



Red Hat Satellite 6.10

配置 Satellite 以使用 Ansible

在 Satellite 中配置 Ansible，以帮助自动执行重复性任务

Red Hat Satellite 6.10 配置 Satellite 以使用 Ansible

在 Satellite 中配置 Ansible，以帮助自动执行重复性任务

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

法律通告

Copyright © 2023 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

摘要

本指南介绍了如何设置和配置红帽卫星以使用 Ansible 执行远程执行和自动化重复性任务。

目录

第 1 章 在 SATELLITE 中使用 ANSIBLE	3
1.1. 将部署配置为运行 ANSIBLE 角色	3
1.2. 导入 ANSIBLE 角色和变量	3
1.3. 在 SATELLITE 中覆盖 ANSIBLE 变量	3
1.4. ADDING RED HAT ENTERPRISE LINUX SYSTEM ROLES	5
第 2 章 使用 ANSIBLE 角色在卫星主机上 AUTOMATE REPETITIVE 任务	6
2.1. 将 ANSIBLE 角色分配给现有主机	6
2.2. 在主机上运行 ANSIBLE 角色	6
2.3. 将 ANSIBLE 角色分配到主机组	7
2.4. 在主机组上运行 ANSIBLE 角色	7
2.5. 在检查模式下运行 ANSIBLE 角色	7
第 3 章 配置和设置远程作业	9
3.1. 关于在主机上运行作业	9
3.2. 远程执行 workflow	10
3.3. 远程执行的权限	11
3.4. 创建作业模板	11
3.5. 在 SATELLITE 中将 FALLBACK 配置为 ANY CAPSULE REMOTE EXECUTION SETTING	13
3.6. 在 SATELLITE 中配置全局胶囊远程执行设置	14
3.7. 配置 SATELLITE 以使用备用目录对主机执行远程作业	15
3.8. 为远程执行分发 SSH 密钥	15
3.9. 手动将 SSH 密钥分发到远程执行	16
3.10. 使用 SATELLITE API OBTAIN SSH KEYS FOR REMOTE EXECUTION	17
3.11. 在置备过程中将 KICKSTART 模板配置为分发 SSH 密钥	17
3.12. 为 KERBEROS TICKET GRANTING TICKETS 配置 KEYTAB	17
3.13. 为远程执行配置 KERBEROS 身份验证	18
3.14. 设置作业模板	19
3.15. 执行远程作业	20
3.16. 监控作业	22
第 4 章 集成 RED HAT SATELLITE 和 ANSIBLE TOWER	24
4.1. 将卫星服务器添加到 ANSIBLE TOWER 中作为动态清单 ITEM	24
4.2. 为主机配置部署回调	25
附录 A. 作业模板示例和扩展	29
A.1. 自定义模板	29
A.2. 默认任务模板类别	29
A.3. RESTORECON 模板示例	30
A.4. 渲染 RESTORECON 模板	31
A.5. 在多个主机上执行 RESTORECON 模板	31
A.6. 模板中包括 POWER ACTIONS	31

第 1 章 在 SATELLITE 中使用 ANSIBLE

使用本指南将 Satellite 配置为使用 Ansible，然后使用 Ansible 进行远程执行的信息。

1.1. 将部署配置为运行 ANSIBLE 角色

在 Satellite 中，您可以导入 Ansible 角色来帮助自动化日常任务。Ansible 仅在 Satellite 上启用。

完成这个步骤，将 Satellite 部署配置为运行 Ansible 角色。

流程

1. 将角色添加到卫星上的 `/etc/ansible/roles` 目录，以及您要其中使用角色的所有胶囊。如果要使用自定义或第三方 Ansible 角色，请确保配置外部版本控制系统，以同步卫星和胶囊之间的角色。
2. 在您要用来在主机上运行 Ansible 角色的胶囊上，启用 Ansible 插件：

```
# satellite-installer --scenario capsule \
--enable-foreman-proxy-plugin-ansible
```

3. 分发 SSH 密钥，以启用胶囊以使用 SSH 连接到主机。如需更多信息，[请参阅管理主机指南中的分配用于远程执行的 SSH 密钥](#)。卫星运行 Ansible 角色与运行远程执行作业的方式相同。
4. 将 Ansible 角色导入到卫星中。
5. 在配置 [卫星以使用 Ansible 时](#)，继续在卫星主机上使用 [Ansible 角色自动化一致的任务](#)。

1.2. 导入 ANSIBLE 角色和变量

您可以从卫星上的 `/etc/ansible/roles` 目录或启用了 Ansible 的胶囊中导入 Ansible 角色和变量。确保您导入的角色和变量位于所有胶囊上的 `/etc/ansible/roles` 目录中，其中您要使用角色。请注意，如果某些角色不可见，这可能是由于某些角色需要更长的导入时间。

1. 在 Satellite Web UI 中，导航到 **Configure > Roles**，再单击包含您要导入的角色和变量的 Capsule。
2. 点 **Submit**。

1.3. 在 SATELLITE 中覆盖 ANSIBLE 变量

如果在 Satellite 中运行 Ansible 角色，您可以使用 Satellite 覆盖这些角色的 Ansible 变量。

覆盖变量的优先级

如果使用 Ansible 角色以不是 **Effective User** 的用户运行任务，则有严格的优先级顺序来覆盖 Ansible 变量。要确保您覆盖的变量遵循正确的优先级顺序，请参阅 [变量优先级：在 Ansible 用户指南中，我应该在哪儿放置变量？](#)

前提条件

- 您必须在 Satellite 中具有 Ansible 变量。
 - 要导入 Ansible 变量，请参阅 [导入 Ansible 变量](#)

- 要创建 Ansible 变量，请参阅[创建 Ansible 变量](#)

以下流程对主机和主机组的引用。有关主机和主机组的更多信息，请参阅[管理主机指南](#)。

流程

1. 在 Satellite Web UI 中，进入 **Configure > Variables**。
2. 选择您要使用 Satellite 覆盖和管理的 Ansible 变量。
3. 导航到 **Default Behavior** 区域，再选择 **Override** 复选框。
4. 从 **Parameter Type** 中为验证选择值类型。例如，**字符串** 或 **布尔值** 变量。
5. 在 **Default Value** 字段中，输入在变量没有匹配项时要使用的默认值。
6. 可选：如果您不想以纯文本显示 Ansible 变量，请选择 **Hidden Values** 复选框，以在 Satellite Web UI 中以星号形式显示变量的内容。
7. 要保存覆盖设置，点 **Submit**。

要使用 Ansible 变量，请将变量作为参数添加到主机或主机组中，或者将变量添加为全局参数。

对于主机组：

1. 在 Satellite Web UI 中，进入 **Configure > Host Groups**，然后选择要使用的主机组。
2. 单击 **Parameters** 选项卡，然后在 **主机组参数** 区域中，单击 **Add Parameter**。
3. 在 **Name** 字段中，添加 Ansible 变量名称。
4. 从 **Type** 列表，选择用于验证的变量类型。
5. 在 **Value** 字段中输入变量的值。

对于主机：

1. 在卫星 Web UI 中，导航到 **Hosts > All Hosts**，然后在您要使用的主机上点击 **Edit** 按钮。
2. 单击 **Parameters** 选项卡，然后在 **Host Parameters** 区域中点击 **Add Parameter**。
3. 在 **Name** 字段中，添加 Ansible 变量名称。
4. 从 **Type** 列表，选择用于验证的变量类型。
5. 在 **Value** 字段中输入变量的值。

将添加为全局参数：

1. 在 Satellite Web UI 中，导航到 **Configure > Global Parameters**，然后点 **Create Parameter**。
2. 在 **Name** 字段中，添加 Ansible 变量名称。
3. 从 **Type** 列表，选择用于验证的变量类型。
4. 在 **Value** 字段中输入变量的值。

5. 可选：如果您不想以纯文本显示 Ansible 变量，请选择 **Hidden Values** 复选框，以在 Satellite Web UI 中以星号形式显示 变量的内容。

1.4. ADDING RED HAT ENTERPRISE LINUX SYSTEM ROLES

Red Hat Enterprise Linux 系统角色是一个远程管理 Red Hat Enterprise Linux 服务器的配置接口。您可以使用 Red Hat Enterprise Linux 系统角色在 Satellite 中添加 Ansible 角色。在卫星中使用 Ansible 角色可以加快配置更快、更轻松地进行配置。

一些 Red Hat Enterprise Linux 系统角色的支持级别可能只是 技术预览。有关 Red Hat Enterprise Linux 系统角色的支持级别和常规信息的最新信息，请参阅 [Red Hat Enterprise Linux 系统角色](#)。

在订阅 Extras 频道前，请查看 [Red Hat Enterprise Linux Extras 产品生命周期](#) 文档。

流程

1. 确保已启用 **rhel-7-server-extras-rpms** 存储库。

```
# subscription-manager repos --enable=rhel-7-server-extras-rpms
```

2. 安装 **rhel-system-roles** 软件包。

```
# satellite-maintain packages install rhel-system-roles
```

rhel-system-roles 软件包会下载到 `/usr/share/ansible/roles/`。在导入前，您可以查看并您对文件所做的任何修改。

3. 在 Satellite Web UI 中，导航到 **Configure > Roles**，再单击包含您要导入的角色的 Capsule。
4. 从 Ansible 角色列表中，选择您要导入的角色的复选框，然后单击 **Update**。

现在，您可以将 Ansible 角色分配到主机或主机组。如需更多信息，请参阅 [配置 Satellite 中的 Ansible 角色到现有主机](#) 以使用 Ansible。

您还可以通过将这些角色中包含的模块添加到 Ansible 作业模板，将它们添加到 Ansible playbook 中。您必须在作业模板中包含 **hosts:all** 行。如需更多信息，请参阅 [Red Hat Enterprise Linux\(RHEL\)系统角色](#)。

第 2 章 使用 ANSIBLE 角色在卫星主机上 AUTOMATE REPETITIVE 任务

2.1. 将 ANSIBLE 角色分配给现有主机

您可以使用 Ansible 角色来远程管理 Red Hat Enterprise Linux 8、7 和 6.9 或更高版本。

先决条件

- 确保已配置了并导入的 Ansible 角色。

流程

1. 在 Satellite Web UI 中，导航到 **Hosts > All Hosts**。
2. 在您要分配 Ansible 角色的主机上，单击 **Edit**。
3. 选择 **Ansible Roles** 选项卡，然后在 **All items** 列表中选择，搜索要添加的角色。
4. 选择您要添加的角色，然后单击箭头图标，将角色移到 **Selected items** 列表中。
5. 点 **Submit**。

将 Ansible 角色分配到主机后，您可以使用 Ansible 进行远程执行。如需更多信息，[请参阅分发用于远程执行的 SSH 密钥](#)。

Overriding Parameter 变量

在 **Parameters** 选项卡中，点 **Add Parameter** 添加您要在运行时传递给作业模板的任何参数变量。这包括您要与主机关联的所有 Ansible playbook 参数和主机参数。要将参数变量与 Ansible 作业模板一起使用，您必须添加 **Host Parameter**。

2.2. 在主机上运行 ANSIBLE 角色

您可以通过 Satellite Web UI 在主机上运行 Ansible 角色。

先决条件

- 您必须将部署配置为运行 Ansible 角色。如需更多信息，[请参阅配置 Satellite 中的 Deployment 来运行 Ansible 角色，以使用 Ansible](#)。
- 您必须将 Ansible 角色分配到主机。

流程

1. 在 Satellite Web UI 中，导航到 **Hosts > All Hosts**。
2. 选择包含您要运行的 Ansible 角色的主机的复选框。
3. 在 **Select Action** 列表中，选择 **Play Ansible roles**。

您可以在 **Run Ansible roles** 页面上查看 Ansible 作业的状态。要重新运行作业，请点击 **Rerun** 按钮。

2.3. 将 ANSIBLE 角色分配到主机组

您可以使用 Ansible 角色来远程管理 Red Hat Enterprise Linux 8、7 和 6.9 或更高版本。

先决条件

- 您必须将部署配置为运行 Ansible 角色。如需更多信息，[请参阅配置 Satellite 中的 Deployment 来运行 Ansible 角色，以使用 Ansible。](#)

流程

1. 在 Satellite Web UI 中，进入 **Configure > Host Groups**。
2. 在主机组列表中，点您要向其添加 Ansible 角色的主机组名称。
3. 选择 **Ansible Roles** 选项卡，然后在 **All items** 列表中选择，搜索要添加的角色。
4. 选择您要添加的角色，然后单击箭头图标，将角色移到 **Selected items** 列表中。
5. 点 **Submit**。

2.4. 在主机组上运行 ANSIBLE 角色

您可以通过卫星 Web UI 在主机组上运行 Ansible 角色。

先决条件

- 您必须将部署配置为运行 Ansible 角色。如需更多信息，[请参阅配置 Satellite 中的 Deployment 来运行 Ansible 角色，以使用 Ansible。](#)
- 您必须将 Ansible 角色分配到主机组。
- 您的主机组中必须至少有一个主机。

流程

1. 在 Satellite Web UI 中，进入 **Configure > Host Groups**。
2. 从主机组的 **Actions** 列中的列表，选择 **Run all Ansible roles**。

您可以在 **Run Ansible roles** 页面上查看 Ansible 作业的状态。要重新运行作业，请点击 **Rerun** 按钮。

2.5. 在检查模式下运行 ANSIBLE 角色

您可以通过 Satellite Web UI 以检查模式运行 Ansible 角色。

先决条件

- 您必须将部署配置为运行 Ansible 角色。如需更多信息，[请参阅配置 Satellite 中的 Deployment 来运行 Ansible 角色，以使用 Ansible。](#)
- 您必须将 Ansible 角色分配到主机组。
- 您的主机组中必须至少有一个主机。

流程

1. 在 Satellite Web UI 中，导航到 **Hosts > All Hosts**。
2. 对于您要启用检查模式的主机，点 **Edit**。
3. 在 **Parameters** 选项卡中，确保主机具有名为 **ansible_roles_check_mode** 的参数，类型为 **boolean**。
4. **点 Submit。**

第 3 章 配置和设置远程作业

使用本节作为配置 **Satellite** 在远程主机上执行作业的指南。

要应用到远程主机的任何命令都必须定义为作业模板。定义了作业模板后，您可以多次执行它。

3.1. 关于在主机上运行作业

您可以使用 **shell** 脚本或 **Ansible** 任务和 **playbook** 从胶囊远程运行作业。这称为远程执行。

对于您创建的自定义 **Ansible** 角色，或者您下载的角色，您必须安装包含 **Capsule** 基础操作系统上角色的软件包。在使用 **Ansible** 角色之前，您必须将角色从安装它们的胶囊导入到卫星中。

通信通过胶囊服务器进行，这意味着卫星服务器不需要直接访问目标主机，并且可以扩展来管理多个主机。远程执行使用必须在目标主机上启用并运行的 **SSH** 服务。确保远程执行胶囊能够访问目标主机上的端口 **22**。

卫星使用 **ERB** 语法作业模板。如需更多信息，[请参阅管理主机指南中的模板编写参考](#)。

默认情况下包含了几个用于 **shell** 脚本和 **Ansible** 的作业模板。如需更多信息，[请参阅设置作业模板](#)。



注意

任何胶囊服务器基础操作系统都是卫星服务器的内部胶囊的客户端，因此本节适用于与卫星服务器连接的任何类型的主机，包括胶囊。

您可以一次在多个主机上运行作业，您可以使用命令中的变量对运行的作业进行更精细的控制。您可以使用主机事实和参数来填充变量值。

另外，您可以在运行命令时为模板指定自定义值。

如需更多信息，[请参阅执行远程作业](#)。

3.2. 远程执行 workflow

当您为每个主机在主机上运行远程作业时，卫星将执行以下操作来查找要使用的远程执行胶囊。

卫星只搜索启用了 **Ansible** 功能的胶囊。

1. *卫星找到选中了 **Remote execution** 复选框的主机接口。*
2. *卫星找到这些接口的子网。*
3. *卫星找到分配给这些子网的远程执行胶囊。*
4. *从这一组胶囊中，**Satellite** 选择具有最少数量的运行作业的胶囊。这样，卫星可确保作业负载在远程执行胶囊之间平衡。*
5. *如果卫星没有在这个阶段找到远程执行胶囊，如果启用了 **Fallback 到 Any Capsule** 设置，则卫星会添加另一组 **Capsules** 来选择远程执行胶囊。**Satellite** 从分配给主机的以下类型的胶囊中选择最轻便加载的胶囊：*
 - *分配给主机子网的 **DHCP、DNS 和 TFTP** 胶囊*
 - *分配给主机的域的 **DNS** 胶囊*
 - *分配给主机的 **realm** 的 **realm Capsule***
 - ***Puppet Master Capsule***
 - ***Puppet CA Capsule***
 - ***OpenSCAP Capsule***

6.

如果 Satellite 没有在这个阶段找到远程执行胶囊，如果启用了 **Enable Global Capsule** 设置，则卫星从主机的组织和位置中所有胶囊中的一系列上选加载的远程执行胶囊，以执行远程作业。

3.3. 远程执行的权限

您可以控制哪些用户可在您的基础架构中运行哪些作业，包括他们可以目标的主机。远程执行功能提供了两个内置角色：

- **远程执行管理器**：此角色允许访问所有远程执行功能。
- **远程执行用户**：此角色仅允许运行作业；它不提供修改作业模板的权限。

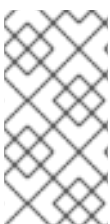
您可以克隆 **Remote Execution User** 角色，并自定义其过滤器以增加粒度。如果您使用 **view_job_templates** 权限调整过滤器，用户只能根据匹配的作业模板查看和触发作业。您可以使用 **view_hosts** 和 **view_smart_proxies** 权限来限制哪些主机或胶囊对角色可见。

execute_template_invocation 权限是一个特殊权限，在执行作业开始前立即检查。此权限定义您可以在特定主机上运行的作业模板。这在指定权限时具有更大的粒度。有关使用角色和权限的更多信息，请参阅 [管理 Red Hat Satellite 中的创建和管理角色](#)。

以下示例显示了 **execute_template_invocation** 权限的过滤器：

```
name = Reboot and host.name = staging.example.com
name = Reboot and host.name ~ *.staging.example.com
name = "Restart service" and host_group.name = webservers
```

本例中的第一行允许用户将 **reboot** 模板 应用到一个所选主机。第二行定义名称以 **.staging.example.com** 结尾的主机池。第三行将模板绑定到主机组。



注意

分配给用户的权限可能会随时间而变化。如果用户已调度一些作业以在以后运行，并且权限已改变，这可能会导致执行失败，因为在作业执行前会立即检查权限。

3.4. 创建作业模板

使用此流程创建作业模板。要使用 CLI 而不是 Web UI，请参阅 [CLI 过程](#)。

流程

1. 进入 **Hosts > Job templates**。
2. 单击 **New Job Template**。
3. 单击 **Template** 选项卡，并在 **Name** 字段中输入作业模板的唯一名称。
4. 选择 **Default** 使模板可用于所有组织和位置。
5. 直接在模板编辑器中创建模板，或通过单击 **Import** 从文本文件上传。
6. 可选：在 **Audit Comment** 字段中添加有关更改的信息。
7. 单击 **Job** 选项卡，然后在 **Job category** 字段中输入您自己的类别，或者从 [Default Job Template Categories](#) 中列出的默认类别中选择。
8. 可选：在 **Description Format** 字段中输入描述模板。例如，安装软件包 `%{package_name}`。您还可以在模板中使用 `%{template_name}` 和 `%{job_category}`。
9. 在 **Provider Type** 列表中，为 **shell** 脚本选择 **SSH**，为 **Ansible 任务或 playbook** 选择 **Ansible**。
10. 可选：在 **Timeout to kill** 字段中，输入超时值来终止作业（如果未完成）。
11. 可选：点 **Add Input** 来定义输入参数。执行作业时，不需要在模板中定义参数。例如，请参阅 [帮助](#) 选项卡。
12. 可选：单击 **Foreign 输入集** 来在此作业中包含其他模板。

13. 可选：在 **Effective 用户** 区域中，如果命令无法使用默认的 `remote_execution_effective_user` 设置，则配置用户。
14. 可选：如果此模板是要包含在其他模板的代码片段，点 **Type** 选项卡并选择 **Snippet**。
15. 单击 **Location** 选项卡，再添加您要使用模板的位置。
16. 单击 **Organizations** 选项卡，再添加您要使用模板的组织。
17. 点 **Submit** 保存您的更改。

您可以通过在模板语法中包含其他模板来扩展和自定义作业模板。如需更多信息，请参阅 **管理主机指南** 中的附加部分。

CLI 过程

1. 要使用 `template-definition` 文件创建作业模板，请输入以下命令：

```
# hammer job-template create \
--file "path_to_template_file" \
--name "template_name" \
--provider-type SSH \
--job-category "category_name"
```

3.5. 在 SATELLITE 中将 FALLBACK 配置为 ANY CAPSULE REMOTE EXECUTION SETTING

您可以启用 **Fallback 到 Any Capsule** 设置，以配置卫星，从分配给主机的 **Capsules** 列表中搜索远程执行胶囊。如果您需要在没有配置子网的主机上运行远程作业，或者如果主机的子网被分配给没有启用远程执行功能的胶囊，这将非常有用。

如果启用了 **Fallback 到 Any Capsule** 设置，卫星会添加另一组胶囊，以从中选择远程执行胶囊。Satellite 还从分配给主机的所有胶囊中选择最轻便载入的胶囊，如下所示：

- 分配给主机子网的 **DHCP**、**DNS** 和 **TFTP** 胶囊

- **分配给主机的域的 DNS 胶囊**
- **分配给主机的 realm 的 realm Capsule**
- **Puppet Master Capsule**
- **Puppet CA Capsule**
- **OpenSCAP Capsule**

流程

1. 在 Satellite Web UI 中，导航到 **Administer > Settings**。
2. 单击 **RemoteExecution**。
3. 将 **Fallback** 配置为 **Any Capsule** 设置。

CLI 过程

在卫星上输入 `hammer settings set` 命令，将 **Fallback** 配置为 **Any Capsule** 设置。例如，要将值设为 `true`，请输入以下命令：

```
# hammer settings set --name=remote_execution_fallback_proxy --value=true
```

3.6. 在 SATELLITE 中配置全局胶囊远程执行设置

默认情况下，无论胶囊是否分配给主机子网，卫星将搜索主机上的远程执行胶囊。如果要限制搜索到分配给主机子网的胶囊，可以禁用 **Enable Global Capsule** 设置。

如果启用了 **Enable Global Capsule** 设置，卫星添加另一组胶囊，以便从中选择远程执行胶囊。卫星还从主机的组织和位置集合中选择最轻量加载的远程执行胶囊，以执行远程作业。

流程

1. 在 Satellite Web UI 中, 导航到 **Administer > Settings**。
2. 单击 **RemoteExecution**。
3. 配置 **Enable Global Capsule** 设置。

CLI 过程

- 在卫星上输入 **hammer settings set** 命令来配置 **Enable Global Capsule** 设置。例如, 要将值设为 **true**, 请输入以下命令:

```
# hammer settings set --name=remote_execution_global_proxy --value=true
```

3.7. 配置 SATELLITE 以使用备用目录对主机执行远程作业

Ansible 将自己的文件放在 **\$HOME/.ansible/tmp** 目录中, 其中 **\$HOME** 是远程用户的主目录。如果需要, 您可以选择设置不同的目录。

流程

1. 创建新目录, 如 **new_place** :
2. 从默认 **var** 目录中复制 **SELinux** 上下文:

```
# mkdir /remote_working_dir
```

```
# chcon --reference=/var /remote_working_dir
```

3. 配置系统:

```
# {foreman-installer} --foreman-proxy-plugin-ansible-working-dir _/remote_working_dir_
```

3.8. 为远程执行分发 SSH 密钥

要使用 SSH 密钥来对远程执行连接进行身份验证，您必须将公共 SSH 密钥从 Capsule 分发到您要管理的附加主机。确保启用了 SSH 服务并在主机上运行。配置任何网络或基于主机的防火墙，以启用对端口 22 的访问。

使用以下方法之一将公共 SSH 密钥从 Capsule 分发到目标主机：

1. [第 3.9 节 “手动将 SSH 密钥分发到远程执行”](#)。
2. [第 3.10 节 “使用 Satellite API Obtain SSH Keys for Remote Execution”](#)。
3. [第 3.11 节 “在置备过程中将 Kickstart 模板配置为分发 SSH 密钥”](#)。
4. 对于新的 Satellite 主机，您可以使用全局注册模板在注册过程中将 SSH 密钥部署到卫星主机。如需更多信息，请参阅使用 [全局注册模板将主机注册到 Red Hat Satellite](#)。

卫星将用于远程执行功能的 SSH 密钥分发到从 Satellite 调配的主机。

如果主机在 Amazon Web Services 上运行，请启用密码身份验证。如需更多信息，请参阅 <https://aws.amazon.com/premiumsupport/knowledge-center/new-user-accounts-linux-instance>。

3.9. 手动将 SSH 密钥分发到远程执行

要手动分发 SSH 密钥，请完成以下步骤：

流程

1. 在 Capsule 上输入以下命令。对您要管理的每个目标主机重复此操作：

```
# ssh-copy-id -i ~foreman-proxy/.ssh/id_rsa_foreman_proxy.pub root@target.example.com
```

2. 要确认密钥已成功复制到目标主机，请在 Capsule 上输入以下命令：

```
# ssh -i ~foreman-proxy/.ssh/id_rsa_foreman_proxy root@target.example.com
```

3.10. 使用 SATELLITE API OBTAIN SSH KEYS FOR REMOTE EXECUTION

要使用 Satellite API 从 Capsule 下载公钥，请在每个目标主机上完成以下步骤。

流程

1. 在目标主机上，创建 `~/.ssh` 目录来存储 SSH 密钥：

```
# mkdir ~/.ssh
```

2. 从 Capsule 下载 SSH 密钥：

```
# curl https://capsule.example.com:9090/ssh/pubkey >> ~/.ssh/authorized_keys
```

3. 为 `~/.ssh` 目录配置权限：

```
# chmod 700 ~/.ssh
```

4. 为 `authorized_keys` 文件配置权限：

```
# chmod 600 ~/.ssh/authorized_keys
```

3.11. 在置备过程中将 KICKSTART 模板配置为分发 SSH 密钥

您可以在自定义 kickstart 模板中添加一个 `remote_execution_ssh_keys` 片段，以在置备期间将 SSH Keys 部署到主机中。卫星提供的 Kickstart 模板默认包括这个代码片段。因此，Satellite 在置备过程中将用于远程执行的 SSH 密钥复制到系统中。

流程

- 要在新置备主机中包含公钥，请在您使用的 Kickstart 模板中添加以下片段：

```
<%= snippet 'remote_execution_ssh_keys' %>
```

3.12. 为 KERBEROS TICKET GRANTING TICKETS 配置 KEYTAB

使用这个流程将 Satellite 配置为使用 keytab 获取 Kerberos ticket 授权票据。如果您没有设置

keytab, 则必须手动检索票据。

流程

1.

查找 foreman-proxy 用户的 ID :

```
# id -u foreman-proxy
```

2.

修改 umask 值, 使新文件的权限为 600 :

```
# umask 077
```

3.

为 keytab 创建目录 :

```
# mkdir -p "/var/kerberos/krb5/user/USER_ID"
```

4.

创建 keytab 或将现有 keytab 复制到目录中 :

```
# cp your_client.keytab /var/kerberos/krb5/user/USER_ID/client.keytab
```

5.

将目录所有者更改为 foreman-proxy 用户 :

```
# chown -R foreman-proxy:foreman-proxy "/var/kerberos/krb5/user/USER_ID"
```

6.

确保 keytab 文件为只读 :

```
# chmod -wx "/var/kerberos/krb5/user/USER_ID/client.keytab"
```

7.

恢复 SELinux 上下文 :

```
# restorecon -RvF /var/kerberos/krb5
```

3.13. 为远程执行配置 KERBEROS 身份验证

您可以使用 Kerberos 身份验证在 Satellite 主机上建立用于远程执行的 SSH 连接。

先决条件

- 在 Kerberos 服务器中注册 Satellite 服务器
- 在 Kerberos 服务器中注册 Satellite 目标主机
- 配置并初始化 Kerberos 用户帐户以进行远程执行
- 确保 Satellite 上的 foreman-proxy 用户具有有效的 Kerberos ticket 授权票据

流程

1. 要为远程执行安装并启用 Kerberos 验证，请输入以下命令：

```
# satellite-installer --scenario satellite \
--foreman-proxy-plugin-remote-execution-ssh-ssh-kerberos-auth true
```

2. 要编辑用于远程执行的默认用户，在 Satellite Web UI 中，导航到 **Administer > Settings** 并点 **RemoteExecution** 选项卡。在 **SSH User** 行中，编辑第二列并添加 Kerberos 帐户的用户名。
3. 导航到 **remote_execution_effective_user**，再编辑第二列来添加 Kerberos 帐户的用户名。

要确认 Kerberos 身份验证已可供使用，请在主机上运行远程作业。

3.14. 设置作业模板

Satellite 提供可用于执行作业的默认作业模板。要查看作业模板列表，请导航到 **Hosts > Job templates**。如果要在不进行任何更改的情况下使用模板，请 [执行远程作业](#)。

您可以使用默认模板作为您自己的基础。默认任务模板已锁定以进行编辑。克隆模板并编辑克隆。

流程

1. 要克隆模板（在 **Actions** 列中），请选择 **Clone**。
2. 为克隆输入唯一名称，点 **Submit** 保存更改。

作业模板使用嵌入式 Ruby(ERB)语法。有关编写模板的更多信息，请参阅 [管理主机](#) 指南中的模板编写参考。

Ansible 注意事项

要创建 Ansible 作业模板，请使用以下步骤而不是 ERB 语法，请使用 YAML 语法。使用 `---` 开始模板。您可以将 Ansible playbook YAML 文件嵌入到作业模板正文中。您还可以添加 ERB 语法，以自定义 YAML Ansible 模板。您还可以在 Satellite 中导入 Ansible playbook。如需更多信息，请参阅 [管理主机](#) 指南中的同步存储库模板。

参数变量

在运行时，作业模板可以接受您为主机定义的参数变量。请注意，只有主机编辑页面中的 **Parameters** 标签页中可见的参数才能用作作业模板的输入参数。如果您不希望 Ansible 作业模板在运行时接受参数变量，在 Satellite Web UI 中导航到 **Administer > Settings**，然后单击 **Ansible** 选项卡。在 **顶级 Ansible 变量** 行中，将 **Value** 参数更改为 **No**。

3.15. 执行远程作业

您可以对一个或多个主机执行基于作业模板的作业。

要使用 CLI 而不是 Web UI，请参阅 [CLI 过程](#)。

流程

1. 进入 **Hosts > All Hosts** 并选择您要在其上执行远程作业的目标主机。您可以使用搜索字段来过滤主机列表。
2. 在 **Select Action** 列表中，选择 **Schedule Remote Job**。
3. 在 **Job invocation** 页面中，定义主作业设置：

4. 选择要使用的 **Job category** 和 **Job 模板**。
5. 可选：在 **Bookmark** 列表中选择一個存储的搜索字符串来指定目标主机。
6. 可选：输入搜索查询来限制目标主机。连续到 行显示受您的查询影响的主机数。使用刷新按钮重新计算更改查询后的数字。preview 图标列出了目标主机。
7. 剩余的设置取决于所选的作业模板。如需有关在模板中添加自定义参数的信息，请参阅创建作业模板。https://access.redhat.com/documentation/zh-cn/red_hat_satellite/6.10/html-single/managing_hosts/index#creating-a-job-template_managing-hosts
8. 可选：要为作业配置高级设置，请点击 **Display advanced fields**。一些高级设置取决于作业模板，以下设置是常规的：
 - 有效的用户 定义了执行作业的用户，默认为 **SSH 用户**。
 - 并发级别 定义了一次执行的最大作业数，这可在大量主机上执行作业时防止超载系统资源。
 - 超时（以秒为单位）定义作业应该被终止的时间间隔（如果作业尚未完成）。在定义的时间间隔期间无法启动的任务（例如，如果上一任务需要很长时间才能完成），则会取消。
 - 查询类型定义了搜索查询何时被评估。这有助于使查询保持最新状态以进行调度任务。
 - 执行顺序 决定了在主机上执行该作业的顺序：字母顺序或随机。

通过 并发级别 和 超时 以中断设置，您可以定制作业执行，以适应基础架构硬件和需求。
9. 要立即运行作业，请确保 **Schedule** 设置为 **Execute now**。您还可以定义一个一次性作业，或者设置周期性作业。对于周期性任务，您可以定义开始和结束日期、运行次数和频率。您还可以使用 **cron** 语法来定义重复操作。有关 **cron** 的详情，请查看 **Red Hat Enterprise Linux 7 系统管理员指南** 中的 "**自动系统任务**" 部分。

10. 点 **Submit**。这将显示 **Job Overview** 页面，以及作业完成时，还显示作业的状态。

CLI 过程

- 在 **Satellite** 中输入以下命令：

```
# hammer settings set --name=remote_execution_global_proxy --value=false
```

要使用自定义参数执行远程作业，请完成以下步骤：

1. 查找您要使用的作业模板 ID：

```
# hammer job-template list
```

2. 显示模板详情以查看模板所需的参数：

```
# hammer job-template info --id template_ID
```

3. 使用自定义参数执行远程作业：

```
# hammer job-invocation create \  
--job-template "template_name" \  
--inputs key1="value",key2="value",... \  
--search-query "query"
```

使用定义主机的过滤器表达式替换 **query**，例如 **"name ~ rex01"**。有关使用 **hammer** 执行远程命令的更多信息，请输入 **hammer job-template --help** 和 **hammer job-invocation --help**。

3.16. 监控作业

您可以在作业运行时监控作业进度。这对可能需要的任何故障排除都有帮助。

Ansible 作业在 100 个主机上运行，因此您无法取消在特定主机上运行的作业。只有在 **Ansible** **playbook** 在批处理中的所有主机中运行后，作业才会完成。

流程

1. 导航到 **Job** 页面。如果您使用 **Execute now** 设置触发作业，则会自动显示此页面。要监控调度的作业，请导航到 **Monitor > Jobs** 并选择您要检查的作业运行。
2. 在 **Job** 页面上，单击 **Hosts** 选项卡。这将显示运行作业的主机列表。
3. 在 **Host** 列中，单击您要检查的主机的名称。这将显示 **Commands** 页面的详细信息，您可以在其中实时监控作业执行。
4. 随时单击 **Back to Job**，以返回到 **Job Details** 页面。

CLI 过程

要在作业运行时监控作业进度，请完成以下步骤：

1. 查找作业的 ID：

```
# hammer job-invocation list
```
2. 监控作业输出：

```
# hammer job-invocation output \  
--id job_ID \  
--host host_name
```
3. 可选：要取消作业，请输入以下命令：

```
# hammer job-invocation cancel \  
--id job_ID
```

第 4 章 集成 RED HAT SATELLITE 和 ANSIBLE TOWER

您可以集成 Red Hat Satellite 和 Ansible Tower，以使用卫星服务器作为 Ansible Tower 的动态清单来源。

您也可以从主机或 Ansible Tower 使用置备回调功能在由 Satellite 管理的主机上运行 playbook。从卫星服务器置备新主机时，您可以使用置备回调功能来触发从 Ansible Tower 运行的 playbook。playbook 配置以下 Kickstart 部署的主机。

4.1. 将卫星服务器添加到 ANSIBLE TOWER 中作为动态清单 ITEM

要将卫星服务器作为动态清单项添加到 Ansible Tower 中，您必须为 Ansible Tower 上的卫星服务器用户创建凭据，添加 Ansible Tower 用户到凭据，再配置清单源。

先决条件

- 如果您的 Satellite 部署非常大，例如，使用非管理员用户管理数千台主机可能会对性能造成负面影响，因为授权检查期间出现问题。对于大型部署，请考虑使用管理员用户。
- 对于非管理员用户，必须将 Ansible Tower 清单 Reader 角色分配给 Satellite Server 用户。有关管理用户、角色和权限过滤器的更多信息，请参阅 [管理 Red Hat Satellite 中的创建和管理角色](#)。
- 您必须在相同的网络或子网上托管卫星服务器和 Ansible Tower。

流程

1. 在 Ansible Tower Web UI 中，为您的 Satellite 创建凭据。有关创建凭证的更多信息，请参阅 [Ansible Tower 用户指南中的添加新凭据和 Red Hat Satellite 6 凭据](#)。<http://docs.ansible.com/ansible-tower/latest/html/userguide/credentials.html#add-a-new-credential>

表 4.1. Satellite 凭证

凭证类型：	Red Hat Satellite 6
Satellite 6 URL：	https://satellite.example.com
用户名：	卫星用户的用户名及集成角色。

凭证类型：	Red Hat Satellite 6
密码：	Satellite 用户的密码。

2. 将 Ansible Tower 用户添加到新凭据。有关将用户添加到凭证的更多信息，请参阅 [Ansible Tower 用户指南](#) 中的使用凭证。
3. 添加新清单。有关更多信息，请参阅 [Ansible Tower 用户指南](#) 中的 [添加新清单](#)。
4. 在新清单中，添加卫星服务器作为清单源，并指定以下清单源选项：如需更多信息，请参阅 [Ansible Tower 用户指南](https://docs.ansible.com/ansible-tower/latest/html/userguide/inventories.html#add-source) 中的添加源。<https://docs.ansible.com/ansible-tower/latest/html/userguide/inventories.html#add-source>

表 4.2. 清单源选项

源	Red Hat Satellite 6
凭证	为 Satellite 服务器创建的凭证。
覆盖	选择
覆盖变量	选择
启动时更新	选择
缓存超时	90

5. 确保您同步您添加的源。

4.2. 为主机配置部署回调

在卫星中创建主机时，您可以使用 Ansible Tower 运行 `playbook` 来配置新创建的主机。这在 Ansible Tower 中称为 `置备回调`。

置备回调功能会触发从 Ansible Tower 运行 `playbook`，作为置备过程的一部分。`playbook` 在 Kickstart 部署后配置主机。

有关置备回调的更多信息，请参阅 [Ansible Tower 用户指南中的 置备回调](#)。

在 **Satellite 服务器**中，**Kickstart Default** 和 **Kickstart Default Finish** 模板包括三个片断：

1. `ansible_provisioning_callback`
2. `ansible_tower_callback_script`
3. `ansible_tower_callback_service`

您可以将参数添加到主机或主机组中，以提供这些代码片段在新创建的主机上运行 **Ansible playbook** 的凭据。

先决条件

在配置置备回调前，您必须在 **Ansible Tower** 中添加 **Satellite** 作为动态清单。如需更多信息，请参阅 [集成 Satellite 和 Ansible Tower](#)。

在 **Ansible Tower web UI** 中，您必须完成以下任务：

1. 为您的新主机创建机器凭证。确保您在凭证中输入相同的密码，以分配给您在 **Satellite** 中创建的主机。有关更多信息，请参阅 [Ansible Tower 用户指南中的 添加新凭据](#)。
2. 创建一个项目。有关更多信息，请参阅 [Ansible Tower 用户指南中的 项目](#)。
3. 将作业模板添加到您的项目中。有关更多信息，请参阅 [Ansible Tower 用户指南中的 作业模板](#)。
4. 在作业模板中，您必须启用置备回调，生成主机配置密钥，并记下作业模板的 `template_ID`。如需有关作业模板的更多信息，请参阅 [Ansible Tower 用户指南中的 作业模板](#)。

流程

1. 在 Red Hat Satellite Web UI 中, 进入 **Configure > Host Group**。
2. 创建主机组或编辑现有的主机组。
3. 在 Host Group 窗口中, 单击 **Parameters** 选项卡。
4. 点 **Add Parameter**。
5. 为每个新参数输入以下信息 :

表 4.3. 主机参数

名称	值	描述
ansible_tower_provisioning	true	启用部署回调。
ansible_tower_fqdn	<i>tower.example.com</i>	Ansible Tower 的完全限定域名(FQDN)。不要添加 https , 因为这已附加了 Ansible Tower。
ansible_job_template_id	<i>template_ID</i>	模板的 URL 中可找到的置备模板的 ID : /templates/job_template/5 。
ansible_host_config_key	<i>config_KEY</i>	您的作业模板在 Ansible Tower 中生成的主机配置密钥。

6. 点 **Submit**。
7. 使用主机组创建主机。
8. 在新主机上, 输入以下命令启动 **ansible-callback** 服务 :


```
# systemctl start ansible-callback
```
9. 在新主机上, 输入以下命令输出 **ansible-callback** 服务的状态 :

```
# systemctl status ansible-callback
```

如果命令返回以下输出，则正确配置置备回调：

```
SAT_host systemd[1]: Started Provisioning callback to Ansible Tower...
```

手动置备回调

您可以使用主机的置备回调 URL 和主机配置密钥来调用 Ansible Tower。例如：

```
# curl -k -s --data curl --insecure --data host_config_key=my_config_key \  
https://tower.example.com/api/v2/job_templates/8/callback/
```

在进入置备回调 URL 时，请确保使用 **https**。

这会触发针对主机在模板中指定的 **playbook** 运行。

附录 A. 作业模板示例和扩展

使用此部分作为帮助修改、自定义和扩展作业模板以满足您的要求的参考。

A.1. 自定义模板

创建作业模板时，您可以在模板编辑器字段中包含现有的模板。这样，您可以组合模板，或者从一般模板中创建更具体的模板。

以下模板组合了在 Red Hat Enterprise Linux 系统中安装和启动 httpd 服务的默认模板：

```
<%= render_template 'Package Action - SSH Default', :action => 'install', :package => 'httpd' %>
<%= render_template 'Service Action - SSH Default', :action => 'start', :service_name => 'httpd' %>
```

以上模板直接指定 rendered 模板的参数值。也可以使用 input () 方法，允许用户在作业执行上为呈现的模板定义输入。例如，您可以使用以下语法：

```
<%= render_template 'Package Action - SSH Default', :action => 'install', :package => input("package") %>
```

使用以上模板，您必须从呈现的模板导入参数定义。为此，请导航到 Jobs 选项卡，点 Add Foreign Input Set，然后从 Target 模板列表中选择呈现的模板。您可以导入所有参数或指定一个用逗号分开的列表。

A.2. 默认任务模板类别

作业模板类别	描述
软件包	用于执行与软件包相关的操作的模板。安装、更新和删除操作默认包含。
Puppet	用于执行 Puppet 的模板在目标主机上运行。
Power	用于执行与电源相关的操作的模板。默认包括重启和关闭操作。
命令	用于在远程主机上执行自定义命令的模板。
服务	用于执行服务相关操作的模板。默认包括 start、stop、restart 和 status 操作。

作业模板类别	描述
Katello	用于执行内容相关操作的模板。这些模板主要用于卫星 Web UI 的不同部分（例如，用于内容主机的批量操作 UI），但可以单独用来执行勘误表安装等操作。

A.3. RESTORECON 模板示例

本例演示了如何创建一个名为 **Run Command - restorecon** 的模板，它恢复目标主机上所选目录中所有文件的默认 SELinux 上下文。

1. 进入 **Hosts > Job templates**。单击 **New Job Template**。
2. 在 **Name** 字段中输入 **Run Command - restorecon**。选择 **Default** 使模板可供所有机构使用。在模板编辑器中添加以下文本：

```
restorecon -RvF <%= input("directory") %>
```

在作业调用过程中，`<%= input("directory") %>` 字符串被用户定义的目录替代。
3. 在 **Job** 选项卡上，将 **Job category** 设置为 **Commands**。
4. 单击 **Add Input** 以允许作业自定义。在 **Name** 字段中输入 **目录**。输入名称必须与模板编辑器中指定的值匹配。
5. 点 **Required**，以便在没有用户指定的参数的情况下无法执行该命令。
6. 从 **Input type** 列表中选择 **User** 输入。在任务调用期间输入描述，例如 **restorecon 的目标目录**。
7. 点 **Submit**。

如需了解如何 [根据此模板执行作业的信息](#)，请参阅在多个主机上执行 **restorecon** 模板。

A.4. 渲染 RESTORECON 模板

本例演示了如何创建从 Run 命令派生的模板 - restorecon 模板在 [Example restorecon Template](#) 中创建的。此模板不需要在作业执行时用户输入，它将在目标主机上的 /home/ 目录下恢复所有文件中的 SELinux 上下文。

按照 [设置作业模板](#) 所述创建新模板，并在模板编辑器中指定以下字符串：

```
<%= render_template("Run Command - restorecon", :directory => "/home") %>
```

A.5. 在多个主机上执行 RESTORECON 模板

本例演示了如何根据在多个主机上 [Example restorecon Template](#) 中创建的模板来运行作业。该作业会在 /home/ 目录下恢复所有文件中的 SELinux 上下文。

1. 进入 Hosts > All hosts 并选择目标主机。从 Select Action 列表中，选择 **Schedule Remote Job**。
2. 在 Job invocation 页面中，选择 **Commands** 作业类别和 **Run Command - restorecon** 作业模板。
3. 在 目录 字段中键入 /home。
4. 将 **Schedule** 设置为 **Execute now**。
5. 点 **Submit**。您会进入 Job invocation 页面，从中可以监控作业执行的状态。

A.6. 模板中包括 POWER ACTIONS

本例演示了如何为执行电源操作（如 reboot）设置作业模板。此流程可防止 Satellite 在重新引导时解释断开连接异常，因此，远程执行作业可以正常工作。

按照 [设置作业模板](#) 所述创建新模板，并在模板编辑器中指定以下字符串：

```
<%= render_template("Power Action - SSH Default", :action => "restart") %>
```