



Red Hat Ansible Automation Platform 2.4

Red Hat Ansible Automation Platform 自动化网 格用于基于 Operator 的安装

以云原生方式大规模自动化

Red Hat Ansible Automation Platform 2.4 Red Hat Ansible Automation Platform 自动化网格用于基于 Operator 的安装

以云原生方式大规模自动化

法律通告

Copyright © 2024 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

本指南演示了如何将自动化网格部署为基于 Operator 的 Ansible Automation Platform 环境的一部分。

目录

前言	3
对红帽文档提供反馈	4
第 1 章 规划基于 OPERATOR 的 RED HAT ANSIBLE AUTOMATION PLATFORM 环境中的自动化网格	5
1.1. 关于自动化网格	5
1.2. 控制和执行平面	5
第 2 章 基于 OPERATOR 的 RED HAT ANSIBLE AUTOMATION PLATFORM 的自动化网格	7
2.1. 先决条件	7
2.2. 设置用于自动化网格的虚拟机	7
2.3. 定义自动化网格节点类型	8
2.4. 创建实例组	12
2.5. 将实例关联到实例组	13
2.6. 在执行节点上运行作业	14
2.7. 为 OPENSIFT CONTAINER PLATFORM 部署拉取 SECRET	15
2.8. 删除实例	15

前言

感谢您对 Red Hat Ansible Automation Platform 的关注。Ansible Automation Platform 是一个商业产品，它可以帮助团队通过增加控制、知识、协调基于 Ansible 的环境来更好地管理多阶的复杂部署环境。

本指南帮助您了解在基于 Operator 的 Red Hat Ansible Automation Platform 安装中设置自动化网格后的要求和流程。本文档已更新，以包含 Ansible Automation Platform 最新版本的信息。

对红帽文档提供反馈

如果您对本文档有任何改进建议，或发现了任何错误，请通过 <https://access.redhat.com> 联系技术支持，以使用 **docs-product** 组件在 Ansible Automation Platform JIRA 项目中创建一个问题。

第 1 章 规划基于 OPERATOR 的 RED HAT ANSIBLE AUTOMATION PLATFORM 环境中的自动化网格

以下主题包含有助于在基于 Operator 的 Red Hat Ansible Automation Platform 环境中规划自动化网格部署的信息。本文档涵盖了在基于 Operator 的部署上设置自动化网格，如 Microsoft Azure 受管应用程序的 OpenShift Container Platform 和 Ansible Automation Platform。

1.1. 关于自动化网格

自动化网格是一个覆盖网络，旨在通过使用现有网络相互建立对等连接的节点，简化在大型且分散的 worker 集合中的工作分布。

Red Hat Ansible Automation Platform 2 使用自动化控制器和自动化中心替换 Ansible Tower 和隔离节点。自动化控制器通过其 UI、RESTful API、RBAC、工作流和 CI/CD 集成提供控制平面，而自动化网格则可用于设置、发现、更改或修改组成控制和执行层的节点。自动化网格对以下情况非常有用：

- 遍历困难的网络拓扑
- 将执行功能（运行 **ansible-playbook** 的机器）更接近您的目标主机

节点(control、hop 和 execution 实例)通过 receptor mesh 互连，组成一个虚拟网络。

自动化网格使用 TLS 加密进行通信，因此遍历外部网络（互联网或其他）的流量在传输中加密。

Automation mesh 引入了：

- 动态集群容量可以独立扩展，可让您以最少的停机时间创建、注册、组、取消组和取消注册节点。
- 控制和执行平面分离，可让您独立于 control plane 容量来缩放 playbook 执行容量。
- 对延迟具有弹性的部署选择，可在不中断的情况下重新配置，并在发生中断时动态重新路由以选择不同的路径。
- 包括符合联邦信息处理标准 (FIPS) 的双向多跃点网络通信可能性连接。

1.2. 控制和执行平面

实例组成相互通信的设备网络。它们是自动化网格的构建块。这些构建块充当网络拓扑中的节点。自动化网格利用唯一的节点类型来创建 **control** 和 **execution plane**。在设计自动化网格拓扑前，了解更多有关控制和执行平面及其节点类型的信息。

1.2.1. Control plane（控制平面）

除了项目更新和管理作业外，control plane 中的实例还运行持久的自动化控制器服务，如 web 服务器和任务分配程序。但是，在基于 Operator 的模型中，没有混合或控制节点。有容器组，它们组成在 Kubernetes 集群上运行的容器。组成 control plane。该 control plane 是部署 Red Hat Ansible Automation Platform 的 kubernetes 集群的本地。

1.2.2. 执行平面

执行平面由代表 control plane 执行自动化且没有控制功能执行的节点组成。hop 节点用于通信。执行平面中的节点仅运行用户空间作业，且可能在地理上将延迟较高的节点与控制平面分隔开。

- **执行节点** - 执行节点在 **ansible-runner** 下以 **podman** 隔离运行作业。此节点类型与隔离的节点类似。这是 execution plane 节点的默认节点类型。
- **hop 节点** 与跳过主机类似，hop 节点会将流量路由到其他执行节点。hop 节点无法执行自动化。

第 2 章 基于 OPERATOR 的 RED HAT ANSIBLE AUTOMATION PLATFORM 的自动化网格

在 Red Hat Ansible Automation Platform 的 OpenShift 部署中扩展自动化网格，可以使用自动化控制器 UI 的 **Instances** 资源动态添加或删除集群中的节点，而无需运行安装脚本。

实例充当网格拓扑中的节点。自动化网格允许您扩展自动化的空间。您启动作业的位置可能与 ansible-playbook 运行的位置不同。

要从自动化控制器 UI 管理实例，必须具有 System Administrator 或 System Auditor 权限。

通常，节点有更多处理器内核(CPU)和内存(RAM)，可以计划一次在该节点上运行。

如需更多信息，[请参阅自动控制器容量确定和作业影响](#)。

2.1. 先决条件

自动化网格依赖于在 Red Hat Enterprise Linux (RHEL)上运行的跃点和执行节点。您的 Red Hat Ansible Automation Platform 订阅可让您 10 个 Red Hat Enterprise Linux 许可证，该许可证可用于运行 Ansible Automation Platform 的组件。

有关 Red Hat Enterprise Linux 订阅的详情，请参考 Red Hat Enterprise Linux 文档中的 [注册系统和管理订阅](#)。

以下步骤准备 RHEL 实例以部署自动化网格。

1. 您需要一个 Red Hat Enterprise Linux 操作系统。网格中的每个节点都需要静态 IP 地址，或者自动化控制器可访问的 DNS 主机名。
2. 在继续操作前，请确保您具有 RHEL 虚拟机的最低要求。如需更多信息，请参阅 [Red Hat Ansible Automation Platform 系统要求](#)。
3. 在需要通信的远程网络中部署 RHEL 实例。有关创建虚拟机的详情，请参考 *Red Hat Enterprise Linux* 文档中的 [创建虚拟机](#)。请记住，以足够的方式扩展虚拟机的容量，以便您的提议的任务可以在它们上运行。
 - RHEL ISO 可以从 access.redhat.com 获取。
 - 可以使用来自 console.redhat.com 的镜像构建器构建 RHEL 云镜像。

2.2. 设置用于自动化网格的虚拟机

流程

1. SSH 到每个 RHEL 实例并执行以下步骤。根据您的网络访问和控制，可能需要 SSH 代理或其他访问模型。
使用以下命令：

```
ssh [username]@[host_ip_address]
```

例如，对于在 Amazon Web Services 上运行的 Ansible Automation Platform 实例。

```
ssh ec2-user@10.0.0.6
```

2. 创建或复制可用于从跃点节点连接到执行节点的 SSH 密钥。这可以是仅用于自动化网格配置的临时密钥，也可以是长期的密钥。后续步骤中使用 SSH 用户和密钥。
3. 使用 **baseos** 和 **appstream** 软件仓库启用 RHEL 订阅。Ansible Automation Platform RPM 存储库只能通过 `subscription-manager` 提供，不适用于 *Red Hat Update Infrastructure (RHUI)*。如果您试图使用其它 Linux 占用空间，包括带有 RHUI 的 RHEL，这会导致错误。

```
sudo subscription-manager register --auto-attach
```

如果您的帐户启用了简单内容访问，请使用：

```
sudo subscription-manager register
```

有关简单内容访问的更多信息，[请参阅开始使用简单内容访问](#)。

4. 启用 Ansible Automation Platform 订阅和正确的 Red Hat Ansible Automation Platform 频道：

```
# subscription-manager repos --enable ansible-automation-platform-2.4-for-rhel-8-x86_64-rpms for RHEL 8
```

```
# subscription-manager repos --enable ansible-automation-platform-2.4-for-rhel-9-x86_64-rpms for RHEL 9
```

5. 确定软件包为最新版本：

```
sudo dnf upgrade -y
```

6. 安装 `ansible-core` 软件包：

```
sudo dnf install -y ansible-core
```

2.3. 定义自动化网格节点类型

要扩展作业容量，请创建一个可以添加的独立 **执行节点**，与自动化控制器部署一起运行。这些执行节点不是自动化控制器 Kubernetes 集群的一部分。控制节点在集群连接中运行，并通过 Receptor 向执行节点提交工作。这些执行节点在自动化控制器中注册为类型 **执行实例**，这意味着它们仅用于运行作业，而不是分配工作或作为控制节点处理 Web 请求。

跃点节点 可以添加到自动化控制器和独立执行节点的 control plane 之间。这些跃点节点不是 Kubernetes 集群的一部分，并在自动化控制器中注册，作为类型跃点(**hop**)的实例，这意味着它们只会处理不同或更严格的网络中的入站和出站流量。

以下流程演示了如何为主机设置节点类型。

流程

1. 在导航面板中，选择 **Administration** → **Instances**。
2. 在 **Instances** 列表页面中，单击 **Add**。 **Create new Instance** 窗口将打开。

Instances

Create new Instance ↻

<p>Host Name *</p> <input type="text"/>	<p>Description</p> <input type="text"/>	<p>Instance State ⓘ</p> <div style="border: 1px solid #ccc; padding: 2px; background-color: #f0f0f0;">installed</div>
<p>Listener Port ⓘ</p> <input type="text"/>	<p>Instance Type *</p> <div style="border: 1px solid #ccc; padding: 2px;">Execution ▼</div>	<p>Options</p> <p><input checked="" type="checkbox"/> Enable Instance ⓘ</p> <p><input checked="" type="checkbox"/> Managed by Policy ⓘ</p> <p><input type="checkbox"/> Peers from control nodes ⓘ</p>

Save Cancel

实例需要以下属性：

- **主机名**：（必需）为您的实例输入完全限定域名（公共 DNS）或 IP 地址。此字段等同于基于安装程序部署的**主机名**。



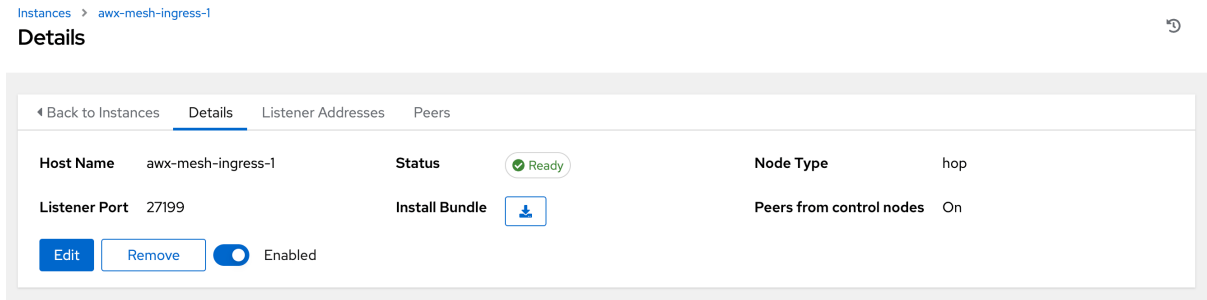
注意

如果实例使用无法从控制集群解析的私有 DNS，DNS 查找路由会失败，并且生成的 SSL 证书无效。改为使用 IP 地址。

- 可选：**描述**：输入实例的描述。
- **Instance State**：此字段已自动填充，表示它正在安装，且无法修改。
- **侦听器** 端口：此端口用于 receptor 侦听进入的连接。您可以将端口设置为适合您的配置的端口。此字段等同于 API 中的 `listener_port`。默认值为 27199，但您可以设置自己的端口值。
- **实例类型**：只能创建 **execution** 和 **hop** 节点。基于 Operator 的部署不支持控制或混合节点。
选项：
 - **启用实例**：选中此框，使它可用于在执行节点上运行。
 - 选中 **Managed by Policy** 复选框，以启用策略来确定如何分配实例。
 - 从控制节点框中选中 **Peers**，以启用控制节点自动到此实例的对等点。对于连接到自动化控制器的节点，请选中 **Peers from Control nodes** 复选框，以在该节点和自动化控制器之间创建直接通信链接。对于所有其他节点：
 - 如果您没有添加跃点节点，请确保 **检查来自 Control 的 Peers**。
 - 如果要添加跃点节点，请确保没有 **检查来自 Control 的 Peers**。
 - 对于与跃点节点通信的执行节点，请不要选中此框。
 - 要将执行节点与跃点节点对等，点 **Peers** 字段旁边的 图标。此时会显示 Select Peers 窗口。

将执行节点与跃点节点对等。

3. 点击 **Save**。




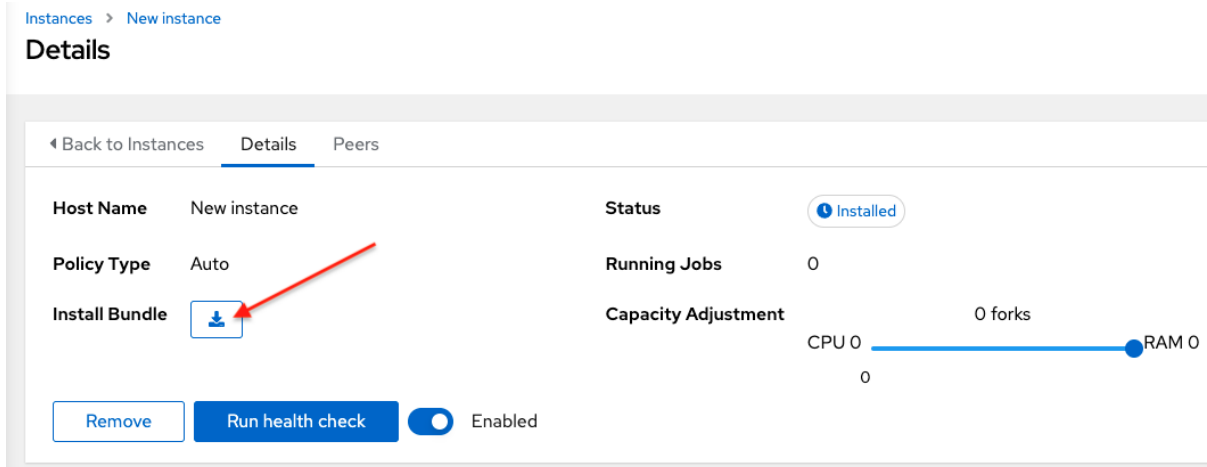
4. 要查看更新拓扑的图形表示，请参阅 [Topology viewer](#)。



注意

从任何可通过 SSH 访问新创建的实例的计算机执行以下步骤。

5. 点 **Install Bundle** 旁边的  图标下载包含这个新实例的 tar 文件，以及将创建的节点安装到自动化网格中所需的文件。



安装捆绑包包含 TLS 证书和密钥、证书颁发机构和正确的 Receptor 配置文件。

```
receptor-ca.crt
work-public-key.pem
receptor.key
install_receptor.yml
inventory.yml
group_vars/all.yml
requirements.yml
```

6. 从您下载的位置中提取下载的 **tar.gz** Install Bundle。为确保这些文件位于远程机器上的正确位置，安装捆绑包包含 **install_receptor.yml** playbook。playbook 需要 Receptor 集合。运行以下命令以下载集合：

```
ansible-galaxy collection install -r requirements.yml
```

7. 在运行 **ansible-playbook** 命令前，请编辑 **inventory.yml** 文件中的以下字段：

```
all:
  hosts:
    remote-execution:
```

```
ansible_host: 10.0.0.6
ansible_user: <username> # user provided
ansible_ssh_private_key_file: ~/.ssh/<id_rsa>
```

- 确保 **ansible_host** 设置为节点的 IP 地址或 DNS。
- 将 **ansible_user** 设置为运行安装的用户名。
- 将 **ansible_ssh_private_key_file** 设置为包含用于连接实例的私钥的文件名。
- **inventory.yml** 文件的内容充当模板，其中包含在网格拓扑中安装和配置 receptor 节点期间应用的角色的变量。您可以修改一些其他字段，或者在高级场景中完全替换该文件。如需更多信息，请参阅 [角色变量](#)。

8. 对于使用私有 DNS 的节点，请将以下行添加到 **inventory.yml** 中：

```
ansible_ssh_common_args: <your ssh ProxyCommand setting>
```

这指示 **install-receptor.yml** playbook 使用 proxy 命令通过本地 DNS 节点连接到私有节点。

9. 配置属性后，单击 **Save**。所创建的实例的 **Details** 页面将打开。

10. 保存文件以继续。

11. 运行安装捆绑包的系统来设置远程节点并运行 **ansible-playbook** 需要安装 **ansible.receptor** 集合：

```
ansible-galaxy collection install ansible.receptor
```

or

```
ansible-galaxy install -r requirements.yml
```

- 从 **requirements.yml** 文件安装 receptor 集合依赖项会持续检索指定的 receptor 版本。另外，它会检索将来可能需要的任何其他集合依赖项。
- 在运行 playbook 的所有节点上安装 receptor 集合，否则会出现错误。

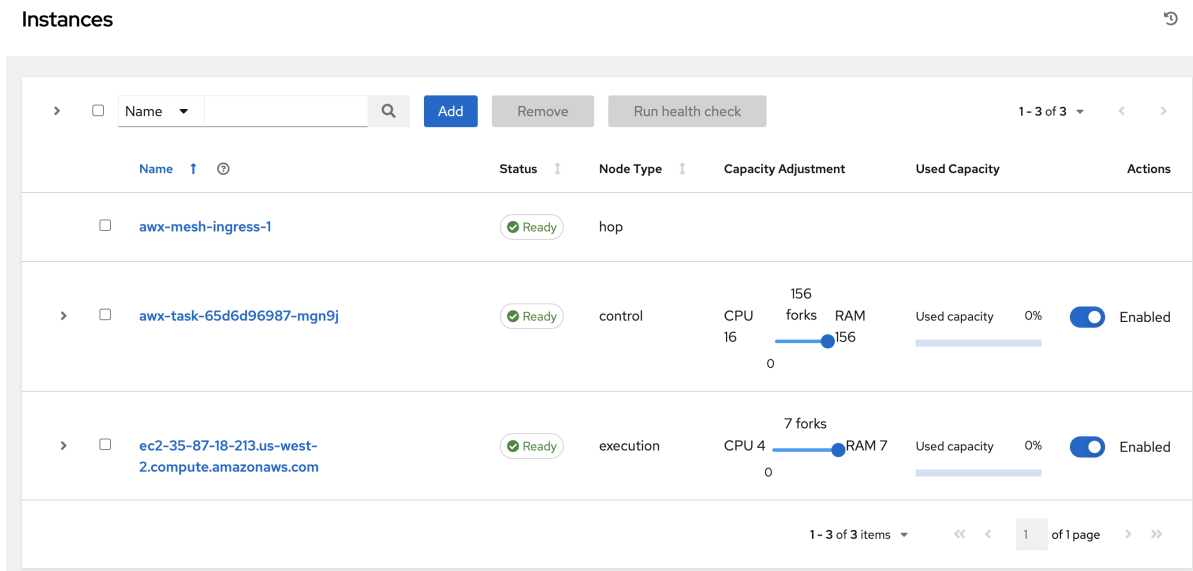
12. 如果定义了 **receptor_listener_port**，机器还需要一个可用的开放端口来建立入站 TCP 连接，例如 27199。运行以下命令，为 receptor 通讯打开端口 27199：

```
sudo firewall-cmd --permanent --zone=public --add-port=27199/tcp
```

13. 在您要更新自动化网络的机器上运行以下 playbook：

```
ansible-playbook -i inventory.yml install_receptor.yml
```

此 playbook 运行后，您的自动化网格会被配置。



要从网格中删除实例，请参阅 [删除实例](#)。

2.4. 创建实例组

使用以下步骤创建新实例组。

流程

1. 在导航面板中，选择 **Administration** → **Instance Groups**。
2. 从 **Add instance group** 列表中选择 **Add**。
3. 在以下字段中输入相关信息：
 - **名称**：名称必须是唯一的，且不能命名为 "controller"。
 - **策略实例最小值**：在新实例上线时，自动分配给此组的最少实例数量。
 - **策略实例百分比**：使用滑块来选择在新实例上线时自动分配给此组的最小实例百分比。



注意

创建新实例组时不需要策略实例字段。如果没有指定值，则 **Policy 实例最小值** 和 **Policy 实例百分比** 默认为 0。

- **最大并发作业**：指定可为任何给定作业运行的最大 fork 数量。
- **最大 fork**：指定可为任何给定作业运行的最大并发作业数。

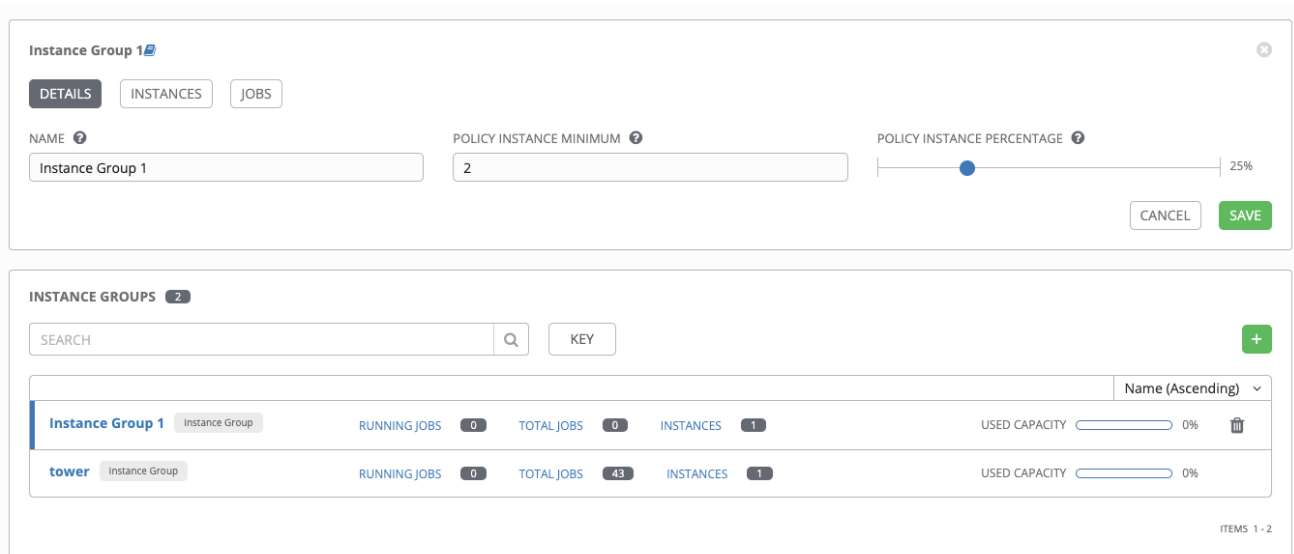


注意

Max concurrent jobs 和 **Max forks** 的默认值 0 表示没有限制。如需更多信息，请参阅 [自动化控制器管理指南中的实例组容量限制](#)。

4. 点击 **Save**。

当您成功创建实例组时，新创建的实例组的 **Details** 选项卡将保留，允许您查看和编辑您的实例组信息。当您点击 **Instance Groups** 列表视图中的 Edit  图标时，就会打开这个界面。您还可以编辑 **实例**，并查看与此实例组关联的 **作业**：



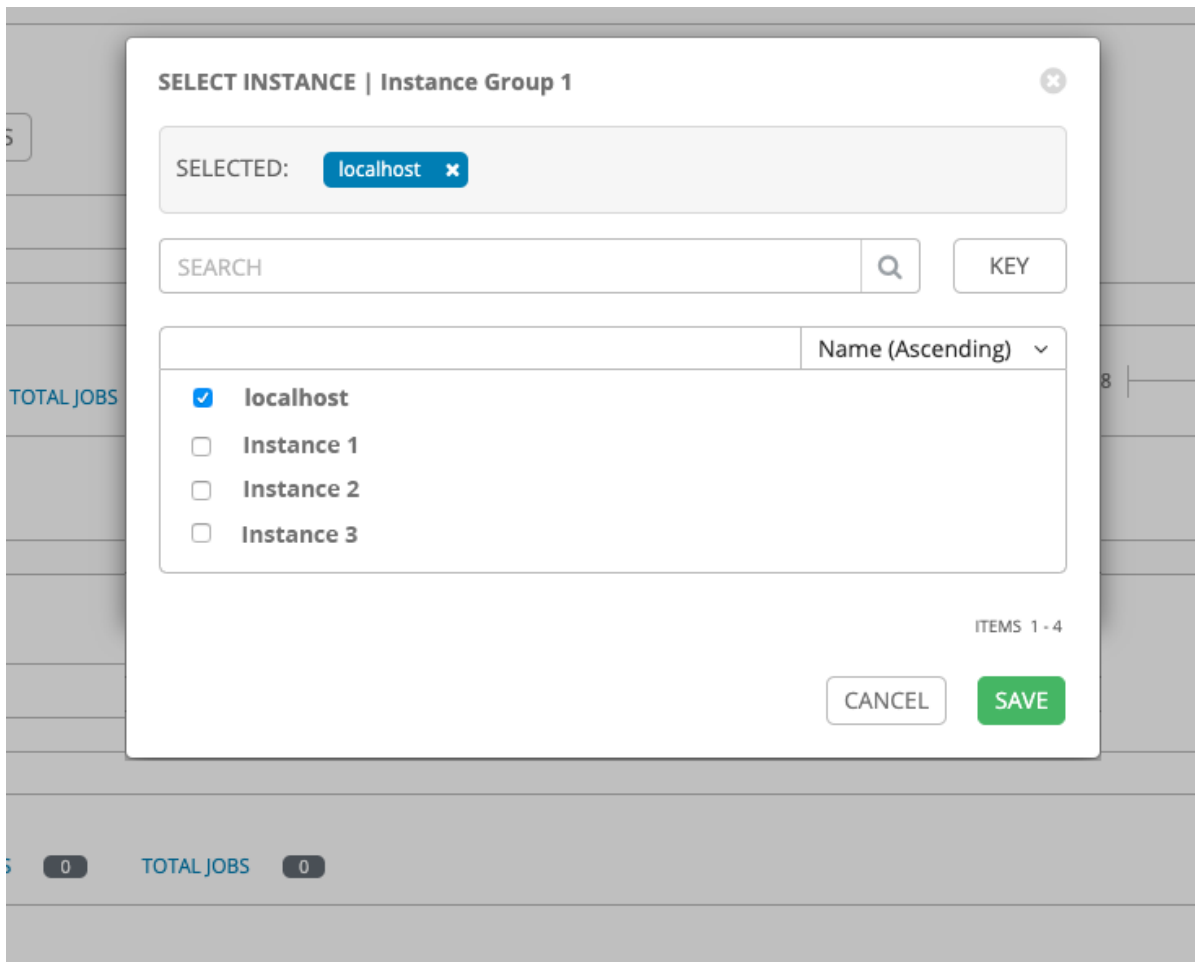
The screenshot shows two parts of the Ansible Automation Platform interface. The top part is the 'Instance Group 1' configuration page, which has three tabs: 'DETAILS', 'INSTANCES', and 'JOBS'. The 'DETAILS' tab is active, showing fields for 'NAME' (Instance Group 1), 'POLICY INSTANCE MINIMUM' (2), and 'POLICY INSTANCE PERCENTAGE' (25%). There are 'CANCEL' and 'SAVE' buttons at the bottom right. The bottom part is the 'INSTANCE GROUPS' list view, which has a search bar and a 'KEY' button. It displays a table with two instance groups: 'Instance Group 1' and 'tower'. The table columns include 'Name (Ascending)', 'RUNNING JOBS', 'TOTAL JOBS', 'INSTANCES', and 'USED CAPACITY'. The 'tower' instance group has 43 total jobs and 1 instance.

Name (Ascending)	RUNNING JOBS	TOTAL JOBS	INSTANCES	USED CAPACITY
Instance Group 1	0	0	1	0%
tower	0	43	1	0%

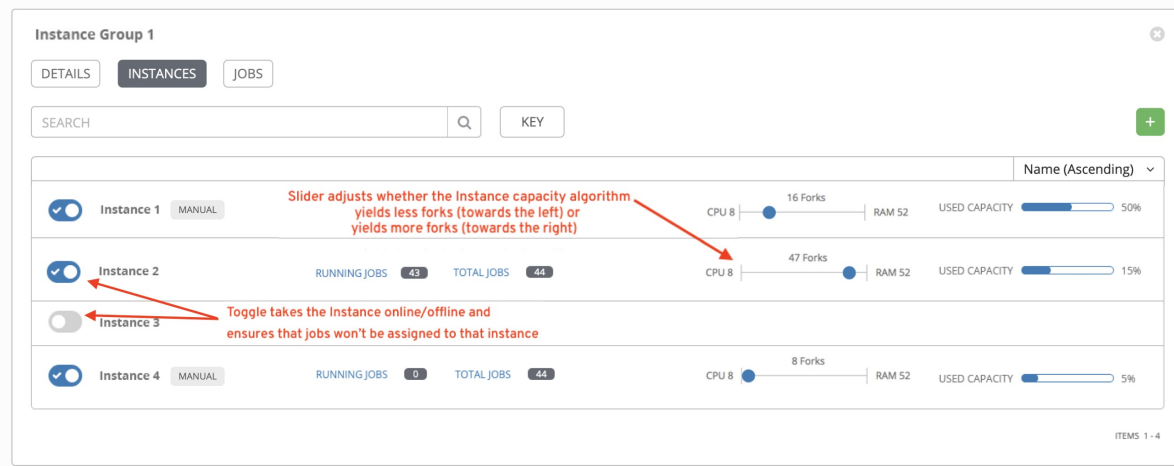
2.5. 将实例关联到实例组

流程

1. 选择 **Instance Groups** 窗口的 **Instances** 选项卡。
2. 点关联。
3. 点击列表中一个或多个可用实例旁边的复选框，以选择要与实例组关联的实例：



4. 在以下示例中，添加到实例组中的实例以及其容量的信息：







2.6. 在执行节点上运行作业

您必须指定作业运行的位置，或者默认在控制集群中运行的。

为此，请设置作业模板。

如需有关作业模板的更多信息，请参阅 [自动化控制器用户指南中的 作业模板](#)。

流程

1. **Templates** 列表视图显示当前可用的作业模板。在此屏幕中，您可以启动 ，编辑 ，并复制  工作流作业模板。
2. 选择您想要的作业并点击  图标。
3. 选择您要运行作业的实例组。请注意，系统管理员必须授予您或团队权限才能在作业模板中使用实例组。如果您选择了多个作业模板，则选择它们的顺序会设置执行优先级。
4. 点击 **Next**。
5. 点 **Launch**。

2.7. 为 OPENSIFT CONTAINER PLATFORM 部署拉取 SECRET



注意

这不适用于 Microsoft Azure 上的 Ansible Automation Platform。

如果您使用自动化控制器提供的默认执行环境在远程执行节点上运行，您必须在包含拉取执行环境镜像的凭证的自动化控制器中添加 pull secret。

要做到这一点，在自动化控制器命名空间中创建 pull secret，并在 Operator 中配置 `ee_pull_credentials_secret` 参数，如下所示：

流程

1. 使用以下命令创建 secret：

```
oc create secret generic ee-pull-secret \
  --from-literal=username=<username> \
  --from-literal=password=<password> \
  --from-literal=url=registry.redhat.io

oc edit automationcontrollers <instance name>
```

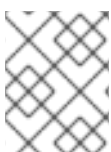
2. 使用以下命令将 `ee_pull_credentials_secret` 和 `ee-pull-secret` 添加到规格中：

```
spec.ee_pull_credentials_secret=ee-pull-secret
```

3. 要从自动化控制器 UI 管理实例，必须具有 System Administrator 或 System Auditor 权限。

2.8. 删除实例

在 Add Instances 页面中，您可以在节点上添加、删除或运行健康检查。



注意

您必须遵循为您创建的任何其他节点安装 RHEL 软件包的步骤。如果将这个额外节点对等到现有的跃点节点，还必须在每个节点上安装 Install Bundle。

使用实例旁边的复选框来选择它以移除它，或者针对它运行健康检查。

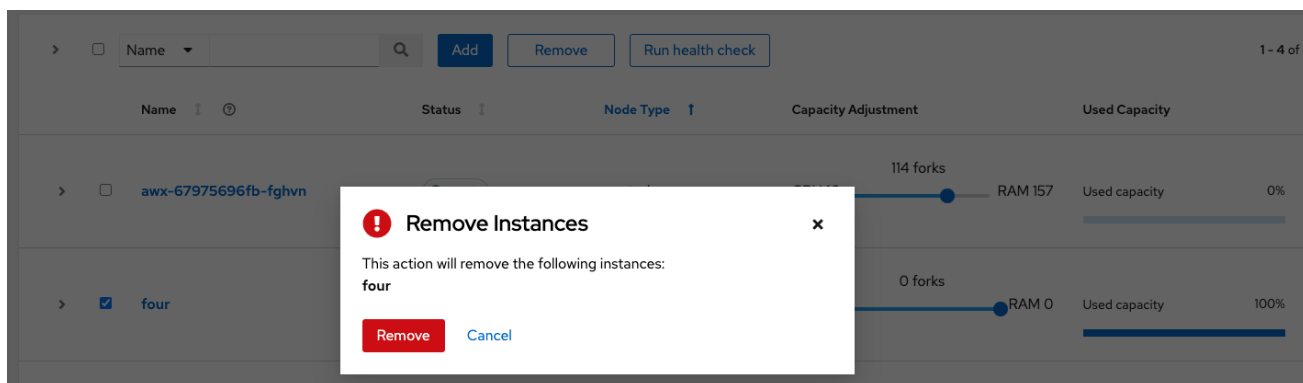


注意

- 如果使用 UI 删除节点，则节点为"removed"，不显示状态。如果在 UI 中删除前删除了节点的虚拟机，它将显示错误。
- 只有拓扑更改通信模式（即 hop 节点或您添加节点）时，才需要重新安装 Install Bundle。

当禁用按钮时，您没有该特定操作的权限。请联系您的管理员，为您提供所需的访问权限级别。

如果您能够删除实例，您会收到确认提示。



注意

您仍然可以删除实例，即使它处于活动状态且作业正在运行。自动化控制器会在删除前等待此节点上运行的作业完成。