配合 Cisco Nexus 设备使用 Chef 客户端

安装指南

简介

要修复软件中的问题，传统的方法是通过引导变量变更流程或不中断服务软件升级 (ISSU) 升级整个软件安装。但思科® NX-OS 软件可以通过安装补丁修复特定软件缺陷，无需通过 ISSU 进行任何软件升级，也不会造成流量中断。

有了 Chef 客户端，您可以自动执行如下操作：

- 设备软件的补丁修复和解除补丁
- 配置管理
- 设备统计信息收集

本文档介绍 Cisco Nexus® 设备上的 Chef 客户端的安装和配置， 重点介绍如何使用 Chef 客户端安装补丁来修复 Cisco Nexus 9000 系列交换机上的软件缺陷。

范围和需求

本文档介绍如何安装和运行 Chef 客户端以为以下设备进行补丁修复：

- Cisco Nexus 3000 系列交换机
- Cisco Nexus 9000 系列交换机

Cisco Nexus 设备上的 Chef 客户端设置

客户端配置前提条件

本节介绍在 Cisco Nexus 设备上安装 Chef 客户端的配置前提条件。

允许与 Chef 客户端进行 SSL 通信

Chef 服务器使用 SSL 在端口 443 上与客户端通信。设备的管理界面可能会丢弃所有 SSL 通信，具体取决于平台。Cisco Nexus3000 系列设备要求执行额外配置以允许在端口 443（图 1）上进行 SSL 通信。

可通过以下两种方式的任意一种允许此行为：

- 覆盖 Chef 服务器的默认 SSL 端口设置。
- 移除 Cisco Nexus 3000 系列管理接口的默认配置策略。

图 1. 允许与 Cisco Nexus3000 系列的 Chef 客户端进行 SSL 通信

```
no mgmt-policy MGMT_DEF_POLICY106
```

注： 图 1 中的配置仅适用于 Cisco Nexus3000 系列交换机。

配置准确的网络时间协议设置

设备需要使用准确的网络时间协议 (NTP) 设置进行配置（图 2）。必须具备此配置以才能执行故障排除和日志分析。强烈建议您使用 NTP 同步设备与 Chef 环境以保持时间戳一致。

图 2. 在 Cisco Nexus 设备上配置 NTP

```
ntp server 10.81.254.202 use-vrf management
```

将 Chef 客户端复制到设备上

您需要将 Chef 客户端 OVA 文件复制到 Cisco Nexus 设备上，才能继续进行安装（图 3）。

图 3. 将 Chef 客户端复制到 Cisco Nexus 设备上

```
copy scp://username@server/path/n9k_chef.ova bootflash: vrf management
```

将 Chef 验证文件复制到设备上

必须具备 Chef 验证文件，才能在服务器上注册 Chef 客户端（图 4 和 5）。必须进行注册才能对客户端和服务器之间的会话进行身份验证。默认情况下，chef 验证文件称为 chef-validator.pem。不过，可以在服务器上创建新的文件并用于客户端。

图 4. 将 Chef 验证文件复制到 Cisco Nexus 设备上

```
copy scp://username@server/path/chef-validator.pem bootflash: vrf management
```

图 5. 将 Chef 验证文件复制到 Chef 客户端上

```
copy bootflash:chef-validator.pem bootflash: virtual-instance/chef/rootfs/tmp/ssl
```

客户端安装和激活

本部分介绍在 Cisco Nexus 设备上安装和激活 Chef 客户端所需执行的步骤。

在思科 NX-OS 上安装 Chef 客户端

使用复制到设备 Bootflash 的 OVA 文件在 Cisco Nexus 设备上安装客户端（图 6）。然后验证安装（图 7）。

图 6. 在 Cisco Nexus 设备上安装 Chef 客户端

```
N9K-INS# virtual-service install name chef package bootflash:n9k_chef.ova


Note: Installing package 'bootflash:/n9k_chef.ova' for virtual service 'chef'.
Once the install has finished, the VM may be activated.Use 'show virtual-service
list' for progress.


2013 Sep 25 00:30:22 N9K-INS %$ VDC-1 %$ %VMAN-2-INSTALL_STATE: Successfully
installed virtual service 'chef'
```

图 7. 在 Cisco Nexus 设备上验证 Chef 安装

```
N9K-INS# show virtual-service list


Virtual Service List:


Name                      Status               Package Name
------------------------------------------------------------------------
chef                      Installed            n9k_chef.ova
```

在思科 NX-OS 上激活 Chef

在成功安装客户端后，需要将其激活，然后才能开始配置，以在 Chef 服务器上注册（图 8 和 9）。

图 8. 激活 Chef 服务

```
N9K-INS(config)# virtual-service chef
N9K-INS(config-virt-serv)# activate

Note: Activating virtual-service 'chef', this might take a few minutes.Use 'show
virtual-service list' for progress.

N9K-INS(config-virt-serv)#

2013 Sep 25 00:41:22 N9K-INS %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE: Successfully
activated virtual service 'chef'
```

图 9. 在思科 NX-OS 上验证 Chef 服务是否激活

```
N9K-INS# show virtual-service list

Virtual Service List:

Name                      Status               Package Name
------------------------------------------------------------------------
chef                      Activated            n9k_chef.ova
```

客户端配置

启用 VTY 服务

启用 VTY 服务（图 10）。

图 10. 启用 VTY 服务

```
onep
  transport type tcp
  service set vty
```

为 Chef 客户端配置域名服务设置

强烈建议在 Cisco Nexus 设备上为 Chef 客户端配置域名服务 (DNS)。Chef 服务器和节点对象的名称解析需要使用此配置（图 11）。

图 11. Chef 客户端的 DNS 配置

```
onep applications chef
  chef v0.8
   vrf management
   name-server 10.123.123.1
   domain-name cisco.com
```

配置 Chef 客户端

需要配置 chef 客户端参数才能在服务器上注册（图 12）。此步骤中配置的参数如下：

- Chef 服务器完全限定域名 (FQDN)
- Chef 服务器端口号
- Cisco Nexus 设备上的客户端节点名称

图 12. 配置 Chef 客户端

```
onep applications chef
  chef v0.8
   server chef-server-ins-f.cisco.com port 443
   vrf management
   validation-client-name chef-validator
   interval 60
   node-name N9K-INS
```

向服务器注册 Chef 客户端

本部分高度概括 Chef 客户端运行流程以及在 Cisco Nexus 设备上向服务器注册所需执行的步骤。

Chef 客户端运行流程

Chef 客户端可以按以下三种方式的任何一种运行：

- 后台守护程序：客户端按所配置的间隔运行和处理运行列表。
- 一次性模式：客户端运行并处理运行列表一次。
- 为什么是运行模式：使用此模式检查如果实际上运行了客户端应该会如何处理。

在 Cisco Nexus 设备上运行客户端

在本部分介绍的补丁修复使用案例中，Chef 客户端将在一次性模式中运行。客户端将在初始配置后运行，以在服务器上注册客户端（图 13)。节点将在第一次客户端运行后在服务器上注册（图 14）。

图 13. Cisco Nexus 设备上的客户端处理

```
execute onep application chef v0.8 chef client-oneshot
```

图 14. 在 Chef 服务器上注册客户端

```
TME-1-9508-2# show onep app chef v0.8 chef client last-exec-log

# Logfile created on 2013-09-30 12:18:11 +0000 by logger.rb/31641
[2013-09-30T12:18:11+00:00] INFO: Forking chef instance to converge...
[2013-09-30T12:18:11+00:00] INFO: Fork successful.Waiting for new chef pid: 15601
[2013-09-30T12:18:11+00:00] INFO: Forked instance now converging
[2013-09-30T12:18:11+00:00] INFO: *** Chef 11.4.0 ***
[2013-09-30T12:18:12+00:00] WARN: unable to detect ipaddress
[2013-09-30T12:18:12+00:00] WARN: unable to detect macaddress
[2013-09-30T12:18:12+00:00] WARN: unable to detect ip6address
[2013-09-30T12:18:12+00:00] INFO: Run List is []
[2013-09-30T12:18:12+00:00] INFO: Run List expands to []
[2013-09-30T12:18:12+00:00] INFO: Starting Chef Run for TME-1-9508-2
[2013-09-30T12:18:12+00:00] INFO: Running start handlers
[2013-09-30T12:18:12+00:00] INFO: Start handlers complete.
[2013-09-30T12:18:12+00:00] INFO: Loading cookbooks []
[2013-09-30T12:18:12+00:00] WARN: Node TME-1-9508-2 has an empty run list.
[2013-09-30T12:18:12+00:00] INFO: Chef Run complete in 0.228609717 seconds
[2013-09-30T12:18:12+00:00] INFO: Running report handlers
[2013-09-30T12:18:12+00:00] INFO: Creating Cisco JSON run report
[2013-09-30T12:18:12+00:00] INFO: Report handlers complete
[2013-09-30T12:18:12+00:00] INFO: Forked child successfully reaped (pid: 15601)
```

Chef 服务器上的配置

在服务器上配置配方

要在设备上执行的与操作相关的配方应在 Chef 工作站上配置并上传到服务器。本部分提供为在 Cisco Nexus 设备上安装补丁所创建配方的摘要（图 15）。

图 15. 用于 Cisco Nexus9000 系列设备补丁修复的 Chef 配方

```
cisco_device "#{name}" do
  username "admin"
  password "xxx"
  action :create
end

..
..
..
..
..

cisco_package "TME-1-9508-2/n9000_CSCuj11591.gbin" do
  source "bootflash:///n9000_CSCuj11591.gbin"
  action :activate
end

..
..
..

cisco_device "TME-1-9508-2" do
  action :destroy
end
```

为节点配置运行列表

在 Chef 服务器上注册节点后，可使用相关配方在服务器上配置运行列表，这些配方将在每次运行服务器时在节点上运行（图 16 和 17）。

图 16. 清空新节点的运行列表

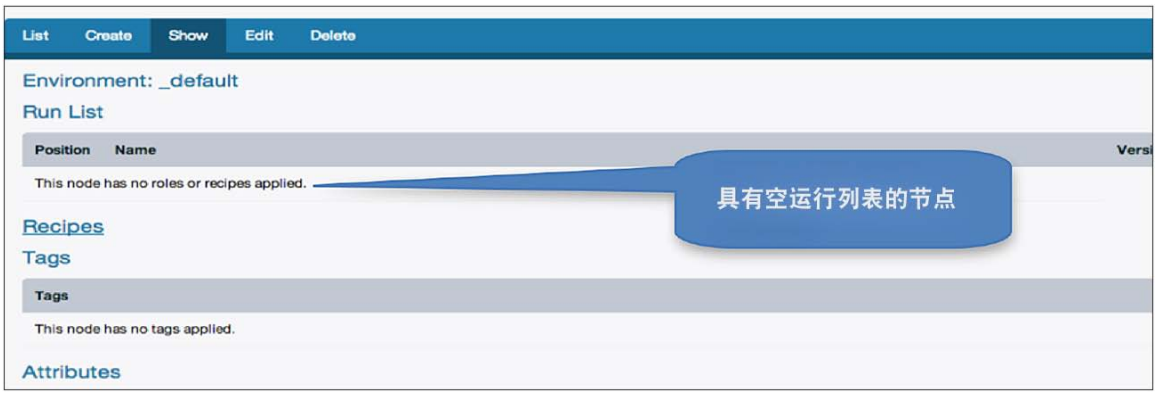


图 17. 将配方添加到节点运行列表

设备补丁修复测试案例

软件缺陷概述

漏洞 ID

CSCuj11591 FD，在用于 security_nginx.out: 功能 nginx 启用/禁用的 securityd 中存在溢漏。

缺陷背景

功能 nginx 用于通过交互式 API (iAPI) 启用对 Cisco Nexus9000 系列交换机的 HTTP 访问。如果未在思科 NX-OS 中启用 nginx 功能，iAPI 将无法与 Cisco Nexus9000 系列交换机通信。

图 18 显示启用 nginx 功能的过程。

图 18. 启用 nginx 功能

```
N9K-INS(config)# feature nginx
N9K-INS(config)# end
```

在每次运行 nginx 功能激活和取消激活时，在安全 ID（安全）中都检测到了文件描述符 (FD) 溢漏（图 19 和 20）。

图 19. 启用和禁用 nginx 功能缺陷

```
N9K-INS(config)# no feature nginx
N9K-INS(config)# feature nginx
N9K-INS(config)# no feature nginx
N9K-INS(config)# no feature nginx
N9K-INS(config)# feature nginx
N9K-INS(config)# no feature nginx
```

图 20. 软件缺陷导致的安全内存溢漏

```
COMMAND     PID    USER   FD   TYPE   DEVICE SIZE/OFF   NODE NAME
securityd 8203    root   16r   REG   0,20   10 37760 /var/tmp/security_nginx.out
(deleted)
securityd 8203    root   17r   REG   0,20   10 66744 /var/tmp/security_nginx.out
(deleted)
securityd 8203    root   18r   REG   0,20    5 37863 /var/tmp/security_nginx.out
(deleted)
securityd 8203    root   19r   REG   0,20    5 65969 /var/tmp/security_nginx.out
(deleted)
nginx     8301    root   16r   REG   0,20   10 37760 /var/tmp/security_nginx.out
(deleted)
nginx     8301    root   17r   REG   0,20   10 66744 /var/tmp/security_nginx.out
(deleted)
nginx     8301    root   18r   REG   0,20    5 37863 /var/tmp/security_nginx.out
(deleted)
```

使用补丁修复配方运行 Chef 客户端

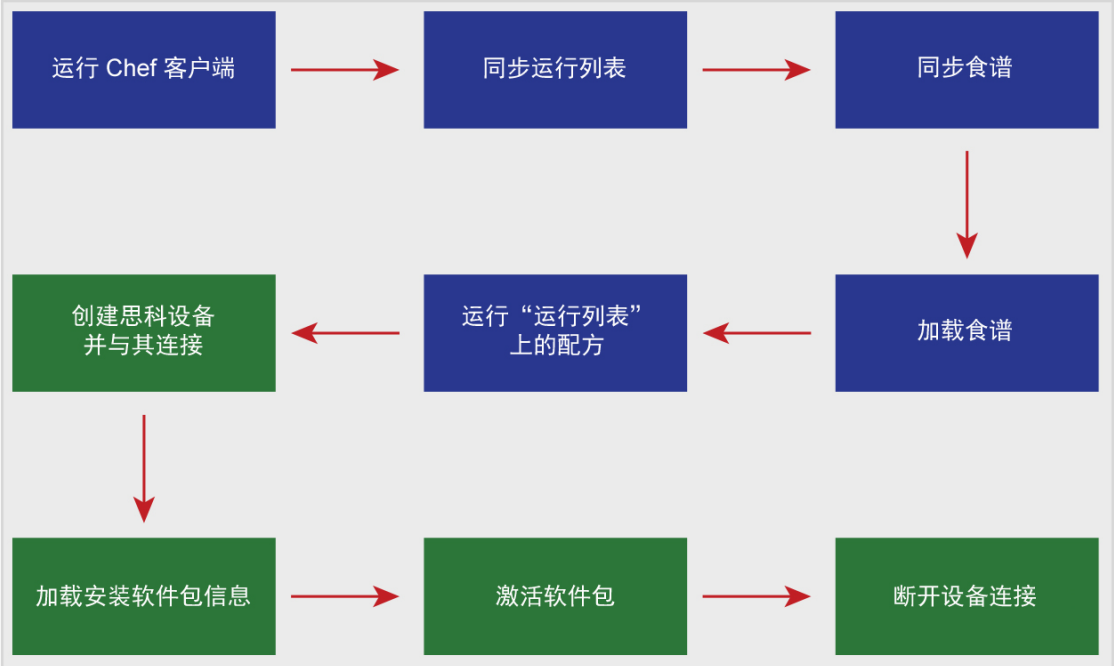
此场景显示在一次性模式下运行 Chef 客户端以补丁修复 Cisco Nexus 设备的情形（图 21）。此设备具有适用于安装设备补丁的正确配方（图 22）。

图 21. 在一次性模式下运行 Chef 客户端

```
N9K-INS# execute onep application chef v0.8 chef client-oneshot

Execute operation in progress, please see status in log using 'sh onep
applications chef <ver><instance name> client last-exec-log'
```

图 22. Chef 客户端处理 Cisco Nexus 设备补丁修复的流程



在日志中验证运行

检查日志以验证 Chef 运行（图 23 和 24）。

图 23. 使用 Chef 运行日志进行验证

```
N9K-INS# show onep application chef v0.8 chef client last-exec-log

# Logfile created on 2013-09-24 22:44:42 +0000 by logger.rb/31641
[2013-09-24T22:44:42+00:00] INFO: Forking chef instance to converge...
[2013-09-24T22:44:42+00:00] INFO: Fork successful.Waiting for new chef pid: 2294
[2013-09-24T22:44:42+00:00] INFO: Forked instance now converging
[2013-09-24T22:44:42+00:00] INFO: *** Chef 11.4.0 ***
[2013-09-24T22:44:43+00:00] WARN: unable to detect ipaddress
[2013-09-24T22:44:43+00:00] WARN: unable to detect macaddress
```

```
[2013-09-24T22:44:43+00:00] WARN: unable to detect ip6address
[2013-09-24T22:44:43+00:00] INFO: Run List is [recipe[utit::9K_patch]]
[2013-09-24T22:44:43+00:00] INFO: Run List expands to [utit::9K_patch]
[2013-09-24T22:44:43+00:00] INFO: Starting Chef Run for N9K-INS
[2013-09-24T22:44:43+00:00] INFO: Running start handlers
[2013-09-24T22:44:43+00:00] INFO: Start handlers complete.
[2013-09-24T22:44:43+00:00] INFO: Loading cookbooks [utit]
[2013-09-24T22:44:43+00:00] INFO: Removing cookbooks/cisco_installmgr/results
from the cache; its cookbook is no longer needed on this client.
[2013-09-24T22:44:43+00:00] INFO: Removing
cookbooks/cisco_installmgr/CHANGELOG.md from the cache; its cookbook is no longer
needed on this client.
..
..
..
..
[2013-09-24T22:44:43+00:00] INFO: Removing
cookbooks/cisco_installmgr/recipes/9K_patch.rb from the cache; its cookbook is no
longer needed on this client.
[2013-09-24T22:44:43+00:00] INFO: Removing cookbooks/cisco_installmgr/metadata.rb
from the cache; its cookbook is no longer needed on this client.
[2013-09-24T22:44:43+00:00] INFO: Storing updated
cookbooks/cisco_installmgr/recipes/default.rb in the cache.
[2013-09-24T22:44:43+00:00] INFO: Storing updated
cookbooks/cisco_installmgr/recipes/rp32.rb in the cache.
..
..
..
..
[2013-09-24T22:44:44+00:00] INFO: Storing updated
cookbooks/cisco_installmgr/recipes/rp28.rb in the cache.
[2013-09-24T22:44:44+00:00] INFO: Storing updated
cookbooks/cisco_installmgr/metadata.rb in the cache.
[2013-09-24T22:44:44+00:00] INFO: Storing updated
cookbooks/cisco_installmgr/CHANGELOG.md in the cache.
[2013-09-24T22:44:44+00:00] INFO: Storing updated
cookbooks/cisco_installmgr/results in the cache.
[2013-09-24T22:44:44+00:00] INFO: Storing updated
cookbooks/cisco_installmgr/README.md in the cache.
[2013-09-24T22:44:45+00:00] WARN: Cloning resource attributes for
cisco_device[N9K-INS] from prior resource (CHEF-3694)
[2013-09-24T22:44:45+00:00] WARN: Previous cisco_device[N9K-INS]:
/var/chef/cache/cookbooks/cisco_installmgr/recipes/9K_patch.rb:47:in `from_file'
[2013-09-24T22:44:45+00:00] WARN: Current cisco_device[N9K-INS]:
/var/chef/cache/cookbooks/cisco_installmgr/recipes/9K_patch.rb:105:in `from_file'
[2013-09-24T22:44:45+00:00] INFO: Processing cisco_device[N9K-INS] action create
(cisco_installmgr::9K_patch line 47)
[2013-09-24T22:44:45+00:00] INFO: In Device Provider cisco_device[N9K-INS] , addr
172.21.128.76
[2013-09-24T22:44:45+00:00] INFO: In the Device Provider cisco_device[N9K-INS]
```

从服务器下载的配方

```
[2013-09-24T22:44:45+00:00] INFO: dev: N9K-INS, login: admin, psswd xxx
[2013-09-24T22:44:45+00:00] INFO: app is nill...so creating
[2013-09-24T22:44:45+00:00] INFO: element is nill, so calling new
[2013-09-24T22:44:45+00:00] INFO: Device is connected over network
[2013-09-24T22:44:45+00:00] INFO: Create element
called for Device: N9K-INS,ipaddr 172.21.128.76 with
username : admin, password : xxx
[2013-09-24T22:44:45+00:00] INFO: Processing
cisco_package[N9K-INS/n9000_CSCuj11591.gbin] action
activate (cisco_installmgr::9K_patch line 71)
[2013-09-24T22:44:45+00:00] INFO: In the Package Provider cisco_package[N9K-
INS/n9000_CSCuj11591.gbin]
[2013-09-24T22:44:45+00:00] INFO: The package source is
bootflash:///n9000_CSCuj11591.gbin and name is n9000_CSCuj11591.gbin
[2013-09-24T22:44:45+00:00] INFO: find device N9K-INS
[2013-09-24T22:44:45+00:00] INFO: In action activate
[2013-09-24T22:44:45+00:00] INFO: The package initial state is 1
[2013-09-24T22:44:45+00:00] INFO: This is executed within converge statement
[2013-09-24T22:44:55+00:00] INFO: End of action activate, the state is 3
[2013-09-24T22:44:55+00:00] INFO: Processing cisco_device[N9K-INS] action destroy
(cisco_installmgr::9K_patch line 105)
[2013-09-24T22:44:55+00:00] INFO: In Device Provider cisco_device[N9K-INS] , addr
172.21.128.76
[2013-09-24T22:44:55+00:00] INFO: In the Device Provider cisco_device[N9K-INS]
[2013-09-24T22:44:55+00:00] INFO: Device is already connected
[2013-09-24T22:44:55+00:00] INFO: Element is still connected, so disconnecting it
[2013-09-24T22:44:59+00:00] INFO: onep_destroy_element has been called for
Device: N9K-INS
[2013-09-24T22:44:59+00:00] INFO: Chef Run
complete in 16.267219576 seconds
[2013-09-24T22:44:59+00:00] INFO: Running report handlers
[2013-09-24T22:44:59+00:00] INFO: Creating Cisco JSON run report
[2013-09-24T22:44:59+00:00] INFO: Report handlers complete
[2013-09-24T22:44:59+00:00] INFO: Forked child successfully reaped (pid: 2294
```

激活补丁

销毁连接并清理

图 24. 在 Cisco Nexus 设备上验证已安装软件包

```
TME-1-9508-2# sh install active
Boot Images:
        Kickstart Image: bootflash:/n9000_dk9.6.1.1.257.gbin
        System Image: package:/isanboot/bin/images/sys

Active Packages:
        n9000_CSCuj11591.gbin
```

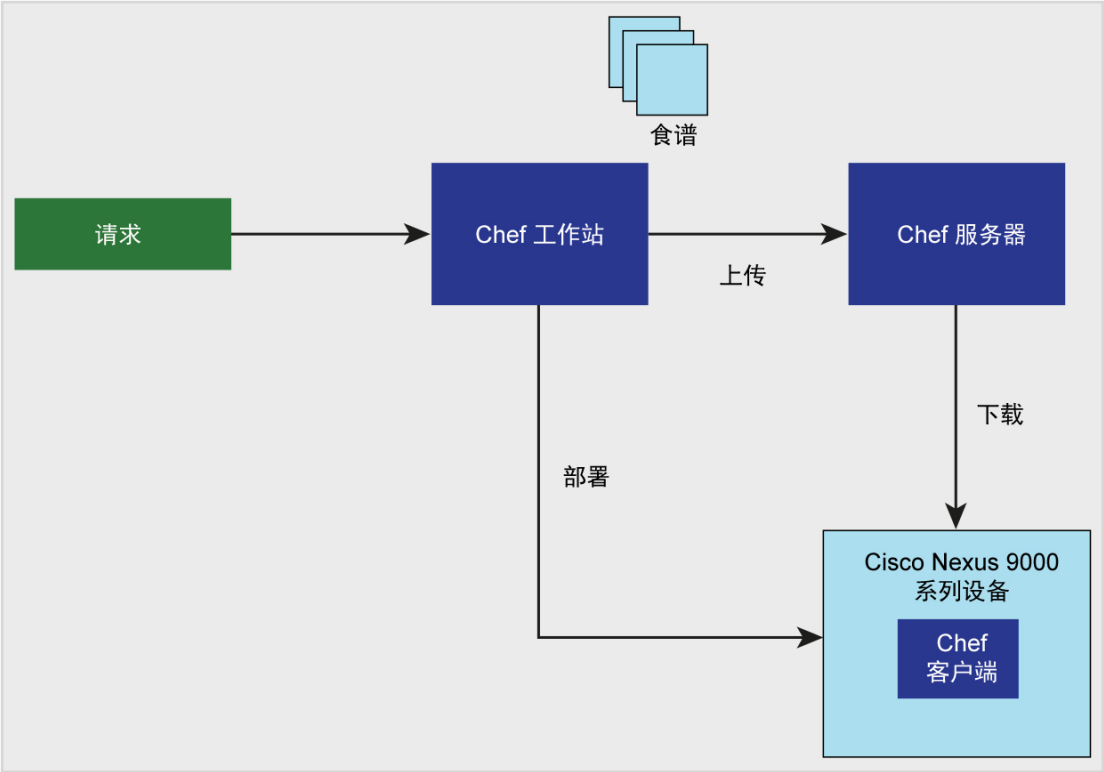
附录 A. Chef 概念

Chef 概述

Chef 是一种系统和云基础设施自动化框架，通过它可以轻松地将服务器和应用部署到任何物理、虚拟或云位置，而且不受基础设施规模大小的影响。

Chef 使用刀工具在该环境中执行各种任务。此刀工具可以在服务器本身上运行，也可以在双服务器模式下，用于实施了运行此刀工具的服务器和工作站中。管理员用户登录运行刀的相关系统以执行各种 Chef 任务，例如创建和修改食谱以及节点管理。食谱通过刀进行配置或上传到服务器。然后，食谱将被推送到受管节点（图 25）。

图 25. Chef 运行模式



定义

- Chef 服务器：服务器充当配置数据的控制中心。服务器存储食谱、向节点应用的策略以及描述各个受 Chef 客户端管理的已注册节点的元数据。
- Chef 工作站：工作站是配置为运行刀工具以同步 Chef 存储库 (chef-repo) 并与单个服务器交互的计算机。工作站是大多数用户执行他们的大部分工作的位置，执行的工作包括：
  - 开发食谱和配方（并使用 Ruby 编写食谱和配方）
  - 保持 chef-repo 与版本来源控制同步
  - 使用刀工具将项目从 chef-repo 上传到服务器
  - 配置组织策略，包括定义角色和环境并帮助确保关键数据存储在数据包中
  - 根据需要与节点交互，例如执行引导程序操作

注： 刀工具可在 Chef 服务器上运行，无需安排专用工作站来运行。

- 刀：刀是提供本地 chef-repo 和服务器之间界面的命令行工具。刀可以帮助用户管理：
  - 节点
  - 食谱和配方
  - 角色
  - JSON 数据（数据包）的存储空间，包括加密数据
  - 环境
  - 云资源，包括调配
  - 在管理工作站上执行的 Chef 客户端安装
  - 服务器上索引数据的搜索
- Chef 客户端：Chef 客户端是在已向服务器注册的每个节点上本地运行的代理。Chef 客户端运行时，会执行使节点进入预期状态所需的所有步骤。
- 节点：节点是被配置为由 Chef 客户端维护的任何服务器或虚拟服务器。节点可以是运行 Chef 客户端的任何物理、虚拟或云设备。
- 食谱：食谱是配置和策略分发的基本单位。每个食谱定义一个场景，例如安装和配置 MySQL 所需的一切，其中包含支持该场景所需的所有组件。
- 食谱：食谱是组织内最基本的配置元素。配方：
  - 使用 Ruby 编写，Ruby 是一种用于以可预测模式读取和运行的编程语言
  - 基本上是 Ruby 语法编写的资源集合，包括一些相关的帮助代码
  - 必须定义配置部分系统所需的一切
  - 必须存储在食谱中
  - 可以包含在配方中
  - 可能使用搜索查询结果和读取数据包内容（包括加密数据包）
  - 可能依赖于一个（或多个）配方
  - 可以进行标记以便于创建存在于组织可能设定的标准命名约定之外的任意分组
  - 必须添加到运行列表中，然后才能由 Chef 客户端使用
  - 总是按运行列表中列出的相同顺序处理
- 运行列表：运行列表是按确切顺序运行的角色和配方的有序列表。运行列表总是特定于它运行所在的节点，尽管多个节点可以拥有类似甚至完全相同的运行列表。

Chef 运行的流程

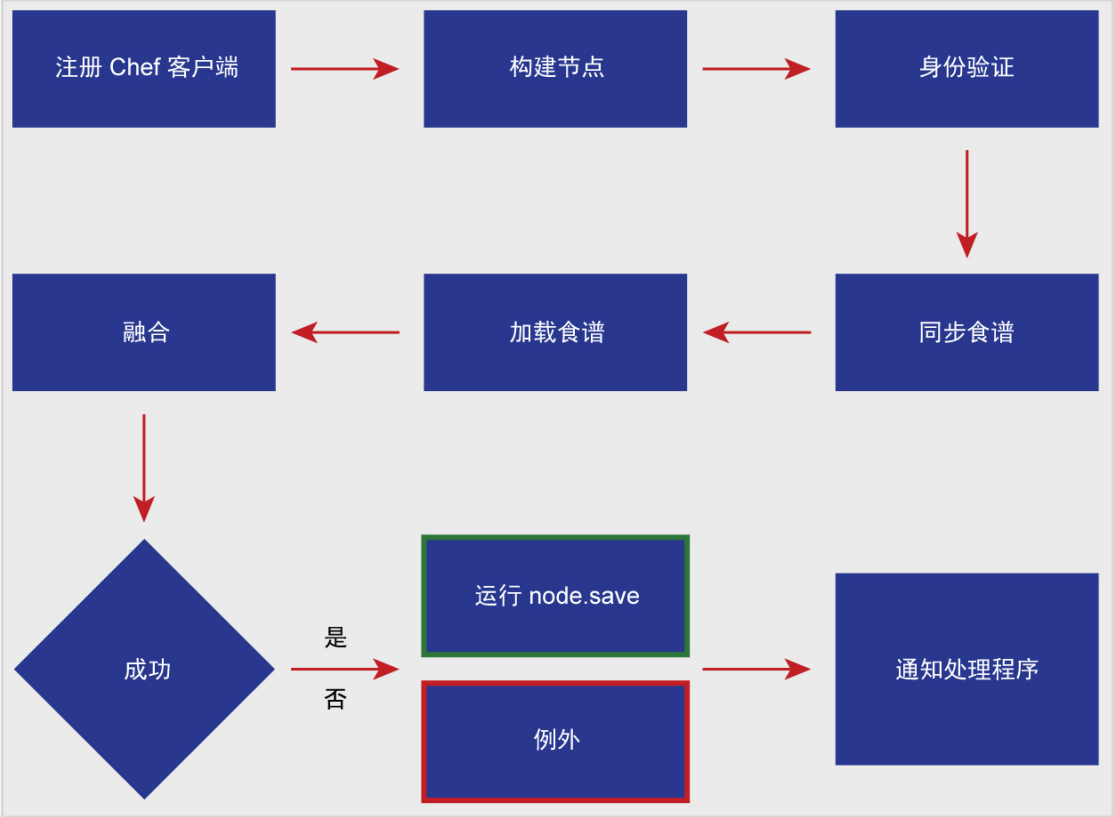
以下步骤发生在 Chef 客户端运行期间（图 26）：

- 注册节点并向服务器进行身份验证。
- 在服务器上构建节点对象。
- 同步食谱。
- 通过加载所需的以下内容编译资源收集：
  - 食谱
  - 配方

- 属性
- 任何其他依赖关系

- 执行适用于运行列表的操作以配置节点。
- 执行例外和通知分析及处理。

图 26. Chef 运行的流程



更多详情

请参阅 docs.opscode.com。

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 www.cisco.com/go/offices 中。

美国印刷 C07-729907-00 10/13