Red Hat Satellite 6.14

Managing Security Compliance

Plan and configure SCAP compliance policies, deploy the policies to hosts, and monitor compliance of your hosts

Last Updated: 2024-08-08

Red Hat Satellite 6.14 Managing Security Compliance

Plan and configure SCAP compliance policies, deploy the policies to hosts, and monitor compliance of your hosts

Red Hat Satellite Documentation Team
satellite-doc-list@redhat.com

Legal Notice

Abstract

With Satellite, you can create security compliance policies, deploy the policies on hosts, and monitor compliance of hosts using those policies to make the hosts adhere to security standards.

Table of Contents

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION 3

CHAPTER 1. SECURITY COMPLIANCE MANAGEMENT 4

CHAPTER 2. SECURITY CONTENT AUTOMATION PROTOCOL 5

CHAPTER 3. SCAP CONTENT IN SATELLITE 6
3.1. SUPPORTED SCAP VERSIONS 6

CHAPTER 4. COMPLIANCE POLICY DEPLOYMENT OPTIONS 7

CHAPTER 5. CONFIGURING COMPLIANCE POLICY DEPLOYMENT METHODS 8

CHAPTER 6. LISTING AVAILABLE SCAP CONTENTS 9

CHAPTER 7. CONFIGURING SCAP CONTENTS 10
7.1. LOADING THE DEFAULT SCAP CONTENTS 10
7.2. GETTING SUPPORTED SCAP CONTENTS FOR RHEL 10
7.3. UPLOADING ADDITIONAL SCAP CONTENT 11
7.4. TAILORING XCCDF PROFILES 12
7.5. UPLOADING A TAILORING FILE 12

CHAPTER 8. MANAGING COMPLIANCE POLICIES 13
8.1. CREATING A COMPLIANCE POLICY 13
8.2. VIEWING A COMPLIANCE POLICY 14
8.3. EDITING A COMPLIANCE POLICY 14
8.4. DELETING A COMPLIANCE POLICY 14

CHAPTER 9. DEPLOYING COMPLIANCE POLICIES 16
9.1. INCLUSION OF REMOTE SCAP RESOURCES 16
9.2. APPLYING REMOTE SCAP RESOURCES IN A DISCONNECTED ENVIRONMENT 17
9.3. DEPLOYING A POLICY IN A HOST GROUP USING ANSIBLE 18
9.4. DEPLOYING A POLICY ON A HOST USING ANSIBLE 19
9.5. DEPLOYING A POLICY IN A HOST GROUP USING PUPPET 20
9.6. DEPLOYING A POLICY ON A HOST USING PUPPET 21

CHAPTER 10. RUNNING A SECURITY COMPLIANCE SCAN ON DEMAND 23

CHAPTER 11. MONITORING COMPLIANCE 24
11.1. SEARCHING COMPLIANCE REPORTS 24
11.2. COMPLIANCE EMAIL NOTIFICATIONS 25
11.3. VIEWING COMPLIANCE POLICY STATISTICS 25
11.4. EXAMINING HOSTS PER RULE COMPLIANCE RESULT 25
11.5. EXAMINING COMPLIANCE FAILURES OF A HOST 26
11.6. DELETING A COMPLIANCE REPORT 27
11.7. DELETING MULTIPLE COMPLIANCE REPORTS 27

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your feedback on our documentation. Let us know how we can improve it.

Use the **Create Issue** form in Red Hat Jira to provide your feedback. The Jira issue is created in the Red Hat Satellite Jira project, where you can track its progress.

Prerequisites

- Ensure you have registered a Red Hat account.

Procedure

1. Click the following link: **Create Issue**. If Jira displays a login error, log in and proceed after you are redirected to the form.
2. Complete the **Summary** and **Description** fields. In the **Description** field, include the documentation URL, chapter or section number, and a detailed description of the issue. Do not modify any other fields in the form.
3. Click **Create**.

CHAPTER 1. SECURITY COMPLIANCE MANAGEMENT

Security compliance management is the ongoing process of defining security policies, auditing systems for compliance with those policies, and resolving instances of non-compliance. Any non-compliance is managed according to the organization's configuration management policies. Security policies range in scope from host-specific to industry-wide, therefore, flexibility in their definition is required.

With Satellite, you can schedule compliance auditing and reporting on all registered hosts.

CHAPTER 2. SECURITY CONTENT AUTOMATION PROTOCOL

Satellite uses the Security Content Automation Protocol (SCAP) standard to define security policies.

SCAP is a framework of several specifications based on XML, such as checklists described in the Extensible Checklist Configuration Description Format (XCCDF) and vulnerabilities described in the Open Vulnerability and Assessment Language (OVAL). These specifications are encapsulated as *data stream* files.

Checklist items in XCCDF, also known as *rules*, express the desired configuration of a system item. For example, a rule may specify that no one can log in to a host over SSH using the **root** user account. Rules can be grouped into one or more *XCCDF profiles*, which allows multiple profiles to share a rule.

The OpenSCAP scanner tool evaluates system items on a host against the rules and generates a report in the Asset Reporting Format (ARF), which is then returned to Satellite for monitoring and analysis.

Table 2.1. Specifications in the SCAP Framework 1.3 supported by the OpenSCAP scanner

Title	Description	Version
SCAP	Security Content Automation Protocol	1.3
XCCDF	Extensible Configuration Checklist Description Format	1.2
OVAL	Open Vulnerability and Assessment Language	5.11
-	Asset Identification	1.1
ARF	Asset Reporting Format	1.1
CCE	Common Configuration Enumeration	5.0
CPE	Common Platform Enumeration	2.3
CVE	Common Vulnerabilities and Exposures	2.0
CVSS	Common Vulnerability Scoring System	2.0

Additional resources

- For more information about SCAP, see the OpenSCAP project.

CHAPTER 3. SCAP CONTENT IN SATELLITE

SCAP content is a SCAP data-stream file that contains implementation of compliance, configuration, or security baselines. A single data stream usually includes multiple XCCDF profiles. An XCCDF profile defines an industry standard or custom security standard against which you can evaluate compliance of host configuration in Satellite, such as Protection Profile for General Purpose Operating Systems (OSPP), Health Insurance Portability and Accountability Act (HIPAA), and PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 9. You can adapt existing XCCDF profiles according to your requirements using *tailoring files*.

In Satellite, you use an XCCDF profile from SCAP content and, eventually, a tailoring file, to define a *compliance policy*. Satellite includes default SCAP contents from SCAP Security Guide provided by the OpenSCAP project.

For more information on how to download, deploy, modify, and create your own content, see:

- *Red Hat Enterprise Linux 9 Security hardening*
- *Red Hat Enterprise Linux 8 Security hardening*
- *Red Hat Enterprise Linux 7 Security Guide*
- *Red Hat Enterprise Linux 6 Security Guide*

3.1. SUPPORTED SCAP VERSIONS

Satellite supports content of SCAP versions 1.2 and 1.3.

CHAPTER 4. COMPLIANCE POLICY DEPLOYMENT OPTIONS

You can use one of the following methods to deploy compliance policies:

Ansible deployment

You use an Ansible role to configure hosts for compliance scans.

Puppet deployment

You use a Puppet class and the Puppet agent to configure hosts for compliance scans.

Manual deployment

You manually configure hosts for compliance scans.

CHAPTER 5. CONFIGURING COMPLIANCE POLICY DEPLOYMENT METHODS

Use one the following procedures to configure Satellite for the method that you have selected to deploy compliance policies. You will select one of these methods when you later create a compliance policy .

Procedure for Ansible deployment

1. Import the **theforeman.foreman_scap_client** Ansible role.
   For more information, see *Managing Configurations Using Ansible Integration in Red Hat Satellite*.

2. Assign the created policy and the **theforeman.foreman_scap_client** Ansible role to a host or host group.

3. To trigger the deployment, run the Ansible role on the host or host group either manually, or set up a recurring job by using remote execution for regular policy updates.
   For more information, see Configuring and Setting Up Remote Jobs in *Managing Hosts*.

Procedure for Puppet deployment

1. Ensure Puppet is enabled.

2. Ensure the Puppet agent is installed on hosts.

3. Import the Puppet environment that contains the **foreman_scap_client** Puppet module.
   For more information, see *Managing Configurations Using Puppet Integration in Red Hat Satellite*.

4. Assign the created policy and the **foreman_scap_client** Puppet class to a host or host group.
   Puppet triggers the deployment on the next regular run or you can run Puppet manually. Puppet runs every 30 minutes by default.

Procedure for manual deployment

- For the manual deployment method, no additional Satellite configuration is required.
  For information on manual deployment, see How to set up OpenSCAP Policies using Manual Deployment option in the *Red Hat Knowledgebase*.

CHAPTER 6. LISTING AVAILABLE SCAP CONTENTS

Use this procedure to view what SCAP contents are already loaded in Satellite. To use the CLI instead of the Satellite web UI, see the CLI procedure.

Prerequisite

- Your user account has a role assigned that has the **view_scap_contents** permission.

Procedure

- In the Satellite web UI, navigate to **Hosts** > **Compliance – SCAP contents**.

CLI procedure

- Run the following Hammer command on Satellite Server:

```
# hammer scap-content list \
--location "My_Location" \
--organization "My_Organization"
```

CHAPTER 7. CONFIGURING SCAP CONTENTS

You can upload SCAP data streams and tailoring files to define compliance policies.

7.1. LOADING THE DEFAULT SCAP CONTENTS

By loading the default SCAP contents on Satellite Server, you ensure that the data streams from the SCAP Security Guide (SSG) are loaded and assigned to all organizations and locations.

SSG is provided by the operating system of Satellite Server and installed in **/usr/share/xml/scap/ssg/content/**. Note that the available data streams depend on the operating system version on which Satellite runs. You can only use this SCAP content to scan hosts that have the same minor RHEL version as your Satellite Server. For more information, see Section 7.2, "Getting Supported SCAP Contents for RHEL".

Prerequisites

- Your user account has a role assigned that has the **create_scap_contents** permission.

Procedure

- Use the following Hammer command on Satellite Server:

```
# hammer scap-content bulk-upload --type default
```

7.2. GETTING SUPPORTED SCAP CONTENTS FOR RHEL

You can get the latest SCAP Security Guide (SSG) for Red Hat Enterprise Linux on the Red Hat Customer Portal. You have to get a version of SSG that is designated for the minor RHEL version of your hosts.

Procedure

1. Access the SCAP Security Guide in the package browser .
2. From the **Version** menu, select the latest SSG version for the minor version of RHEL that your hosts are running. For example, for RHEL 8.6, select a version named ***.el8_6**.
3. Download the package RPM.
4. Extract the data-stream file (***-ds.xml**) from the RPM. For example:

```
$ rpm2cpio scap-security-guide-0.1.69-3.el8_6.noarch.rpm \
| cpio -iv --to-stdout ./usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml \
> ssg-rhel-8.6-ds.xml
```

5. Upload the data stream to Satellite. For more information, see Section 7.3, "Uploading Additional SCAP Content".

Additional resources

- Supported versions of the SCAP Security Guide in RHEL in the *Red Hat Knowledgebase*

- SCAP Security Guide profiles supported in RHEL 9 in *Red Hat Enterprise Linux 9 Security hardening*
- SCAP Security Guide profiles supported in RHEL 8 in *Red Hat Enterprise Linux 8 Security hardening*
- SCAP Security Guide profiles supported in RHEL 7 in *Red Hat Enterprise Linux 7 Security Guide*

7.3. UPLOADING ADDITIONAL SCAP CONTENT

You can upload additional SCAP content into Satellite Server, either content created by yourself or obtained elsewhere. Note that Red Hat only provides support for SCAP content obtained from Red Hat. To use the CLI instead of the Satellite web UI, see the CLI procedure.

Prerequisite

- Your user account has a role assigned that has the **create_scap_contents** permission.
- You have acquired a SCAP data-stream file.

Procedure

1. In the Satellite web UI, navigate to **Hosts** > **Compliance** > **SCAP contents**.
2. Click **Upload New SCAP Content**.
3. Enter a title in the **Title** text box, such as ***My SCAP Content***.
4. In **Scap File**, click **Choose file**, navigate to the location containing a SCAP data-stream file and click **Open**.
5. On the **Locations** tab, select locations.
6. On the **Organizations** tab, select organizations.
7. Click **Submit**.

If the SCAP content file is loaded successfully, a message similar to **Successfully created *My SCAP Content*** is displayed.

CLI procedure

1. Place the SCAP data-stream file to a directory on your Satellite Server, such as ***/usr/share/xml/scap/my_content/***.
2. Run the following Hammer command on Satellite Server:

```
# hammer scap-content bulk-upload --type directory \
--directory /usr/share/xml/scap/my_content/ \
--location "My_Location" \
--organization "My_Organization"
```

Verification

- List the available SCAP contents. The list of SCAP contents includes the new title.

7.4. TAILORING XCCDF PROFILES

You can customize existing XCCDF profiles using *tailoring files* without editing the original SCAP content. A single tailoring file can contain customizations of multiple XCCDF profiles.

You can create a tailoring file using the SCAP Workbench tool. For more information on using the SCAP Workbench tool, see Customizing SCAP Security Guide for your use case .

Then you can assign a tailoring file to a compliance policy to customize an XCCDF profile in the policy.

7.5. UPLOADING A TAILORING FILE

After uploading a tailoring file, you can apply it in a compliance policy to customize an XCCDF profile.

Prerequisite

- Your user account has a role assigned that has the **create_tailoring_files** permission.

Procedure

1. In the Satellite web UI, navigate to **Hosts** > **Compliance – Tailoring Files** and click **New Tailoring File**.
2. Enter a name in the **Name** text box.
3. Click **Choose File**, navigate to the location containing the tailoring file and select **Open**.
4. Click **Submit** to upload the chosen tailoring file.

CHAPTER 8. MANAGING COMPLIANCE POLICIES

A *compliance policy* is a scheduled audit that checks the specified hosts for compliance against a specific XCCDF profile from a SCAP content.

You specify the schedule for scans on Satellite Server and the scans are performed on hosts. When a scan completes, a report in ARF format is generated and uploaded to Satellite Server. The compliance policy makes no changes to the scanned host.

A compliance policy defines a SCAP client configuration and a cron schedule. The policy is then deployed together with the SCAP client on hosts to which the policy is assigned.

8.1. CREATING A COMPLIANCE POLICY

By creating a compliance policy, you can define and plan your security compliance requirements, and ensure that your hosts remain compliant to your security policies.

Prerequisites

- You have configured Satellite for your selected compliance policy deployment method.
- You have available SCAP contents, and eventually tailoring files, in Satellite.
  - To verify what SCAP contents are available, see Chapter 6, *Listing Available SCAP Contents*.
  - To upload SCAP contents and tailoring files, see Chapter 7, *Configuring SCAP Contents*.
- Your user account has a role assigned that has the **view_policies** and **create_policies** permissions.

Procedure

1. In the Satellite web UI, navigate to **Hosts** > **Compliance – Policies**.
2. Click **New Policy** or **New Compliance Policy**.
3. Select the deployment method: **Ansible**, **Puppet**, or **Manual**. Then click **Next**.
4. Enter a name for this policy, a description (optional), then click **Next**.
5. Select the **SCAP Content** and **XCCDF Profile** to be applied, then click **Next**.
   Note that Satellite does not detect whether the selected XCCDF profile contains any rules. An empty XCCDF profile, such as the **Default XCCDF Profile**, will return empty reports.
6. Optional: To customize the XCCDF profile, select a **Tailoring File** and a **XCCDF Profile in Tailoring File**, then click **Next**.
7. Specify the scheduled time when the policy is to be applied. Select **Weekly**, **Monthly**, or **Custom** from the **Period** list. The **Custom** option allows for greater flexibility in the policy's schedule.
   - If you select **Weekly**, also select the desired day of the week from the **Weekday** list.
   - If you select **Monthly**, also specify the desired day of the month in the **Day of month** field.

- If you select **Custom**, enter a valid Cron expression in the **Cron line** field.

8. Select the locations to which to apply the policy, then click **Next**.
9. Select the organizations to which to apply the policy, then click **Next**.
10. Optional: Select the host groups to which to assign the policy.
11. Click **Submit**.

8.2. VIEWING A COMPLIANCE POLICY

You can preview the rules which will be applied by specific OpenSCAP content and profile combination. This is useful when you plan policies.

Prerequisite

- Your user account has a role assigned that has the **view_policies** permission.

Procedure

1. In the Satellite web UI, navigate to **Hosts** > **Compliance – Policies**.
2. In the **Actions** column of the required policy, click **Show Guide** or select it from the list.

8.3. EDITING A COMPLIANCE POLICY

In the Satellite web UI, you can edit compliance policies.

Puppet agent applies an edited policy to the host on the next run. By default, this occurs every 30 minutes. If you use Ansible, you must run the Ansible role manually again or have configured a recurring remote execution job that runs the Ansible role on hosts.

Prerequisite

- Your user account has a role assigned that has the **view_policies** and **edit_policies** permissions.

Procedure

1. In the Satellite web UI, navigate to **Hosts** > **Compliance – Policies**.
2. Click the name of the required policy.
3. Edit the necessary attributes.
4. Click **Submit**.

8.4. DELETING A COMPLIANCE POLICY

In the Satellite web UI, you can delete existing compliance policies.

Prerequisite

- Your user account has a role assigned that has the **view_policies** and **destroy_policies** permissions.

Procedure

1. In the Satellite web UI, navigate to **Hosts** > **Compliance – Policies**.
2. In the **Actions** column of the required policy, select **Delete** from the list.
3. Click **OK** in the confirmation message.

CHAPTER 9. DEPLOYING COMPLIANCE POLICIES

To deploy a compliance policy, you must install the SCAP client, update the cron schedule file, and upload the SCAP content selected in the policy onto a host.

9.1. INCLUSION OF REMOTE SCAP RESOURCES

SCAP data streams can reference remote resources, such as OVAL files, that the SCAP client fetches over the internet when it runs on hosts. If a data stream requires a remote resource, you can see a warning from the OpenSCAP Scanner tool on your Satellite Server, such as:

```
# oscap info /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml | grep "WARNING"
WARNING: Datastream component 'scap_org.open-scap_cref_security-data-oval-com.redhat.rhsa-RHEL8.xml.bz2'
points out to the remote 'https://access.redhat.com/security/data/oval/com.redhat.rhsa-RHEL8.xml.bz2'.
Use '--fetch-remote-resources' option to download it.
WARNING: Skipping 'https://access.redhat.com/security/data/oval/com.redhat.rhsa-RHEL8.xml.bz2' file
which is referenced from datastream
```

By default, the SCAP client is configured to ignore the remote resources and skip the XCCDF rules that rely on the resources. The skipped rules then result in the **notchecked** status.

For hosts with internet access, you can enable the download of remote resources on hosts in Satellite. For information about applying remote SCAP resources to hosts that cannot access the internet, see Section 9.2, “Applying Remote SCAP Resources in a Disconnected Environment” .

Using the Ansible deployment method

Override the following Ansible variable:

- Name: **foreman_scap_client_fetch_remote_resources**
- Type: **boolean**
- Value: **true**

For more information, see Overriding Ansible Variables in Satellite in *Managing Configurations Using Ansible Integration in Red Hat Satellite*.

Using the Puppet deployment method

Configure the following Puppet Smart Class Parameter:

- Name: **fetch_remote_resources**
- Type: **boolean**
- Value: **true**

For more information, see Configuring Puppet Smart Class Parameters in *Managing Configurations Using Puppet Integration in Red Hat Satellite*.

9.2. APPLYING REMOTE SCAP RESOURCES IN A DISCONNECTED ENVIRONMENT

SCAP data streams can contain remote resources, such as OVAL files, that the SCAP client can fetch over the internet when it runs on hosts. If your hosts do not have internet access, you must download remote SCAP resources and distribute them from Satellite Server to your hosts as local files by downloading the files on hosts from a custom file type repository .

Prerequisites

- You have registered your host to Satellite with remote execution enabled.
- Fetching remote resources must be disabled, which is the default. For more information, see Section 9.1, “Inclusion of Remote SCAP Resources”.

Procedure

1. On your Satellite Server, examine the data stream you use in your compliance policy to find out which missing resource you must download:

```
# oscap info /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml | grep "WARNING"
WARNING: Datastream component 'scap_org.open-scap_cref_security-data-oval-com.redhat.rhsa-RHEL8.xml.bz2'
points out to the remote 'https://access.redhat.com/security/data/oval/com.redhat.rhsa-RHEL8.xml.bz2'.
Use '--fetch-remote-resources' option to download it.
WARNING: Skipping 'https://access.redhat.com/security/data/oval/com.redhat.rhsa-RHEL8.xml.bz2' file
which is referenced from datastream
```

2. Examine the name of the local file that is referenced by the data stream:

```
# oscap info /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
...
  Referenced check files:
   ssg-rhel8-oval.xml
    system: http://oval.mitre.org/XMLSchema/oval-definitions-5
   ssg-rhel8-ocil.xml
    system: http://scap.nist.gov/schema/ocil/2
   security-data-oval-com.redhat.rhsa-RHEL8.xml.bz2
    system: http://oval.mitre.org/XMLSchema/oval-definitions-5
...
```

3. On an online machine, download the missing resource:

```
# curl -o security-data-oval-com.redhat.rhsa-RHEL8.xml.bz2
https://www.redhat.com/security/data/oval/com.redhat.rhsa-RHEL8.xml.bz2
```

IMPORTANT

Ensure that the name of the downloaded file matches the name the data stream references.

4. Add the file as new custom file type content into your Satellite Server. For more information, see Managing Custom File Type Content in *Managing Content*.
   Note the URL on which your repository is published, such as **http://*satellite.example.com*/pulp/content/*My_Organization_Label*/Library/custom/*My_Product_Label*/*My_Repo_Label*/**.

5. Schedule a remote job to upload the file to the home directory of **root** on your host. For example, use the **Run Command - Script Default** job template and enter the following command:

   ```
   # curl -o /root/security-data-oval-com.redhat.rhsa-RHEL8.xml.bz2
   http://satellite.example.com/pulp/content/My_Organization_Label/Library/custom/My_Product_Label/My_Repo_Label/security-data-oval-com.redhat.rhsa-RHEL8.xml.bz2
   ```

   For more information about running remote jobs, see Executing a Remote Job in *Managing Hosts*.

6. Continue with deploying your compliance policy.

9.3. DEPLOYING A POLICY IN A HOST GROUP USING ANSIBLE

After you deploy a compliance policy in a host group using Ansible, the Ansible role installs the SCAP client and configures OpenSCAP scans on the hosts according to the selected compliance policy.

The SCAP content in the compliance policy might require remote resources. For more information, see Section 9.1, “Inclusion of Remote SCAP Resources”.

Prerequisites

- You have enabled OpenSCAP on your Capsule. For more information, see Enabling OpenSCAP on Capsule Servers in *Installing Capsule Server*.
- Repositories for the operating system version of the host are synchronized on Satellite Server and enabled on the host.
  - Red Hat Enterprise Linux 9 BaseOS and Appstream RPMs repositories
  - Red Hat Enterprise Linux 8 BaseOS and Appstream RPMs repositories
  - Red Hat Enterprise Linux 7 Server and Extras RPMs repositories
- Red Hat Satellite Client 6 repository for the operating system version of the host is synchronized on Satellite Server, available in the content view and the lifecycle environment of the host, and enabled for the host. For more information, see Changing the repository sets status for a host in Satellite in *Managing Content*. This repository is required for installing the SCAP client.
- You have created a compliance policy with the Ansible deployment option and assigned the host group.

Procedure

1. In the Satellite web UI, navigate to **Configure** > **Host Groups**.
2. Click the host group that you want to configure for OpenSCAP reporting.

3. From the **OpenSCAP Capsule** list, select the Capsule with OpenSCAP enabled that you want to use.
4. On the **Ansible Roles** tab, assign the **theforeman.foreman_scap_client** Ansible role.
5. Optional: On the **Parameters** tab, configure any Ansible variables of the role.
6. Click **Submit** to save your changes.
7. In the row of the required host group, navigate to the **Actions** column and select **Run all Ansible roles**.

9.4. DEPLOYING A POLICY ON A HOST USING ANSIBLE

After you deploy a compliance policy on a host using Ansible, the Ansible role installs the SCAP client and configures OpenSCAP scans on the host according to the selected compliance policy.

The SCAP content in the compliance policy might require remote resources. For more information, see Section 9.1, "Inclusion of Remote SCAP Resources".

Prerequisites

- You have enabled OpenSCAP on your Capsule. For more information, see Enabling OpenSCAP on Capsule Servers in *Installing Capsule Server*.
- Repositories for the operating system version of the host are synchronized on Satellite Server and enabled on the host.
  - Red Hat Enterprise Linux 9 BaseOS and Appstream RPMs repositories
  - Red Hat Enterprise Linux 8 BaseOS and Appstream RPMs repositories
  - Red Hat Enterprise Linux 7 Server and Extras RPMs repositories
- Red Hat Satellite Client 6 repository for the operating system version of the host is synchronized on Satellite Server, available in the content view and the lifecycle environment of the host, and enabled for the host. For more information, see Changing the repository sets status for a host in Satellite in *Managing Content*. This repository is required for installing the SCAP client.
- You have created a compliance policy with the Ansible deployment option.

Procedure

1. In the Satellite web UI, navigate to **Hosts** > **All Hosts**, and select **Edit** on the host you want to configure for OpenSCAP reporting.
2. From the **OpenSCAP Capsule** list, select the Capsule with OpenSCAP enabled that you want to use.
3. On the **Ansible Roles** tab, add the **theforeman.foreman_scap_client** Ansible role.
4. Optional: On the **Parameters** tab, configure any Ansible variables of the role.
5. Click **Submit** to save your changes.

6. Click the **Hosts** breadcrumbs link to navigate back to the host index page.
7. Select the host or hosts to which you want to add the policy.
8. Click **Select Action**.
9. Select **Assign Compliance Policy** from the list.
10. In the **Assign Compliance Policy** window, select **Remember hosts selection for the next bulk action**.
11. Select the required policy from the list of available policies and click **Submit**.
12. Click **Select Action**.
13. Select **Run all Ansible roles** from the list.

9.5. DEPLOYING A POLICY IN A HOST GROUP USING PUPPET

After you deploy a compliance policy in a host group using Puppet, the Puppet agent installs the SCAP client and configures OpenSCAP scans on the hosts on the next Puppet run according to the selected compliance policy.

The SCAP content in your compliance policy might require remote resources. For more information, see Section 9.1, "Inclusion of Remote SCAP Resources".

Prerequisites

- You have enabled OpenSCAP on your Capsule. For more information, see Enabling OpenSCAP on Capsule Servers in *Installing Capsule Server*.
- Repositories for the operating system version of the host are synchronized on Satellite Server and enabled on the host.
  - Red Hat Enterprise Linux 9 BaseOS and Appstream RPMs repositories
  - Red Hat Enterprise Linux 8 BaseOS and Appstream RPMs repositories
  - Red Hat Enterprise Linux 7 Server and Extras RPMs repositories
- Red Hat Satellite Client 6 repository for the operating system version of the host is synchronized on Satellite Server, available in the content view and the lifecycle environment of the host, and enabled for the host. For more information, see Changing the repository sets status for a host in Satellite in *Managing Content*. This repository is required for installing the SCAP client.
- You have created a compliance policy with the Puppet deployment option and assigned the host group.

Procedure

1. In the Satellite web UI, navigate to **Configure** > **Host Groups**.
2. Click the host group that you want to configure for OpenSCAP reporting.

3. In the **Environment** list, select the Puppet environment that contains the **foreman_scap_client*** Puppet classes.
4. In the **OpenSCAP Capsule** list, select the Capsule with OpenSCAP enabled that you want to use.
5. On the **Puppet ENC** tab, add the **foreman_scap_client** Puppet class.
6. Optional: Configure any **Puppet Class Parameters**.
7. Click **Submit** to save your changes.

9.6. DEPLOYING A POLICY ON A HOST USING PUPPET

After you deploy a compliance policy on a host using Puppet, the Puppet agent installs the SCAP client and configures OpenSCAP scans on the host on the next Puppet run according to the selected compliance policy.

The SCAP content in your compliance policy might require remote resources. For more information, see Section 9.1, "Inclusion of Remote SCAP Resources".

Prerequisites

- You have enabled OpenSCAP on your Capsule. For more information, see Enabling OpenSCAP on Capsule Servers in *Installing Capsule Server*.
- Repositories for the operating system version of the host are synchronized on Satellite Server and enabled on the host.
  - Red Hat Enterprise Linux 9 BaseOS and Appstream RPMs repositories
  - Red Hat Enterprise Linux 8 BaseOS and Appstream RPMs repositories
  - Red Hat Enterprise Linux 7 Server and Extras RPMs repositories
- Red Hat Satellite Client 6 repository for the operating system version of the host is synchronized on Satellite Server, available in the content view and the lifecycle environment of the host, and enabled for the host. For more information, see Changing the repository sets status for a host in Satellite in *Managing Content*. This repository is required for installing the SCAP client.
- You have created a compliance policy with the Puppet deployment option.

Procedure

1. In the Satellite web UI, navigate to **Hosts** > **All Hosts**, and select **Edit** on the host you want to configure for OpenSCAP reporting.
2. From the **Environment** list, select the Puppet environment that contains the **foreman_scap_client** and **foreman_scap_client::params** Puppet classes.
3. From the **OpenSCAP Capsule** list, select the Capsule with OpenSCAP enabled that you want to use.
4. On the **Puppet ENC** tab, add the **foreman_scap_client** Puppet class.

5. Optional: Configure any **Puppet Class Parameters**.
6. Click the **Hosts** breadcrumbs link to navigate back to the host index page.
7. Select the host or hosts to which you want to add the policy.
8. Click **Select Action**.
9. Select **Assign Compliance Policy** from the list.
10. In the **Assign Compliance Policy** window, select **Remember hosts selection for the next bulk action**.
11. Select the required policy from the list of available policies and click **Submit**.

CHAPTER 10. RUNNING A SECURITY COMPLIANCE SCAN ON DEMAND

Hosts perform OpenSCAP scans regularly by the CRON schedule defined in the compliance policies assigned to hosts. However, you can also run a scan on a host for all configured compliance policies manually at any time.

Prerequisites

- Your user account has a role assigned that has the **view_hosts**, **create_job_invocations**, and **view_job_invocations** permissions.
- You have created a compliance policy and deployed it on the host.
  - For more information about managing policies, see Chapter 8, *Managing Compliance Policies*.
  - For more information about deploying policies, see Chapter 9, *Deploying Compliance Policies*.

Procedure

1. Navigate to **Hosts** > **All Hosts**.
2. Click the hostname of the required host.
3. On the host details page, expand the **Schedule a job** dropdown menu.
4. Select **Run OpenSCAP scan**

Verification

1. In the host details overview, locate the **Recent jobs** card.
2. Select the **Running** tab. Unless the job has already finished, the table shows a job called **Run scan for all OpenSCAP policies**.
3. On the **Recent jobs** card, select the **Finished** tab.
4. If the job has finished successfully, you should see the **succeeded** status in the row of the job.
5. Optional: Click the job name to review invocation details.

CHAPTER 11. MONITORING COMPLIANCE

With Satellite, you can centralize compliance monitoring and management. A compliance dashboard provides an overview of compliance of hosts and the ability to view details for each host within the scope of that policy. Compliance reports provide a detailed analysis of compliance of each host with the applicable policy. With this information, you can evaluate the risks presented by each host and manage the resources required to bring hosts into compliance. By monitoring compliance with SCAP, you can verify policy compliance and detect changes in compliance.

11.1. SEARCHING COMPLIANCE REPORTS

Use the Compliance Reports search field to filter the list of available reports on any subset of hosts.

Procedure

1. In the Satellite web UI, navigate to **Hosts** > **Reports**.
2. Optional: To see a list of available search parameters, click the empty **Search** field.
3. Enter the search query in the **Search** field and click **Search**. The search query is case insensitive.

Search Query Examples

Find all compliance reports for which more than five rules failed

```
failed > 5
```

Find all compliance reports created after January 1, 2023, for hosts with hostnames that contain prod-

```
host ~ prod- AND date > "Jan 1, 2023"
```

Find all reports generated by the rhel7_audit compliance policy from an hour ago

```
"1 hour ago" AND compliance_policy = date = "1 hour ago" AND compliance_policy = rhel7_audit
```

Find reports that pass an XCCDF rule

```
xccdf_rule_passed = xccdf_org.ssgproject.content_rule_firefox_preferences-auto-download_actions
```

Find reports that fail an XCCDF rule

```
xccdf_rule_failed = xccdf_org.ssgproject.content_rule_firefox_preferences-auto-download_actions
```

Find reports that have a result different than fail or pass for an XCCDF rule

```
xccdf_rule_othered = xccdf_org.ssgproject.content_rule_firefox_preferences-auto-download_actions
```

Additional Information

- You can create complex queries with the following logical operators: **and**, **not** and **has**. For more information about logical operators, see Supported Operators for Granular Search in *Administering Red Hat Satellite*.
- You cannot use regular expressions in a search query. However, you can use multiple fields in a single search expression. For more information about all available search operators, see Supported Operators for Granular Search in *Administering Red Hat Satellite*.
- You can bookmark a search to reuse the same search query. For more information, see Creating Bookmarks in *Administering Red Hat Satellite*.

11.2. COMPLIANCE EMAIL NOTIFICATIONS

Satellite Server sends an OpenSCAP Summary email to all users who subscribe to the **Compliance policy summary** email notifications. For more information on subscribing to email notifications, see Configuring Email Notification Preferences in *Administering Red Hat Satellite*.

Each time a policy is run, Satellite checks the results against the previous run, noting any changes between them. The email is sent according to the frequency requested by each subscriber, providing a summary of each policy and its most recent result.

11.3. VIEWING COMPLIANCE POLICY STATISTICS

You can view a compliance policy dashboard to verify compliance reports of a particular policy. The compliance policy dashboard provides a statistical summary of compliance of hosts and the ability to view report details for each host within the scope of that policy.

Consider prioritizing the following hosts when viewing compliance reports:

- Hosts which were evaluated as **Failed**
- Hosts labelled as **Never audited** because their status is unknown

Prerequisite

- Your user account has a role assigned that has the **view_policies** permission.

Procedure

1. In the Satellite web UI, navigate to **Hosts** > **Policies**.
2. In the row of the required policy, navigate to the **Actions** column and click **Dashboard**.

11.4. EXAMINING HOSTS PER RULE COMPLIANCE RESULT

You can examine a simplified report and use policy rules to list hosts that have a certain compliance result, such as failing a particular rule.

Prerequisite

- Your user account has a role assigned that has the **view_arf_reports** and **view_hosts** permissions.

Procedure

1. In the Satellite web UI, navigate to **Hosts** > **Reports**.
2. In the **Reported At** column, navigate to the report of the required host and compliance policy, and click the time link.
3. Satellite displays a simplified list of policy rules with the results of the scan.
4. Optional: Filter the rules by check result. From the **Show log messages** dropdown list, select one of the following filters:
   - **Failed and othered** – to view rules that have failed or have not been checked during the scan,
   - **Failed only** – to view only rules that have failed.
5. Optional: Examine the details of the rule. In the **Message** column, click the icon next to the name of the rule.
6. In the row of the required rule, navigate to the **Actions** column and click **Hosts failing this rule**.

11.5. EXAMINING COMPLIANCE FAILURES OF A HOST

You can examine a full compliance report, determine why a host failed compliance on a rule, and, in some cases, see how to remediate a case of non-compliance.

WARNING

Do not implement any of the recommended remedial actions or scripts without first testing them in a non-production environment. Remediation might render the system non-functional.

A compliance report consists of the following areas:

- Introduction
- Evaluation Characteristics
- Compliance and Scoring
- Rule Overview

Prerequisite

- Your user account has a role assigned that has the **view_arf_reports** and **view_hosts** permissions.

Procedure

1. In the Satellite web UI, navigate to **Hosts** > **Reports** to list all compliance reports.

2. In the row of the required host, navigate to the **Actions** column and click **Full Report** to view the complete details of an evaluation report.
3. Navigate to the **Evaluation Characteristics** area to review basic details about the evaluation of the host against a specific profile.
4. Navigate to the **Compliance and Scoring** area to review evaluation statistics and the host compliance score.
5. Navigate to the **Rule Overview** to examine the rules.
6. Optional: Deselect the check statuses that you want to hide, such as **pass**, **notapplicable**, or **fixed**.
7. Optional: From the **Group rule by** dropdown menu, select the criterion for the grouping of rules, such as **Severity**.
8. Optional: Enter a search string into the search field to filter rules by title. The search is case insensitive and applied dynamically as you type.
9. Click the title of a rule to inspect further result details:
    - A description of the rule with instructions for bringing the host into compliance if available.
    - The rationale for the rule.
    - In some cases, a remediation script.

11.6. DELETING A COMPLIANCE REPORT

You can delete compliance reports on your Satellite.

Prerequisite

- Your user account has a role assigned that has the **view_arf_reports** and **destroy_arf_reports** permissions.

Procedure

1. In the Satellite web UI, navigate to **Hosts** > **Reports**.
2. In the Compliance Reports window, identify the policy that you want to delete and, on the right of the policy's name, select **Delete**.
3. Click **OK**.

11.7. DELETING MULTIPLE COMPLIANCE REPORTS

You can delete multiple compliance policies simultaneously. However, in the Satellite web UI, compliance policies are paginated, so you must delete one page of reports at a time. If you want to delete all OpenSCAP reports, use the script in Deleting OpenSCAP Reports in the *API Guide*.

Prerequisite

- Your user account has a role assigned that has the **view_arf_reports** and **destroy_arf_reports** permissions.

Procedure

1. In the Satellite web UI, navigate to **Hosts** > **Reports**.
2. In the Compliance Reports window, select the compliance reports that you want to delete.
3. In the upper right of the list, select **Delete reports**.
4. Repeat these steps for as many pages as you want to delete.