QRadar. BigFix doesn't use Web Reports TLS by default. You configure TLS communication and BigFix Web Reports.

Before you begin

The following components must be installed on your network:

- A BigFix server.
- A BigFix Console.
- A BigFix agent on each asset in your network that you scan.
- An IBM QRadar Console.
- A licensed installation of QRadar Vulnerability Manager.

You must have QRadar V7.2.6 or later with the most recent updates.

Note: To prepare for this integration, it is good practice to run **Auto Update** from the **Admin** tab to get the most recent scan tools.

Procedure

1. To configure TLS, complete the following steps:
   a) Download the public key certificate from BigFix to your QRadar Console by typing the following command at the shell prompt of your QRadar Console.

   ```
   openssl x509 -in <(openssl s_client -connect <bigfix ip address>:<port>
   -prexit 2>/dev/null) > /opt/qvm/iem/iem_cert.pem
   ```

   Typically, BigFix listens on port 52312.

   b) To create a truststore in QRadar, type
   the following command:

   ```
   keytool -keystore /opt/qvm/iem/truststore.jks -genkey -alias
   iem_webreports
   ```

   c) Import the BigFix public key certificate to your QRadar truststore by typing the following command:

```
keytool -importcert -file /opt/qvm/iem/iem_cert.pem
-keystore /opt/qvm/iem/truststore.jks -storepass
<your_truststore_password> -alias BigFix_webreports
```

d) At the **Trust this certificate?** prompt, type **Yes**.

2. To configure TLS and BigFix Web Reports for QRadar Vulnerability Manager, complete the following steps:

a) Use SSH to log in to the QRadar console as the root user.

b) Type `./iem-setup-webreports.pl` and when prompted, type the host name, host port, user name, and password for the BigFix server.

You can run this command from any directory. The files are created in the `/opt/qvm/iem` directory.

c) At the **Use SSL/TLS encryption?** prompt, type the appropriate response.

d) Follow the prompts.

e) To view the contents of the `webreports.properties` file, type the following command at the shell prompt:

```
more /opt/qvm/iem/webreports.properties
```

The `webreports.properties` file contains the allowed SSL/TLS transport protocols, for example `webreports.tls.protocols=TLSv1.2` or a comma-separated list `webreports.tls.protocols=TLSv1.2,TLSv1.1`

Verify that the following line contains a port number that follows the IP address:

```
webreports.endpoint=http://<IP_address>:<port>/webreports
```

If you want to use a different port, edit the `/opt/qvm/iem/webreports.properties` file and change the port number.

Configuring QRadar Vulnerability Manager to send vulnerability data to BigFix

Install and configure the BigFix adapter on the QRadar Console to enable IBM QRadar Vulnerability Manager to send vulnerability data with risk scores to HCL BigFix.

Procedure

1. Log in to the QRadar Console as the root user.
2. Configure the BigFix adapter setup:

a) Go to the `/opt/qvm/adaptor/config` directory and run the setup script: `./setup-adaptor.sh`

b) Enter a new password to create the truststore that stores theBigFix server certificate.

The truststore is created in `/opt/qvm/adaptor/truststore.jks`

The following property files are created in the `/opt/qvm/adaptor/config` directory.

- `adaptor.properties`
- `adaptor-bigfix.properties`
- `plugin-bigfix.properties`

c) Verify that the `plugin-bigfix.properties` file has a TLS entry, for example, `TLSv1.2` or a comma separated TLS list `TLSv1.2,TLSv1.1,SSLv1.3`

The first entry in the list is used to create the security context: `bes.rest.allowed.protocols=TLSv1.2`

d) At the prompts, provide details for the BigFix REST API server by entering the host name or IP address, user name, and password for the BigFix server.

The user name and password that you enter are the same as the credentials that are used for the BigFix REST API. The REST API is used to send vulnerability data to BigFix.

e) Restart the asset profiler by typing the following command:

```
/opt/qradar/init/assetprofiler restart
```

To ensure optimum performance, don't restart the asset profiler when QRadar Vulnerability Manager scans are running, or when you are expecting vulnerability imports from a third-party scanner.

The `adaptor.properties` is created. This file contains the configuration parameters for the vulnerability data that is sent to BigFix.

3. Verify that the setup process completed successfully:

a) In the `/opt/qvm/adaptor/config/adaptor.properties` file, verify that these properties are set:

```
qvm.adaptor.listener.enabled=true
```

```
qvm.adaptor.process.daemon=false
```

b) Set the risk score and asset update granularity in the `adaptor.properties` file by editing the following properties:

Table 14. Adaptor properties and descriptions

Property name (API)	Description
qvm.adaptor.minimum.vuln.riskscore=n	Defines the threshold for each vulnerability risk score. Those vulnerabilities equal to or above the set value are sent to BigFix. For example, if you set the value to 5, vulnerabilities with risk scores equal to or above 5 only are sent to BigFix.
qvm.adaptor.minimum.asset.riskscore=n	The cumulative risk score of all the vulnerabilities that are on that asset. Vulnerabilities on assets that have a score less than this value are not sent to BigFix, unless the asset has vulnerabilities equal to, or above the set value for **minimum.vuln.riskscore**. **Note:** The **minimum.vuln.riskscore** overrides the **minimum.asset.riskscore**. If the **minimum.vuln.riskscore** is set to 0, then all vulnerabilities are sent to BigFix, regardless of the **minimum.asset.riskscore** value. Use the **minimum.asset.riskscore** parameter to capture vulnerabilities on assets with multiple low-risk vulnerabilities that result in a high cumulative risk score for an asset. When you set this value, you must be aware of the impact of the **minimum.vuln.riskscore** value on this setting.

Table 14. Adaptor properties and descriptions (continued)	
Property name (API)	**Description**
qvm.adaptor.assetupdate.limit=n	Defines how the BigFix dashboard data resource is split. A split does not occur until all CVE IDs are populated for the last asset. • For example, **qvm.adaptor.assetupdate.limit=20**, asset 1 has 19 CVE IDs, and asset 2 has 30 CVE IDs. One data resource is generated and contains both assets, with a total of 49 CVE IDs. • For example, **qvm.adaptor.assetupdate.limit=19**, asset 1 has 19 CVE IDs, and asset 2 has 30 CVE IDs. Two data resources are generated, each containing an asset.
qvm.adaptor.source.data.delay=n	Defines how often data is sent to BigFix. For example, when n=15, then vulnerability data is sent to BigFix every 15 minutes, if there is vulnerability data available to send to BigFix.

By editing the `adaptor.properties` file, the vulnerability data that you're sending to BigFix is filtered.

c) Verify that the BigFix plugin configuration creates the following directories:

- `/store/qvm/adaptor/data`
- `/store/qvm/adaptor/bigfix`

d) Verify that logging is enabled in the `/opt/qvm/adaptor/log4j.xml` file.

Log files are in the: `/var/log/qvm-integration-adaptor.log` and the `/var/log/qvm-adaptor-cron.log` files.

Note: If you don't download the certificate because the BigFix server is unreachable, the setup does not fail. You can download the certificate later by running the following command:

```
./install-cert.sh <truststore_location>
<truststore_password><truststore_IP_address: port>
```

For example, use the following command format:

```
./install-cert.sh /opt/qvm/adaptor/truststore.jks <abc3password>
<192.0.2.0>:<63455>
```

Troubleshooting the BigFix and QRadar Vulnerability Manager integration

Troubleshoot issues that might occur when you configure your BigFix and QRadar Vulnerability Manager integration.

Troubleshooting contents

- “Is the BigFix scan feature installed?” on page 119
- “Password reset” on page 119
- Password exception error
- “Vulnerability scan data is not sent to BigFix” on page 119
- “Is the asset model updated?” on page 120

BigFix certificate is not imported because of a failed connection to the HCL BigFix server

If the certificate is not imported to QRadar because of a failed connection to the BigFix server, you might see the following error message:

```
ERROR [TrustStoreConfig] Failed to configure trust store with peer certificates :
```

```
Connection timed out java.net.ConnectException: Connection timed out.
```

The configuration is successful, but the certificates are not present in the truststore.

You must manually load the certificates by doing the following steps when you have access to the BigFix server.

1. Go to the `/store/qvm/adaptor` directory.
2. Run the setup script: `./install-cert.sh` *<truststore_location> <truststore_password><truststore_IP_address:port>* The port is the port of service that the certificate belongs to.

Verify connectivity with HCL BigFix

To verify connectivity with HCL BigFix do these steps:

1. Type the following URL in a web browser:

   `https://`*IP_address or DNS_hostname for BigFix:8080*`/webreports?page=QNA`
2. Enter the following string on a single line at the command prompt:

   ```
   (id of site of it,id of it,name of it,cve id list of it) of fixlets whose
   (cve id list of it as lowercase contains "cve") of bes sites
   ```
3. Click **Evaluate**

The following string is an example of the output for one result:

```
2, 104301, MS01-043: NNTP Service in Windows NT 4.0
Contains Memory Leak, CVE-2001-0543
```

The following table describes the breakdown of this result:

Table 15. Query result

Result	Query parameter	Description
2	(id of site of it)	Fixlet site ID
104301	(id of it)	Fixlet ID
MS01-043: NNTP Service in Windows NT 4.0 Contains Memory Leak	(name of it)	Fixlet name
CVE-2001-0543	(cve id list of it)	CVE ID

Are the most recent scan tools installed?

You must run auto updates to get the most recent scan tools for new installations of QRadar because they are required for this integration to work. Run auto update from the **Admin** tab, by clicking the **Auto Update** icon.

For more information about installing QRadar auto updates, see the *IBM QRadar Administration Guide*.

Is the BigFix scan feature installed?

Run the following command to test whether BigFix scan feature is installed on QRadar:

```
grep -rl 'BIG_FIX_AGENT_ID' /opt/qvm
```

The following results are returned if the BigFix scan feature is installed:

- `/opt/qvm/sys/perl/scanner/FusionVM/smb_patch_scanning.pm`
- `/opt/qvm/bin/ssh/packages/bin/ssh-packages`

If you don't see these files, run auto update from the **Admin** tab, by clicking the **Auto Update** icon.

Password reset

If your BigFix details change, you might need to change your password.

1. Edit the `plugin-bigfix.properties` file that is in the `/opt/qvm/adaptor/config` directory.
2. Replace the following line:

   `_decrypt.bes.rest.password=lUb5qzr7FIVH+J319erc+g==`

   with the following line:

   `_encrypt.bes.rest.password=newpassword`

   where `newpassword` is your new password.
3. Run the following script to encrypt your new password:

   `./password-property-encrypt.sh plugin-bigfix.properties`

Password exception error in the `/var/log/iem-cron.log` file

You might see the following error in the in the `/var/log/iem-cron.log` file.

```
Exception in thread "main" java.lang.NoClassDefFoundError:
com.sun.org.apache.xerces.internal.dom.ElementNSImpl
```

This password exception error happens when the `/opt/qvm/iem/webreports.properties` file uses an invalid password.

To fix this error, at the shell prompt, run `/opt/qvm/iem/iem-setup-webreports.pl` and then enter the correct password.

Vulnerability scan data is not sent to BigFix

Verify that the scanner can authenticate on the asset and access the required information.

1. Click the **Vulnerabilities** tab.
2. In the scan name row, click the number in the **Assets** column.
3. Hover over any warning symbols that appear in the column with the flag icon.
4. Check any credential issues in the scan profile or check asset configuration issues that prevent the scanner from accessing the required information.

Is the asset model updated?

To verify that the asset model is updated with your scan results.

1. Click the **Vulnerabilities** tab.
2. On the navigation menu, click **Scan Results**.

   If you see a red warning triangle, the asset model is not updated with your scan results.

Disabling the BigFix and QRadar Vulnerability Manager integration

Use the following procedure if you want to disable the BigFix and QRadar Vulnerability Manager integration.

Procedure

1. Log in to the QRadar Console as the root user.
2. To disable the QRadar Vulnerability Manager adapter, type the following commands:
   - `systemctl stop qvmadaptor.timer`
   - `systemctl disable qvmadaptor.timer`
   - `systemctl daemon-reload`
3. Type the following command to rename the `/store/qvm/adaptor` directory:
   `mv /store/qvm/adaptor /store/BigFix.old/`
4. Type the following command to restart the asset Profiler:
   `systemctl restart assetprofiler`

   Tip: If you want to enable the BigFix integration again at another time, you can reverse the process above.

Chapter 17. IBM Security SiteProtector integration

QRadar Vulnerability Manager integrates with IBM Security SiteProtector to help direct intrusion prevention system (IPS) policy.

When you configure IBM Security SiteProtector, the vulnerabilities that are detected by QRadar Vulnerability Manager scans are automatically forwarded to SiteProtector.

QRadar Vulnerability Manager forwards vulnerabilities from scan results that are tagged with ISS X-Force IDs to IBM Security SiteProtector. QRadar Vulnerability Manager uses the MSL agent to forward the vulnerabilities.

Connecting to IBM Security SiteProtector

You can forward vulnerability data from IBM QRadar Vulnerability Manager to IBM Security SiteProtector to help direct intrusion prevention system (IPS) policy.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click **System and License Management** > **Deployment Actions** > **Manage Vulnerability Deployment**.
3. Click **Use SiteProtector**.
4. In the **SiteProtector IP Address** field, type the IP address of the IBM Security SiteProtector agent manager server.

   The default port for this connection is 3995.
5. Click **Save** and then click **Close**.
6. On the **Admin** tab toolbar, click **Advanced** > **Deploy Full Configuration**.
7. Click **OK**.

What to do next

Scan your network assets to determine if the vulnerability data is displayed in your IBM Security SiteProtector installation.

© Copyright IBM Corp. 2012, 2020

Chapter 18. Vulnerability research, news, and advisories

You can use IBM QRadar Vulnerability Manager to remain aware of the vulnerability threat level and manage security in your organization.

A vulnerability library contains common vulnerabilities that are gathered from a list of external sources. The most significant external resource is the National Vulnerability Database (NVD). You can research specific vulnerabilities by using a number of criteria for example, vendor, product, and date range. You might be interested in specific vulnerabilities that exist in products or services that you use in your enterprise.

QRadar Vulnerability Manager also provides a list of security-related news articles and advisories, gathered from an external list of resources and vendors. Articles and advisories are a useful source of security information from around the world. Articles also help you to keep up-to-date with current security risks.

Viewing detailed information about published vulnerabilities

In IBM QRadar Vulnerability Manager, you can display detailed vulnerability information.

Using the **Research Vulnerabilities** page, you can investigate CVSS metrics and access information from IBM X-Force® research and development.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Research** > **Vulnerabilities**.
3. If no vulnerabilities are displayed, select an alternative time range from the **Viewing vulnerabilities from** list.
4. To search the vulnerabilities, on the toolbar, select **Search** > **New Search**.
5. Identify the vulnerability that you want to investigate.
6. Click the vulnerability link in the **Vulnerability Name** column.

Remaining aware of global security developments

In IBM QRadar Vulnerability Manager, you can view security news from across the world to help keep you updated about current security developments.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Research** > **News**.
3. If no news articles are displayed, select an alternative time range from the **Viewing news from** list.
4. To search the news articles, on the toolbar, select **Search** > **New Search**.
5. Identify the news article that you want to find out more about.
6. Click the news article link in the **Article Title** column.

Viewing security advisories from vulnerability vendors

In IBM QRadar Vulnerability Manager, you can view the vulnerability advisories that are issued by software vendors. Use advisory information to help you identify the risks in your technology, and understand the implications of the risk.

© Copyright IBM Corp. 2012, 2020

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Research** > **Advisories**.
3. If no advisories are displayed, select an alternative time range from the **Viewing advisories from** list.
4. If you want to search the security advisories, on the toolbar, select **Search** > **New Search**.
5. Click the advisory link in the **Advisory** column.

   Each security advisory might include vulnerability references, solutions, and workarounds.

Searching vulnerabilities, news, and advisories

In IBM QRadar Vulnerability Manager, you can manually search the latest vulnerability news and advisories that are issued by software vendors. You can also filter vulnerabilities by using the quick search capability.

About this task

For more information about quick searches, see "Vulnerability quick searches" on page 85.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click one of the following options:
   - **Research** > **Vulnerabilities**.
   - **Research** > **News**.
   - **Research** > **Advisories**.
3. On the toolbar, select **Search** > **New Search**.
4. Type a search phrase in the **Phrase** field.
5. If you are searching news items, select a news source from the **Source** list.
6. In the **By Date Range** area, specify the date period for the news or advisory that you are interested in.
7. If you are searching a published vulnerability, specify a vendor, product, and product version in the **By Product** area.
8. If you are searching a published vulnerability, specify a CVE, Vulnerability, or OSVDB ID in the **By ID** area.

Chapter 19. IBM QRadar Vulnerability Manager Engine for OpenVAS Network Vulnerability Tests

The IBM QRadar Vulnerability Manager (QVM) Engine for OpenVAS Network Vulnerability Tests (NVT) implements the Full Scan Plus policy, which adds a deeper dimension to uncredentialed scanning.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

About the QVM Engine for OpenVAS NVTs

The open source project OpenVAS provides about 50,000 individual Network Vulnerability Tests (NVTs) through their Community Feed. These NVTs are individual tests that can assess a vulnerability. The QVM Engine for OpenVAS NVTs provides the ability to run these tests as part of a QVM Scan.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Features

The QVM Engine for OpenVAS NVTs installs a new scan policy called Full Scan Plus, separate from your existing scan policies. Because it contains more vulnerability tests, extra time is required to run the scans. Previously configured scans use the Opencast Nets in addition to the capabilities of QRadar Vulnerability Manager.

The Full Scan Plus policy includes thousands of additional vulnerability tests provided by the OpenVAS project.

NVTs are updated nightly through existing automatic updates. No extra configuration is required.

Requirements

The QVM Engine for OpenVAS NVTs requires QRadar 7.3.1, Patch 3 or later with a QRadar Vulnerability Manager license.

Installation requires Console access and automatic updates. See “Adding the Full Scan Plus scan policy to IBM QRadar Vulnerability Manager” on page 126.

Frequently asked questions

Does the QVM Engine for OpenVAS NVTs allow importing vulnerabilities into QRadar Vulnerability Manager from a stand-alone OpenVAS deployment?

No. This plugin enables QVM to run OpenVAS Network Vulnerability Tests as part of QVM scans, but it is not designed to provide integration with a separately provided instance of OpenVAS.

Does the Full Scan Plus policy run only OpenVAS NVTs?

No. The Full Scan Plus Policy uses a combination of QVM scanning tests with the NVTs for maximum coverage.

© Copyright IBM Corp. 2012, 2020

About the Full Scan Plus policy

Full Scan Plus executes the OpenVAS NVTs, as well as the tools of the existing Full Scan policy. As a result, vulnerability detection is enhanced where unauthenticated scans are required and time permits to run those additional tests.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Note: You must install the Full Scan Plus policy RPM to use this scan policy.

The Full Scan Plus policy uses a daily updated feed of about 50,000 individual Network Vulnerability Tests (NVT) provided by the OpenVAS open source project.

By default, the policy discovers network assets by using a FAST scan port range. An authenticated scan is run when credentials are provided.

A full scan has the following phases:

Scan type	Description
Discovery scan.	Discovers network assets, and then scans ports to identify key asset characteristics, such as operating system, device type, and services. Vulnerabilities are not scanned.
Uncredentialed scan	Checks services that do not require credentials, for example, reading banners and responses for version information, SSL certificate expiry, testing default accounts, and testing responses for vulnerabilities. **Note:** The most powerful feature of the Full Scan Plus scan is its comprehensive uncredentialed scan, which runs more tests that the Full Scan, which are provided by the open source community. This scan is more detailed than the Full Scan but it takes longer and uses more resources. Run this scan during quiet periods in your network, ideally overnight or at weekends.
Credentialed scan	QRadar Vulnerability Manager logs on to the asset and gathers information about the installed application inventory and required configuration, and raises or suppresses vulnerabilities.

Adding the Full Scan Plus scan policy to IBM QRadar Vulnerability Manager

To add the Full Scan Plus scan policy to IBM QRadar Vulnerability Manager, you must download the QVM Engine for OpenVAS NVTs RPM Package Manager (RPM) from IBM® Fix Central and install it on your IBM QRadar Console.

Before you begin

- You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).
- Ensure you have QRadar version 7.3.1, Patch 3 or later installed.
- Ensure the QRadar Vulnerability Manager processor and scanner are enabled.

Procedure

1. Download the RPM from IBM Fix Central (http://www.ibm.com/support/fixcentral/swg/quickorder?parent=IBM%20Security&product=ibm/Other+software/

IBM+Security+QRadar+Vulnerability+Manager&release=All&platform=All&function=fixId&fixids=7.3.x.x-QRADAR-QVM-Engine-for-OpenVAS-NVTs-v1.1-5&includeSupersedes=0&source=fc).

2. Save the RPM in the `/store/rpms` directory on the QRadar Console.
3. Type the following command to install the RPM on the QRadar Console:

   ```
   rpm -ivh /store/rpms/qvm-openvas-x.x-x.noarch.rpm
   ```

   Note: In a High Availability environment, perform this step only on the primary console.
4. Type the following command to enable the Full Scan Plus scan policy:

   ```
   /store/qvm/openvas/openvas_switch.sh enable
   ```

   Note: Complete this step on the QRadar Console only. This step deploys the configuration to the entire system. No actions are required on Managed Hosts.
5. Run automatic updates:

   a) On the navigation menu (☰), click **Admin**.

   b) In the **System Configuration** section, click **Auto Update**.

   c) Click **Get New Updates**.

   d) If new updates appear on the list, click **Install** > **All Updates**.

   Important: You must trigger Auto Update to complete the installation of the Full Scan Plus policy. After you trigger Auto Update, more tools are downloaded and installed. The scan policy will be available in the UI after this installation is complete. You must complete this step, even if Auto Update already ran for the current day.

Running a scan

Follow the steps below to run a scan with the Full Scan Plus policy.

Before you begin

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Procedure

1. Configure the new Full Scan Plus policy as required.

   For instructions on configuring a scan policy, see below.
2. Create a Scan Profile and select **Full Scan Plus**, or the policy you created in Step 1 from the **Scan Policies** menu.

   For instructions on creating a scan policy, see below.

Configuring a scan policy

In IBM QRadar Vulnerability Manager, you can configure a scan policy to meet any specific requirements for your vulnerability scans. You can copy and rename a preconfigured scan policy or you can add a new scan policy. You can't edit a preconfigured scan policy.

Before you begin

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Policies**.
3. On the toolbar, click **Add**.
4. Type the name and description of your scan policy.

   To configure a scan policy, you must at least configure the mandatory fields in the **New Scan Policy** window, which are the **Name** and **Description** fields.
5. From the **Scan Type** list, select the scan type.
6. To manage and optimize the asset-discovery process, click the **Asset Discovery** tab.
7. To manage the ports and protocols that are used for a scan, click the **Port Scan** tab.
8. To include specific vulnerabilities in your patch scan policy, click the **Vulnerabilities** tab.

   Note: The **Vulnerabilities** tab is available only when you select a patch scan.
9. To include or exclude tool groups from your scan policy, click the **Tool Groups** tab.

   Note: The **Tool Groups** tab is available only when you select a zero-credentialed full-scan or full-scan plus policy.
10. To include or exclude tools from a scan policy, click the **Tools** tab.

    Note: The **Tools** tab is available only when you select a zero-credentialed Full Scan or Full Scan Plus policy.

    Important: If you do not modify the tools or tool groups, and you select the **Full** option as your scan type, then all the tools and tool groups that are associated with a full scan are included in your scan policy.
11. Click **Save**.

Creating a scan profile

In IBM QRadar Vulnerability Manager, you configure scan profiles to specify how and when your network assets are scanned for vulnerabilities.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or IBM Customer Support (www.ibm.com/support/).

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Administrative** > **Scan Profiles**.
3. On the toolbar, click **Add**.

   When you create a scan profile, the only mandatory fields are **Name** and **IP Addresses** on the **Details** tab of the **Scan Profile Configuration** page. In addition, you can also configure the following optional settings.

   - If you added more scanners to your QRadar Vulnerability Manager deployment, select a scanner from the **Scan Server** list. This step is unnecessary if you want to use dynamic scanning.
   - To enable this profile for on-demand scanning, click the **On Demand Scanning Enabled** check box.

     By selecting this option, you make the profile available to use if you want to trigger a scan in response to a custom rule event. It also enables on-demand vulnerability scanning by using the right-click menu on the **Assets** page.
   - By selecting the **Dynamic Server Selection** check box, you can choose the most appropriate scanner that is available. Ensure that you define the scanners in the **Administrative** > **Scanners** page.

Security profiles must be updated with an associated domain. Domain-level restrictions are not applied until the security profiles are updated, and the changes are deployed.

- To scan your network by using a predefined set of scanning criteria, select a scan type from the **Scan Policies** list.
- If you configured centralized credentials for assets, click the **Use Centralized Credentials** check box. For more information, see the *IBM QRadar Administration Guide*.

4. Click **Save**.

Related concepts

Network bandwidth for simultaneous asset scans

By adjusting the network bandwidth setting, you change the number of assets that can be scanned concurrently and the number of vulnerability tools that can be used concurrently to scan the assets. Some scans use more vulnerability tools to scan, which impacts the number of assets that can be scanned concurrently.

Dynamic scanning

Use dynamic scanning in IBM QRadar Vulnerability Manager to associate individual scanners with an IP address, CIDR ranges, IP address ranges, or a domain that you specify in the scan profile. Dynamic scanning is most beneficial when you deploy several scanners. For example, if you deploy more than 5 scanners, you might save time by using dynamic scanning.

Options for adding scanners to your QRadar Vulnerability Manager deployment

Scan policies

Dynamic vulnerability scans

In IBM QRadar Vulnerability Manager, you can configure a scan to use certain vulnerability scanners for specific CIDR ranges in your network. For example, your scanners might have access only to certain areas of your network.

Related tasks

Associating vulnerability scanners with CIDR ranges

In IBM QRadar Vulnerability Manager, to do dynamic scanning, you must associate vulnerability scanners with different segments of your network.

Rescanning an asset by using the right-click menu option

Configuring a scan policy

In IBM QRadar Vulnerability Manager, you can configure a scan policy to meet any specific requirements for your vulnerability scans. You can copy and rename a preconfigured scan policy or you can add a new scan policy. You can't edit a preconfigured scan policy.

Notices

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

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

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

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

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

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

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

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

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

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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

© Copyright IBM Corp. 2012, 2020

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

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions..

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

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

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

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

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

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

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

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

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

VMware, the VMware logo, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

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

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

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

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details/ the section entitled “Cookies, Web Beacons and Other Technologies”.

General Data Protection Regulation

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing

advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Learn more about the IBM GDPR readiness journey and our GDPR capabilities and Offerings here: https://ibm.com/gdpr

Glossary

This glossary provides terms and definitions for the IBM QRadar Vulnerability Manager software and products.

The following cross-references are used in this glossary:

- *See* refers you from a non-preferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

advisory
A document that contains information and analysis about a threat or vulnerability.

asset
A manageable object that is either deployed or intended to be deployed in an operational environment.

C

CDP
See collateral damage potential.

CIDR
See Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

client
A software program or computer that requests services from a server.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

common vulnerability scoring system (CVSS)
A scoring system by which the severity of a vulnerability is measured.

console
A web-based interface from which an operator can control and observe the system operation.

CVSS
See common vulnerability scoring system.

D

DNS
See Domain Name System.

DNS zone transfer
A transaction that replicates a Domain Name System (DNS) database.

© Copyright IBM Corp. 2012, 2020

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

E

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

F

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

H

HA
See high availability.

high availability (HA)
Pertaining to a clustered system that is reconfigured when node or daemon failures occur so that workloads can be redistributed to the remaining nodes in the cluster.

I

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network. See also Transmission Control Protocol.

IP
See Internet Protocol.

N

national vulnerability database (NVD)
A United States repository of standards-based vulnerability management data.

NVD
See national vulnerability database.

O

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

operational window
A configured time period within which a scan is permitted to run.

P

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card

payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

R

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

S

scan exclusion list
A list of assets, network groups, and CIDR ranges that are ignored by scans.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB).

SNMP
See Simple Network Management Protocol.

T

TCP
See Transmission Control Protocol.

Transmission Control Protocol (TCP)
A communication protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for internetwork protocol. TCP provides a reliable host-to-host protocol in packet-switched communication networks and in interconnected systems of such networks. See also Internet Protocol.

U

UDP
See User Datagram Protocol.

User Datagram Protocol (UDP)
An Internet protocol that provides unreliable, connectionless datagram service. It enables an application program on one machine or process to send a datagram to an application program on another machine or process.

V

vulnerability
A security exposure in an operating system, system software, or application software component.

Index

M

N

O

P

Q

R

S

T

U

V

W