Subscription Central 1-latest

使用 Discovery

了解发现

Last Updated: 2024-07-02

Subscription Central 1-latest 使用 Discovery

了解发现

法律通告

摘要

目录

第 1 章 关于发现 **3**
1.1. 什么是发现？ 3
1.2. 发现哪些产品？ 3
1.3. 发现是否适合我？ 4

第 2 章 访问发现用户界面 **5**
2.1. 登录到 DISCOVERY 用户界面 5
2.2. 注销 DISCOVERY 用户界面 5

第 3 章 添加源和凭证 **7**
3.1. 添加网络源和凭证 7
3.2. 添加 SATELLITE 源和凭证 12
3.3. 添加 VCENTER 源和凭证 15
3.4. 添加 OPENSHIFT 源和凭证 17
3.5. 添加 ANSIBLE 源和凭证 20
3.6. 为 KUBERNETES 源和凭证添加 RED HAT ADVANCED CLUSTER SECURITY 22

第 4 章 运行和管理扫描 **26**
4.1. 运行和管理标准扫描 26
4.2. 运行和管理深度扫描 30

第 5 章 下载报告 **35**
5.1. 下载报告 35

第 6 章 向混合云控制台发送报告 **40**
6.1. 下载 INSIGHTS 报告并将其发送到混合云控制台 40
6.2. 什么是见解报告？ 41

对红帽文档提供反馈 **43**

第 1 章 关于发现

Discovery 旨在帮助用户收集有关他们使用特定红帽软件的数据。通过使用发现功能，用户可以减少计算和报告这些红帽产品使用情况所需的时间和工作量。

了解更多

要了解更多有关 Discovery 的目的、优点和特性的信息，请查看以下信息：

- 什么是发现？

要了解有关 Discovery 可以查找和检查的产品和产品版本的更多信息，请参阅以下信息：

- 发现哪些产品？

要评估 Discovery 是否为正确的解决方案，请查看以下信息：

- 发现是否适合我？

1.1. 什么是发现？

Discovery 是一个检查和报告工具。它旨在查找、识别和报告环境数据或事实，如网络上的物理和虚拟系统数量、其操作系统和其他配置数据。此外，它还旨在查找、识别和报告相应网络 IT 资源的关键红帽软件包和产品的更详细的事实。

检查网络中运行的软件和系统的功能可让您了解和报告您的订阅使用情况。最终，这种检查和报告过程是管理清单更大的系统管理任务的一部分。

发现需要配置两个基本结构来访问 IT 资源并运行检查过程。*凭证* 包含用户访问数据，如具有足够颁发机构的用户的用户名和密码或 SSH 密钥，以便在特定源或该源上的某些资产上运行检查过程。*源* 包含有关要检查的单个资产或多个资产的数据。这些资产可以是物理机、虚拟机或容器，它们标识为主机名、IP 地址、IP 范围或子网。这些资产也可以是 vCenter Server 或 Red Hat Satellite Server 等系统管理解决方案，也可以是在 Red Hat OpenShift Container Platform 上部署的集群。

注意

目前，发现的唯一虚拟化部署可以使用虚拟化基础架构的专用源进行扫描，即 VMware vCenter。红帽不支持的其他虚拟化基础架构可通过特殊扫描进行扫描。网络的一般扫描可能仍然找到这些资产，而不会由特殊扫描返回的确切元数据。

您可以在各种组合中保存多个凭证和源以用于 Discovery，因为您运行检查过程或 *扫描*。完成扫描后，您可以将输出中的这些事实作为格式化数据的集合访问，或 *报告* 以查看结果。

默认情况下，使用 Discovery 时创建的凭证和源在数据库中加密。该值使用 AES-256 加密。当发现服务器使用 vault 密码运行扫描时，它们会被解密，以访问存储在数据库中的加密值。

发现是一个无代理检查工具，因此不需要在要检查的每个源上安装该工具。但是，安装 Discovery 的系统必须有权访问要发现和检查的系统。

1.2. 发现哪些产品？

发现以下红帽产品：对于每个版本或发行版本，会列出最早的版本，其中会包括适用的版本。

如果产品最近更改了名称，以便您可能更熟悉该产品的当前名称，则该名称会作为附加信息提供。除非还列出该产品的特定版本，否则不会包括较新的产品名称。

Red Hat Enterprise Linux

- Red Hat Enterprise Linux 5 及更新的版本
- Red Hat Enterprise Linux 6 及更新的版本
- Red Hat Enterprise Linux 版本 7 及更新的版本
- Red Hat Enterprise Linux 版本 8 及更新的版本
- Red Hat Enterprise Linux 9 及更新的版本

Red Hat Application Services 产品（以前称为 Red Hat Middleware）

- Red Hat JBoss BRMS 版本 5.0.1 及更新版本，版本 6.0.0 及更新的版本（也称为 Red Hat Decision Manager，目前是 Red Hat Process Automation Manager 的一部分）
- JBoss Enterprise Web Server 版本 1 及更高版本；Red Hat JBoss Web Server 3.0.1 及更高版本
- Red Hat JBoss Enterprise Application Platform 版本 4.2 及更新的版本，版本 4.3 及更新的版本，版本 5 及更新的版本，版本 6 及更新的版本，版本 7 及更新的版本
- Red Hat Fuse 版本 6.0 及更新的版本

Red Hat Ansible Automation Platform

- Ansible Automation Platform 版本 2 及更新的版本

Red Hat OpenShift Container Platform

- Red Hat OpenShift Container Platform 版本 4 及更新的版本

Red Hat Advanced Cluster Security for Kubernetes

- Red Hat Advanced Cluster Security for Kubernetes 版本 4 及更新的版本

Red Hat Advanced Cluster Management for Kubernetes

- Red Hat Advanced Cluster Management for Kubernetes 版本 2 及更新的版本

1.3. 发现是否适合我？

发现旨在帮助您查找并了解您的红帽产品清单，包括复杂网络间的未知产品使用。通过与红帽解决方案架构师(SA)或大客户经理(TAM)或大客户经理(TAM)合作，或通过订阅教育和认知计划(SEAP)提供的分析和帮助，您最好理解 Discovery 生成的报告。

虽然您可以独立安装和使用发现，然后生成和查看报告数据，但 Discovery 文档不提供任何信息以帮助您解释报告结果。另外，虽然红帽支持可以提供一些与安装和配置 Discovery 相关的基本帮助，但支持团队不提供任何帮助以帮助您了解报告。

Discovery 工具不会自动与红帽共享数据。相反，您可以选择是否准备向红帽发送报告数据，以便红帽工具和服务。您可以在本地使用 Discovery 工具扫描您的网络以获取当前支持的红帽产品，然后使用生成的报告进行自己的内部目的。

第 2 章 访问发现用户界面

您可以通过浏览器访问发现图形用户界面。

了解更多

如需了解更多有关登录到 Discovery 图形用户界面的要求和步骤的信息，请查看以下信息：

- 登录到 Discovery 用户界面
- 注销 Discovery 用户界面

2.1. 登录到 DISCOVERY 用户界面

要登录到发现用户界面，您需要安装 Discovery 服务器的系统的 IP 地址，如果在服务器安装过程中更改了默认端口，以及登录时要使用的服务器管理员用户名和密码。如果您没有此信息，请联系安装 Discovery 服务器的管理员。

先决条件

- 要使用 Discovery 图形用户界面，您要在其上运行用户界面的系统必须能够与安装 Discovery 服务器的系统进行通信。

流程

1. 在浏览器中，以以下格式输入 Discovery 服务器的 URL：**https://*IPaddress*:*server_port***，其中 ***IPaddress*** 是 Discovery 服务器的 IP 地址，***server_port*** 是公开的服务器端口。
   以下示例演示了根据您要从中登录的系统以及是否使用默认端口的两种不同方法进入 URL：

   - 如果您从安装服务器的系统登录并使用默认端口 **9443**，您可以使用回环地址（也称为 localhost）作为 IP 地址，如下例所示：

     ```
     https://127.0.0.1:9443
     ```

   - 如果您从服务器远程的系统登录，服务器在 IP 地址 **192.0.2.0** 上运行，且默认端口在安装过程中改为 **8443**，您将以如下例所示登录：

     ```
     https://192.0.2.0:8443
     ```

   输入服务器的 URL 后，将会显示 Discovery 登录页面。

2. 在登录页面上，输入 Discovery 服务器管理员帐户的用户名和密码，然后单击 **Log in** 以登录到服务器。

验证步骤

如果这是您第一次登录 Discovery 时，将会显示 Welcome 页面。您可从添加可在扫描中使用的源和凭证开始。如果您之前已登录到 Discovery，Welcome 页面会被跳过，您可以与之前创建的源、凭证和扫描进行交互。

2.2. 注销 DISCOVERY 用户界面

流程

1. 在应用程序工具栏中，点 person 图标或您的用户名。
2. 单击 **Logout**。

第 3 章 添加源和凭证

要准备发现以运行扫描，您必须添加您要扫描的一个或多个源的 IT 基础架构部分。您还必须添加身份验证信息，如用户名和密码或 SSH 密钥，作为一个或多个凭证访问这些源。由于不同的配置要求，您可以根据您要扫描的源类型添加源和凭证。

了解更多

作为添加包含 IT 基础架构不同部分的源和凭证的一般流程的一部分，您可能需要完成很多任务。

添加网络源和凭证来扫描资产，如网络中的物理机、虚拟机或容器。如需更多信息，请参阅以下信息：

- 添加网络源和凭证

添加 satellite 源和凭证来扫描您的 Red Hat Satellite 服务器部署，以查找它管理的资产。如需更多信息，请参阅以下信息：

- 添加 Satellite 源和凭证

添加 vcenter 源和凭证来扫描您的 vCenter 服务器部署，以查找它管理的资产。如需更多信息，请参阅以下信息：

- 添加 vCenter 源和凭证

添加 OpenShift 源和凭证来扫描 Red Hat OpenShift Container Platform 集群的部署。如需更多信息，请参阅以下信息：

- 添加 OpenShift 源和凭证

添加 Ansible 源和凭证来扫描部署 Ansible Automation Platform，以查找它管理的安全集群。如需更多信息，请参阅以下信息：

- 添加 Ansible 源和凭证

添加 RHACS 源和凭证来扫描 Red Hat Advanced Cluster Security for Kubernetes 的部署，以查找 RHACS 管理的安全集群。如需更多信息，请参阅以下信息：

- 添加 RHACS 源和凭证

3.1. 添加网络源和凭证

要在网络上的一个或多个物理机器、虚拟机或容器上运行扫描，您必须添加一个源来标识要扫描的每个资产。然后，您必须添加包含身份验证数据的凭证来访问每个资产。

了解更多

添加一个或多个网络源和凭证，以提供在网络中扫描资产所需的信息。如需更多信息，请参阅以下信息：

- 要添加网络源，请参阅 添加网络源。
- 要添加网络凭证，请参阅 添加网络凭证。

要了解更多有关源和凭证以及如何使用它们的信息，请参阅以下信息：

- 关于源和凭证

要了解更多有关通过网络上的资产进行身份验证的信息，请参阅以下信息。此信息包括有关以升级权限运行命令的指导信息，这是在网络凭证配置过程中可能需要做出的选择：

- 网络验证
- 扫描远程网络资产中使用的命令

3.1.1. 添加网络源

您可以从初始 Welcome 页面或 Sources 视图中添加源。

流程

1. 点击选项根据您的位置添加新凭证：
   - 在 Welcome 页面中，单击 **Add Source**。
   - 从 Sources 视图，单击 **Add**。

   此时会打开 Add Source 向导。
2. 在 Type 页面上，选择 **Network Range** 作为源类型，然后点 **Next**。
3. 在 Credentials 页面中，输入以下信息：
   a. 在 **Name** 字段中输入描述性名称。
   b. 在 **Search Addresses** 字段中输入一个或多个用逗号分开的网络标识符。您可以输入主机名、IP 地址和 IP 范围。
      - 输入主机名作为 DNS 主机名，例如 **server1.example.com**。
      - 以 CIDR 或 Ansible 表示法输入 IP 范围，例如 **192.168.1.0/24** 代表 CIDR 表示法，或者为 Ansible 表示法输入 **192.168.1.[1:254]**。

   c. 可选：在 **Port** 字段中，如果您不希望扫描此源在默认端口 22 上运行，请输入不同的端口。
   d. 在 **Credentials** 列表中，选择访问此源网络资源所需的凭证。如果所需的凭证不存在，点 **Add a credential** 图标打开 Add Credential 向导。
   e. 如果您的网络资源需要 Ansible 连接方法是 Python SSH 实现，Paramiko 而不是默认的 OpenSSH 实施，请选择 **Connect using Paramiko 而不是 OpenSSH** 复选框。
4. 点 **Save** 保存源，然后点 **Close** 关闭 Add Source 向导。

3.1.2. 添加网络凭证

您可以在创建源的过程中从 Credentials 视图或 Add Source 向导添加凭证。您可能需要添加多个凭证来对单一源中包含的所有资产进行身份验证。

先决条件

- 如果要将 SSH 密钥身份验证类型用于网络凭证，您要使用的每个 SSH 私钥都必须复制到在 Discovery 服务器安装过程中映射到 **/sshkeys** 的目录中。此目录的默认路径为 **"${HOME}"/.local/share/discovery/sshkeys**。

有关 **/sshkeys** 目录中可用的 SSH 密钥的更多信息，或者请求向该目录添加密钥，请联系管理发现服务器的管理员。

流程

1. 点击选项根据您的位置添加新凭证：
   - 从 Credentials 视图，单击 **Add → Network Credential**。
   - 在 Add Source 向导中，点 **Credentials** 字段的 **Add a credential** 图标。

   此时会打开 Add Credential 向导。
2. 在 **Credential Name** 字段中输入描述性名称。
3. 在 **Authentication Type** 字段中，选择要使用的身份验证类型。您可以选择 **Username 和 Password** 或 **SSH Key**。
4. 根据身份验证类型，在适当的字段中输入身份验证数据。
   - 对于用户名和密码身份验证，请为用户输入用户名和密码。此用户必须具有对网络的根级别访问权限，或者要扫描的网络子集。或者，此用户必须能够通过所选 become 方法获取 root 级别的访问权限。
   - 对于 SSH 密钥身份验证，请输入用户名和到 Discovery 服务器容器本地的 SSH keyfile 的路径。例如，如果 keyfile 位于服务器上的 **"${HOME}"/.local/share/discovery/sshkeys** 默认路径中，请在 **SSH Key File** 字段中输入该路径。输入密码短语是可选的。
5. 输入权限提升的 become 方法。需要权限提升，才能在网络扫描期间运行一些命令。为 become 方法输入用户名和密码是可选的。
6. 点 **Save** 保存凭证并关闭 Add Credential 向导。

3.1.3. 关于源和凭证

要运行扫描，您必须为两个基本结构配置数据： sources 和 credentials。在扫描期间要检查的源类型决定了源和凭证配置所需的数据类型。

源 包含单个资产或一组要在扫描期间检查的多个资产。您可以配置以下类型的源：

网络源

一个或多个物理机器、虚拟机或容器。这些资产可以表示为主机名、IP 地址、IP 范围或子网。

vCenter 源

管理所有或部分 IT 基础架构的 vCenter Server 系统管理解决方案。

Satellite 源

管理所有或部分 IT 基础架构的 Satellite 系统管理解决方案。

Red Hat OpenShift 源

管理所有或部分 Red Hat OpenShift Container Platform 集群的 Red Hat OpenShift Container Platform 集群。

Ansible 源

管理 Ansible 节点和工作负载的 Ansible 管理解决方案。

Red Hat Advanced Cluster Security for Kubernetes 源

保护 Kubernetes 环境的 RHACS 安全平台解决方案。

当您使用网络源时，您可以确定您应该在单个源中拥有多少个资产。目前，您只能为网络源添加多个资产。以下列表包含您在添加源时应考虑的一些其他因素：

- 无论资产是开发、测试还是生产环境的一部分，以及计算能力和类似问题的需求都是这些资产的考虑因素。
- 因为内部业务实践（如频繁更改安装的软件），还是要更频繁地扫描特定的实体或一组实体。

凭证 包含的数据，如具有足够颁发机构的用户的用户名和密码或 SSH 密钥，以便在该源中包含的资产的所有或部分运行扫描。与源一样，凭证被配置为网络、vCenter、satellite、OpenShift、Ansible 或 RHACS 类型。通常，网络源可能需要多个网络凭证，因为预期许多凭证需要访问广泛 IP 范围内的所有资产。相反，vCenter 或 satellite 源通常使用单个 vCenter 或 satellite 凭证（如果适用）来访问特定的系统管理解决方案服务器，OpenShift、Ansible 或 RHACS 源将使用单个凭证访问单个集群。

您可以从 Sources 视图中添加新源，您可以从 Credentials 视图中添加新凭证。您还可以在源创建过程中添加新或选择之前现有凭证。在源创建过程中，您要直接将凭证与源关联。由于源和凭证必须具有匹配的类型，所以您在源创建过程中添加的任何凭证共享与源相同的类型。另外，如果您要在源创建过程中使用现有凭证，可用凭证列表仅包含同一类型的凭证。例如，在网络源创建过程中，只有网络凭证可供选择。

3.1.4. 网络验证

发现服务器使用 Ansible 的 SSH 远程连接功能来检查网络扫描中的远程系统。添加网络凭证时，您可以使用用户名和密码或用户名和 SSH keyfile 对来配置 SSH 连接。如果使用 SSH 密钥身份验证访问远程系统，您也可以提供密码短语。

另外，在网络凭证配置过程中，您可以启用 become 方法。在扫描期间使用 become 方法来提升特权。这些升级的权限需要运行命令并在您要扫描的系统上获取数据。有关在扫描过程中不需要提升权限 的命令的更多信息，请参阅扫描远程网络资产中使用的 命令。

3.1.4.1. 扫描远程网络资产中使用的命令

运行网络扫描时，Discovery 必须使用您提供的凭证在网络中的远程系统中运行某些命令。其中一些命令必须以升级的特权运行。此访问通常是通过使用 **sudo** 命令或类似命令来获取的。必须收集 Discovery 用来构建已安装产品的报告的事实类型。

尽管可以在没有提升权限的情况下对网络源运行扫描，但是该扫描的结果不完整。网络扫描的不完整结果将会影响所生成的扫描报告的质量。

以下信息列出了发现在网络扫描期间在远程主机上运行的命令。该信息包括可在没有任何提升权限的情况下运行的基本命令，以及必须使用升级特权运行的命令，以便为报告收集最准确和完整信息。

注意

除了以下命令外，发现还依赖于标准 shell 功能，如 **bash** shell 提供的设备。

3.1.4.1.1. 不需要提升权限的基本命令

以下命令不需要提高权限以在扫描期间收集事实：

- cat
- egrep
- sort
- uname

- ctime
- grep
- rpm
- virsh
- date
- id
- test
- whereis
- echo
- sed
- tune2fs
- xargs

3.1.4.1.2. 需要升级权限的命令

以下命令需要升级的特权，以便在扫描期间收集事实。每个命令都包含发现在扫描期间尝试查找的事实或事实类别的列表。如果该命令没有升级的特权，则无法将这些事实包含在报告中。

- **awk**
- **cat**
- **chkconfig**
- **命令**
- **df**
- **dirname**
- **dmidecode**
- **echo**
- **egrep**
- **fgrep**
- **查找**
- **ifconfig**
- **ip**
- **java**
- **locate**

- ls
- ps
- readlink
- sed
- sort
- stat
- subscription-manager
- systemctl
- tail
- test
- tr
- unzip
- virt-what
- xargs
- yum

3.2. 添加 SATELLITE 源和凭证

要在 Red Hat Satellite Server 部署上运行扫描，您必须添加一个标识要扫描的 Satellite 服务器的源。然后，您必须添加一个包含访问该服务器的身份验证数据的凭证。

了解更多

添加 satellite 源和凭证，以提供扫描 Satellite 服务器所需的信息。如需更多信息，请参阅以下信息：

- 要添加 satellite 源，请参阅 添加 satellite 源。
- 要添加 satellite 凭据，请参阅 添加 satellite 凭据。

要了解更多有关源和凭证以及如何使用它们的信息，请参阅以下信息：

- 关于源和凭证

要了解更多有关发现如何通过 Satellite 服务器进行身份验证的信息，请参阅以下信息：此信息包括有关在 satellite 凭证配置过程中可能需要进行的证书验证和 SSL 通信选项的指导。

- Satellite 服务器身份验证

3.2.1. 添加 Satellite 源

您可以从初始 Welcome 页面或 Sources 视图中添加源。

流程

1. 点击选项根据您的位置添加新凭证：
   - 在 Welcome 页面中，单击 **Add Source**。
   - 从 Sources 视图，单击 **Add**。

   此时会打开 Add Source 向导。
2. 在 Type 页面上，选择 **Satellite** 作为源类型，然后点 **Next**。
3. 在 Credentials 页面中，输入以下信息：
   a. 在 **Name** 字段中输入描述性名称。
   b. 在 **IP Address 或 Hostname** 字段中，为这个源输入 Satellite 服务器的 IP 地址或主机名。如果您不希望扫描此源在默认端口 443 上运行，请输入不同的端口。例如，如果 Satellite 服务器的 IP 地址为 192.0.2.15，而您要将端口更改为 80，则请输入 **192.0.2.15:80**。
   c. 在 **Credentials** 列表中，选择访问此源的 Satellite 服务器所需的凭据。如果所需的凭证不存在，点 **Add a credential** 图标打开 Add Credential 向导。
   d. 在 **Connection** 列表中，选择要在扫描此源期间用于安全连接的 SSL 协议。

   注意

   Satellite 服务器不支持禁用 SSL。如果您选择 **Disable SSL** 选项，这个选项将被忽略。

   e. 如果您需要升级 Satellite 服务器的 SSL 验证，以便从证书颁发机构检查验证的 SSL 证书，请选择 **Verify SSL Certificate** 复选框。
4. 点 **Save** 保存源，然后点 **Close** 关闭 Add Source 向导。

3.2.2. 添加 satellite 凭证

您可以在创建源的过程中从 Credentials 视图或 Add Source 向导添加凭证。

流程

1. 点击选项根据您的位置添加新凭证：
   - 从 Credentials 视图，单击 **Add → Satellite Credential**。
   - 在 Add Source 向导中，点 **Credentials** 字段的 **Add a credential** 图标。

   此时会打开 Add Credential 向导。
2. 在 **Credential Name** 字段中输入描述性名称。
3. 输入 Satellite 服务器管理员的用户名和密码。
4. 点 **Save** 保存凭证并关闭 Add Credential 向导。

3.2.3. 关于源和凭证

要运行扫描，您必须为两个基本结构配置数据： sources 和 credentials。在扫描期间要检查的源类型决定了源和凭证配置所需的数据类型。

源 包含单个资产或一组要在扫描期间检查的多个资产。您可以配置以下类型的源：

网络源

一个或多个物理机器、虚拟机或容器。这些资产可以表示为主机名、IP 地址、IP 范围或子网。

vCenter 源

管理所有或部分 IT 基础架构的 vCenter Server 系统管理解决方案。

Satellite 源

管理所有或部分 IT 基础架构的 Satellite 系统管理解决方案。

Red Hat OpenShift 源

管理所有或部分 Red Hat OpenShift Container Platform 集群的 Red Hat OpenShift Container Platform 集群。

Ansible 源

管理 Ansible 节点和工作负载的 Ansible 管理解决方案。

Red Hat Advanced Cluster Security for Kubernetes 源

保护 Kubernetes 环境的 RHACS 安全平台解决方案。

当您使用网络源时，您可以确定您应该在单个源中拥有多少个资产。目前，您只能为网络源添加多个资产。以下列表包含您在添加源时应考虑的一些其他因素：

- 无论资产是开发、测试还是生产环境的一部分，以及计算能力和类似问题的需求都是这些资产的考虑因素。
- 因为内部业务实践（如频繁更改安装的软件），还是要更频繁地扫描特定的实体或一组实体。

凭证 包含的数据，如具有足够颁发机构的用户的用户名和密码或 SSH 密钥，以便在该源中包含的资产的所有或部分运行扫描。与源一样，凭证被配置为网络、vCenter、satellite、OpenShift、Ansible 或 RHACS 类型。通常，网络源可能需要多个网络凭证，因为预期许多凭证需要访问广泛 IP 范围内的所有资产。相反，vCenter 或 satellite 源通常使用单个 vCenter 或 satellite 凭证（如果适用）来访问特定的系统管理解决方案服务器，OpenShift、Ansible 或 RHACS 源将使用单个凭证访问单个集群。

您可以从 Sources 视图中添加新源，您可以从 Credentials 视图中添加新凭证。您还可以在源创建过程中添加新或选择之前现有凭证。在源创建过程中，您要直接将凭证与源关联。由于源和凭证必须具有匹配的类型，所以您在源创建过程中添加的任何凭证共享与源相同的类型。另外，如果您要在源创建过程中使用现有凭证，可用凭证列表仅包含同一类型的凭证。例如，在网络源创建过程中，只有网络凭证可供选择。

3.2.4. Satellite 服务器身份验证

对于 satellite 扫描，对 Satellite 服务器的连接和访问从通过 HTTPS 加密的基本身份验证（用户名和密码）生成。默认情况下，satellite 扫描通过 SSL （安全套接字层）协议使用证书验证和安全通信运行。在源创建过程中，您可以从多个不同的 SSL 和 TLS （传输层安全）协议中选择，以用于证书验证和安全通信。

注意

您用于 satellite 扫描的 Satellite 服务器凭证必须是具有角色的用户，其中包含主机、订阅和机构查看权限。

您可能需要在扫描过程中调整证书验证级别，以正确连接到 Satellite 服务器。例如，您的 Satellite 服务器可能会使用来自证书颁发机构验证的 SSL 证书。在源创建过程中，您可以在扫描该源过程中升级 SSL

证书验证来检查该证书。相反，您的 Satellite 服务器可能会使用自签名证书。在源创建过程中，您可以保留 SSL 验证，以便对该源的扫描不会检查证书。选择保留自签名证书的默认值，可能会避免扫描错误。

虽然界面中目前提供了禁用 SSL 的选项，但 Satellite 服务器不支持禁用 SSL。如果您在创建 satellite 源时选择了 **Disable SSL** 选项，则忽略这个选项。

3.3. 添加 VCENTER 源和凭证

要在 vCenter Server 部署上运行扫描，您必须添加一个标识要扫描的 vCenter Server 服务器的源。然后，您必须添加一个包含访问该服务器的身份验证数据的凭证。

了解更多

添加 vcenter 源和凭证，以提供扫描 vCenter Server 所需的信息。如需更多信息，请参阅以下信息：

- 要添加 vcenter 源，请参阅 添加 vcenter 源。
- 要添加 vcenter 凭证，请参阅 添加 vcenter 凭证。

要了解更多有关源和凭证以及如何使用它们的信息，请参阅以下信息：

- 关于源和凭证

要了解更多有关通过 vCenter Server 服务器进行身份验证的信息，请参阅以下信息。此信息包括有关在 vcenter 凭证配置过程中可能需要进行的证书验证和 SSL 通信选项的指导信息：

- vCenter 服务器身份验证

3.3.1. 添加 vcenter 源

您可以从初始 Welcome 页面或 Sources 视图中添加源。

注意

vCenter 源仅与 vCenter 部署兼容。您不能使用此源扫描其他虚拟化基础架构，即使红帽支持的基础架构也是如此。

流程

1. 点击选项根据您的位置添加新凭证：
   - 在 Welcome 页面中，单击 **Add Source**。
   - 从 Sources 视图，单击 **Add**。

   此时会打开 Add Source 向导。
2. 在 Type 页面中，选择 **vCenter Server** 作为源类型，然后点 **Next**。
3. 在 Credentials 页面中，输入以下信息：
   a. 在 **Name** 字段中输入描述性名称。
   b. 在 **IP Address 或 Hostname** 字段中，为这个源输入 vCenter 服务器的 IP 地址或主机名。如果您不希望扫描此源在默认端口 443 上运行，请输入不同的端口。例如，如果 vCenter 服务器的 IP 地址为 192.0.2.15，而您要将端口更改为 80，则请输入 **192.0.2.15:80**。

c. 在 **Credentials** 列表中，选择访问此源所需的凭证。如果所需的凭证不存在，点 **Add a credential** 图标打开 Add Credential 向导。

d. 在 **Connection** 列表中，选择要在扫描此源期间用于安全连接的 SSL 协议。选择 **Disable SSL** 在扫描此源期间禁用安全通信。

e. 如果您需要升级 vCenter 服务器的 SSL 验证，以便从证书颁发机构检查验证的 SSL 证书，请选择 **Verify SSL Certificate** 复选框。

4. 点 **Save** 保存源，然后点 **Close** 关闭 Add Source 向导。

3.3.2. 添加 vcenter 凭证

您可以在创建源的过程中从 Credentials 视图或 Add Source 向导添加凭证。

流程

1. 点击选项根据您的位置添加新凭证：
   - 从 Credentials 视图，单击 **Add → VCenter Credential**。
   - 在 Add Source 向导中，点 **Credentials** 字段的 **Add a credential** 图标。

   此时会打开 Add Credential 向导。
2. 在 **Credential Name** 字段中输入描述性名称。
3. 输入 vCenter Server 管理员的用户名和密码。
4. 点 **Save** 保存凭证并关闭 Add Credential 向导。

3.3.3. 关于源和凭证

要运行扫描，您必须为两个基本结构配置数据： sources 和 credentials。在扫描期间要检查的源类型决定了源和凭证配置所需的数据类型。

源 包含单个资产或一组要在扫描期间检查的多个资产。您可以配置以下类型的源：

网络源

一个或多个物理机器、虚拟机或容器。这些资产可以表示为主机名、IP 地址、IP 范围或子网。

vCenter 源

管理所有或部分 IT 基础架构的 vCenter Server 系统管理解决方案。

Satellite 源

管理所有或部分 IT 基础架构的 Satellite 系统管理解决方案。

Red Hat OpenShift 源

管理所有或部分 Red Hat OpenShift Container Platform 集群的 Red Hat OpenShift Container Platform 集群。

Ansible 源

管理 Ansible 节点和工作负载的 Ansible 管理解决方案。

Red Hat Advanced Cluster Security for Kubernetes 源

保护 Kubernetes 环境的 RHACS 安全平台解决方案。

当您使用网络源时，您可以确定您应该在单个源中拥有多少个资产。目前，您只能为网络源添加多个资产。以下列表包含您在添加源时应考虑的一些其他因素：

- 无论资产是开发、测试还是生产环境的一部分，以及计算能力和类似问题的需求都是这些资产的考虑因素。
- 因为内部业务实践（如频繁更改安装的软件），还是要更频繁地扫描特定的实体或一组实体。

凭证 包含的数据，如具有足够颁发机构的用户的用户名和密码或 SSH 密钥，以便在该源中包含的资产的所有或部分运行扫描。与源一样，凭证被配置为网络、vCenter、satellite、OpenShift、Ansible 或 RHACS 类型。通常，网络源可能需要多个网络凭证，因为预期许多凭证需要访问广泛 IP 范围内的所有资产。相反，vCenter 或 satellite 源通常使用单个 vCenter 或 satellite 凭证（如果适用）来访问特定的系统管理解决方案服务器，OpenShift、Ansible 或 RHACS 源将使用单个凭证访问单个集群。

您可以从 Sources 视图中添加新源，您可以从 Credentials 视图中添加新凭证。您还可以在源创建过程中添加新或选择之前现有凭证。在源创建过程中，您要直接将凭证与源关联。由于源和凭证必须具有匹配的类型，所以您在源创建过程中添加的任何凭证共享与源相同的类型。另外，如果您要在源创建过程中使用现有凭证，可用凭证列表仅包含同一类型的凭证。例如，在网络源创建过程中，只有网络凭证可供选择。

3.3.4. vCenter 服务器身份验证

对于 vcenter 扫描，对 vCenter 服务器的连接和访问来自通过 HTTPS 加密的基本身份验证（用户名和密码）。默认情况下，vcenter 扫描通过 SSL （安全套接字层）协议运行并带有证书验证和安全通信。在源创建过程中，您可以从多个不同的 SSL 和 TLS （传输层安全）协议中选择，以用于证书验证和安全通信。

您可能需要调整证书验证级别，以便在扫描过程中正确连接到 vCenter 服务器。例如，您的 vCenter 服务器可能会使用来自证书颁发机构验证的 SSL 证书。在源创建过程中，您可以在扫描该源过程中升级 SSL 证书验证来检查该证书。相反，您的 vCenter 服务器可能会使用自签名证书。在源创建过程中，您可以默认保留 SSL 验证，以便扫描该源不会检查证书。选择保留自签名证书的默认值，可能会避免扫描错误。

如果 vCenter 服务器没有配置为将 SSL 用于 Web 应用程序，您可能还需要禁用 SSL 作为扫描过程中的安全通信方法。例如，您的 vCenter 服务器可能会配置为使用 HTTP 和端口 80 与 Web 应用程序通信。如果是这样，则在源创建过程中，您可以禁用对该源的 SSL 通信扫描。

3.4. 添加 OPENSHIFT 源和凭证

要在 Red Hat OpenShift Container Platform 部署上运行扫描，您必须添加一个标识要扫描的 Red Hat OpenShift Container Platform 集群的源。然后，您必须添加一个包含访问该集群的验证数据的凭证。

了解更多

添加 OpenShift 源和凭证，以提供扫描 Red Hat OpenShift Container Platform 集群所需的信息。如需更多信息，请参阅以下信息：

- 要添加 OpenShift 源，请参阅 添加 OpenShift 源。
- 要添加 OpenShift 凭据，请参阅 添加 OpenShift 凭据。

要了解更多有关源和凭证以及如何使用它们的信息，请参阅以下信息：

- 关于源和凭证

要了解更多有关与 Red Hat OpenShift Container Platform 集群进行身份验证的信息，请参阅以下信息。此信息包括有关在 OpenShift 凭证配置过程中可能需要进行的证书验证和 SSL 通信选项的指导信息：

- Red Hat OpenShift Container Platform 身份验证

3.4.1. 添加 Red Hat OpenShift Container Platform 源

您可以从初始 Welcome 页面或 Sources 视图中添加源。

先决条件

- 您需要访问 Red Hat OpenShift Container Platform Web 控制台管理员视角来获取 API 地址和令牌值。

流程

1. 点击选项根据您的位置添加新凭证：
   - 在 Welcome 页面中，单击 **Add Source**。
   - 从 Sources 视图，单击 **Add**。

   此时会打开 Add Source 向导。
2. 在 Type 页面上，选择 **OpenShift** 作为源类型，然后单击 **Next**。
3. 在 Credentials 页面中，输入以下信息：
   a. 在 **Name** 字段中输入描述性名称。
   b. 在 **IP Address 或 Hostname** 字段中，为这个源输入 Red Hat OpenShift Container Platform 集群 API 地址。您可以通过在 web 控制台中查看集群的概述详情来查找集群 API 地址
   c. 在 **Credentials** 列表中，选择访问此源集群所需的凭证。如果所需的凭证不存在，点 **Add a credential** 图标打开 Add Credential 向导。
   d. 在 **Connection** 列表中，选择要在扫描此源期间用于安全连接的 SSL 协议。选择 **Disable SSL** 在扫描此源期间禁用安全通信。
   e. 如果您需要升级集群的 SSL 验证，以便从证书颁发机构检查验证的 SSL 证书，请选择 **Verify SSL Certificate** 复选框。
4. 点 **Save** 保存源，然后点 **Close** 关闭 Add Source 向导。

3.4.2. 添加 Red Hat OpenShift Container Platform 凭证

您可以在创建源的过程中从 Credentials 视图或 Add Source 向导添加凭证。

先决条件

- 您需要访问 Red Hat OpenShift Container Platform Web 控制台管理员视角来获取 API 地址和令牌值。

流程

1. 点击选项根据您的位置添加新凭证：
   - 从 Credentials 视图，点 **Add → OpenShift**。
   - 在 Add Source 向导中，点 **Credentials** 字段的 **Add a credential** 图标。

此时会打开 Add Credential 向导。

2. 在 **Credential Name** 字段中输入描述性名称。

3. 从 Administrator 控制台输入 Red Hat OpenShift Container Platform 集群的 API 令牌。您可以通过单击控制台中的用户名来查找 API 令牌，单击 **Display Token** 选项并复制为 **API 令牌显示的值**为。

4. 点 **Save** 保存凭证并关闭 Add Credential 向导。

3.4.3. 关于源和凭证

要运行扫描，您必须为两个基本结构配置数据： sources 和 credentials。在扫描期间要检查的源类型决定了源和凭证配置所需的数据类型。

源 包含单个资产或一组要在扫描期间检查的多个资产。您可以配置以下类型的源：

网络源

一个或多个物理机器、虚拟机或容器。这些资产可以表示为主机名、IP 地址、IP 范围或子网。

vCenter 源

管理所有或部分 IT 基础架构的 vCenter Server 系统管理解决方案。

Satellite 源

管理所有或部分 IT 基础架构的 Satellite 系统管理解决方案。

Red Hat OpenShift 源

管理所有或部分 Red Hat OpenShift Container Platform 集群的 Red Hat OpenShift Container Platform 集群。

Ansible 源

管理 Ansible 节点和工作负载的 Ansible 管理解决方案。

Red Hat Advanced Cluster Security for Kubernetes 源

保护 Kubernetes 环境的 RHACS 安全平台解决方案。

当您使用网络源时，您可以确定您应该在单个源中拥有多少个资产。目前，您只能为网络源添加多个资产。以下列表包含您在添加源时应考虑的一些其他因素：

- 无论资产是开发、测试还是生产环境的一部分，以及计算能力和类似问题的需求都是这些资产的考虑因素。

- 因为内部业务实践（如频繁更改安装的软件），还是要更频繁地扫描特定的实体或一组实体。

凭证 包含的数据，如具有足够颁发机构的用户的用户名和密码或 SSH 密钥，以便在该源中包含的资产的所有或部分运行扫描。与源一样，凭证被配置为网络、vCenter、satellite、OpenShift、Ansible 或 RHACS 类型。通常，网络源可能需要多个网络凭证，因为预期许多凭证需要访问广泛 IP 范围内的所有资产。相反，vCenter 或 satellite 源通常使用单个 vCenter 或 satellite 凭证（如果适用）来访问特定的系统管理解决方案服务器，OpenShift、Ansible 或 RHACS 源将使用单个凭证访问单个集群。

您可以从 Sources 视图中添加新源，您可以从 Credentials 视图中添加新凭证。您还可以在源创建过程中添加新或选择之前现有凭证。在源创建过程中，您要直接将凭证与源关联。由于源和凭证必须具有匹配的类型，所以您在源创建过程中添加的任何凭证共享与源相同的类型。另外，如果您要在源创建过程中使用现有凭证，可用凭证列表仅包含同一类型的凭证。例如，在网络源创建过程中，只有网络凭证可供选择。

3.4.4. Red Hat OpenShift Container Platform 身份验证

对于 OpenShift 扫描，OpenShift 集群 API 地址的连接和访问利用集群 API 地址以及通过 HTTPS 加密的 API 令牌生成对 OpenShift 集群 API 地址的连接和访问。默认情况下，OpenShift 扫描通过 SSL （安全套接字层）协议运行并带有证书验证和安全通信。在源创建过程中，您可以从多个不同的 SSL 和 TLS （传输层安全）协议中选择，以用于证书验证和安全通信。

您可能需要在扫描过程中调整证书验证级别，以正确连接到 Red Hat OpenShift Container Platform 集群 API 地址。例如，您的 OpenShift 集群 API 地址可能会使用来自证书颁发机构验证的 SSL 证书。在源创建过程中，您可以在扫描该源过程中升级 SSL 证书验证来检查该证书。相反，集群 API 地址可能会使用自签名证书。在源创建过程中，您可以默认保留 SSL 验证，以便扫描该源不会检查证书。选择保留自签名证书的默认值，可能会避免扫描错误。

如果没有将 OpenShift 集群 API 地址配置为使用 Web 应用的 SSL 通信，则您可能还需要禁用 SSL 作为扫描期间的安全通信方法。例如，您的 OpenShift 服务器可能会配置为使用 HTTP 和端口 80 与 Web 应用通信。如果是这样，则在源创建过程中，您可以禁用对该源的 SSL 通信扫描。

3.5. 添加 ANSIBLE 源和凭证

要在 Ansible 部署上运行扫描，您必须添加一个标识要扫描的 Ansible Automation Platform 的源。然后，您必须添加一个包含访问该集群的验证数据的凭证。

了解更多

添加 Ansible 源和凭证，以提供扫描 Ansible Automation Platform 部署所需的信息。如需更多信息，请参阅以下信息：

- 要添加 Ansible 源，请参阅 添加 Ansible 源。
- 要添加 Ansible 凭据，请参阅 添加 Ansible 凭据。

要了解更多有关源和凭证以及如何使用它们的信息，请参阅以下信息：

- 关于源和凭证

要了解更多有关发现如何通过 Ansible 部署进行身份验证的信息，请参阅以下信息：此信息包括有关在 Ansible 凭证配置过程中可能需要进行的证书验证和 SSL 通信选项的指导信息：

- Ansible Automation Platform

3.5.1. 添加 Red Hat Ansible Automation Platform 源

您可以从初始 Welcome 页面或 Sources 视图中添加源。

流程

1. 点击选项根据您的位置添加新凭证：
   - 在 Welcome 页面中，单击 **Add Source**。
   - 从 Sources 视图，单击 **Add Source**。

   此时会打开 Add Source 向导。
2. 在 Type 页面中，选择 **Ansible Controller** 作为源类型，然后点 **Next**。
3. 在 Credentials 页面中，输入以下信息：
   a. 在 **Name** 字段中输入描述性名称。

b. 在 **IP Address 或 Hostname** 字段中输入此源的 Ansible 主机 IP 地址。您可以通过查看门户中的控制器概述详情来查找主机 IP 地址。

c. 在 **Credentials** 列表中，选择访问此源集群所需的凭证。如果所需的凭证不存在，点 **Add a credential** 图标打开 Add Credential 向导。

d. 在 **Connection** 列表中，选择要在扫描此源期间用于安全连接的 SSL 协议。选择 **Disable SSL** 在扫描此源期间禁用安全通信。

e. 如果您需要升级集群的 SSL 验证，以便从证书颁发机构检查验证的 SSL 证书，请选择 **Verify SSL Certificate** 复选框。

4. 点 **Save** 保存源，然后点 **Close** 关闭 Add Source 向导。

3.5.2. 添加 Red Hat Ansible Automation Platform 凭证

您可以在创建源的过程中从 Credentials 视图或 Add Source 向导添加凭证。

流程

1. 点击选项根据您的位置添加新凭证：

   - 从 Credentials 视图，单击 **Add → Ansible Credential**。
   - 在 Add Source 向导中，点 **Credentials** 字段的 **Add a credential** 图标。

   此时会打开 Add Credential 向导。

2. 在 **Credential Name** 字段中输入描述性名称。
3. 在 **User Name** 字段中输入 Ansible Controller 实例的用户名。
4. 在 **Password** 字段中，输入 Ansible Controller 实例的密码。
5. 点 **Save** 保存凭证。Add credential 向导关闭。

3.5.3. 关于源和凭证

要运行扫描，您必须为两个基本结构配置数据： sources 和 credentials。在扫描期间要检查的源类型决定了源和凭证配置所需的数据类型。

源 包含单个资产或一组要在扫描期间检查的多个资产。您可以配置以下类型的源：

网络源

一个或多个物理机器、虚拟机或容器。这些资产可以表示为主机名、IP 地址、IP 范围或子网。

vCenter 源

管理所有或部分 IT 基础架构的 vCenter Server 系统管理解决方案。

Satellite 源

管理所有或部分 IT 基础架构的 Satellite 系统管理解决方案。

Red Hat OpenShift 源

管理所有或部分 Red Hat OpenShift Container Platform 集群的 Red Hat OpenShift Container Platform 集群。

Ansible 源

管理 Ansible 节点和工作负载的 Ansible 管理解决方案。

Red Hat Advanced Cluster Security for Kubernetes 源

保护 Kubernetes 环境的 RHACS 安全平台解决方案。

当您使用网络源时，您可以确定您应该在单个源中拥有多少个资产。目前，您只能为网络源添加多个资产。以下列表包含您在添加源时应考虑的一些其他因素：

- 无论资产是开发、测试还是生产环境的一部分，以及计算能力和类似问题的需求都是这些资产的考虑因素。
- 因为内部业务实践（如频繁更改安装的软件），还是要更频繁地扫描特定的实体或一组实体。

凭证 包含的数据，如具有足够颁发机构的用户的用户名和密码或 SSH 密钥，以便在该源中包含的资产的所有或部分运行扫描。与源一样，凭证被配置为网络、vCenter、satellite、OpenShift、Ansible 或 RHACS 类型。通常，网络源可能需要多个网络凭证，因为预期许多凭证需要访问广泛 IP 范围内的所有资产。相反，vCenter 或 satellite 源通常使用单个 vCenter 或 satellite 凭证（如果适用）来访问特定的系统管理解决方案服务器，OpenShift、Ansible 或 RHACS 源将使用单个凭证访问单个集群。

您可以从 Sources 视图中添加新源，您可以从 Credentials 视图中添加新凭证。您还可以在源创建过程中添加新或选择之前现有凭证。在源创建过程中，您要直接将凭证与源关联。由于源和凭证必须具有匹配的类型，所以您在源创建过程中添加的任何凭证共享与源相同的类型。另外，如果您要在源创建过程中使用现有凭证，可用凭证列表仅包含同一类型的凭证。例如，在网络源创建过程中，只有网络凭证可供选择。

3.5.4. Ansible 身份验证

对于 Ansible 扫描，对 Ansible 主机 IP 地址的连接和访问利用主机 IP 地址以及通过 HTTPS 加密的密码生成对 Ansible 主机 IP 地址的连接和访问。默认情况下，Ansible 扫描通过 SSL （安全套接字层）协议运行并带有证书验证和安全通信。在源创建过程中，您可以从多个不同的 SSL 和 TLS （传输层安全）协议中选择，以用于证书验证和安全通信。

您可能需要调整证书验证级别，以便在扫描过程中正确连接到 Ansible 主机 IP 地址。例如，您的 Ansible 主机 Ip 地址可能会使用来自证书颁发机构的验证 SSL 证书。在源创建过程中，您可以在扫描该源过程中升级 SSL 证书验证来检查该证书。相反，您的主机 IP 地址可能会使用自签名证书。在源创建过程中，您可以默认保留 SSL 验证，以便扫描该源不会检查证书。选择保留自签名证书的默认值，可能会避免扫描错误。

如果没有将 Ansible 主机 IP 地址配置为使用 Web 应用的 SSL 通信，则您可能还需要禁用 SSL 作为扫描期间的安全通信方法。例如，您的 Ansible 主机 IP 地址可能会配置为使用 HTTP 和端口 80 与 Web 应用通信。如果是这样，则在源创建过程中，您可以禁用对该源的 SSL 通信扫描。

3.6. 为 KUBERNETES 源和凭证添加 RED HAT ADVANCED CLUSTER SECURITY

要在 Red Hat Advanced Cluster Security for Kubernetes (RHACS)部署上运行扫描，您必须添加一个标识要扫描的 RHACS 实例的源。然后，您必须添加一个包含访问该实例的身份验证数据的凭证。

了解更多

添加 RHACS 源和凭证，以提供扫描 RHACS 实例所需的信息。如需更多信息，请参阅以下信息：

- 要添加 RHACS 源，请参阅 添加 RHACS 源。
- 要添加 RHACS 凭证，请参阅 添加 RHACS 凭证。

要了解更多有关源和凭证以及如何使用它们的信息，请参阅以下信息：

- 关于源和凭证

要了解更多有关与 Red Hat Advanced Cluster Security for Kubernetes 实例进行身份验证的信息，请参阅以下信息。此信息包括有关在 RHACS 凭证配置过程中可能需要进行的证书验证和 SSL 通信选项的指导信息：

- Red Hat Advanced Cluster Security for Kubernetes

3.6.1. 为 Kubernetes 源添加 Red Hat Advanced Cluster Security

您可以从初始 Welcome 页面或 Sources 视图中添加源。

先决条件

- 您需要访问 Red Hat Advanced Cluster Security for Kubernetes (RHACS)门户来生成 admin API 令牌值。
- 您需要访问 RHACS 门户来查找 RHACS Central 端点，或者访问 RHACS 配置管理云服务实例详情。

流程

1. 点击选项根据您的位置添加新凭证：
   - 在 Welcome 页面中，单击 **Add Source**。
   - 从 Sources 视图，单击 **Add**。

   此时会打开 Add Source 向导。
2. 在 Type 页面中，选择 **RHACS** 作为源类型，然后点 **Next**。
3. 在 Credentials 页面中，输入以下信息：
   a. 在 **Name** 字段中输入描述性名称。
   b. 在 **IP Address 或 Hostname** 字段中，为这个源输入 Red Hat Advanced Cluster Security for Kubernetes Central 地址。
      - 如果在 OpenShift 上部署了 RHACS，您可以查看集群的网络路由来查找地址。
      - 如果 RHACS 部署在云中，您可以在实例详情中找到此信息。
   c. 在 **Credentials** 列表中，选择访问此源集群所需的凭证。如果所需的凭证不存在，点 **Add a credential** 图标打开 Add Credential 向导。
   d. 在 **Connection** 列表中，选择要在扫描此源期间用于安全连接的 SSL 协议。选择 **Disable SSL** 在扫描此源期间禁用安全通信。
   e. 如果您需要升级集群的 SSL 验证，以便从证书颁发机构检查验证的 SSL 证书，请选择 **Verify SSL Certificate** 复选框。
4. 点 **Save** 保存源，然后点 **Close** 关闭 Add Source 向导。

3.6.2. 添加 RHACS 凭证

您可以在创建源的过程中从 Credentials 视图或 Add Source 向导添加凭证。

先决条件

- 您需要访问 Red Hat Advanced Cluster Security for Kubernetes (RHACS)门户来生成 admin API 令牌值。
- 您需要访问 RHACS 门户来查找 RHACS Central 端点，或者访问 RHACS 配置管理云服务实例详情。

流程

1. 点击选项根据您的位置添加新凭证：
   - 在 Credentials 视图中，点 **Add → RHACS**。
   - 在 Add Source 向导中，点 **Credentials** 字段的 **Add a credential** 图标。

   此时会打开 Add Credential 向导。
2. 在 **Credential Name** 字段中输入描述性名称。
3. 从RHACS 门户输入 RHACS 的 API 令牌。如果您还没有令牌，您可以在 RHACSConfiguration 管理云服务门户上生成令牌。
4. 点 **Save** 保存凭证并关闭 Add Credential 向导。

3.6.3. 关于源和凭证

要运行扫描，您必须为两个基本结构配置数据： sources 和 credentials。在扫描期间要检查的源类型决定了源和凭证配置所需的数据类型。

源 包含单个资产或一组要在扫描期间检查的多个资产。您可以配置以下类型的源：

网络源

一个或多个物理机器、虚拟机或容器。这些资产可以表示为主机名、IP 地址、IP 范围或子网。

vCenter 源

管理所有或部分 IT 基础架构的 vCenter Server 系统管理解决方案。

Satellite 源

管理所有或部分 IT 基础架构的 Satellite 系统管理解决方案。

Red Hat OpenShift 源

管理所有或部分 Red Hat OpenShift Container Platform 集群的 Red Hat OpenShift Container Platform 集群。

Ansible 源

管理 Ansible 节点和工作负载的 Ansible 管理解决方案。

Red Hat Advanced Cluster Security for Kubernetes 源

保护 Kubernetes 环境的 RHACS 安全平台解决方案。

当您使用网络源时，您可以确定您应该在单个源中拥有多少个资产。目前，您只能为网络源添加多个资产。以下列表包含您在添加源时应考虑的一些其他因素：

- 无论资产是开发、测试还是生产环境的一部分，以及计算能力和类似问题的需求都是这些资产的考虑因素。
- 因为内部业务实践（如频繁更改安装的软件），还是要更频繁地扫描特定的实体或一组实体。

*凭证*包含的数据，如具有足够颁发机构的用户的用户名和密码或 SSH 密钥，以便在该源中包含的资产的所有或部分运行扫描。与源一样，凭证被配置为网络、vCenter、satellite、OpenShift、Ansible 或 RHACS 类型。通常，网络源可能需要多个网络凭证，因为预期许多凭证需要访问广泛 IP 范围内的所有资产。相反，vCenter 或 satellite 源通常使用单个 vCenter 或 satellite 凭证（如果适用）来访问特定的系统管理解决方案服务器，OpenShift、Ansible 或 RHACS 源将使用单个凭证访问单个集群。

您可以从 Sources 视图中添加新源，您可以从 Credentials 视图中添加新凭证。您还可以在源创建过程中添加新或选择之前现有凭证。在源创建过程中，您要直接将凭证与源关联。由于源和凭证必须具有匹配的类型，所以您在源创建过程中添加的任何凭证共享与源相同的类型。另外，如果您要在源创建过程中使用现有凭证，可用凭证列表仅包含同一类型的凭证。例如，在网络源创建过程中，只有网络凭证可供选择。

3.6.4. Red Hat Advanced Cluster Security for Kubernetes 身份验证

对于 Red Hat Advanced Cluster Security for Kubernetes (RHACS)扫描，通过 TLS (Transport Layer Security)加密的 API 令牌从 bearer 令牌身份验证生成连接和访问。默认情况下，RHACS 扫描使用证书验证和安全通信通过 TLS 协议运行。在源创建过程中，您可以从多个不同的 SSL （安全套接字层）和 TLS 协议中选择，以用于证书验证和安全通信。

您可能需要调整证书验证级别，以便在扫描过程中连接到 RHACS 门户。例如，您的 RHACS 实例可能会使用来自证书颁发机构验证的 TLS 证书。在源创建过程中，您可以在扫描该源的过程中升级 TLS 证书验证来检查该证书。相反，您的 RHACS 实例可能会使用自签名证书。在源创建过程中，您可以将 TLS 验证保留为默认值，以便扫描该源不会检查证书。选择保留自签名证书的默认值，可能会避免扫描错误。

如果 RHACS 实例没有配置为使用 Web 应用程序的 TSL 通信，则您可能还需要禁用 TSL 作为扫描期间安全通信的方法。例如，您的 RHACS 实例可能会配置为使用 HTTP 和端口 80 与 Web 应用程序通信。如果是这样，则可以在源创建过程中禁用该源扫描的 TSL 通信。

第 4 章 运行和管理扫描

在为您要扫描的 IT 基础架构的部分添加源和凭证后，您可以创建并运行扫描。在创建扫描时，您可以选择扫描单个源，或者组合来自不同源类型的多个源。您还可以选择是否为安装的默认安装过程和位置的产品运行标准扫描，或者在产品可能使用非标准进程或位置安装时运行深度扫描。

注意

目前，您无法将 OpenShift、Ansible 或 RHACS 扫描与扫描中任何其他类型的源合并。但是，单个 OpenShift、Ansible 或 RHACS 扫描可以包含相同类型的多个源，每个源都只与单个集群关联。

创建扫描后，您可以多次运行该扫描。该扫描的每个实例都会保存为扫描作业。

了解更多

要了解更多有关运行不使用对产品的深度扫描的标准扫描的信息，请参阅以下信息：

- 运行和管理标准扫描

要了解更多有关运行深度扫描的信息，可以找到可能已使用非标准进程或非标准位置安装的产品的扫描，请查看以下信息：

- 运行和管理深度扫描

4.1. 运行和管理标准扫描

在为您要扫描的 IT 基础架构的部分添加源和凭证后，您可以开始运行扫描。在大多数情况下，您可以运行标准扫描来查找报告红帽产品所需的环境和产品数据。

了解更多

运行标准扫描以在标准位置查找产品。如需更多信息，请参阅以下信息：

- 运行标准扫描

当您开始运行扫描时，您可以执行一些任务来管理扫描。这些任务包括通过运行新的扫描作业并通过暂停、恢复和取消管理活动扫描来更新扫描的数据。完成扫描后，您可以将其删除。如需更多信息，请参阅以下信息：

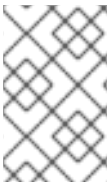
- 运行新的扫描作业
- 暂停、恢复和取消扫描
- 删除扫描

要了解更多有关扫描和扫描作业工作的信息，包括扫描作业是如何由 Discovery 处理的，以及扫描作业在其生命周期中移动的状态，请参阅以下信息：

- 关于扫描和扫描作业
- 扫描作业处理
- 扫描作业生命周期

4.1.1. 运行标准扫描

您可以从 Sources 视图运行新的扫描。您可以对单个源运行扫描，或者选择多个源来组合为一个扫描。每次您使用 Sources 视图来运行扫描时，系统会提示您将其保存为新的扫描。



注意

目前，您无法将 OpenShift、Ansible 或 RHACS 扫描与扫描中任何其他类型的源合并。但是，单个 OpenShift、Ansible 或 RHACS 扫描可以包含相同类型的多个源，每个源都只与单个集群关联。

第一次运行扫描后，扫描会保存到 Scans 视图中。在该视图中，您可以再次运行该扫描以更新其数据。每次从 Scans 视图运行扫描时，都会将其保存为该扫描的新扫描作业。

先决条件

- 要运行扫描，您必须首先添加您要扫描的源以及用于访问这些源的凭证。

流程

1. 从 Sources 视图中，选择一个或多个源。您可以选择不同类型的源将其合并到单个扫描中。
2. 点适合所选源的 **Scan** 按钮：
   - 对于单个源，请单击该源所在行上的 **Scan**。选择源的复选框是可选的。
   - 如果您选择了多个源，点工具栏中的 **Scan**。

   Scan 向导将打开。
3. 在 **Name** 字段中输入扫描的描述性名称。
4. 如果要更改默认并发扫描数，请在 **Maximum concurrent** scan 字段中设置新值。这个值是在扫描期间并行扫描的物理机或虚拟机的最大数量。
5. 要使用默认扫描过程，允许对 **这些产品复选框进行 Deep 扫描**，以保持在默认的清除状态。
6. 要开始扫描过程，请单击 **Scan**。

验证步骤

扫描过程开始时，在 Sources 视图中会显示通知。运行的扫描也会在 Scans 视图中显示，其中包含有关扫描进度的消息。

4.1.2. 运行新的扫描作业

在命名扫描并第一次运行它后，会将其添加到 Scans 视图中。然后，您可以运行该扫描的新实例，称为扫描作业，以更新为该扫描收集的数据。

流程

1. 在 Scans 视图中，单击扫描详情中的 **Run Scan** 图标。

注意

在扫描详情中，如果最新的扫描作业没有成功完成，则此图标会被标记为 **Retry Scan**。

验证步骤

扫描进程启动时，会显示一条通知，其中包含有关扫描进度的消息。如果要查看已完成的扫描，您可以查看扫描详情并展开 **Previous** 来查看所有之前的扫描作业。

4.1.3. 暂停、恢复和取消扫描

当您开始运行扫描时，您可能需要停止当前运行的扫描作业。可能会因为您的 IT 健康监控系统发出警报，或者需要运行比当前运行的 CPU 资源更多的优先级扫描的需要执行紧急修复所需的各种商业原因。

您可以通过暂停或取消扫描作业来停止扫描作业。您可以恢复暂停的扫描作业，但您无法恢复已取消的扫描作业。

流程

暂停正在运行的扫描作业：

1. 在 Scans 视图中，找到包含您要暂停的扫描作业的扫描。
2. 单击 **暂停扫描**。

注意

如果您同时运行多个扫描，则可能需要稍等片刻后，启动一个 **暂停扫描** 图标才会出现。

恢复暂停的扫描作业：

1. 在 Scans 视图中，找到包含您要恢复的扫描作业的扫描。
2. 点 **Resume Scan**。

取消正在运行的扫描作业：

1. 在 Scans 视图中，找到包含您要取消的扫描作业的扫描。
2. 单击 **Cancel Scan**。

4.1.4. 删除扫描

删除扫描是不可逆的操作，会删除扫描以及该扫描的所有扫描作业。无法检索删除的扫描。

先决条件

- 要删除扫描，需要首先运行扫描才可以显示在 **Scans** 导航中。

流程

1. 从导航中，单击 **Scans**。
2. 找到包含您要删除的扫描的行。
3. 点该行的 **Delete** 图标。

结果

- 您的扫描已删除。

4.1.5. 关于扫描和扫描作业

创建源和凭证后，您可以创建扫描。*扫描* 是一个对象，可将源分组到一个单元中，可以以可重复的方式检查或扫描。每次运行保存的扫描时，该实例都会保存为 *扫描作业*。扫描作业的输出是一个 *报告*，即为源中包含的所有 IT 资源收集的事实集合。

扫描至少包含一个源，以及在源创建时与该源关联的凭证。扫描作业运行时，它会使用提供的凭证联系源中包含的资产，然后检查资产以收集有关报告资产的事实。您可以在单个扫描中添加多个源，包括不同类型的源到单个扫描中。

注意

目前，您无法将 OpenShift 源与扫描中的任何其他类型源合并。但是，单个 OpenShift 扫描可以包含多个 OpenShift 源，每个源都仅与单个集群关联。

4.1.6. 扫描作业处理

扫描作业在处理两个阶段或任务时移动。这两个任务是连接任务和检查任务。

4.1.6.1. 扫描作业连接和检查任务

扫描任务期间运行的第一项任务是连接任务。*连接任务* 决定了连接到源的能力，并查找可以为定义的源检查的系统数量。运行的第二个任务是检查任务。*检查任务* 是从定义的源中的每个可访问系统中收集数据的任务，将扫描结果输出到报告中。

如果扫描配置为包含多个源，则在扫描作业运行时，会为每个源创建这两个任务。首先，所有源的所有连接任务都运行以建立与源的连接，并查找要检查的系统。然后，所有源的所有检查任务都运行来检查源中包含的可访问系统的内容。

4.1.6.2. 这些任务的处理方式

当扫描作业运行源的连接任务时，它会尝试连接到网络、服务器、集群或使用的实例。如果连接失败，则连接任务会失败。对于网络扫描，如果网络无法访问，或者凭证无效，连接任务会报告 0 (0)个成功系统。如果只访问一些网络扫描的系统，连接任务会报告成功访问的系统，连接任务也不会失败。

您可以在 Scans 视图中查看连接任务状态的信息。扫描的行将连接任务结果显示为最新扫描作业成功系统连接的数量。您还可以扩展前面的扫描作业，以查看之前扫描作业的连接任务结果。

当扫描作业运行源的检查任务时，它会检查连接任务的状态。如果连接任务显示失败状态，或者零(0)个成功连接，则扫描作业将转换为失败状态。但是，如果连接任务报告至少一个成功连接，则检查任务将继续。然后，扫描作业的结果会显示每个系统的成功和失败数据。如果检查任务无法从成功的系统收集结果，或者在检查任务过程中发生另一个意外错误，则扫描作业将转换为失败状态。

如果扫描包含多个源，每个源都有自己的连接和检查任务。这些任务独立于其他来源的任务独立处理。如果任何源的任何任务都失败，则扫描作业将转换为失败状态。只有在所有源的所有扫描作业任务成功完成时，扫描作业才会过渡到 completed 状态。

如果扫描作业成功完成，则该扫描作业的数据将生成为报告。在 Scans 视图中，您可以下载每个成功扫描作业的报告。

4.1.7. 扫描作业生命周期

扫描作业（或扫描的单个实例）在其生命周期内进入多个状态。

当您启动扫描时，会创建一个扫描作业，扫描作业处于 *创建* 的状态。然后，扫描作业会排队进行处理，扫描作业过渡到 *pending* 状态。扫描作业按顺序运行，按照它们启动的顺序运行。

由于 Discovery 服务器到达队列中的特定扫描作业，该扫描作业会在扫描作业开始的处理时从 *pending* 状态过渡到 *running* 状态。如果扫描过程成功完成，扫描作业将转换为 *完成* 的状态，扫描作业会生成可在报告中查看的结果。如果扫描过程导致错误阻止成功完成扫描，则扫描作业将停止，扫描作业会过渡到 *失败状态*。失败扫描的额外状态消息包含有助于确定故障原因的信息。

在扫描作业上执行的用户操作中扫描作业结果的其他状态。您可以在扫描作业待处理或运行时暂停或取消扫描作业。可以恢复处于 *暂停状态* 的扫描作业。处于 *已取消状态的* 扫描作业无法恢复。

4.2. 运行和管理深度扫描

在为您要扫描的 IT 基础架构的部分添加源和凭证后，您可以开始运行扫描。在某些情况下，运行标准扫描不足以查找报告红帽产品所需的环境和产品数据。

默认情况下，Discovery 使用与这些产品相关的已知元数据搜索和指纹产品。但是，您可以使用一个进程或安装位置安装这些产品，从而使搜索和指纹算法无效。在这种情况下，您需要使用深度扫描来查找这些产品。

了解更多

运行深度扫描，以查找非标准位置的产品。如需更多信息，请参阅以下信息：

- 使用深度扫描运行扫描

当您开始运行扫描时，您可以执行一些任务来管理扫描。这些任务包括通过运行新的扫描作业并通过暂停、恢复和取消管理活动扫描来更新扫描的数据。完成扫描后，您可以将其删除。如需更多信息，请参阅以下信息：

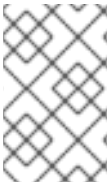
- 运行新的扫描作业
- 暂停、恢复和取消扫描
- 删除扫描

要了解更多有关扫描和扫描作业工作的信息，包括扫描作业是如何由 Discovery 处理的，以及扫描作业在其生命周期中移动的状态，请参阅以下信息：

- 关于扫描和扫描作业
- 扫描作业处理
- 扫描作业生命周期

4.2.1. 使用深度扫描运行扫描

您可以从 Sources 视图运行新的扫描。您可以对单个源运行扫描，或者选择多个源来组合为一个扫描。作为扫描配置的一部分，您可以选择使用深度扫描过程在非标准位置搜索产品。



注意

目前，您无法将 OpenShift、Ansible 或 RHACS 扫描与扫描中的任何其他类型源合并。但是，单个 OpenShift、Ansible 或 RHACS 扫描可以包含多个 OpenShift、Ansible 或 RHACS 源，每个源都只与单个集群关联。

深度扫描过程使用 **find** 命令，因此搜索过程可能是正在扫描的系统的 CPU 资源。因此，在为需要持续可用性的系统（如生产系统）选择深度扫描时，您应该自由裁量使用。

第一次运行扫描后，扫描会保存到 Scans 视图中。在该视图中，您可以再次运行扫描以更新其数据。

先决条件

- 要运行扫描，您必须首先添加您要扫描的源以及用于访问这些源的凭证。

流程

1. 从 Sources 视图中，选择一个或多个源。您可以选择不同类型的源将其合并到单个扫描中。
2. 点适合所选源的 **Scan** 按钮：
   - 对于单个源，请单击该源所在行上的 **Scan**。选择源的复选框是可选的。
   - 如果您选择了多个源，点工具栏中的 **Scan**。

   Scan 向导将打开。
3. 在 **Name** 字段中输入扫描的描述性名称。
4. 如果要更改默认并发扫描数，请在 **Maximum concurrent** scan 字段中设置新值。这个值是在扫描期间并行扫描的物理机或虚拟机的最大数量。
5. 要在一个或多个产品中使用深度扫描过程，请提供以下信息：
   - 选中 **适用于这些产品复选框的适用 Deep 扫描**。
   - （可选）输入您要发现要扫描的目录。深度扫描中使用的默认目录是 /、**/opt**、 **/app**、**/home** 和 **/usr** 目录。
6. 要开始扫描过程，请单击 **Scan**。

验证步骤

扫描过程开始时，在 Sources 视图中会显示通知。运行的扫描也会在 Scans 视图中显示，其中包含有关扫描进度的消息。

4.2.2. 运行新的扫描作业

在命名扫描并第一次运行它后，会将其添加到 Scans 视图中。然后，您可以运行该扫描的新实例，称为扫描作业，以更新为该扫描收集的数据。

流程

1. 在 Scans 视图中，单击扫描详情中的 **Run Scan** 图标。

注意

在扫描详情中，如果最新的扫描作业没有成功完成，则此图标会被标记为 **Retry Scan**。

验证步骤

扫描进程启动时，会显示一条通知，其中包含有关扫描进度的消息。如果要查看已完成的扫描，您可以查看扫描详情并展开 **Previous** 来查看所有之前的扫描作业。

4.2.3. 暂停、恢复和取消扫描

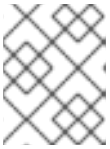
当您开始运行扫描时，您可能需要停止当前运行的扫描作业。可能会因为您的 IT 健康监控系统发出警报，或者需要运行比当前运行的 CPU 资源更多的优先级扫描的需要执行紧急修复所需的各种商业原因。

您可以通过暂停或取消扫描作业来停止扫描作业。您可以恢复暂停的扫描作业，但您无法恢复已取消的扫描作业。

流程

暂停正在运行的扫描作业：

1. 在 Scans 视图中，找到包含您要暂停的扫描作业的扫描。
2. 单击 **暂停扫描**。



注意

如果您同时运行多个扫描，则可能需要稍等片刻后，启动一个 **暂停扫描** 图标才会出现。

恢复暂停的扫描作业：

1. 在 Scans 视图中，找到包含您要恢复的扫描作业的扫描。
2. 点 **Resume Scan**。

取消正在运行的扫描作业：

1. 在 Scans 视图中，找到包含您要取消的扫描作业的扫描。
2. 单击 **Cancel Scan**。

4.2.4. 删除扫描

删除扫描是不可逆的操作，会删除扫描以及该扫描的所有扫描作业。无法检索删除的扫描。

先决条件

- 要删除扫描，需要首先运行扫描才可以显示在 **Scans** 导航中。

流程

1. 从导航中，单击 **Scans**。
2. 找到包含您要删除的扫描的行。
3. 点该行的 **Delete** 图标。

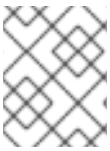
结果

- 您的扫描已删除。

4.2.5. 关于扫描和扫描作业

创建源和凭证后，您可以创建扫描。*扫描* 是一个对象，可将源分组到一个单元中，可以以可重复的方式检查或扫描。每次运行保存的扫描时，该实例都会保存为 *扫描作业*。扫描作业的输出是一个 *报告*，即为源中包含的所有 IT 资源收集的事实集合。

扫描至少包含一个源，以及在源创建时与该源关联的凭证。扫描作业运行时，它会使用提供的凭证联系源中包含的资产，然后检查资产以收集有关报告资产的事实。您可以在单个扫描中添加多个源，包括不同类型的源到单个扫描中。



注意

目前，您无法将 OpenShift 源与扫描中的任何其他类型源合并。但是，单个 OpenShift 扫描可以包含多个 OpenShift 源，每个源都仅与单个集群关联。

4.2.6. 扫描作业处理

扫描作业在处理两个阶段或任务时移动。这两个任务是连接任务和检查任务。

4.2.6.1. 扫描作业连接和检查任务

扫描任务期间运行的第一项任务是连接任务。*连接任务* 决定了连接到源的能力，并查找可以为定义的源检查的系统数量。运行的第二个任务是检查任务。*检查任务* 是从定义的源中的每个可访问系统中收集数据的任务，将扫描结果输出到报告中。

如果扫描配置为包含多个源，则在扫描作业运行时，会为每个源创建这两个任务。首先，所有源的所有连接任务都运行以建立与源的连接，并查找要检查的系统。然后，所有源的所有检查任务都运行来检查源中包含的可访问系统的内容。

4.2.6.2. 这些任务的处理方式

当扫描作业运行源的连接任务时，它会尝试连接到网络、服务器、集群或使用的实例。如果连接失败，则连接任务会失败。对于网络扫描，如果网络无法访问，或者凭证无效，连接任务会报告 0 (0)个成功系统。如果只访问一些网络扫描的系统，连接任务会报告成功访问的系统，连接任务也不会失败。

您可以在 Scans 视图中查看连接任务状态的信息。扫描的行将连接任务结果显示为最新扫描作业成功系统连接的数量。您还可以扩展前面的扫描作业，以查看之前扫描作业的连接任务结果。

当扫描作业运行源的检查任务时，它会检查连接任务的状态。如果连接任务显示失败状态，或者零(0)个成功连接，则扫描作业将转换为失败状态。但是，如果连接任务报告至少一个成功连接，则检查任务将继续。然后，扫描作业的结果会显示每个系统的成功和失败数据。如果检查任务无法从成功的系统收集结果，或者在检查任务过程中发生另一个意外错误，则扫描作业将转换为失败状态。

如果扫描包含多个源，每个源都有自己的连接和检查任务。这些任务独立于其他来源的任务独立处理。如果任何源的任何任务都失败，则扫描作业将转换为失败状态。只有在所有源的所有扫描作业任务成功完成时，扫描作业才会过渡到 completed 状态。

如果扫描作业成功完成，则该扫描作业的数据将生成为报告。在 Scans 视图中，您可以下载每个成功扫描作业的报告。

4.2.7. 扫描作业生命周期

扫描作业（或扫描的单个实例）在其生命周期内进入多个状态。

当您启动扫描时，会创建一个扫描作业，扫描作业处于 *创建* 的状态。然后，扫描作业会排队进行处理，扫描作业过渡到 *pending* 状态。扫描作业按顺序运行，按照它们启动的顺序运行。

由于 Discovery 服务器到达队列中的特定扫描作业，该扫描作业会在扫描作业开始的处理时从 *pending* 状态过渡到 *running* 状态。如果扫描过程成功完成，扫描作业将转换为 *完成* 的状态，扫描作业会生成可在报告中查看的结果。如果扫描过程导致错误阻止成功完成扫描，则扫描作业将停止，扫描作业会过渡到 *失败状态*。失败扫描的额外状态消息包含有助于确定故障原因的信息。

在扫描作业上执行的用户操作中扫描作业结果的其他状态。您可以在扫描作业待处理或运行时暂停或取消扫描作业。可以恢复处于 *暂停状态* 的扫描作业。处于 *已取消状态的* 扫描作业无法恢复。

第 5 章 下载报告

运行扫描后，您可以下载该扫描的报告，以查看该扫描期间收集和处理的数据。

了解更多

要了解有关下载报告的更多信息，请参阅以下信息：

- 下载报告

5.1. 下载报告

运行扫描后，您可以下载该扫描的报告，以查看该扫描期间收集和处理的数据。

扫描的报告有两种格式，即以逗号分隔的变量(CSV)格式和 JavaScript Object Notation (JSON)格式。它们也可以在两种内容类型中提供，扫描中的原始输出作为详细信息报告，并作为部署报告处理内容。

注意

提供了第三类报告，即 insights 报告，但只能通过 Discovery 命令行界面生成此报告。下载 insights 报告提供了一个 **.tar.gz** 文件，您可以传输到 cloud.redhat.com 上的混合云控制台。传输此文件允许在 Red Hat Insights 清单服务和订阅服务中使用报告数据。

了解更多

要了解更多有关合并和下载报告的信息，请参阅以下信息：

- 下载报告

要了解有关如何创建报告的更多信息，请参阅以下信息。此信息包括报告生成进程的时序。这些进程将详细信息报告的原始事实更改为指纹数据，然后将指纹数据更改为部署报告的去除重复数据并合并的数据。此信息还包括一个部分指纹示例，用于显示用于创建发现报告的数据类型。

- 如何创建报告
- 指纹示例

5.1.1. 下载报告

在 Scans 视图中，您可以选择一个或多个报告，并下载它们来查看报告数据。

先决条件

如果要下载扫描的报告，该扫描的最新扫描作业必须成功完成。

流程

1. 在 Scans 视图中，导航到您要下载报告的扫描行。
2. 点 **Download** for that scan。

验证步骤

下载的报告作为 **.tar.gz** 文件保存到浏览器的下载位置，例如 **report_id_224_20190702_173309.tar.gz**。文件名格式为 **report_id_*ID_DATE_TIME*.tar.gz**，其中 ***ID*** 是服务器分配的唯一报告 ID， ***DATE*** 是 *yyyymmdd* 格式的日期， ***TIME*** 是 *hhmmss* 格式的时间，基于 24 小时系统。日期和时间数据由运行客户

端与服务器 API 的浏览器的交互来确定。

要查看报告，请将 **.tar.gz** 文件解压缩到 **report_id_*ID*** 目录中。未压缩的报告捆绑包包含四个报告文件：两个 CSV 和 JSON 格式的详细信息报告，以及 CSV 和 JSON 格式的两个部署报告。

注意

虽然您可以为您自己的内部进程查看和使用这些报告的输出，但 Discovery 文档不提供任何信息以帮助您解释报告结果。另外，虽然红帽支持可以提供一些与安装和使用 Discovery 相关的基本帮助，但支持团队不提供任何帮助以帮助您了解报告。报告及其格式旨在供红帽订阅教育和认知计划(SEAP)团队在客户互动期间使用，并为其他红帽内部流程提供数据，如向各种混合云控制台服务提供数据。

5.1.2. 如何创建报告

扫描过程用于发现您的 IT 基础架构中的系统，检查和收集这些系统的性质和内容的信息，并从每个系统检查期间收集的信息创建报告。

系统是 任何可通过 SSH 连接、vCenter Server 数据、Satellite Server API 或 Red Hat OpenShift 集群 API 进行干预的实体。因此，系统可以是物理或虚拟机，也可以是不同类型的实体，如容器或集群。

5.1.2.1. 事实和指纹

在扫描过程中，会为每个源中包含的每个系统收集一组事实。*事实是* 有关系统的单一数据，如操作系统版本、CPU 内核数或红帽产品使用的权利。

处理事实的目的是为每个系统创建一组汇总的数据，称为指纹。*指纹* 是标识唯一系统及其特征的一组事实，包括架构、操作系统、安装在该系统及其版本的不同产品、在该系统上使用的权利等。

运行扫描作业时生成指纹数据，但数据仅用于创建一种报告类型。当您请求详情报告时，您会收到该扫描的原始事实，而无需任何指纹。当您请求部署报告时，您会收到包括去除重复数据、合并和后处理过程的结果的指纹数据。这些进程包括识别从原始事实识别已安装的产品和版本，查找已使用的权利、从不同源查找和合并重复产品实例，以及查找在非默认位置安装的产品以及其他步骤。

5.1.2.2. 系统去除重复数据和系统合并

在扫描期间，可在多个源中找到单个系统。例如，vCenter 服务器上的虚拟机也可以运行由 Satellite 管理的 Red Hat Enterprise Linux 操作系统安装。如果您构造了一个包含每种源、vcenter、satellite 和 network 的扫描，则单个系统会在扫描期间由所有三个源报告。

注意

目前，您无法将 OpenShift 或 Ansible 源与扫描中的任何其他源组合，因此重复数据删除和合并过程不适用于 OpenShift 或 Ansible 扫描。

要解决这个问题并构建准确的指纹，Discovery 会将未处理的系统事实从扫描发送到指纹引擎。指纹引擎通过使用重复数据删除和合并过程，为在多个源中找到的系统匹配和合并数据。

系统去除重复数据进程使用有关系统的特定事实来识别重复系统。这个过程分为几个阶段，使用这些事实在连续更广泛的数据中合并重复的系统：

- 来自网络源的所有系统都合并到一个网络系统中。如果系统对于 **subscription_manager_id** 或 **bios_uuid** 事实的值相同，则系统被视为重复。

- vcenter 源中的所有系统组合为一个 vcenter 系统集。如果系统对 **vm_uuid** 事实的值具有相同的值，则系统被视为重复。
- satellite 源中的所有系统合并到一个 satellite 系统集合中。如果系统对于 **subscription_manager_id** 事实的值相同，则系统被视为重复。
- 网络系统设置与 satellite 系统集合并，以组成单个网络 Satellite 系统集。如果系统对于 **subscription_manager** 事实的值或者 **mac_addresses** 事实中的 MAC 地址值相同，则系统被视为重复。
- network-satellite 系统集与 vcenter 系统集合并，以形成完整的系统集。如果系统在 **mac_addresses** 事实中有匹配的 MAC 地址值，或者 **vm_uuid** 事实的 vcenter 值与 **bios_uuid** 事实的网络值匹配，则系统被视为重复。

5.1.2.2.1. 系统合并

在去除重复数据过程后，下一步是执行这两个系统的合并。合并的系统来自每个源的系统事实合并。当两个系统中出现的事实合并时，合并过程使用以下优先级来合并事实（从最高到最低）：

1. 网络源事实
2. Satellite 源事实
3. vCenter 源事实

系统指纹包含一个 **元数据** 字典，用于捕获该系统的每个事实的原始源。

5.1.2.3. 系统后处理

完成去除重复数据和合并后，有一个创建派生系统事实的后处理阶段。*派生的系统事实* 是从对多个系统事实的评估生成的。大多数派生的系统事实都与产品标识数据相关，如存在特定产品及其版本。

以下示例演示了如何创建派生的系统事实 **system_creation_date**。

system_creation_date 事实是一个派生的系统事实，包含真实系统创建时间。此事实的值由以下事实评估确定：每个事实的值都会按照以下优先级顺序进行检查，其优先级顺序由与真实系统创建时间匹配的准确性决定。最高非空值用于决定 **system_creation_date** 事实的值。

1. **date_machine_id**
2. **registration_time**
3. **date_anaconda_log**
4. **date_filesystem_create**
5. **date_yum_history**

5.1.2.4. 报告创建

在处理报告数据后，报告创建过程会使用两种不同的格式构建两个报告，即 JavaScript Object Notation (JSON)和以逗号分隔的变量(CSV)。每个格式 *的详情* 报告包含没有处理的原始事实，并且每个格式的 *部署* 报告包含原始事实通过指纹、重复数据删除、合并和后处理过程后的输出。

报告格式旨在供红帽订阅教育和认知计划(SEAP)团队在客户互动和其他红帽内部过程中使用。

注意

虽然您可以为您自己的内部进程查看和使用这些报告的输出，但 Discovery 文档不提供任何信息以帮助您解释报告结果。另外，虽然红帽支持可以提供一些与安装和使用 Discovery 相关的基本帮助，但支持团队不提供任何帮助以帮助您了解报告。报告及其格式旨在供红帽订阅教育和认知计划(SEAP)团队在客户互动期间使用，并为其他红帽内部流程提供数据，如向各种混合云控制台服务提供数据。

5.1.2.5. 指纹示例

指纹由一组有关单一系统的事实组成，除了有关该系统上产品、授权、源和元数据的事实。以下示例显示了指纹数据。单一系统的指纹（即使其中安装很少的红帽产品）可以是很多行。因此，本例中只使用一个部分指纹。

Example


```
{
    "os_release": "Red Hat Enterprise Linux Atomic Host 7.4",
    "cpu_count": 4,
    "products": [
        {
            "name": "JBoss EAP",
            "version": null,
            "presence": "absent",
            "metadata": {
                "source_id": 5,
                "source_name": "S62Source",
                "source_type": "satellite",
                "raw_fact_key": null
            }
        }
    ],
    "entitlements": [
        {
            "name": "Satellite Tools 6.3",
            "entitlement_id": 54,
            "metadata": {
                "source_id": 5,
                "source_name": "S62Source",
                "source_type": "satellite",
                "raw_fact_key": "entitlements"
            }
        }
    ],
    "metadata": {
        "os_release": {
            "source_id": 5,
            "source_name": "S62Source",
            "source_type": "satellite",
            "raw_fact_key": "os_release"
        },
        "cpu_count": {
            "source_id": 4,
            "source_name": "NetworkSource",
            "source_type": "network",
            "raw_fact_key": "os_release"
```

```
        }
    },
    "sources": [
        {
            "id": 4,
            "source_type": "network",
            "name": "NetworkSource"
        },
        {
            "id": 5,
            "source_type": "satellite",
            "name": "S62Source"
        }
    ]
}
```

指纹的前几行显示系统的事实，包括有关操作系统和 CPU 的事实。在本例中，**os_release** 事实描述了已安装的操作系统和发行版本，作为 **Red Hat Enterprise Linux Atomic Host 7.4**。

接下来，指纹会在 **products** 部分中列出安装的产品。产品具有名称、版本、存在和元数据字段。在 JBoss EAP 部分中，**presence** 字段显示 **absent** 作为值，因此本例中的系统没有安装 Red Hat JBoss Enterprise Application Platform。

指纹还列出该系统在 **entitlements** 部分中消耗的权利。列表中的每个权利都有一个名称、ID 和元数据，用于描述该事实的原始源。在示例指纹中，系统有 **Satellite Tools 6.3** 权利。

除了 **products** 和 **entitlements** 部分中的元数据字段外，指纹还包含用于系统事实 **元数据** 的元数据部分。对于每个系统事实，指纹的 **metadata** 部分中有一个对应的条目，用于标识该系统事实的原始源。在示例中，在扫描 satellite 源的过程中，在 Satellite 服务器中找到 **os_release** 事实。

最后，指纹会在 sources 部分中列出包含此系统的 **源**。系统可以包含在多个源中。例如，对于包含网络源和 satellite 源的扫描，可在扫描的两个部分中找到单一系统。

第 6 章 向混合云控制台发送报告

运行扫描后，您可以将该扫描的报告发送到 cloud.redhat.com 的混合云控制台。您生成和发送的报告不是详情报告或部署报告。相反，这是第三个报告，称为 *insights 报告*。这种类型的报告被混合云控制台服务格式化，特别是 ingestion。

当您向混合云控制台发送 insights 报告时，报告数据可以被混合云控制台服务使用，如 Red Hat Insights 的 inventory 服务，以显示基于主机的清单数据和订阅服务来显示订阅使用情况数据。

了解更多

要了解更多有关如何使用 insights 报告的信息，请参阅以下信息：

- 下载 Insights 报告并将其发送到混合云控制台

要了解更多有关 insights 报告概念的信息，请参阅以下信息：

- 什么是见解报告？

6.1. 下载 INSIGHTS 报告并将其发送到混合云控制台

当您需要向 Red Hat Insights 清单服务和订阅服务等混合云控制台服务提供报告数据时，您可以下载并发送 insights 报告。

这种类型的报告与详情报告或部署报告不同。*深入了解报告* 是一个发现报告，它的数据类似于部署报告，但它的内容和格式被设计，特别被混合云控制台服务使用。另外，无法从 Discovery 图形用户界面创建 insights 报告。它必须通过使用 Discovery 命令行界面创建。

先决条件

如果要下载并发送 insights 报告，您必须满足以下要求：

- 该扫描的最新扫描作业必须成功完成。
- Discovery 命令行界面必须安装在与 Discovery 服务器相同的系统上，以便您可以从命令行界面执行以下步骤。您无法从图形用户界面下载并发送 insights 报告。

流程

1. 登录到命令行界面，其中 ***server_administrator_username*** 是 Discovery 服务器管理员的用户名，***server_administrator_password*** 是服务器管理员的密码：

```
$ dsc server login --username server_administrator_username --password
server_administrator_password
```

2. 找到您要用来创建 insights 报告的扫描作业的 **report_identifier** （报告 ID）值。以下命令返回所有创建的扫描对象的摘要详情：

```
$ dsc scan list
```

注意

如果您知道要使用的扫描名称，但不知道 **report_identifier** 值，您还可以使用 **qpc scan show --name *scan_name*** 命令只显示该扫描的扫描作业。

3. 使用您找到的 **report_identifier** 值，下载扫描作业的 insights 报告。在以下示例中，分配给下载报告的文件名为 **report.tar.gz**，但您可以根据需要更改此文件名：

```
$ dsc report insights --report report_identifier --output-file report.tar.gz
```

4. 将用于登录到混合云控制台的凭证（通常是您的红帽客户门户网站帐户）添加到命令行界面配置中。此步骤是必需的，以便在下一步中使用这些凭证向混合云控制台发送 insights 报告。

```
$ dsc insights login
```

5. 使用 **publish** 子命令，将 insights 报告数据发送到混合云控制台，以及可以使用报告的服务，如库存服务和订阅服务。

```
$ dsc insights publish --input-file report.tar.gz
```

注意

虽然您可以查看 insights 报告的输出，但 Discovery 文档不提供任何信息以帮助您解释 insights 报告结果。另外，虽然红帽支持可以提供一些与安装和使用 Discovery 相关的基本帮助，但支持团队不提供任何帮助以帮助您了解 insights 报告。见解报告及其格式旨在由红帽内部流程使用，如为各种混合云控制台服务提供数据。

其他资源

- 有关安装和配置 Discovery 命令行界面的更多信息，请参阅 *安装和配置发现* 指南。

6.2. 什么是见解报告？

在对 IT 基础架构或 IT 基础架构的部分运行扫描后，您可以使用 Discovery 通过扫描中的数据创建 insights 报告。insights 报告是一个特殊的报告，旨在发送到混合云控制台服务，如 Red Hat Insights 的清单服务，以显示基于主机的清单数据和订阅服务来显示订阅使用情况数据。

虽然 Discovery 可用于扫描和报告您的 IT 基础架构的所有部分、连接和断开连接，但当您的 IT 基础架构的某些部分断开连接或 air-gapped 时，会向混合云控制台服务发送见解报告特别有用。通过使用 Discovery 收集网络这些部分的数据，您可以获得整个网络的更完整且更策展的视图。当 insights 报告的数据与支持混合云控制台的工具的其他数据收集相结合时，它可让您查看统一清单并在单一位置(Hybrid Cloud Console)中查看订阅使用的完整视图。

6.2.1. 报告频率

所有断开连接的或 air-gapped 系统必须定期扫描并通过 insights 报告报告报告，以确保准确数据到达混合云控制台。发送 insights 报告的每周节奏是当前的推荐。每周的节奏提供了足够的里程碑，以便有效地监控订阅服务中的订阅使用情况。

6.2.2. 避免系统重复

根据您在 insights 报告中提供的数据类型，对数据的屏蔽可能会影响该报告的质量，特别是对于报告创建的去除重复数据和合并过程。

例如，如果 insights 报告包含您 IT 基础架构连接和断开连接的部分数据，且您在该报告中屏蔽数据，那么通过其他方法（如 Red Hat Satellite 或 Red Hat Insights）报告的系统也会重复。因此，如果您已经通过 Red Hat Insights、Satellite、Red Hat Subscription Management 或类似工具直接报告系统，您应该避免在生成 insights 报告时屏蔽主机名、IP 地址和类似事实。

通常，对于只涵盖 IT 基础架构的断开连接的部分扫描，或者为 100% 断开连接的客户扫描，如果使用了一致的哈希值，则屏蔽是一个可选步骤。但是，不建议屏蔽。由于屏蔽消除了用于区分各个系统的信息类型，因此使用掩码可防止您获得 Red Hat Insights 和其他混合云控制台工具（如订阅服务）的大多数好处。

对红帽文档提供反馈

我们感谢您对我们文档的反馈。要提供反馈，请打开一个 JIRA 问题来描述您的问题。尽可能提供更详细的信息，以便可以快速解决您的请求。

先决条件

- 您有红帽客户门户网站帐户。此帐户允许您登录到 Red Hat Jira Software 实例。如果您没有帐户，系统会提示您创建一个帐户。

流程

要提供反馈，请执行以下步骤：

1. 单击以下链接： 创建问题。
2. 在 **Summary** 文本框中，输入问题的简短描述。
3. 在 **Description** 文本框中，提供有关此问题的更多详细信息。包括您找到问题的 URL。
4. 为任何其他必填字段提供信息。允许包含默认信息的所有字段都保留在默认值中。
5. 点 **Create** 为文档团队创建 JIRA 问题。

将创建一个文档问题，并路由到适当的文档团队。感谢您抽出时间提供反馈。