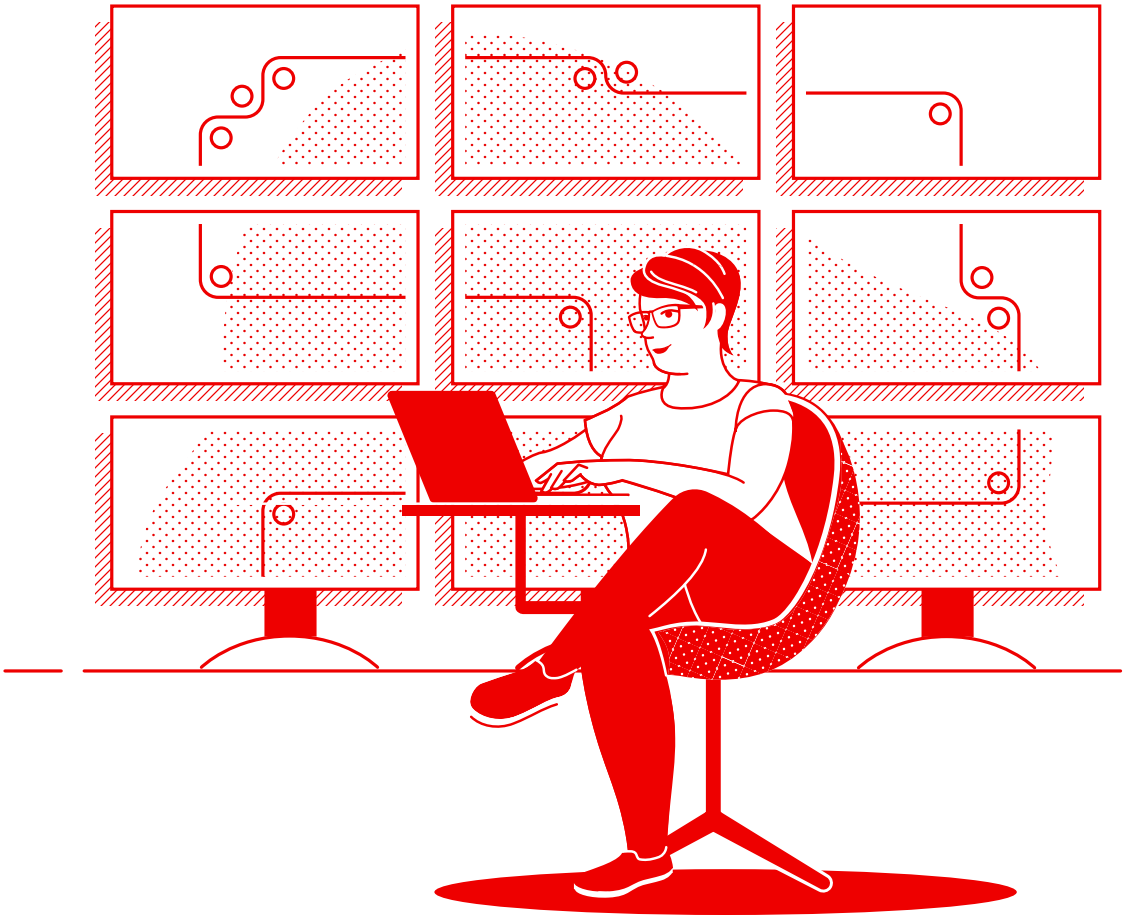
Red Hat



借助红帽实现网络自动化

使用红帽 Ansible 自动化平台来实施常见的网络自动化任务的技术手册

目录

通过网络自动化加快运营

传统手动网络配置和更新方法过于缓慢且容易出错，无法有效支持当今快速变化的应用和数据传输要求。可编程、基于软件的自动化技术可以帮助您的团队更好地支持您企业的数字计划。

借助网络自动化，网络运营 (NetOps) 团队可以快速响应用户对容量、应用安全性、负载平衡和多云集成的动态需求。还可以实现自助服务和按需网络活动。

因此，NetOps 团队可以像应用和基础架构团队一样敏捷灵活，以支持现代业务需求。

借助红帽 Ansible 自动化平台加快运营

借助**红帽® Ansible® 自动化平台**，红帽将热门社区 Ansible 项目引入公司，大规模添加基于团队的自动化所需的特性和功能。这个强大的 IT 自动化平台将简单、易读的自动化语言与可信、可组合的执行环境相结合，同时融合了专注于安全性的共享与协作功能。因为不要求具备编程技能，所以您组织内的所有角色都能快速使用 Ansible 自动化平台。

Ansible 自动化平台可帮助您简化和管理从服务器和网络到应用和 DevOps 的复杂数据中心环境。该平台在多供应商虚拟和物理环境中为传统和开放式网络基础架构设备提供支持，因此您可以使用单一工具实现整个网络的自动化。

该电子书介绍了如何开始执行常见的网络自动化任务。

关键资源

查看这些资源，了解关于红帽 Ansible 自动化平台的基本信息：

- 在线培训：**Ansible 必备技能**
- 电子书：**面向所有人的网络自动化**

注：本电子书中的命令专为 1.x 版 Ansible 自动化平台编写，不适用于 2.0 或更高版本的 Ansible 自动化平台。

安装并配置红帽 Ansible 自动化平台

安装红帽 Ansible 自动化平台

红帽 Ansible 自动化平台的安装与设置简单且快捷

步骤 1a

使用 yum 安装命令行 Ansible

运行以下命令：

```
$ sudo yum install ansible
```

完整说明，请参阅 **Ansible 安装指南**。

步骤 1b

使用安装工具来安装 Ansible 自动化平台

1. 确保您已获得**最新版本**或访问 **red.ht/try_ansible** 下载试用版。
2. 解压 tar 文件（版本和名称可能不同）：

   ```
   $ tar xvzf ansible-automation-platform-setup-bundle-1.2.1-1.tar.gz
   ```

3. 设置密码：
   - `admin_password` 用于管理
   - `rabbitmq_password` 用于消息传递
   - `pg_password` 用于数据库
4. 运行安装脚本。安装完成后，打开谷歌浏览器或火狐浏览器，使用主机名或 IP 地址导航到您的 Ansible 自动化平台主机。

完整说明，请参阅 **Ansible 自动化平台快速安装指南**。

步骤 2

为网络安装 Ansible 自动化平台内容集

红帽通过 **Ansible 自动化中心**提供经过认证的受支持**内容集**，可用于各种网络设备、工具和基础架构。每个内容集都有一个命名空间，其中包含一个或多个内容集。使用 `ansible-galaxy` 命令来安装这些内容集：

```
$ ansible-galaxy collection install namespace.collection_name
```

按照**红帽 Ansible 自动化平台文档**中的指示来配置 Ansible 自动化中心，以访问和管理您的内容集。您可在 **Ansible Galaxy** 上找到受社区支持的内容集。

设置您的网络环境

建议您按照这些最佳实践为红帽 Ansible 自动化平台配置您的网络环境

确保与您的网络环境建立连接

在您的路由器和交换机上安装一个 Ansible 自动化平台服务帐户，用于登录和身份验证。Ansible 自动化平台支持采用公司身份验证方法，如终端访问控制器访问控制系统 +（TACACS+）和远程访问拨入用户服务（RADIUS）。更多详情，请参阅本文档中的**“设置公司身份验证”部分**。

创建您的 playbook 存储库

通过**在 Web 界面中设置项目**来将 Ansible 自动化平台连接到您的源控制管理（SCM）工具，以获得相应项目存储库中所有 playbook 的访问权限。

配置您的清单

创建一个您要自动化的网络设备**清单**。Ansible 自动化平台可以管理很多清单。您可使用**清单插件**从 Amazon Web Services EC2、Microsoft Azure 资源中心和 VMware vCenter 等人气工具动态加载清单。您还可以从 Ansible 自动化平台项目**加载清单**。本电子书的**第 3 章**详细介绍了如何构建和使用清单。

设置您的网络防火墙规则

设置您的防火墙规则，允许 Ansible 自动化平台使用默认的安全 Shell（SSH）端口 22 连接到路由器和交换机。必要时，您可以使用 `ansible_port` **主机变量**来变更这一端口号。

设置您的 Ansible 自动化平台密码

创建一个**凭据**用于存放密码。您可以向用户和团队授予凭据使用权，而不必真正向用户公开凭据。

创建 Ansible 作业模板

创建**作业模板**以连接您的清单、凭据和项目。作业模板定义了运行自动化作业的参数集，便于您多次执行同一组任务，以及在不同团队中重复使用内容。每个作业模板包含：

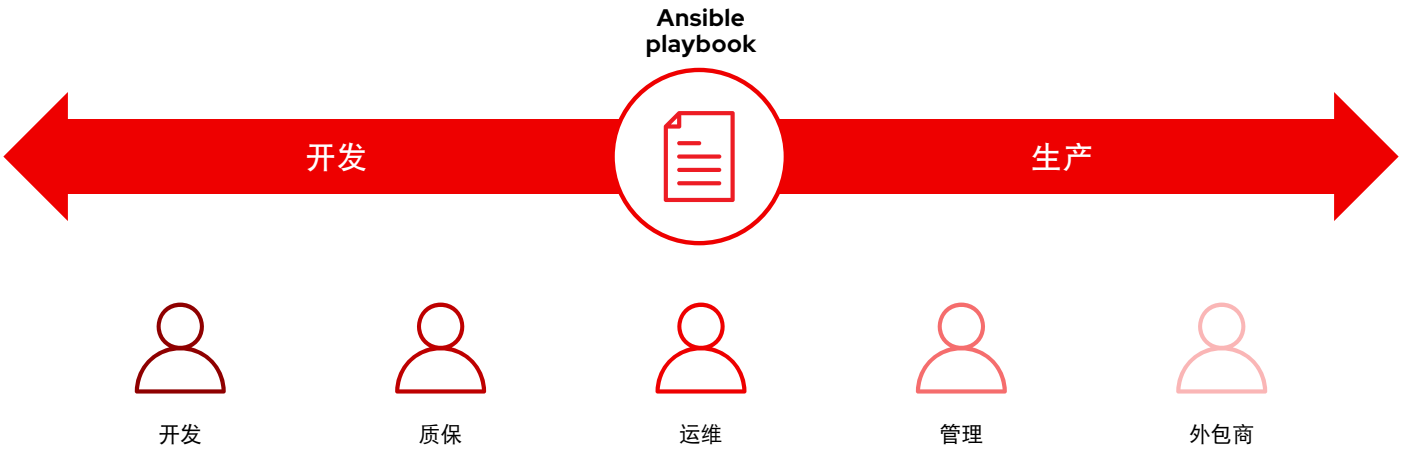
- 从中加载 Ansible playbook 的**项目**。
- 类似于网络交换机的**清单**或自动化目标列表。
- 用于登录和自动化您清单中设备的**凭据**。

运行您的第一个命令和 playbook

了解 playbook

playbook 是 Ansible 的配置、部署和编排语言。由称为 play 的人员可读指令集组成，这些指令定义主机清单中的自动化。每个 play 包括一个或多个针对清单中的一个、多个或所有主机的任务。每个任务调用一个 Ansible 模块，该模块执行特定功能，如收集有用信息，备份网络文件，管理网络配置或验证连接。

playbook 可以由多个团队共享和重用，以创建可重复的自动化。



playbook 解析

本例显示 Ansible playbook 中的常见组成部分

```
1  ---
2  - name: add vlans
3    hosts: arista
4    gather_facts: false
5
6    vars:
7      vlans:
8        - name: desktops
9          vlan_id: 20
10       - name: servers
11         vlan_id: 30
12       - name: DMZ
13         vlan_id: 50
14
15   tasks:
16     - name: add VLAN configuration
17       arista.eos.eos_vlans:
18         state: merged
19         config: "{{ vlans }}"
```

表示 playbook 的开端

调用一个名为 `arista` 的设备或设备组

用于检索事实的可选参数

变量定义

在本 playbook 中，我们会直接定义变量值。

如果您正在使用红帽 Ansible 自动化平台 Web 界面，您还可以**创建调查**，以便在用户运行您的 playbook 时提醒用户变量值。这种情况下，请将第 9、11 和 13 行替换为：

```
# {{variable_name}} input
```

关于调查的更多详情，请参阅第 6 页上的**“创建红帽 Ansible 调查”**部分。

任务

任务与 Ansible 模块之间具有一对一相关性。这部分会调用模块，为 `vars` 部分定义的三个变量分别配置虚拟局域网（VLAN）。

创建红帽 Ansible 调查

调查会以用户友好的问答方式为您的 playbook 设置额外变量。如需创建调查：

1. 请点击红帽 Ansible 自动化平台 Web 界面上的***添加调查***按钮。
2. 请填写每个问题的以下信息：
   - **名称**：要询问用户的问题
   - **描述（可选）**：对问题内容的描述
   - **回答变量名称**：用于存储回答的 Ansible 变量名称
   - **回答类型**：回答格式——输入的文本、选择题或数字
   - **默认回答**：变量的默认值
   - **必填**：问题是否为选答题
3. 点击 **+** 按钮将问题添加到调查。
4. 重复步骤 3 将更多问题添加到调查。
5. 完成后可点击***保存***按钮来保存调查。

更多详情，请参阅 Ansible 自动化平台文档中的**“调查”部分**。

运行您的 playbook

playbook 运行起来很简单，但在命令行 Ansible 中运行与在 Ansible 自动化平台 Web 界面中运行的过程不同。

命令行 Ansible

运行以下命令：

```
ansible-playbook <playbook name> -i <inventory file>
```

红帽 Ansible 自动化平台 Web 界面

按下 Ansible 自动化平台 Web 界面中您的模板旁边的启动作业（火箭）按钮。

构建您的清单

了解清单

清单是一个主机集合，可使用 Ansible 命令和 playbook 进行操作。清单文件用于对主机分组，可用作您的网络的可信来源。这些文件可以采取简单的 INI 或 YAML 格式。为保持与 playbook 一致，很多组织选择以 YAML 格式编写清单。利用清单文件，单个 playbook 可以使用一条命令维护数百台网络设备。

本章将介绍如何构建清单文件。

创建基础的 INI 格式清单

首先，将您的清单按逻辑分组。最好按照***对象***（应用、堆栈或微服务）、***位置***（数据中心或区域）和***时间***（开发阶段）对服务器和网络设备进行分组。

- **对象**：`db`、`web`、`leaf`、`spine`
- **位置**：`east`、`west`、`floor_19`、`building_A`
- **时间**：`dev`、`test`、`staging`、`prod`

这是一个 INI 格式的示例代码，列出了一个非常小的数据中心的基本组结构。您可以使用语法 `[metagroupname:children]` 对组进行分组，并将组列为元组成员。

这里的 `network` 组包含所有的 leaf 和 spine。`datacenter` 组包含所有网络设备和所有网络服务器。

更多详情，请参阅 Ansible 中的“构建您的清单”部分。您还可在 GitHub 上找到简单的清单报告 playbook。

```
[leafs]
leaf01
leaf02

[spines]
spine01
spine02

[network:children]
leafs
spines

[webservers]
webserver01
webserver02

[datacenter:children]
network
webservers
```

YAML 格式清单解析

```
1  ---
2  all:
3    vars:
4      ansible_user: admin
5      ansible_password: password123
6      ansible_become_pass: password123
7      ansible_become: True
8      ansible_become_method: enable
9      ansible_network_cli_ssh_type: libssh
10   children:
11     routers:
12       children:
13         arista:
14         cisco:
15         juniper:
16     arista:
17       hosts:
18         rtr2:
19           ansible_host: 172.16.100.2
20         rtr4:
21           ansible_host: 172.16.100.4
22       vars:
23         ansible_network_os: arista.eos.eos
24         ansible_connection: ansible.netcommon.network_cli
25     cisco:
26       hosts:
27         rtr1:
28           ansible_host: 172.16.100.1
29       vars:
30         ansible_network_os: cisco.ios.ios
31         ansible_connection: ansible.netcommon.network_cli
32     juniper:
33       hosts:
34         rtr3:
35           ansible_host: 172.16.100.3
36       vars:
37         ansible_network_os: junipernetworks.junos.junos
38         ansible_connection: ansible.netcommon.netconf
```

表示 playbook 的开端

定义适用于清单中所有主机的变量，不限组别

组的层级结构

第 10-15 行确定了该清单中的主机组。这种情况下，`routers` 组包含三个子组，分别为：`arista`、`cisco` 和 `juniper`。

组定义

`hosts` 命令定义了哪个主机属于哪个组。本例中，`arista` 组包含两台通过 IP 地址识别的主机。

组变量

每个组都可以有自己的变量集。这个清单定义了每个组的操作系统和连接类型。这两个变量都指向内容集中包含的项目。

关于这些变量的更多详情，请参阅第 10 页上的 **“对变量分组”部分**。

按平台对清单分组

随着清单越来越长，您可能会希望按平台对设备分组，以便轻松为特定平台的所有设备定义平台专用变量。示例清单的第 10-15 行确定了该清单的主机组层次结构。`routers` 组包含三个按平台分类的子组：`arista`、`cisco` 和 `juniper`。每个子组都包含一个或多个主机，在第 16-21、25-28 和 32-35 行按 IP 地址定义。

```
10    children:
11      routers:
12        children:
13          arista:
14          cisco:
15          juniper:
16      arista:
17        hosts:
18          rtr2:
19            ansible_host: 172.16.100.2
20          rtr4:
21            ansible_host: 172.16.100.4
```

更多详情，请参阅 Ansible 文档中的**“按平台对清单分组”部分**。

设置变量

您可以在清单中为您的第一个 Ansible 命令中所需的很多变量设置值，这样便可在 `ansible-playbook` 命令中跳过这些变量值。示例清单的第 2-9 行定义了适用于清单中列出的所有主机的变量，不限组别。

```
2  all:
3    vars:
4      ansible_user: admin
5      ansible_password: password123
6      ansible_become_pass: password123
7      ansible_become: True
8      ansible_become_method: enable
9      ansible_network_cli_ssh_type: libssh
```

您可在多个不同文件中设置和存储变量。最好在清单文件或 playbook 中设置用于连接设备的变量，如登录信息或 IP 地址。在存储于 `group_vars` 目录下的单独文件中设置与设备配置相关的变量。更多详情，请参阅 Ansible 文档中的**“组织主机和组变量”部分**。

对组变量进行分组

当同组设备共享相同的变量值时，如操作系统（OS）或 SSH 用户，您可通过将这些变量合并到组变量中来减少重复和简化维护。组变量在各自组定义中进行设置。示例清单的第 22-24、29-31 和 36-38 行分别为三个主机组设置了组变量值。

```
22        vars:
23          ansible_network_os: arista.eos.eos
24          ansible_connection: ansible.netcommon.network_cli
```

本例分别对三个子组的网络操作系统（NOS）和连接类型变量进行了定义。这种情况下，这些变量指向红帽 Ansible 自动化平台内容集中包含的项目。内容集项目的格式为 `namespace.collection_name.item`。例如，`arista.eos.eos` 指向通过 Arista 命名空间提供的 EOS 集中的EOS 操作系统插件，而 `ansible.netcommon.network_cli` 则指向通过 Ansible 命名空间提供的 Netcommon 集中的网络 CLI 插件。

变量语法

变量值语法在清单、playbook 和 group_vars 文件中各不相同。尽管 playbook 和 group_vars 文件均以 YAML 格式编写，但每个文件中使用的变量却不同。

INI 格式清单文件

`key=value` 语法用于以下变量值：

```
ansible_network_os=cisco.ios.ios
```

带有 .YML 和 .YAML 扩展名的文件

使用 YAML 语法：

```
key: value
```

Group_vars 和 playbook 文件

使用完整的密钥名称：

```
ansible_network_os: cisco.ios.ios
```

更多详情，请参阅 Ansible 文档中的**“变量语法”部分**。

保护敏感变量

对于密码之类的敏感变量，最好使用额外保护。

红帽 Ansible 自动化平台可针对密码和关键信息提供凭据管理服务。您可通过 Web 界面上的***凭据***页面，向用户和团队授予凭据使用权，而不必向用户公开凭据。更多详情，请参阅 Ansible 文档中的**“凭据”部分**。

请注意，Ansible 自动化平台可在启用**联邦信息处理标准（FIPS）模式**的系统中运行。

实施常见用例

本章将介绍适用于常见网络自动化用例的 playbook 示例

添加 VLAN

对于 NetOps 来说，配置跨多个网络设备的 VLAN 需要持续进行。Ansible 降低了创建 VLAN 并在全网传播的难度。

```
---
- name: add vlans
  hosts: arista
  gather_facts: false
  vars:
    vlans:
      - name: desktops
        vlan_id: 20
      - name: servers
        vlan_id: 30
      - name: DMZ
        vlan_id: 50

  tasks:
    - name: add VLAN configuration
      arista.eos.eos_vlans:
        state: merged
        config: "{{ vlans }}"
```

收集事实

大多数网络包含很多不同的平台和设备。Ansible 可以查询、存储和报告网络数据，如软件版本和界面信息。

```
---
- name: use facts module
  hosts: cisco
  gather_facts: false

  tasks:
    - name: retrieve facts
      cisco.ios.ios_facts:

    - name: display version
      debug:
        msg: "{{ ansible_net_version }}"

    - name: display serial number
      debug:
        msg: "{{ ansible_net_serialnum }}"
```

检索资源信息

Ansible **网络资源模块**简化并规范了不同网络设备的管理方式。任何资源模块都可以使用 `state: gathered` 来检索网络资源信息。

```
---
- name: retrieve interface information
  hosts: cisco
  gather_facts: false

  tasks:
    - name: use state gathered
      cisco.ios.ios_interfaces:
        state: gathered
      register: interfaces_info

    - name: print out interfaces information
      debug:
        msg: "{{ interfaces_info }}"
```

备份配置

存储配置备份是 NetOps 的关键活动。Ansible 自动化平台降低了从网络设备中提取部分或完整配置的难度。

```
---
- hosts: cisco
  gather_facts: false

  tasks:
  - name: back up config
    cisco.ios.ios_config:
      backup: yes
```

访问有关红帽 Ansible 自动化平台的内容

您可访问现成可用的自动化内容，更快更轻松地采用红帽 Ansible 自动化平台。

Ansible 内容集

内容集是 Ansible 内容的一种标准化分布格式，可以包含 playbook、角色、模块和插件等。这种新格式将 Ansible 可执行文件从大部分自动化内容中分离出来，为您提供更大的灵活性和可移植性。您可以从 **Ansible Galaxy** 安装受社区支持的内容集，也可以从 **Ansible Automation Hub** 安装受全面支持且**经过认证的内容集**。

Ansible 角色

Ansible 角色可捆绑自动化内容，以便重复利用。您可以使用角色将任务组织并分解成更小、更独立的工作单元，而不用创建包含数百个任务的长 playbook。单个角色可以包含完成一个工作单元需要的所有任务、变量和处理程序。角色可作为独立实体进行分发，也可作为内容集的组成部分进行分发。

Ansible 自动化中心

通过 **Ansible 自动化中心**，红帽 Ansible 自动化平台的订阅用户可访问由红帽及其技术合作伙伴开发、测试和维护的受全面支持且经过认证的内容集。该中心
为您提供了一个内容集安全门户，以及一个用于内部和第三方自动化内容的专用网络。自动化中心是一个事实内容存储库，用于生产自动化环境。

Ansible Galaxy

Ansible Galaxy 包含所有社区 Ansible 集合，以及现有独立角色。您也可以通过 Ansible Galaxy 向社区贡献您所创建的集合和角色。

了解更多信息

红帽为红帽 Ansible 自动化平台提供了许多资源，包括详细的文档、文章、视频和讨论。大部分资源可在 ansible.com 和**红帽客户门户**中找到。

- 产品网站：
  红帽 Ansible 网络自动化
- 主存储库：
  Ansible 文档
- 文档：
  网络平台索引
- 用户指南：
  清单和变量
  调查
  凭据
- 电子书：
  面向所有人的网络自动化
- 培训课程：
  Ansible 必备技能
  Ansible 网络自动化
- 免费试用：
  红帽 Ansible 自动化平台试用版下载

准备自动化您的网络?

红帽 Ansible 自动化平台使用一种直观的人员可读语言，为您提供了一条简单而强大的现代化网络运维之路，并且支持您的当前流程和现有基础架构。利用灵活、可扩展的自动化框架，您可以更加轻松地提高基础架构的可用性、员工生产力、网络安全性和配置合规性。

免费试用 Ansible 自动化平台，请访问：
red.ht/try_ansible

在红帽专家的帮助下加快部署

网络自动化看起来可能任务艰巨，但红帽咨询可以提供帮助。所有红帽咨询服务都从“为期半天的现场免费业务探讨”会话开始。通过这些会话，红帽专家将和您一起确定您最紧迫的业务挑战，寻找克服挑战的可行方法，并明确实施网络自动化的预期结果。

免费的业务探讨预约，请访问：
redhat.com/zh/services/consulting

F28378_0421_KVM

Red Hat