Red Hat Satellite 6.14

管理安全合规性

规划并配置 SCAP 合规策略，将策略部署到主机，并监控主机的合规性

Last Updated: 2024-08-10

Red Hat Satellite 6.14 管理安全合规性

规划并配置 SCAP 合规策略，将策略部署到主机，并监控主机的合规性

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

法律通告

摘要

通过 Satellite，您可以创建安全合规策略，在主机上部署策略，并使用这些策略监控主机的合规性，使主机符合安全标准。

目录

向红帽文档提供反馈

我们感谢您对我们文档的反馈。让我们了解如何改进它。

使用 Red Hat JIRA 中的 **Create Issue** 表单提供您的反馈。JIRA 问题在 Red Hat Satellite Jira 项目中创建，您可以在其中跟踪其进度。

先决条件

- 确保您已注册了 红帽帐户。

流程

1. 单击以下链接： **创建问题**。如果 Jira 显示登录错误，则登录并在您重定向到表单后继续。
2. 完成 **Summary** 和 **Description** 字段。在 **Description** 字段中，包含文档 URL、章节号以及问题的详细描述。不要修改表单中的任何其他字段。
3. 点 **Create**。

第 1 章 安全合规管理

安全合规管理是定义安全策略的持续流程，审计系统符合这些政策，并解决不合规实例。任何不合规都根据机构的配置管理策略进行管理。安全策略的范围包括特定于行业的主机，因此要求在其定义中具有灵活性。

使用 Satellite，您可以在所有注册的主机上调度合规审计和报告。

第 2 章 安全内容自动化协议

Satellite 使用安全内容自动化协议(SCAP)标准来定义安全策略。

SCAP 是基于 XML 的多个规格的框架，如可扩展检查列表配置描述格式(XCCDF)和开放漏洞和评估语言(OVAL)中描述的漏洞。这些规格被封装为 *数据流文件*。

XCCDF 中的清单项目（也称为 *规则*）表达了系统项目所需的配置。例如，规则可以指定没有人可以使用 **root** 用户帐户通过 SSH 登录主机。规则可以分组到一个或多个 *XCCDF 配置集* 中，允许多个配置集共享规则。

OpenSCAP 扫描程序工具针对规则评估主机上的系统项目，并在资产报告格式(ARF)中生成报告，然后返回到 Satellite 来监控和分析。

表 2.1. OpenSCAP 扫描程序支持的 SCAP Framework 1.3 中的规格

标题	描述	Version
SCAP	安全内容自动化协议	1.3
XCCDF	可扩展配置检查列表描述格式	1.2
OVAL	开放漏洞和评估语言	5.11
-	asset Identification	1.1
ARF	资产报告格式	1.1
CCE	通用配置枚举	5.0
CPE	通用平台枚举	2.3
CVE	常见漏洞和风险	2.0
CVSS	通用漏洞评分系统	2.0

其他资源

- 有关 SCAP 的更多信息，请参阅 OpenSCAP 项目。

第 3 章 SATELLITE 中的 SCAP 内容

SCAP 内容是一个 SCAP 数据流文件，其中包含合规性、配置或安全基准的实施。单个数据流通常包含多个 XCCDF 配置集。XCCDF 配置集定义了一个行业标准或自定义安全标准，您可以评估 Satellite 中主机配置的合规性，如通用目的操作系统(OSPP)、健康保险可移植性和责任法案(HIPAA)和 PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 9。您可以使用 *定制文件* 根据要求调整现有的 XCCDF 配置集。

在 Satellite 中，您可以使用 SCAP 内容中的 XCCDF 配置集，最终是定制文件来定义 *合规策略*。Satellite 包括 OpenSCAP 项目 提供的 SCAP 安全指南中的默认 SCAP 内容。

有关如何下载、部署、修改和创建自己的内容的更多信息，请参阅：

- *Red Hat Enterprise Linux 9 安全强化*
- *Red Hat Enterprise Linux 8 安全强化*
- *Red Hat Enterprise Linux 7 安全指南*
- *Red Hat Enterprise Linux 6 安全指南*

3.1. 支持的 SCAP 版本

Satellite 支持 SCAP 版本 1.2 和 1.3 的内容。

第 4 章 合规策略部署选项

您可以使用以下方法之一部署合规策略：

Ansible 部署

您可以使用 Ansible 角色配置主机以进行合规性扫描。

Puppet 部署

您可以使用 Puppet 类和 Puppet 代理配置主机以进行合规性扫描。

手动部署

您可以手动为合规性扫描配置主机。

第 5 章 配置合规策略部署方法

使用以下步骤为您选择的方法配置 Satellite 来部署合规策略。在稍后 创建合规策略 时，您将选择这些方法之一。

Ansible 部署的步骤

1. 导入 **foreman.foreman_scap_client** Ansible 角色。
   如需更多信息，请参阅在 *Red Hat Satellite 中使用 Ansible 集成管理配置* 。
2. 将创建的策略和 **foreman.foreman_scap_client** Ansible 角色分配到主机或主机组。
3. 若要触发部署，请手动对主机或主机组运行 Ansible 角色，或者使用远程执行进行常规策略更新来设置周期性作业。
   如需更多信息，请参阅管理主机中的配置和设置远程作业。

Puppet 部署的步骤

1. *确保 Puppet 已启用。*
2. *确保主机上安装了 Puppet 代理。*
3. *导入包含 **foreman_scap_client** Puppet 模块的 Puppet 环境。*
   如需更多信息，请参阅在 Red Hat Satellite 中使用 Puppet 集成管理配置 。
4. *将创建的策略和 **foreman_scap_client** Puppet 类分配给主机或主机组。*
   Puppet 会触发下一次常规运行的部署，也可以手动运行 Puppet。Puppet 默认每 30 分钟运行一次。

手动部署的步骤

- *对于手动部署方法，不需要额外的 Satellite 配置。*
  有关手动部署的详情，请参考 红帽知识库 中的使用 Manual Deployment 选项设置 OpenSCAP 策略。

第 6 章 列出可用的 SCAP 内容

使用这个流程查看已在 Satellite 中载入的 SCAP 内容。要使用 CLI 而不是 Satellite Web UI，请参阅 CLI 流程。

前提条件

- 您的用户帐户分配了 **view_scap_contents** 权限的角色。

流程

- 在 Satellite Web UI 中，进入到 **Hosts** > **Compliance - SCAP contents**。

CLI 过程

- 在 Satellite 服务器上运行以下 Hammer 命令：

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

第 7 章 配置 SCAP 内容

您可以上传 SCAP 数据流和定制文件来定义合规策略。

7.1. 加载默认 SCAP 内容

通过在 Satellite 服务器上载入默认 SCAP 内容，您可以确保加载 SCAP 安全指南(SSG) 中的数据流，并分配给所有机构和位置。

SSG 由 Satellite 服务器的操作系统提供，并安装在 **/usr/share/xml/scap/ssg/content/** 中。请注意，可用的数据流取决于 Satellite 运行的操作系统版本。您只能使用此 SCAP 内容扫描与 Satellite 服务器具有相同次 RHEL 版本的主机。如需更多信息，请参阅 第 7.2 节 "为 RHEL 获取支持的 SCAP 内容"。

先决条件

- 您的用户帐户分配了 **create_scap_contents** 权限的角色。

流程

- 在 Satellite 服务器上使用以下 Hammer 命令：

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

7.2. 为 RHEL 获取支持的 SCAP 内容

您可以在红帽客户门户网站上获取 Red Hat Enterprise Linux 的最新 SCAP 安全指南(SSG)。您必须获取为主机的次要 RHEL 版本指定的 SSG 版本。

流程

1. 在软件包浏览器中访问 SCAP 安全指南。
2. 在 **Version** 菜单中，为您的主机运行的 RHEL 的次版本选择最新的 SSG 版本。例如，对于 RHEL 8.6，请选择名为 If **el8_6 的版本**。
3. 下载软件包 RPM。
4. 从 RPM 中提取 data-stream 文件(***-ds.xml**)。例如：

```
$ 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. 将数据流上传到 Satellite。如需更多信息，请参阅 第 7.3 节 "上传额外的 SCAP 内容"。

其他资源

- 红帽知识库 中的 RHEL 中支持的 SCAP 安全指南版本
- Red Hat Enterprise Linux 9 安全强化中的 RHEL 9 支持的 SCAP 安全指南配置文件
- Red Hat Enterprise Linux 8 安全强化中的 RHEL 8 支持的 SCAP 安全指南配置文件

- Red Hat Enterprise Linux 7 安全指南中 RHEL 7 支持的 SCAP 安全指南配置文件

7.3. 上传额外的 SCAP 内容

您可以将其他 SCAP 内容上传到 Satellite 服务器，可以是自己创建的内容，或者在其他位置获取。请注意，红帽只提供对从红帽获取的 SCAP 内容的支持。要使用 CLI 而不是 Satellite Web UI，请参阅 CLI 过程。

前提条件

- 您的用户帐户分配了 **create_scap_contents** 权限的角色。
- 您已获取了 SCAP 数据流文件。

流程

1. 在 Satellite Web UI 中，进入到 **Hosts** > **Compliance** > **SCAP contents**。
2. 单击 **Upload New SCAP Content**。
3. 在 **Title** 文本框中输入标题，如 **My SCAP Content**。
4. 在 **Scap File** 中，单击 **Choose file**，导航到包含 SCAP data-stream 文件的位置，然后单击 **Open**。
5. 在 **位置** 选项卡上，选择位置。
6. 在 组织选项卡上，选择组织。
7. 点 **Submit**。

如果成功加载 SCAP 内容文件，则会显示类似于 **Successfully created My SCAP Content** 的消息。

CLI 过程

1. 将 SCAP data-stream 文件放在 Satellite 服务器上的目录中，如 **/usr/share/xml/scap/my_content/**。
2. 在 Satellite 服务器上运行以下 Hammer 命令：

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

验证

- 列出可用的 SCAP 内容。SCAP 内容列表包含新标题。

7.4. 定制 XCCDF 配置集

您可以使用 定制文件 自定义现有的 XCCDF 配置集，而无需编辑原始 SCAP 内容。单个定制文件可以包含多个 XCCDF 配置集的自定义。

您可以使用 SCAP Workbench 工具创建定制文件。有关使用 SCAP Workbench 工具的更多信息，请参阅为您的用例自定义 SCAP 安全指南。

然后，您可以将定制文件分配给合规策略，以在策略中自定义 XCCDF 配置集。

7.5. 上传定制文件

上传定制文件后，您可以在自定义策略中应用它来自定义 XCCDF 配置集。

前提条件

- 您的用户帐户分配了 **create_tailoring_files** 权限的角色。

流程

1. 在 Satellite Web UI 中，导航到 **Hosts** > **Compliance - Tailoring Files**，再点 **New Tailoring File**。
2. 在 **Name** 文本框中输入名称。
3. 单击 **Choose File**，导航到包含定制文件的位置，然后选择 **Open**。
4. 单击 **Submit** 以上传所选的定制文件。

第 8 章 管理合规策略

合规策略 是一个调度的审计，用于检查指定的主机是否符合 SCAP 内容中的特定 XCCDF 配置集。

您可以指定 Satellite 服务器上扫描的调度，并在主机上执行扫描。扫描完成后，会生成 ARF 格式的报告并上传到 Satellite 服务器。合规策略不对扫描的主机进行任何更改。

合规策略定义 SCAP 客户端配置和 cron 计划。然后，策略会与分配策略的主机上的 SCAP 客户端一起部署。

8.1. 创建合规策略

通过创建合规策略，您可以定义和规划安全合规要求，并确保您的主机保持符合您的安全策略。

先决条件

- 您已为所选 合规策略部署方法 配置了 Satellite。
- 您已在 Satellite 中可用 SCAP 内容，最终定制文件。
  - 要验证可用的 SCAP 内容，请参阅 第 6 章 列出可用的 SCAP 内容。
  - 要上传 SCAP 内容和定制文件，请参阅 第 7 章 配置 SCAP 内容。
- 您的用户帐户分配了 **view_policies** 和 **create_policies** 权限的角色。

流程

1. 在 Satellite Web UI 中，进入到 **Hosts** > **Compliance - Policies**。
2. 单击 **New Policy** 或 **New Compliance Policy**。
3. 选择部署方法： **Ansible**、**Puppet** 或 **Manual**。然后单击 **"下一步"**。
4. 输入此策略的名称，描述（可选），然后点 **Next**。
5. 选择要应用的 **SCAP Content** 和 **XCCDF Profile**，然后单击 **Next**。
   请注意，Satellite 不会检测所选 XCCDF 配置集是否包含任何规则。一个空的 XCCDF 配置集（如 **Default XCCDF Profile**）将返回空的报告。
6. 可选： 要自定义 XCCDF 配置集，请选择 **Tailoring File** 和 **XCCDF Profile in Tailoring File**，然后点 **Next**。
7. 指定应用策略时的调度时间。从 **Period** 列表中选择 **Weekly**、**Monthly** 或 **Custom**。**Custom** 选项允许在策略调度中更大的灵活性。
   - 如果您选择 **Weekly**，还要从 **Weekday** 列表中选择一周的所需日期。
   - 如果您选择了 **Monthly**，还在 **Day of month** 字段中指定了日期。
   - 如果您选择 **Custom**，请在 **Cron line** 字段中输入有效的 Cron 表达式。
8. 选择要应用策略的位置，然后单击 **Next**。
9. 选择要应用该策略的组织，**然后单击下一步**。

10. 可选：选择要为其分配策略的主机组。
11. 点 **Submit**。

8.2. 查看合规策略

您可以预览将由特定 OpenSCAP 内容和配置集组合应用的规则。当您计划策略时，这非常有用。

前提条件

- 您的用户帐户分配了具有 **view_policies** 权限的角色。

流程

1. 在 Satellite Web UI 中，进入到 **Hosts** > **Compliance - Policies**。
2. 在所需策略的 **Actions** 列中，点 **Show Guide** 或从列表中选择它。

8.3. 编辑合规性策略

在 Satellite Web UI 中，您可以编辑合规策略。

Puppet 代理在下次运行时将编辑的策略应用到主机。默认情况下，每 30 分钟进行一次。如果使用 Ansible，您必须手动运行 Ansible 角色，或者配置了在主机上运行 Ansible 角色的周期性远程执行作业。

前提条件

- 您的用户帐户分配了 **view_policies** 和 **edit_policies** 权限的角色。

流程

1. 在 Satellite Web UI 中，进入到 **Hosts** > **Compliance - Policies**。
2. 点所需策略的名称。
3. 编辑必要的属性。
4. 点 **Submit**。

8.4. 删除 COMPLIANCE 策略

在 Satellite Web UI 中，您可以删除现有的合规策略。

前提条件

- 您的用户帐户分配了 **view_policies** 和 **destroy_policies** 权限的角色。

流程

1. 在 Satellite Web UI 中，进入到 **Hosts** > **Compliance - Policies**。
2. 在所需策略的 **Actions** 列中，从列表中选择 **Delete**。
3. 在确认消息中点 **OK**。

第 9 章 部署合规策略

若要部署合规策略，您必须安装 SCAP 客户端，更新 cron 调度文件，并将策略中选择的 SCAP 内容上传到主机上。

9.1. 包含远程 SCAP 资源

SCAP 数据流可以引用在主机上运行时 SCAP 客户端通过互联网获取的远程资源，如 OVAL 文件。如果数据流需要远程资源，您可以在 Satellite 服务器上看到 OpenSCAP Scanner 工具的警告，例如：

```
# 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
```

默认情况下，SCAP 客户端配置为忽略远程资源，并跳过依赖资源的 XCCDF 规则。然后，跳过的规则会导致 **notchecked** 状态。

对于可访问互联网的主机，您可以在 Satellite 中的主机上下载远程资源。有关将远程 SCAP 资源应用到无法访问互联网的主机的详情，请参考 第 9.2 节 “在断开连接的环境中应用远程 SCAP 资源”。

使用 Ansible 部署方法

覆盖以下 Ansible 变量：

- 名称： **foreman_scap_client_fetch_remote_resources**
- 类型： **布尔值**
- Value: **true**

如需更多信息，请参阅在 Red Hat Satellite 中使用 Ansible 集成管理配置 中的 在 Satellite 中 覆盖 Ansible 变量。

使用 Puppet 部署方法

配置以下 Puppet 智能类参数：

- 名称： **fetch_remote_resources**
- 类型： **布尔值**
- Value: **true**

如需更多信息，请参阅在 Red Hat Satellite 中使用 Puppet 集成管理配置 中的 配置 Puppet 智能类参数。

9.2. 在断开连接的环境中应用远程 SCAP 资源

SCAP 数据流可以包含远程资源，如 OVAL 文件，SCAP 客户端可以在主机上运行时通过互联网获取。如果您的主机无法访问互联网，则必须下载远程 SCAP 资源，并通过 从自定义文件类型存储库下载主机上的文件，将它们从 Satellite 服务器分发到您的主机，方法是从自定义文件类型存储库下载主机上的文件。

先决条件

- 您已将主机注册到 Satellite，并启用了远程执行。
- 必须禁用远程资源，这是默认设置。如需更多信息，请参阅 第 9.1 节 "包含远程 SCAP 资源"。

流程

1. 在 Satellite 服务器上，检查您在合规策略中使用的数据流，以查找您必须下载哪些缺少的资源：

```
# 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. 检查数据流引用的本地文件的名称：

```
# 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. 在在线机器上下载缺少的资源：

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

重要

确保下载的文件名与数据流引用的名称匹配。

4. 将文件作为新的自定义文件类型内容添加到 Satellite 服务器中。如需更多信息，请参阅管理内容中的管理自定义文件类型 内容。
注意发布您的存储库的 URL，如 **http://satellite.example.com/pulp/content/My_Organization_Label/Library/custom/My_Product_Label/My_Repo_Label/**。

5. 调度一个远程作业，将文件上传到主机上的 **root** 主目录。例如，使用 **Run Command - Script Default** 作业模板并输入以下命令：

```
# 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
```

有关运行远程作业的更多信息，请参阅管理主机中的执行远程作业。

6. 继续部署您的合规策略。

9.3. 使用 ANSIBLE 在主机组中部署策略

使用 Ansible 在主机组中部署合规策略后，Ansible 角色将安装 SCAP 客户端并根据所选的合规策略在主机上配置 OpenSCAP 扫描。

合规策略中的 SCAP 内容可能需要远程资源。如需更多信息，请参阅 第 9.1 节 "包含远程 SCAP 资源"。

先决条件

- 您已在 Capsule 上启用了 OpenSCAP。如需更多信息，请参阅安装 Capsule 服务器 中的 在 Capsule 服务器上启用 OpenSCAP。
- 主机操作系统版本的存储库在 Satellite 服务器上同步并在主机上启用。
  - Red Hat Enterprise Linux 9 BaseOS 和 Appstream RPM 软件仓库
  - Red Hat Enterprise Linux 8 BaseOS 和 Appstream RPM 软件仓库
  - Red Hat Enterprise Linux 7 Server 和 Extras RPM 软件仓库
- 用于主机的操作系统的 Red Hat Satellite Client 6 存储库已同步到 Satellite 服务器上，可在内容视图和主机的生命周期环境中同步，并为主机启用。如需更多信息，请参阅管理内容 中的更改 Satellite 中的主机存储库设置 状态 。安装 SCAP 客户端需要此软件仓库。
- 您已使用 Ansible 部署选项 创建了合规策略， 并分配了主机组。

流程

1. 在 Satellite Web UI 中，导航到 **Configure** > **Host Groups**。
2. 点您要为 OpenSCAP 报告配置的主机组。
3. 从 **OpenSCAP Capsule** 列表中，选择启用了 OpenSCAP 的胶囊。
4. 在 **Ansible Roles** 选项卡上，分配 **foreman.foreman_scap_client** Ansible 角色。
5. 可选：在 **Parameters** 选项卡中，配置角色的任何 Ansible 变量。
6. 点 **Submit** 保存您的更改。
7. 在所需主机组的行中，导航到 **Actions** 列，再选择 **Run all Ansible roles**。

9.4. 使用 ANSIBLE 在主机上部署策略

使用 Ansible 在主机上部署合规策略后，Ansible 角色将安装 SCAP 客户端并根据所选的合规策略在主机上配置 OpenSCAP 扫描。

合规策略中的SCAP 内容可能需要远程资源。如需更多信息，请参阅 第 9.1 节 "包含远程 SCAP 资源"。

先决条件

- 您已在 Capsule 上启用了 OpenSCAP。如需更多信息，请参阅安装 Capsule 服务器 中的 在 Capsule 服务器上启用 OpenSCAP。
- 主机操作系统版本的存储库在 Satellite 服务器上同步并在主机上启用。
  - Red Hat Enterprise Linux 9 BaseOS 和 Appstream RPM 软件仓库
  - Red Hat Enterprise Linux 8 BaseOS 和 Appstream RPM 软件仓库
  - Red Hat Enterprise Linux 7 Server 和 Extras RPM 软件仓库
- 用于主机的操作系统的 Red Hat Satellite Client 6 存储库已同步到 Satellite 服务器上，可在内容视图和主机的生命周期环境中同步，并为主机启用。如需更多信息，请参阅管理内容 中的更改 Satellite 中的主机存储库设置 状态 。安装 SCAP 客户端需要此软件仓库。
- 您已使用 Ansible 部署选项 创建了合规策略。

流程

1. 在 Satellite Web UI 中，导航到 **Hosts** > **All Hosts**，然后在您要为 OpenSCAP 报告配置的主机上选择 **Edit**。
2. 从 **OpenSCAP Capsule** 列表中，选择启用了 OpenSCAP 的胶囊。
3. 在 **Ansible Roles** 选项卡上，添加 **foreman.foreman_scap_client** Ansible 角色。
4. 可选：在 **Parameters** 选项卡中，配置角色的任何 Ansible 变量。
5. 点 **Submit** 保存您的更改。
6. 单击 **Hosts** breadcrumbs 链接，以返回主机索引页面。
7. 选择您要添加策略的主机或主机。
8. 单击 **Select Action**。
9. 从列表中选择 **Assign Compliance Policy**。
10. 在 **Assign Compliance Policy** 窗口中，为**下一个批量操作**选择 **Remember hosts**。
11. 从可用策略列表中选择所需的策略，然后单击 **Submit**。
12. 单击 **Select Action**。
13. 从列表中选择 **Run all Ansible roles**。

9.5. 使用 PUPPET 在主机组中部署策略

使用 Puppet 在主机组中部署合规策略后，Puppet 代理将安装 SCAP 客户端，并根据所选的合规性策略在下一个 Puppet 上的主机上配置 OpenSCAP 扫描。

合规策略中的SCAP 内容可能需要远程资源。如需更多信息，请参阅 第 9.1 节 "包含远程 SCAP 资源"。

先决条件

- 您已在 Capsule 上启用了 OpenSCAP。如需更多信息，请参阅安装 Capsule 服务器 中的 在 Capsule 服务器上启用 OpenSCAP。
- 主机操作系统版本的存储库在 Satellite 服务器上同步并在主机上启用。
  - Red Hat Enterprise Linux 9 BaseOS 和 Appstream RPM 软件仓库
  - Red Hat Enterprise Linux 8 BaseOS 和 Appstream RPM 软件仓库
  - Red Hat Enterprise Linux 7 Server 和 Extras RPM 软件仓库
- 用于主机的操作系统的 Red Hat Satellite Client 6 存储库已同步到 Satellite 服务器上，可在内容视图和主机的生命周期环境中同步，并为主机启用。如需更多信息，请参阅管理内容 中的更改 Satellite 中的主机存储库设置 状态 。安装 SCAP 客户端需要此软件仓库。
- 您已使用 Puppet 部署选项 创建了合规策略， 并分配了主机组。

流程

1. 在 Satellite Web UI 中，导航到 **Configure** > **Host Groups**。
2. 点您要为 OpenSCAP 报告配置的主机组。
3. 在 **Environment** 列表中，选择包含 **foreman_scap_client*** Puppet 类的 Puppet 环境。
4. 在 **OpenSCAP Capsule** 列表中，选择启用了 OpenSCAP 的 Capsule。
5. 在 **Puppet ENC** 选项卡中，添加 **foreman_scap_client** Puppet 类。
6. 可选：配置任何 **Puppet 类参数**。
7. 点 **Submit** 保存您的更改。

9.6. 使用 PUPPET 在主机上部署策略

使用 Puppet 在主机上部署合规策略后，Puppet 代理将安装 SCAP 客户端，并根据所选的合规策略在下一次 Puppet 的主机上配置 OpenSCAP 扫描。

合规策略中的 SCAP 内容可能需要远程资源。如需更多信息，请参阅 第 9.1 节 “包含远程 SCAP 资源”。

先决条件

- 您已在 Capsule 上启用了 OpenSCAP。如需更多信息，请参阅安装 Capsule 服务器 中的 在 Capsule 服务器上启用 OpenSCAP。
- 主机操作系统版本的存储库在 Satellite 服务器上同步并在主机上启用。
  - Red Hat Enterprise Linux 9 BaseOS 和 Appstream RPM 软件仓库
  - Red Hat Enterprise Linux 8 BaseOS 和 Appstream RPM 软件仓库
  - Red Hat Enterprise Linux 7 Server 和 Extras RPM 软件仓库

- 用于主机的操作系统的 Red Hat Satellite Client 6 存储库已同步到 Satellite 服务器上，可在内容视图和主机的生命周期环境中同步，并为主机启用。如需更多信息，请参阅管理内容 中的更改 Satellite 中的主机存储库设置 状态 。安装 SCAP 客户端需要此软件仓库。
- 您已使用 Puppet 部署选项 创建了合规策略。

流程

1. 在 Satellite Web UI 中，导航到 **Hosts** > **All Hosts**，然后在您要为 OpenSCAP 报告配置的主机上选择 **Edit**。
2. 从 **Environment** 列表中，选择包含 **foreman_scap_client** 和 **foreman_scap_client::params** Puppet 类的 Puppet 环境。
3. 从 **OpenSCAP Capsule** 列表中，选择启用了 OpenSCAP 的胶囊。
4. 在 **Puppet ENC** 选项卡中，添加 **foreman_scap_client** Puppet 类。
5. 可选：配置任何 **Puppet 类参数**。
6. 单击 **Hosts** breadcrumbs 链接，以返回主机索引页面。
7. 选择您要添加策略的主机或主机。
8. 单击 **Select Action**。
9. 从列表中选择 **Assign Compliance Policy**。
10. 在 **Assign Compliance Policy** 窗口中，为**下一个批量操作**选择 **Remember hosts**。
11. 从可用策略列表中选择所需的策略，然后单击 **Submit**。

第 10 章 对需求运行安全合规扫描

主机由分配给主机的合规策略中定义的 CRON 调度定期执行 OpenSCAP 扫描。但是，您也可以随时手动针对所有配置的合规策略在主机上运行扫描。

先决条件

- 您的用户帐户分配了 **view_hosts**、**create_job_invocations** 和 **view_job_invocations** 权限的角色。
- 您已创建了安全策略并将其部署到主机上。
  - 有关管理策略的更多信息，请参阅 第 8 章 管理合规策略。
  - 有关部署策略的更多信息，请参阅 第 9 章 部署合规策略。

流程

1. 导航到 **Hosts** > **All Hosts**。
2. 点所需主机的主机名。
3. 在主机详情页面上，展开 **Schedule a job** 下拉菜单。
4. 选择 **Run OpenSCAP scan**。

验证

1. 在主机详情概述中找到 **Recent 作业** 卡。
2. 选择 **Running** 选项卡。除非作业已完成，表 **显示所有 OpenSCAP 策略的 Run scan** 作业。
3. 在 **Recent jobs** 卡中，选择 **Finished** 选项卡。
4. 如果作业成功完成，您应该在作业所在行中看到 **succeeded** 状态。
5. 可选：点击作业名称来查看调用详情。

第 11 章 监控合规性

借助 Satellite，您可以集中进行合规监控和管理。合规仪表板提供主机的合规性概述，以及查看该策略范围内每个主机的详细信息。合规性报告提供每个主机与适用策略的合规性的详细分析。使用此信息，您可以评估每个主机带来的风险，并管理使主机符合要求的资源。通过监控 SCAP 合规性，您可以验证策略合规性并检测合规性中的更改。

11.1. 搜索合规报告

使用 Compliance Reports 搜索字段过滤对任何主机子集的可用报告列表。

流程

1. 在 Satellite Web UI 中，导航到 **Hosts** > **Reports**。
2. 可选：要查看可用搜索参数列表，请点空 **Search** 字段。
3. 在 **Search** 字段中输入搜索查询，然后单击 **Search**。搜索查询不区分大小写。

搜索查询示例

查找超过五个规则失败的所有合规性报告

```
failed > 5
```

查找 2023 年 1 月 1 日之后创建的所有合规性报告，以用于包含prod-的主机名的主机。

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

从一小时前查找 **rhel7_audit** 合规策略生成的所有报告

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

查找通过 XCCDF 规则的报告

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

查找没有 XCCDF 规则的报告

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

查找与 XCCDF 规则不同的结果或不通过的报告

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

其它信息

- 您可以针对以下逻辑运算符创建复杂的查询：**and**，**not** 和 **has**。有关逻辑运算符的更多信息，请参阅管理 Red Hat Satellite 中的 Granular Search 支持的 Operator。

- 您不能在搜索查询中使用正则表达式。但是，您可以在单个搜索表达式中使用多个字段。有关所有可用搜索运算符的更多信息，请参阅管理 Red Hat Satellite 中的 支持的 Operator for Granular Search。
- 您可以对搜索添加书签，以重复利用相同的搜索查询。如需更多信息，请参阅管理 Red Hat Satellite 中的 创建书签。

11.2. 合规性电子邮件通知

Satellite 服务器向订阅合规策略摘要电子邮件通知的所有用户发送 OpenSCAP Summary 电子邮件。**有关订阅电子邮件通知的更多信息，请参阅管理 Red Hat Satellite 中的配置电子邮件通知首选项。**

每次运行策略时，Satellite 都会检查对上一运行的结果，注意它们之间的任何更改。该电子邮件会根据每个订阅者请求的频率发送，提供每个策略及其最近结果的摘要。

11.3. 查看合规策略统计

您可以查看合规策略仪表板，以验证特定策略的合规性报告。合规策略控制面板提供主机合规性的统计信息，以及查看该策略范围内每个主机的报告详细信息的能力。

在查看合规报告时，请考虑优先选择以下主机：

- **被评估为 Failed的主机**
- 标记为 **Never** 审计的主机，因为它们的状态为 unknown

前提条件

- **您的用户帐户分配了具有 view_policies 权限的角色。**

流程

1. **在 Satellite Web UI 中，导航到 Hosts > Policies。**
2. **在所需策略所在的行中，导航到 Actions 列，再单击 Dashboard。**

11.4. 检查每个规则合规结果的主机

您可以检查简化的报告，并使用策略规则列出具有特定合规性结果的主机，如特定规则失败。

前提条件

- **您的用户帐户分配了 view_arf_reports 和 view_hosts 权限的角色。**

流程

1. **在 Satellite Web UI 中，导航到 Hosts > Reports。**
2. **在 Reported At 列中，导航到所需主机和合规策略的报告，然后单击时间链接。**
3. **Satellite 使用扫描结果显示简化的策略规则列表。**
4. **可选：通过检查结果过滤规则。从 Show log messages 下拉列表中，选择以下过滤器之一：**

- 失败和其他 - 查看扫描期间或未检查的规则，
- 仅失败 - 仅查看失败的规则。

5. 可选：检查规则的详情。在 Message 列中，单击规则名称旁边的图标。
6. 在必要规则的行中，导航到 Actions 列，再单击 Hosts failing this rule。

11.5. 检查主机的合规性故障

您可以检查完整的合规性报告，确定主机对规则是否合规的原因，在某些情况下，请参阅如何修复不合规的情况。

> **警告**
>
> 不要在非生产环境中首先测试它们的情况下实施推荐的补救操作或脚本。补救可能会导致系统无法正常工作。

合规性报告由以下区域组成：

- 简介
- 评估特性
- Compliance 和 Scoring
- 规则概述

前提条件

- 您的用户帐户分配了 view_arf_reports 和 view_hosts 权限的角色。

流程

1. 在 Satellite Web UI 中，导航到 Hosts > Reports 以列出所有合规性报告。
2. 在所需主机的行中，导航到 Actions 列，再单击 Full Report 以查看评估报告的完整详情。
3. 导航到 Evaluation Characteristics 区域，以查看有关针对特定配置文件评估主机的基本详情。
4. 导航到 Compliance 和 Scoring 区域，以检查评估统计信息和主机合规性分数。
5. 导航到 Rule Overview 以检查规则。
6. 可选：取消选择您要隐藏的检查状态，如 通过、不可应用或 固定。
7. 可选：在组规则 下拉菜单中，选择规则分组条件，如严重性。
8. 可选：在搜索字段中输入搜索字符串，以根据标题过滤规则。在输入时，搜索是区分大小写的，并动态应用。

9. 点规则的标题检查进一步的结果详情：
    - 有关将主机置于合规性（如果可用）的说明的规则描述。
    - 规则的比率。
    - 在某些情况下，补救脚本。

11.6. 删除合规性报告

您可以删除 Satellite 的合规性报告。

前提条件

- 您的用户帐户分配了 view_arf_reports 和 destroy_arf_reports 权限的角色。

流程

1. 在 Satellite Web UI 中，导航到 Hosts > Reports。
2. 在 Compliance Reports 窗口中，识别您要删除的策略，并在策略名称右侧选择 Delete。
3. 点击 确定。

11.7. 删除多个合规性报告

您可以同时删除多个合规策略。但是，在 Satellite Web UI 中，策略会被分页，因此您必须一次删除一个报告页面。如果要删除所有 OpenSCAP 报告，请使用 API 指南中的 删除 OpenSCAP 报告 中的 脚本。

前提条件

- 您的用户帐户分配了 view_arf_reports 和 destroy_arf_reports 权限的角色。

流程

1. 在 Satellite Web UI 中，导航到 Hosts > Reports。
2. 在 Compliance Reports 窗口中，选择您要删除的合规性报告。
3. 在列表右上角，选择 Delete report。
4. 对您要删除的多个页面重复这些步骤。