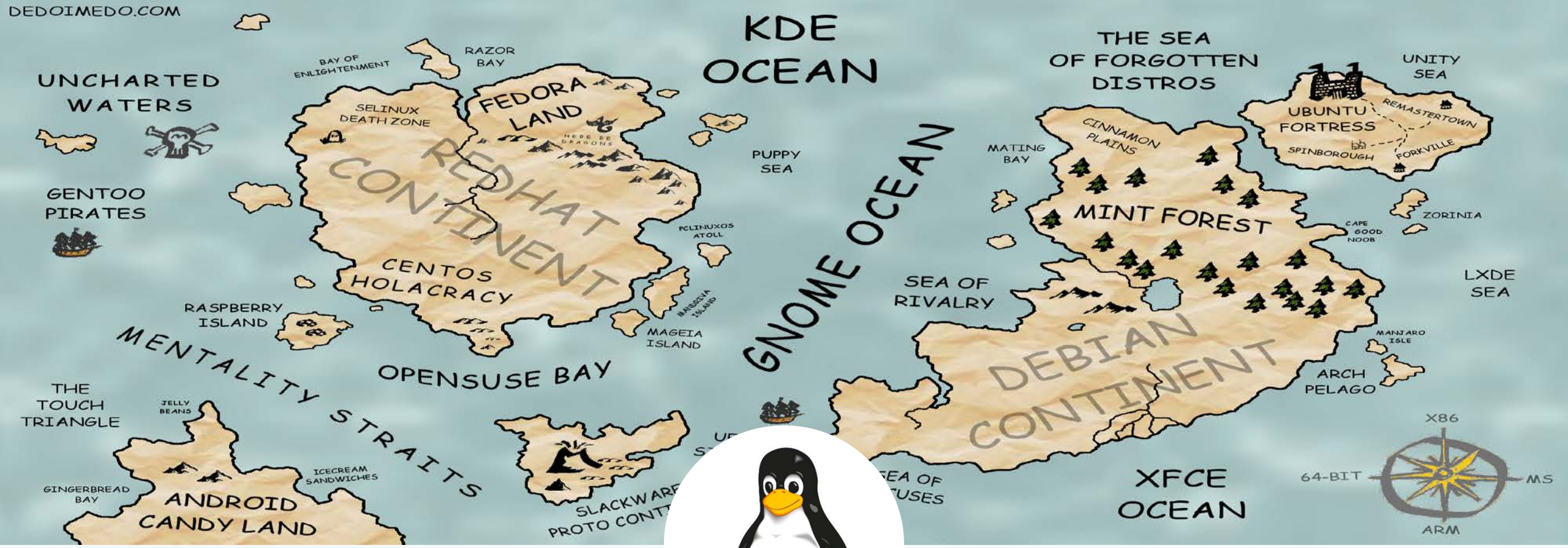


使用Ansible服务实现自动化运维

任课教师：刘遄 www.LinuxProbe.com

课程概述

01 **Ansible介绍与安装**
Ansible Introduction And Installation

02 **设置主机清单**
Set Host List

03 **运行临时命令**
Run Temporary Command

04 **剧本文件实战**
Script Document Actual Combat

05 **创建及使用角色**
Creating And Using Roles

06 **创建和使用逻辑卷**
Create And Use Logical Volumes

07 **判断主机组名**
Determine Host Group Name

08 **管理文件属性**
Manage File Properties

09 **管理密码库文件**
Manage Password Library Files

前言

01 Ansible是最近几年特别火的一款开源运维自动化工具，它能够帮助运维人员肉眼可见地提高工作效率，并减少人为失误。Ansible有上千个功能丰富且实用的模块，而且有详尽的帮助信息可供查阅，因此即便是小白用户也可以轻松上手。

02 介绍Ansible服务的产生背景、相关术语以及主机清单的配置，深入学习ping、yum、firewalld、service、template、setup、lvol、lvg、copy、file、debug等十余个常用的Ansible模块，以满足日常工作中的需要。

03 采用动手实操的方式介绍了从系统中加载角色、从外部环境获取角色以及自行创建角色的方法，学到如何在生产环境中掌控任务工作流程。

03 通过精心编写的playbook（剧本）文件，以动手实操的方式介绍了创建逻辑卷设备，依据主机改写文件、管理文件属性的方法。以使用Ansible的vault对变量以及剧本文件进行加密来收尾。

Ansible介绍与安装

Ansible Introduction And Installation

Ansible介绍

Ansible

Ansible目前是运维自动化工具中最简单、容易上手的一款优秀软件，能够用来管理各种资源。用户可以使用Ansible自动部署应用程序，以此实现IT基础架构的全面部署。

优势

相较于Chef、Puppet、SaltStack等C/S（客户端/服务器）架构的自动化工具来讲，尽管Ansible的性能并不是最好的，但由于它基于SSH远程会话协议，不需要客户端程序，只要知道受管主机的账号密码，就能直接用SSH协议进行远程控制，因此使用起来优势明显。

模块

Ansible服务本身并没有批量部署的功能，它仅仅是一个框架，真正具有批量部署能力的是其所运行的模块。Ansible内置了上千个模块，会在安装Ansible时一并安装，通过调用指定的模块，就能实现特定的功能。

Ansible的专用术语对照表

英文	中文	含义
control node	控制节点	安装了Ansible服务的主机，也称为Ansible控制端，主要是用来发布运行任务、调用功能模块，以及对其他主机进行批量控制
managed node	受控节点	被Ansible服务所管理的主机，也被称为受控主机或客户端，是模块命令的被执行对象
inventory	主机清单	受控节点的列表，可以是IP地址、主机名或者域名
module	模块	用于实现特定功能的代码；Ansiblie默认带有上千款模块；可以在Ansible Galaxy中选择更多的模块
task	任务	要在Ansible客户端上执行的操作
playbook	剧本	通过YAML语言编写的可重复执行的任务列表；把重复性的操作写入到剧本文件中后，下次可直接调用剧本文件来执行这些操作
role	角色	从Ansible 1.2版本开始引入的新特性，用于结构化地组织剧本；通过调用角色可实现一连串的功能

部署Ansible服务程序

第1步

在“虚拟机设置”界面中，将“网络适配器”的“网络连接”选项调整为“桥接模式”，并将系统的网卡设置成“Automatic（DHCP）”模式。

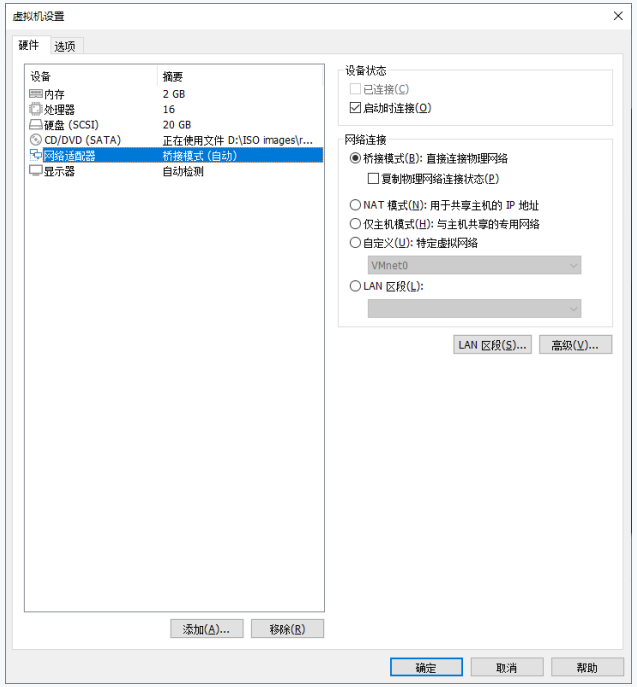
第2步

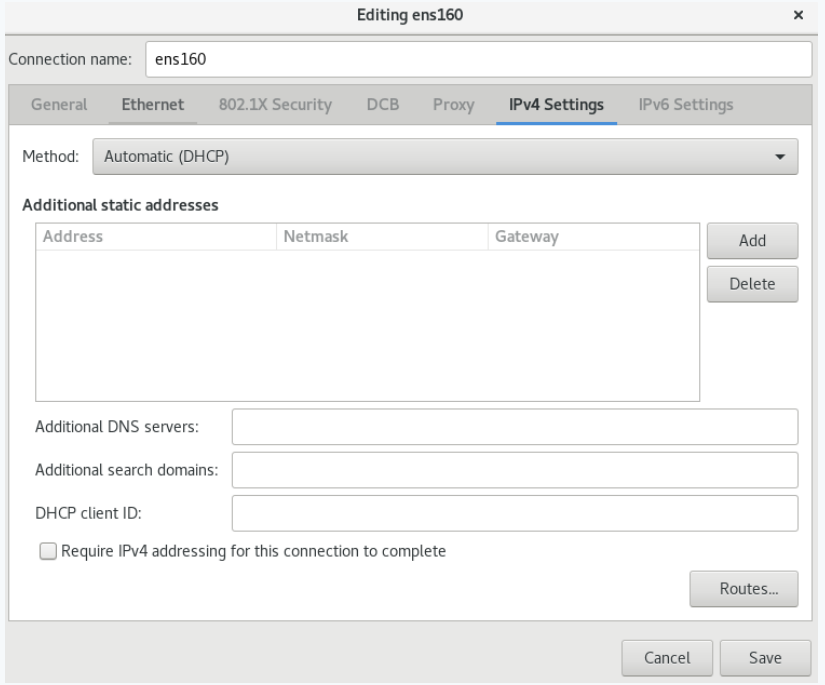
在原有软件仓库配置的下方，追加EPEL扩展软件包安装源的信息。

第3步

安装！安装完毕后，Ansible服务便默认已经启动。使用--version参数可以看到Ansible服务的版本及配置信息。

部署Ansible服务程序





将“网络连接”设置为“桥接模式”

将网卡设置为“Automatic（DHCP）”模式

PART
TWO

设置主机清单

Set Host List

Ansible服务主配置文件优先级顺序

优先级	级文件位置
高	./ansible.cfg
中	~/ansible.cfg
低	/etc/ansible/ansible.cfg

设置主机清单

主机清单

既然Ansible服务是用于实现主机批量自动化控制的管理工具，受管的主机一定不是一两台台，而是数十台甚至成百上千台，那么主机清单（inventory）在生产环境中就可以帮上大忙了。用户可以把要管理的主机IP地址预先写入/etc/ansible/hosts文件，这样后续再通过执行ansible命令来执行任务时就自动包含这些主机了，也就不需要每次都重复输入受管主机的地址了。

操作系统	IP地址	功能用途
RHEL 8	192.168.10.20	dev
RHEL 8	192.168.10.21	test
RHEL 8	192.168.10.22	prod
RHEL 8	192.168.10.23	prod
RHEL 8	192.168.10.24	balancers

受管主机的信息

设置主机清单

第1步

受管主机的系统默认使用RHEL 8，这是为了避免大家在准备实验机阶段产生歧义而给出的建议值，也可以用其他Linux系统。主机清单文件/etc/ansible/hosts中默认存在大量的注释信息，建议全部删除，然后替换成实验信息。

第2步

为了增加实验难度，“通吃”生产环境中的常见需求，我们又为这5台主机分别规划了功能用途，有开发机（dev）、测试机（test）、产品机（prod）（两台）和负载均衡机（balancers）。在对主机进行分组标注后，后期在管理时就方便多了。

第3步

主机清单文件在修改后会立即生效，一般使用“ansible-inventory --graph”命令以结构化的方式显示出受管主机的信息。因为我们对受管主机进行了分组，因此这种方式非常便于我们的阅读。

设置主机清单

第4步

sshd服务在初次连接时会要求用户接受一次对方主机的指纹信息。准备输入受管主机的账号和密码。用户只需要将对应的变量及信息填写到主机清单文件中，在执行任务时便会自动对账号和密码进行匹配，而不用每次重复输入它们。继续修改主机清单文件。

第5步

将Ansible主配置文件中的第71行设置成默认不需要SSH协议的指纹验证，以及将第107行设置成默认执行剧本时所使用的管理员名称为root。

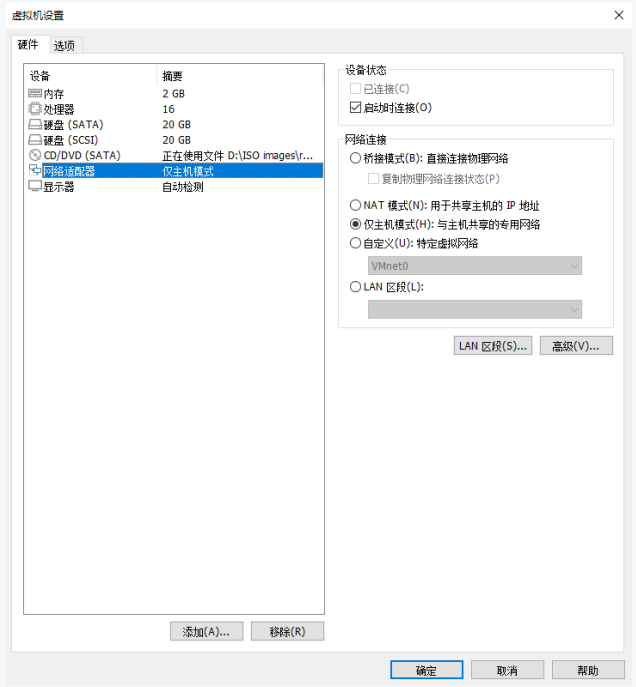
第6步

不需要重启服务，在以上操作完全搞定后就可以开始后面的实验了。将网络适配器修改回“仅主机模式”以及192.168.10.10/24的IP地址。在修改完成后重启网卡，然后自行在主机之间执行ping操作。保证主机之间的网络能够互通是后续实验的基石。

设置主机清单

参数	作用
ansible_ssh_host	受管主机名
ansible_ssh_port	端口号
ansible_ssh_user	默认账号
ansible_ssh_pass	默认密码
ansible_shell_type	Shell终端类型

Ansible常用变量汇总



将网络适配器改回“仅主机模式”

运行临时命令

Run Temporary Command

运行临时命令

Ansible服务

Ansible服务的强大之处在于只需要一条命令，便可以操控成千上万台的主机节点，而ansible命令便是最得力的工具之一。Ansible服务实际上只是一个框架，能够完成工作的是模块化功能代码。Ansible的常用模块大致有20多个。

用来做什么

在Ansible服务中，ansible是用于执行临时任务的命令。在使用ansible命令时，必须指明受管主机的信息，如果已经设置过主机清单文件（/etc/ansible/hosts），则可以使用all参数来指代全体受管主机，或是用dev、test等主机组名称来指代某一组的主机。

语法格式

ansible命令常用的语法格式为“ansible受管主机节点 -m模块名称[-a模块参数]”，常见的参数如表16-6所示。其中，-a是要传递给模块的参数，只有功能极其简单的模块才不需要额外参数，所以大多情况下-m与-a参数都会同时出现。

Ansible服务的常用模块名称及作用

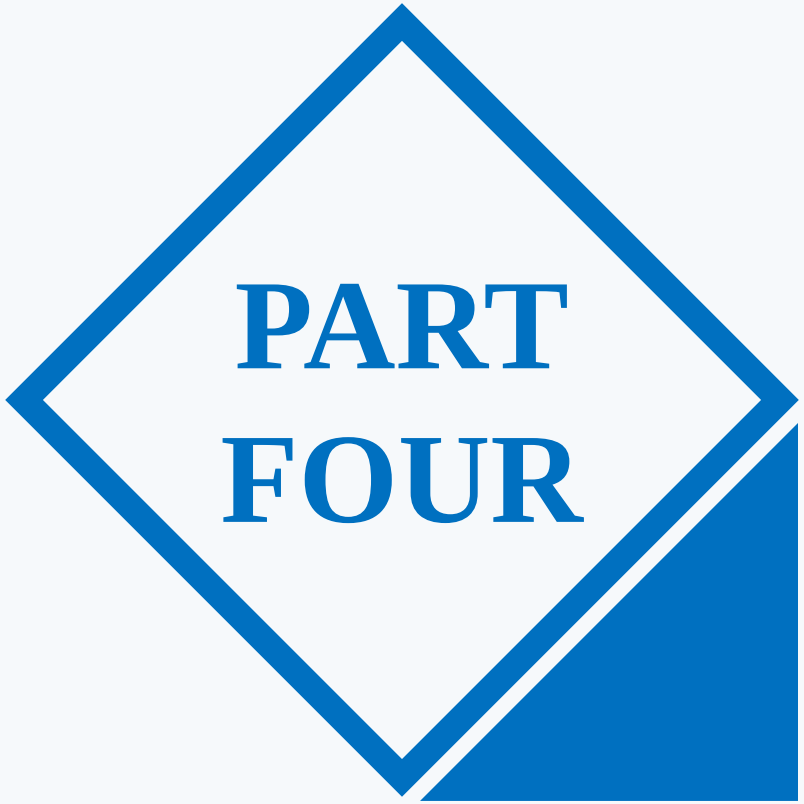
模块名称	模块作用
ping	检查受管主机的网络是否能够连通
yum	安装、更新及卸载软件包
yum_repository	管理主机的软件仓库配置文件
template	复制模板文件到受管主机
copy	新建、修改及复制文件
user	创建、修改及删除用户
group	创建、修改及删除用户组
service	启动、关闭及查看服务状态
get_url	从网络中下载文件
file	设置文件权限及创建快捷方式
cron	添加、修改及删除计划任务
command	直接执行用户指定的命令
shell	直接执行用户指定的命令（支持特殊字符）
debug	输出调试或报错信息
mount	挂载硬盘设备文件
filesystem	格式化硬盘设备文件
lineinfile	通过正则表达式修改文件内容
setup	收集受管主机上的系统及变量信息
firewalld	添加、修改及删除防火墙策略
lvg	管理主机的物理卷及卷组设备
lvol	管理主机的逻辑卷设备

ansible命令的常用参数

参数	作用
-k	手动输入SSH协议的密码
-I	指定主机清单文件
-m	指定要使用的模块名
-M	指定要使用的模块路径
-S	使用su命令
-T	设置SSH协议的连接超时时间
-a	设置传递给模块的参数
--version	查看版本信息
-h	帮助信息

新增软件仓库的信息

仓库名称	EX294_BASE
仓库描述	EX294 base software
仓库地址	file:///media/cdrom/BaseOS
GPG签名	启用
GPG密钥文件	file:///media/cdrom/RPM-GPG-KEY-redhat-release



剧本文件实战

Script Document Actual Combat

剧本文件实战

YAML语言

Ansible服务的剧本（playbook）文件采用YAML语言编写，具有强制性的格式规范，它通过空格将不同信息分组，因此有时会因一两个空格错位而导致报错。

YAML文件的开头需要先写3个减号（---），多个分组的信息需要间隔一致才能执行，而且上下也要对齐，后缀名一般为.yml。

剧本文件在执行后，会在屏幕上输出运行界面，内容会根据工作的不同而变化。

在运行界面中，绿色表示成功，黄色表示执行成功并进行了修改，而红色则表示执行失败。

1. **target**
   用于定义要执行剧本的主机范围。
2. **variable**
   用于定义剧本执行时要用到的变量。
3. **task**
   用于定义将在远程主机上执行的任务列表。
4. **handler**
   用于定义执行完成后需要调用的后续任务。

一个剧本正确的写法

```
[root@linuxprobe~]# vim packages.yml
---
- name: 安装软件包
 hosts: dev,test,prod
 tasks:
          - name: one
            yum:
                        name: mariadb
                        state: latest
[root@linuxprobe~]#
```

- YAML语言编写的Ansible剧本文件会按照从上到下的顺序自动运行，其形式类似于Shell脚本，但格式有严格的要求。
- name字段表示此项play（动作）的名字，用于在执行过程中提示用户执行到了哪一步，以及帮助管理员在日后阅读时能想起这段代码的作用。hosts字段表示要在哪些主机上执行该剧本，多个主机组之间用逗号间隔；如果需要对全部主机进行操作，则使用all参数。tasks字段用于定义要执行的任务，每个任务都要有一个独立的name字段进行命名，并且每个任务的name字段和模块名称都要严格上下对齐，参数要单独缩进。

创建及使用角色

Creating And Using Roles

创建及使用角色

角色的定义

角色（role）这一功能则是自Ansible 1.2版本开始引入的新特性，用于层次性、结构化地组织剧本。角色功能分别把变量、文件、任务、模块及处理器配置放在各个独立的目录中，然后对其进行便捷加载。

技术封装

Ansible服务的角色功能类似于编程中的封装技术—将具体的功能封装起来，用户不仅可以方便地调用它，而且甚至可以不用完全理解其中的原理。

角色的好处

角色的好处就在于将剧本组织成了一个简洁的、可重复调用的抽象对象，使得用户把注意力放到剧本的宏观大局上，统筹各个关键性任务，只有在需要时才去深入了解细节。

角色的获取方法

加载系统内置角色

在使用RHEL系统的内置角色时，我们不需要联网就能实现。用户只需要配置好软件仓库的配置文件，然后安装包含系统角色的软件包rhel-system-roles，随后便可以在系统中找到它们了，然后就能够使用剧本文件调用角色了。

从外部环境获取角色

Ansible Galaxy是Ansible的一个官方社区，用于共享角色和功能代码，用户可以在网站自由地共享和下载Ansible角色。该社区是管理和使用角色的不二之选。

自行创建角色

除了能够使用系统自带的角色和从Ansible Galaxy中获取的角色之外，也可以自行创建符合工作需求的角色。这种定制化的编写工作能够更好地贴合生产环境的实际情况，但难度也会稍高一些。

加载系统内置角色

角色名称	作用
rhel-system-roles.kdump	配置kdump崩溃恢复服务
rhel-system-roles.network	配置网络接口
rhel-system-roles.selinux	配置SELinux策略及模式
rhel-system-roles.timesync	配置网络时间协议
rhel-system-roles.postfix	配置邮件传输服务
rhel-system-roles.firewall	配置防火墙服务
rhel-system-roles.tuned	配置系统调优选项

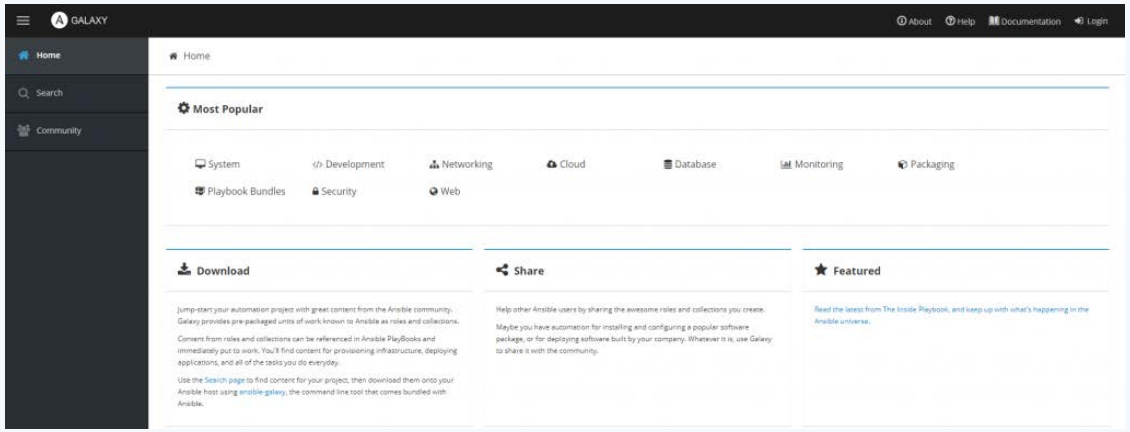
Ansible常用变量汇总

参数	作用
hostname	NTP服务器的主机名
iburst	启用快速同步

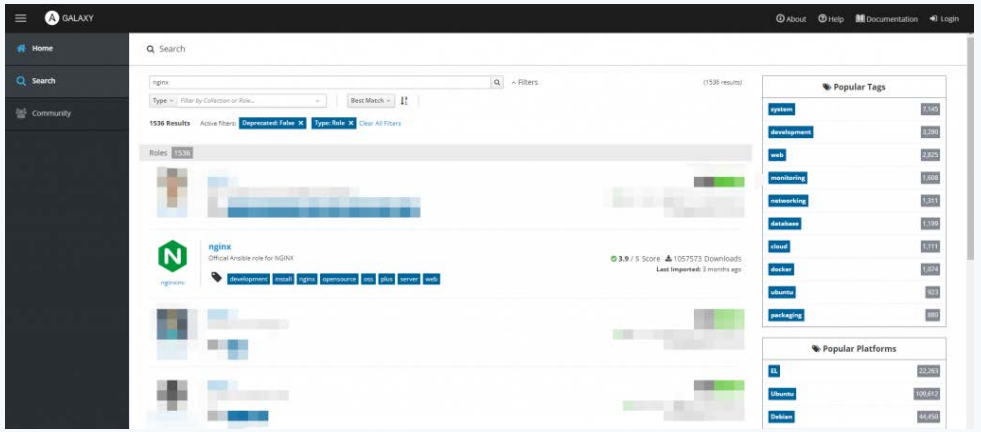
timesync_ntp_servers变量的参数含义

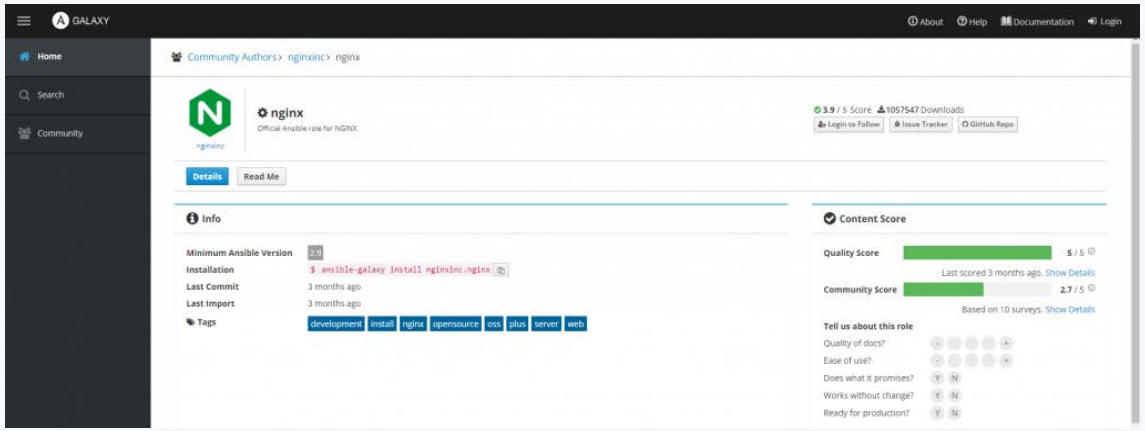
从外部环境获取角色

Ansible Galaxy的官网首页面



在搜索界面中找到的nginx角色信息





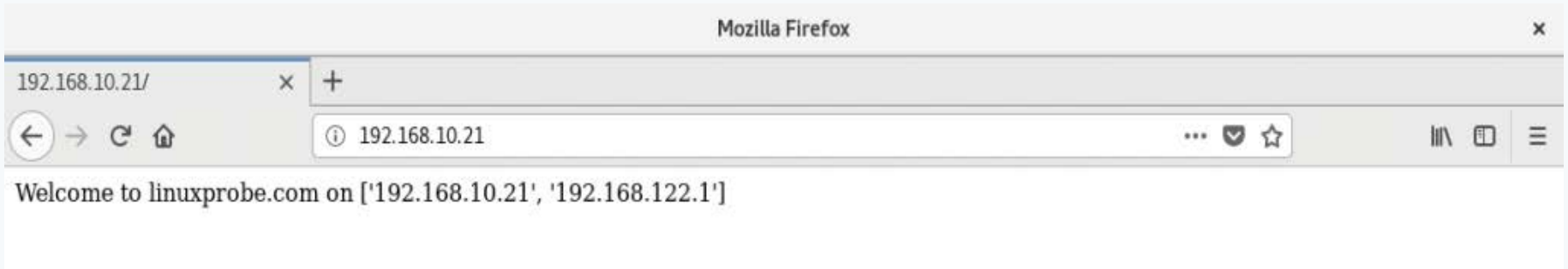
nginx角色的详情页

自行创建角色

目录	含义
defaults	包含角色变量的默认值（优先级低）
files	包含角色执行任务时所引用的静态文件
handlers	包含角色的处理程序定义
meta	包含角色的作者、许可证、平台和依赖关系等信息
tasks	包含角色所执行的任务
templates	包含角色任务所使用的Jinja2模板
tests	包含用于测试角色的剧本文件
vars	包含角色变量的默认值（优先级高）

Ansible常用变量汇总

随机访问一台主机的网站主页面



创建和使用逻辑卷

Create And Use Logical Volumes

创建和使用逻辑卷

逻辑卷设备

创建一个能批量、自动管理逻辑卷设备的剧本，不但能大大提高硬盘设备的管理效率，而且还能避免手动创建带来的错误。

让操作更标准

Ansible模块化的功能让操作更标准，只要在执行过程中无报错，那么便会依据远程主机的系统版本及配置自动做出判断和操作，不用担心因系统变化而导致命令失效的问题。

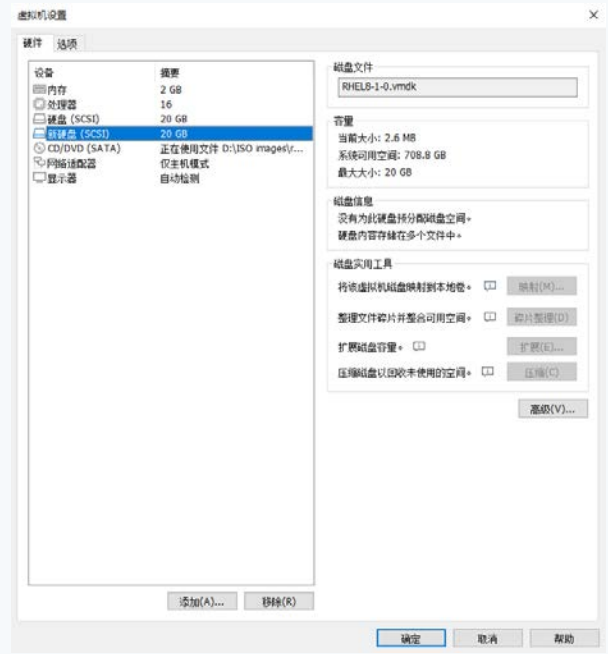
进行判断

Ansible服务在执行剧本文件时会进行判断：如果该文件或该设备已经被创建过，或是某个动作（play）已经被执行过，则绝对不会再重复执行；而使用Shell脚本有可能导致设备被重复格式化，导致数据丢失。

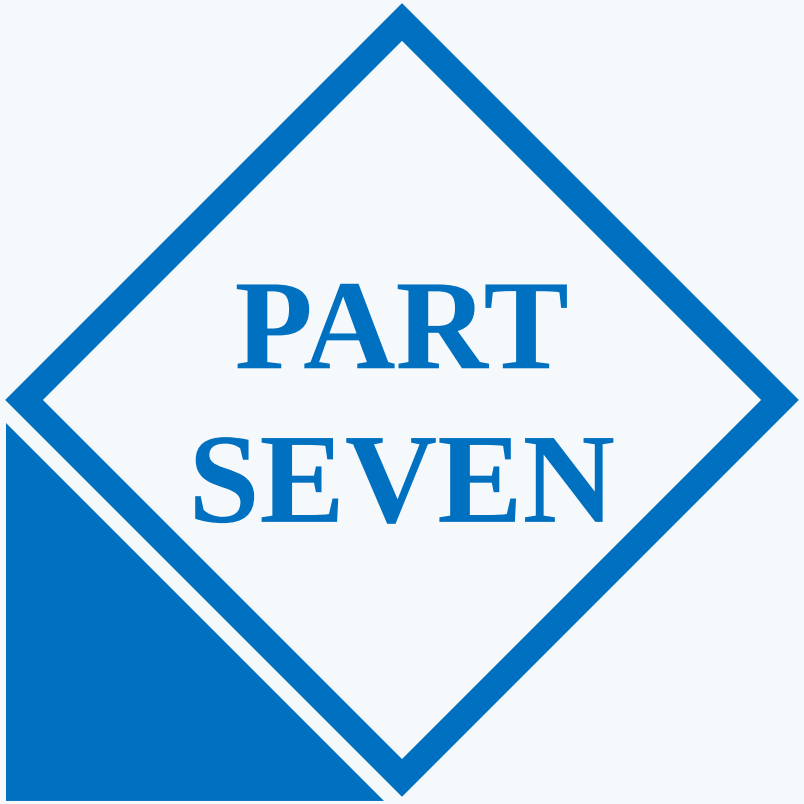
创建和使用逻辑卷

添加一块新硬盘

设置硬盘类型



新硬盘添加完毕



判断主机组名

Determine Host Group Name

判断主机组名

1. 若主机在dev分组中，则修改/etc/issue文件内容为Development;
2. 若主机在test分组中，则修改/etc/issue文件内容为Test;
3. 若主机在prod分组中，则修改/etc/issue文件内容为Production。

管理文件属性

Manage File Properties

file模块的基本参数

Ansible服务将常用的文件管理功能都合并到了file模块中，大家不用再为了寻找模块而“东奔西跑”了。

1. path参数定义了文件的路径
2. owner参数定义了文件所有者
3. group参数定义了文件所属组
4. mode参数定义了文件权限
5. src参数定义了源文件的路径
6. dest参数定义了目标文件的路径
7. state参数则定义了文件类型

管理密码库文件

Manage Password Library Files

管理密码库文件

vault

自 Ansible 1.5 版本发布后，vault作为一项新功能进入到了运维人员的视野。

优势

它不仅能对密码、剧本等敏感信息进行加密，而且还可以加密变量名称和变量值，从而确保数据不会被他人轻易阅读。

功能

使用ansible-vault命令可以实现内容的新建（create）、加密（encrypt）、解密（decrypt）、修改密码（rekey）及查看（view）等功能。

复习题

✓ **1．当前已经搭建好软件仓库，但却不能用dnf命令安装Ansible服务。这有可能是什么原因呢?**

答：RHEL 8系统中默认的BaseOS和AppStream软件仓库不包含Ansible服务软件包，需要额外配置EPEL安装源。

✓ **2．当/etc/ansible/ansible.cfg与~/.ansible.cfg两个主配置文件都同时存在时，以哪个为准?**

答：个人家目录中的主配置文件的优先级更高。

✓ **3．使用Ansible的哪个模块能启动服务，使用Ansbile的哪个模块能挂载硬盘设备文件?**

答：使用service模块可以启动服务，使用mount模块可以挂载设备文件。

✓ **4．我们想了解一个模块的作用，可以使用什么命令来查询它的帮助信息?**

答：可以使用ansible-doc命令查询模块的帮助信息。

✓ **5．Ansible角色有几种获取方法?**

答：有3种，分别是加载系统内置角色、从外部环境获取角色以及自行创建角色。

✓ **6．在执行剧本文件时，出现了黄色显示的changed字样，这表示什么意思?**

答：表示剧本文件执行成功并进行了修改。

✓ **7．在使用ansible-vault命令进行加密时，默认使用的是哪种加密方式?**

答：AES 256。

祝同学们学习顺利，爱上Linux系统。