



Red Hat Virtualization 4.4

灾难恢复指南

为灾难恢复配置 Red Hat Virtualization 4.4

Red Hat Virtualization 4.4 灾难恢复指南

为灾难恢复配置 Red Hat Virtualization 4.4

Enter your first name here. Enter your surname here.

Enter your organisation's name here. Enter your organisational division here.

Enter your email address here.

法律通告

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Disaster_Recovery_Guide.ent file |.

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

您可以对 Red Hat Virtualization 进行配置，确保即使在发生灾难时环境仍保持运行。本文档提供了配置 Red Hat Virtualization 环境以进行灾难恢复的信息和说明。

目录

第 1 章 灾难恢复解决方案	3
第 2 章 ACTIVE-ACTIVE (主动-主动) 灾难恢复	4
2.1. ACTIVE-ACTIVE 概述	4
2.2. 网络注意事项	5
2.3. 存储注意事项	5
2.4. 配置自托管引擎STRETCH 集群环境	6
2.5. 配置独立管理器 STRETCH 集群环境	7
第 3 章 ACTIVE-PASSIVE (主动-被动) 灾难恢复	8
3.1. 主动-被动概述	8
3.2. 网络注意事项	10
3.3. 存储注意事项	10
3.4. 创建所需的 ANSIBLE PLAYBOOK	10
3.4.1. Ansible 任务的 ovirt-dr 脚本	11
3.4.2. 创建用于生成映射文件的 Playbook	12
3.4.3. 创建 Failover 和 Failback Playbook	12
3.4.4. 创建 Playbook 以清理主要站点	14
3.5. 执行故障	14
3.6. 清理主站点	14
3.7. 执行故障转移	15
附录 A. 映射文件属性	16
附录 B. 测试主动配置	19
B.1. 磁盘故障切换测试	19
B.2. 磁盘故障切换和反馈测试	19
B.3. 完全故障和反馈测试	20
附录 C. 法律通知	22

第 1 章 灾难恢复解决方案

Red Hat Virtualization 支持两种类型的灾难恢复解决方案，以确保环境能够在站点中断时恢复。两种解决方案都支持两个站点，每个站点都需要复制存储。

Active-Active（主动-主动）灾难恢复

此解决方案使用扩展集群配置来实施。这意味着有一个 RHV 环境，其中包含一个集群，包含能够在主站点和次站点中运行所需虚拟机的主机。如果发生中断，虚拟机将自动迁移到次站点中的主机。但是，环境必须满足对延迟和网络的要求。如需更多信息，请参阅[主动-主动概述](#)。

Active-Passive（主动-被动）灾难恢复

此灾难恢复解决方案也称为站点到站点故障切换，通过配置两个独立的 RHV 环境来实施：主动主环境和被动辅助（备份）环境。站点间故障转移和故障恢复必须手动执行，并由 Ansible 管理。如需更多信息，请参阅[主动-被动概述](#)。

第 2 章 ACTIVE-ACTIVE（主动-主动）灾难恢复

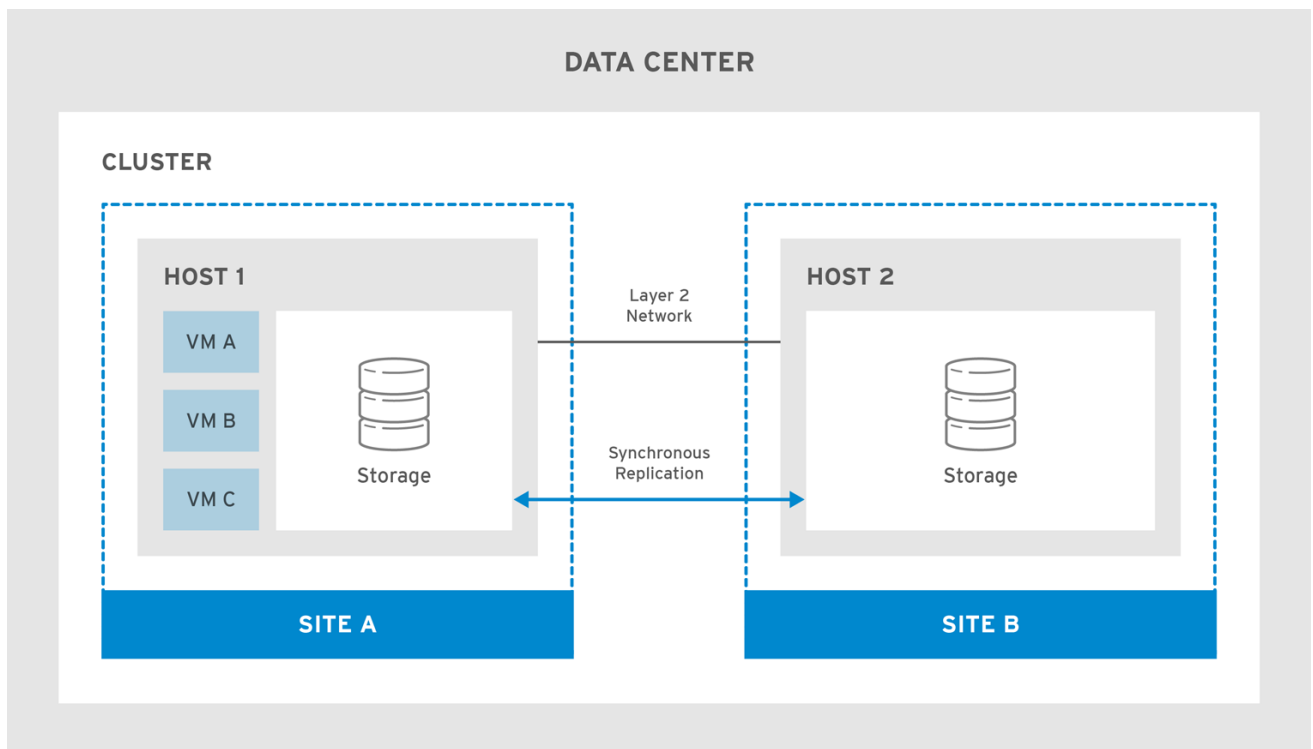
2.1. ACTIVE-ACTIVE 概述

主动-主动灾难恢复故障转移配置可跨越两个站点。两个站点都处于活动状态，如果主站点不可用，Red Hat Virtualization 环境将继续在次站点中运行，以确保业务连续性。

主动-主动故障转移配置包括一个扩展群集，在其中能够运行虚拟机的主机位于主站点和次站点中。所有主机都属于相同的 Red Hat Virtualization 集群。

此配置要求复制可在两个站点上写入的存储，以便虚拟机可以在两个站点之间迁移，并继续在两个站点的存储上运行。

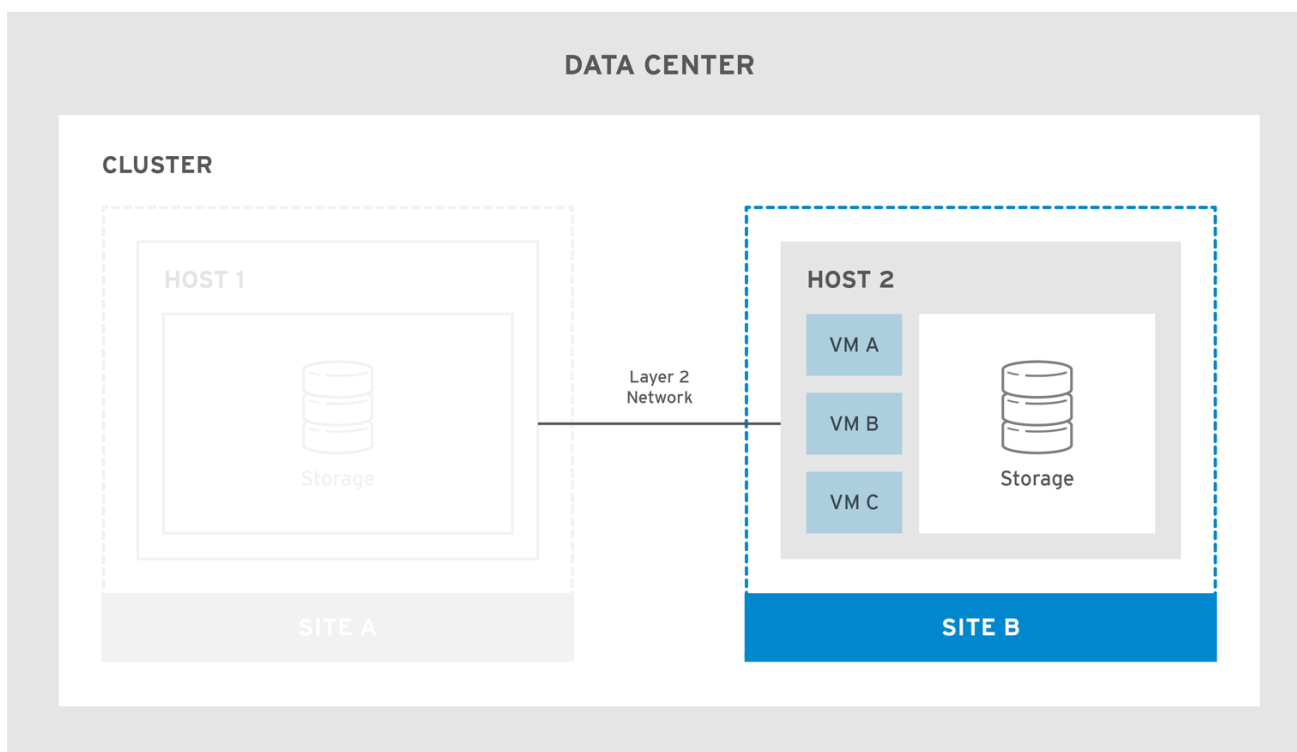
图 2.1. 扩展集群配置



RHV_460251_1017

如果主站点不可用，虚拟机将迁移到次站点。当站点可用且存储复制到两个站点时，虚拟机会自动恢复到主站点。

图 2.2. 通过 Stretch 集群失败



RHV_460251_1017

重要

确保虚拟机故障切换和故障恢复正常工作：

- 虚拟机必须配置为高可用性，并且每个虚拟机都必须在目标存储域上拥有租用，以确保虚拟机可以启动，即使没有电源管理。
- 必须配置软实施虚拟机到主机关联性，以确保虚拟机仅在选定主机上启动。

如需更多信息，请参阅 *虚拟机管理指南* 中的 [使用虚拟机高可用性](#) 和 [关联组](#) 提高正常运行时间。

扩展群集配置可以使用自托管引擎环境或单机管理器环境来实施。有关不同类型的部署的更多信息，请参阅 *产品指南* 中的 [红帽虚拟化架构](#)。

2.2. 网络注意事项

集群中的所有主机都必须通过 L2 网络位于同一广播域中。因此两个站点之间的连接必须是 L2。

L2 网络中的站点之间的最大延迟要求因两个设置的不同而有所不同。单机管理器环境需要最大延迟 100ms，而自托管引擎环境则要求最大延迟为 7ms。

2.3. 存储注意事项

Red Hat Virtualization 的存储域可以包括块设备（SAN - iSCSI 或 FCP）或者文件系统（NAS - NFS、GlusterFS 或其他 POSIX 兼容文件系统）。有关 Red Hat Virtualization 存储的更多信息，请参阅 *管理指南* 中的 [存储](#)。



注意

GlusterFS 存储已弃用，并将在以后的发行版本中删除。

站点需要同步复制的存储，这些数据可以在具有共享第 2 层(L2)网络连接的两个站点上写入。需要复制存储，以允许虚拟机在站点之间迁移，并继续在站点的存储上运行。Red Hat Enterprise Linux 7 及之后的版本支持的所有存储复制选项都可用于扩展群集。



重要

如果您有存储供应商推荐的自定义多路径配置，请参阅[针对 SAN 供应商自定义多路径配置](#)的说明和重要限制。

将主站点主机上的 SPM 角色设置为具有优先权。为此，请将主站点主机中的 SPM 优先级配置为高，而将 SPM 优先级配置为次要站点主机上的低级站点。如果您有一个影响主站点内网络设备的主要站点故障，导致 SPM 主机的隔离设备无法访问（如电源丢失），则第二个站点的主机无法接管 SPM 角色。

在这种情况下，虚拟机执行故障转移，但无法执行需要 SPM 角色的操作，包括添加新磁盘、扩展现有磁盘和导出虚拟机。

要恢复全部功能，检测灾难的实际性质，修复根本原因并重新引导 SPM 主机后，选择 SPM 主机 **确认"主机已重新启动"**。

其他资源

[管理指南](#)中的[手动隔离或隔离非响应主机](#)。

2.4. 配置自托管引擎STRETCH 集群环境

此流程提供使用自托管引擎部署配置扩展集群的说明。

先决条件

- 两个站点的可写入存储服务器，且具有 L2 网络连接。
- 用于复制存储的实时存储复制服务。

限制

- 站点间的最大延迟为 7ms。

配置自托管引擎Stretch 集群

1. 部署自托管引擎。请参阅[使用命令行将 Red Hat Virtualization 安装为自托管引擎](#)。
 2. 在每个站点安装额外的自托管引擎节点，并将它们添加到集群中。请参阅[使用命令行将 Red Hat Virtualization 安装自托管引擎的将自托管引擎添加到 Red Hat Virtualization Manager 管理器中](#)。
 3. （可选）安装其他标准主机。请参阅[使用命令行将 Red Hat Virtualization 安装自托管引擎的将标准主机添加到 Red Hat Virtualization Manager 管理器中](#)。
1. 将主站点中的所有主机上的 SPM 优先级配置为仅在主站点中的所有主机不可用时才进行 SPM 故障切换至次要站点。请参阅 [管理指南](#)中的 [SPM 优先级](#)。

2. 配置必须故障转移为高可用性的所有虚拟机，并确保虚拟机在目标存储域上具有租用。请参阅[虚拟机管理指南](#)中的[配置高可用性虚拟机](#)。
3. 配置虚拟机以托管软关联性，再定义您从关联性组中期望的行为。请参阅[虚拟机管理指南](#)中的[关联组](#)和[管理指南](#)中的[调用策略](#)。

主动-主动故障转移可以通过将主站点的主机置于维护模式来手动执行。

2.5. 配置独立管理器 STRETCH 集群环境

此流程提供使用独立管理器部署配置扩展集群的说明。

先决条件

- 两个站点的可写入存储服务器，且具有 L2 网络连接。
- 用于复制存储的实时存储复制服务。

限制

- 站点之间最大延迟为 100ms。

重要

Manager 必须高度可用，以便虚拟机在站点间进行故障转移和故障恢复。如果管理器与站点停机，虚拟机将不会故障转移。

单机管理器仅在外部管理时具有高可用性。例如：

- 使用红帽的高可用性附加组件。
- 在单独的虚拟化环境中作为高可用性虚拟机。
- 使用 Red Hat Enterprise Linux Cluster Suite。
- 在公共云中。

流程

1. 安装和配置 Red Hat Virtualization Manager 请参阅 [使用本地数据库将 Red Hat Virtualization 安装为独立管理器](#)。
2. 在每个站点中安装主机，并将它们添加到集群中。请参阅 [使用本地数据库安装 Red Hat Virtualization 作为一个独立的 Manager](#) 中的 [为 Red Hat Virtualization 安装主机](#)。
1. 将主站点中的所有主机上的 SPM 优先级配置为仅在主站点中的所有主机不可用时才进行 SPM 故障切换至次要站点。请参阅 [管理指南](#) 中的 [SPM 优先级](#)。
2. 配置必须故障转移为高可用性的所有虚拟机，并确保虚拟机在目标存储域上具有租用。请参阅 [虚拟机管理指南](#) 中的 [配置高可用性虚拟机](#)。
3. 配置虚拟机以托管软关联性，再定义您从关联性组中期望的行为。请参阅 [虚拟机管理指南](#) 中的 [关联组](#) 和 [管理指南](#) 中的 [调用策略](#)。

主动-主动故障转移可以通过将主站点的主机置于维护模式来手动执行。

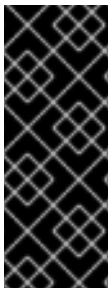
第 3 章 ACTIVE-PASSIVE（主动-被动）灾难恢复

3.1. 主动-被动概述

Red Hat Virtualization 支持可跨越两个站点的主动 - 被动灾难恢复解决方案。如果主站点不可用，则 Red Hat Virtualization 环境可能会被强制故障切换到辅助（备份）站点。

通过在第二个站点中配置 Red Hat Virtualization 环境来实现故障切换，这需要：

- 一个活跃的 Red Hat Virtualization Manager
- 一个数据中心和集群。
- 与主站点具有相同通用连接的网络。
- 故障转移后能够运行关键虚拟机的活动主机。



重要

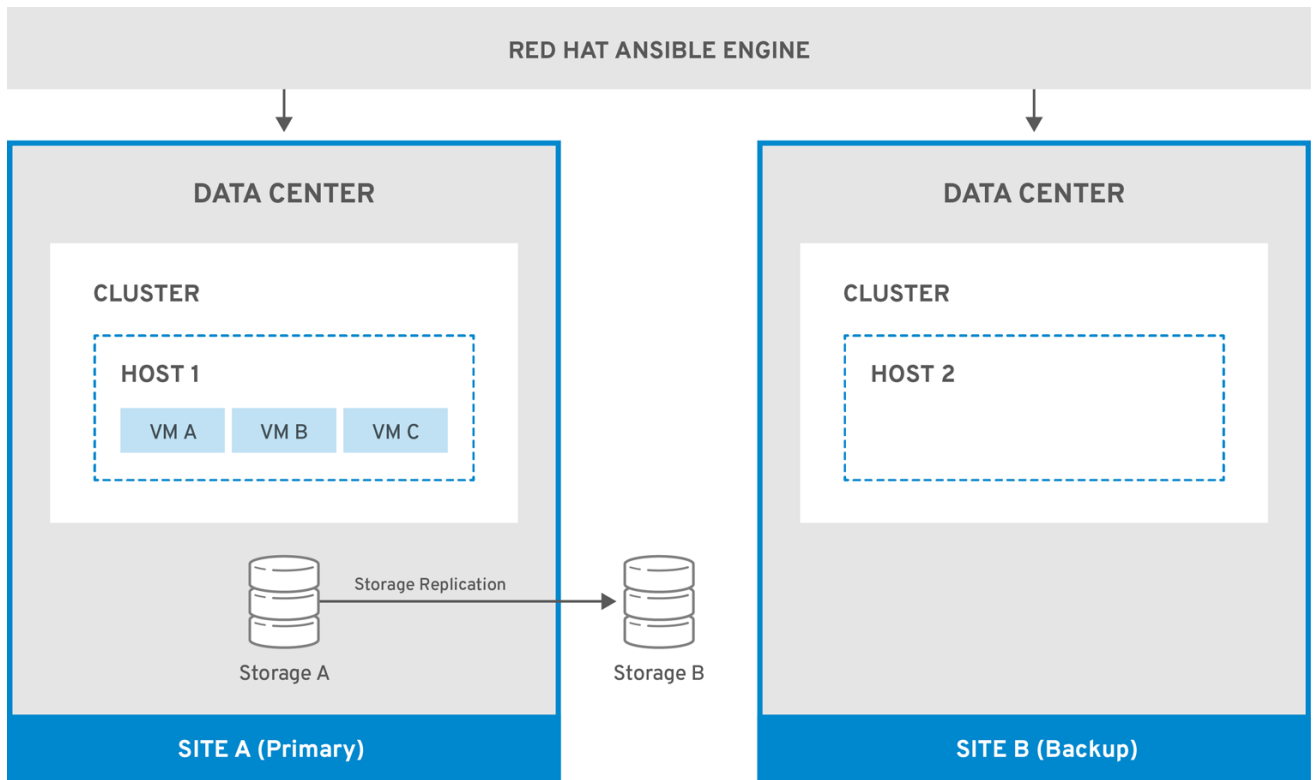
您必须确保次要环境有足够的资源在虚拟机上运行故障，并且主环境和次要环境具有相同的管理器版本、数据中心和集群兼容性级别以及 PostgreSQL 版本。支持的最小兼容性级别为 4.2。

主站点中包含虚拟机磁盘和模板的存储域必须复制。这些复制存储域不得附加到次要站点。

必须手动执行故障转移和故障恢复过程。为此，您必须创建 Ansible playbook 来映射站点之间的实体，以及管理故障切换和故障恢复进程。映射文件指示 Red Hat Virtualization 组件在目标站点上的故障切换或失败的位置。

下图描述了一个主动 - 被动设置，其中运行 Red Hat Ansible Engine 的机器具有高可用性，并可访问 **oVirt.disaster-recovery** Ansible 角色、配置的 playbook 和映射文件。在站点 A 中存储虚拟机磁盘的存储域将被复制。站点 B 没有虚拟机或附加的存储域。

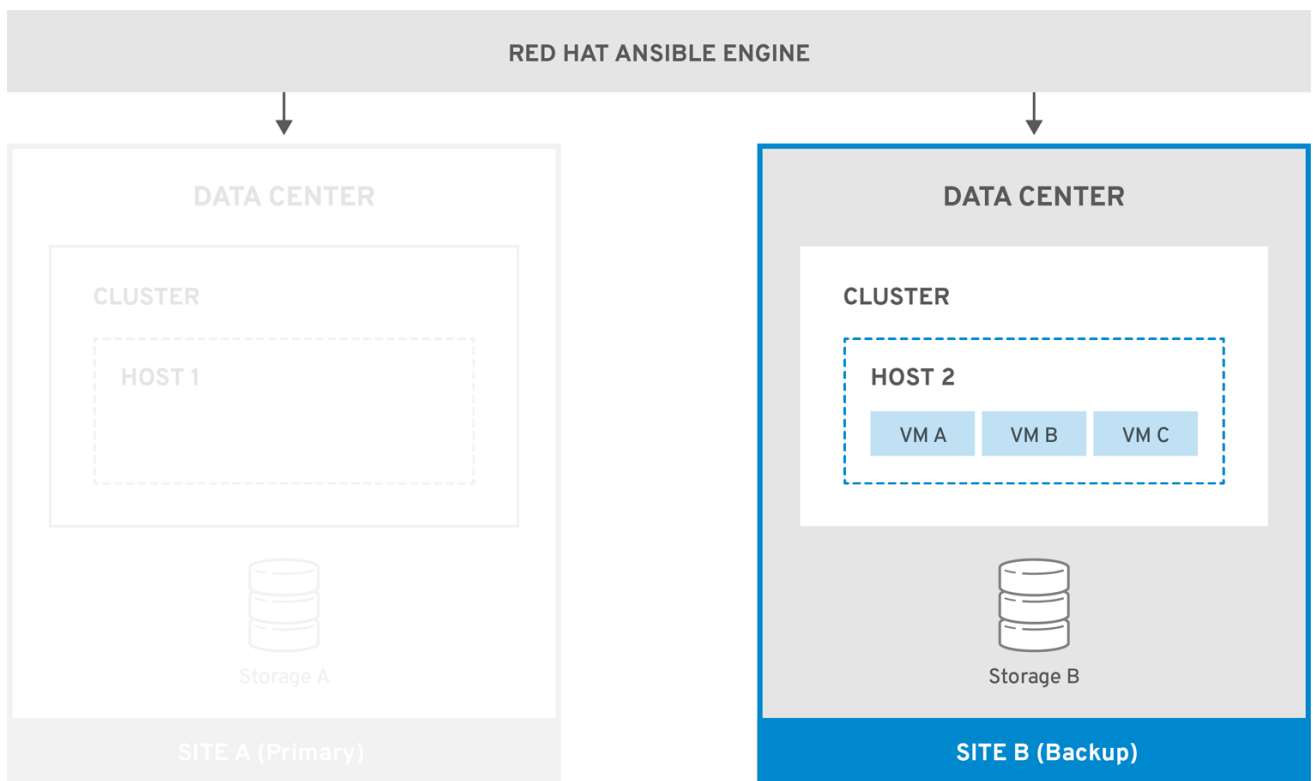
图 3.1. 主动-被动配置



RHV_466010_0218

当环境切换到 Site B 时，存储域首先在 Site B 的数据中心中连接并激活，然后注册虚拟机。高可用性虚拟机将首先出现故障。

图 3.2. 切换到备份站点



RHV_466010_0218

再次运行时，您必须手动切换到主站点(Site A)。

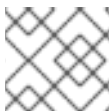
3.2. 网络注意事项

您必须确保在主站点和次要站点中存在相同的通用连接。

如果您有多个网络或多个数据中心，您必须在映射文件中使用空网络映射，以确保所有实体在故障转移过程中在目标上注册。如需更多信息，请参阅[映射文件属性](#)。

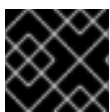
3.3. 存储注意事项

Red Hat Virtualization 的存储域可以包括块设备（SAN - iSCSI 或 FCP）或者文件系统（NAS - NFS、GlusterFS 或其他 POSIX 兼容文件系统）。有关红帽虚拟化存储的更多信息，请参阅[管理指南中的存储](#)。



注意

GlusterFS 存储已弃用，并将在以后的发行版本中删除。



重要

本地存储域在灾难恢复时不受支持。

需要主和次要存储副本。必须复制包含虚拟机磁盘或模板的主存储域的块设备或共享。辅助存储不得附加到任何数据中心，并在故障转移期间添加到备份站点的数据中心。

如果您要使用自托管引擎实施灾难恢复，请确保 Manager 虚拟机使用的存储域不包含虚拟机磁盘，因为在这种情况下，存储域不会故障转移。

所有具有 Red Hat Enterprise Linux 7 及更高版本支持的复制选项的存储解决方案均可使用。

3.4. 创建所需的 ANSIBLE PLAYBOOK

Ansible 用于启动和管理灾难恢复故障转移和故障恢复。因此，您必须创建 Ansible playbook 来促进此目标。有关创建 Ansible playbook 的更多信息，请参阅[Ansible 文档](#)。

先决条件

- 在主站点中全面运行 Red Hat Virtualization 环境。
- 二级站点中的备份环境，其数据中心和集群兼容性级别与主要环境相同。备份环境必须具有：
 - Red Hat Virtualization Manager。
 - 能够运行虚拟机并连接到复制存储域的活动主机。
 - 具有集群的数据中心。
 - 与主站点具有相同通用连接的网络。
- 复制存储。如需更多信息，请参阅[存储注意事项](#)。



注意

包含虚拟机和模板的复制存储不得附加到次站点。

- **oVirt.disaster-recovery** 软件包必须安装在高度可用的红帽 Ansible Engine 机器上，该机器上将自动化故障转移和故障恢复。
- 运行 Red Hat Ansible Engine 的机器必须能够使用 SSH 连接到主站点和次要站点中的 Manager。

另外，建议在次要站点上创建主站点中存在的环境属性，如关联性组、关联标签、用户。



注意

Ansible playbook 的默认策略可以在 `/usr/share/ansible/roles/oVirt.disaster-recovery/defaults/main.yml` 文件中配置。

必须创建以下 playbook：

- 用于创建在主和次站点间映射项的文件的 playbook。
- 故障转移 playbook。
- 故障转移 playbook。

您还可以创建一个可选的 playbook，以便在失败前清除主站点。

在管理故障转移和故障恢复的 Ansible 机器上，在 `/usr/share/ansible/roles/oVirt.disaster-recovery/` 中创建 playbook 及关联的文件。如果您有多台 Ansible 计算机可以进行管理，请确保将文件复制到所有这些计算机上。

您可以使用一个或多个测试过程测试 [Active-Passive 配置](#)。

3.4.1. Ansible 任务的 `ovirt-dr` 脚本

`ovirt-dr` 脚本简化了以下 Ansible 任务：

- 为故障切换和回退生成主和次站点的 `var` 映射文件
- 验证 `var` 映射文件
- 在目标站点上执行故障转移
- 执行从目标站点到源站点的故障恢复

此脚本位于 `/usr/share/ansible/roles/oVirt.disaster-recovery/files` 中

使用方法

```
# ./ovirt-dr generate/validate/failover/failback
    [--conf-file=dr.conf]
    [--log-file=ovirt-dr-log_number.log]
    [--log-level=DEBUG/INFO/WARNING/ERROR]
```

您可以在配置文件 `/usr/share/ansible/roles/oVirt.disaster-recovery/files/dr.conf` 中设置脚本操作的参数。

您可以使用 `--conf-file` 选项更改配置文件的位置。

您可以使用 `--log-file` 和 `--log-level` 选项设置日志记录详情的位置和级别。

3.4.2. 创建用于生成映射文件的 Playbook

用于生成映射文件的 Ansible playbook 将利用目标（主）站点的实体预先填充文件。然后，您必须手动将备份站点的实体（如 IP 地址、集群、关联性组、关联性标签、外部 LUN 磁盘、授权域、角色和 vNIC 配置集）添加到文件中。



重要

如果您自托管引擎的存储域上有任何虚拟机磁盘，则映射文件生成将失败。此外，映射文件不包含此存储域的属性，因为它不能失败。

在本例中，Ansible playbook 名为 **dr-rhv-setup.yml**，在主站点的 Manager 计算机上执行。

流程

1. 创建 Ansible playbook 来生成映射文件。例如：

```
---
- name: Generate mapping
  hosts: localhost
  connection: local

  vars:
    site: https://example.engine.redhat.com/ovirt-engine/api
    username: admin@internal
    password: my_password
    ca: /etc/pki/ovirt-engine/ca.pem
    var_file: disaster_recovery_vars.yml

  roles:
    - oVirt.disaster-recovery
```



注意

为提高安全性，您可以在一个 **.yml** 文件中加密您的 Manager 密码。如需更多信息，请参阅 [管理指南中的使用 Ansible 角色配置 Red Hat Virtualization](#)。

2. 运行 Ansible 命令，以生成映射文件。主站点的配置将预先填充。

```
# ansible-playbook dr-rhv-setup.yml --tags "generate_mapping"
```

3. 使用备份站点的配置配置映射文件（本例中为 **disaster_recovery_vars.yml**）。有关 [映射文件](#) 属性的更多信息，请参阅映射文件属性。

如果您有多台 Ansible 计算机可以执行故障转移和故障恢复，请将该映射文件复制到所有相关计算机上。

3.4.3. 创建 Failover 和 Failback Playbook

确保您已创建并配置了映射文件，在本例中为 **disaster_recovery_vars.yml**，因为它必须添加到 playbook 中。

您可以定义一个密码文件（如 **password.yml**）来存储主站点和次站点的 Manager 密码。例如：


```

---
# This file is in plain text, if you want to
# encrypt this file, please execute following command:
#
# $ ansible-vault encrypt passwords.yml
#
# It will ask you for a password, which you must then pass to
# ansible interactively when executing the playbook.
#
# $ ansible-playbook myplaybook.yml --ask-vault-pass
#
dr_sites_primary_password: primary_password
dr_sites_secondary_password: secondary_password

```



注意

若要提高安全性，您可以加密密码文件。但是，在运行 playbook 时，您必须使用 **--ask-vault-pass** 参数。如需更多信息，请参阅 [管理指南](#) 中的使用 *Ansible 角色配置 Red Hat Virtualization*。

在这些示例中，要故障转移和故障恢复的 Ansible playbook 被命名为 **dr-rhv-failover.yml** 和 **dr-rhv-failback.yml**。

创建以下 Ansible playbook 以故障切换环境：

```

---
- name: Failover RHV
  hosts: localhost
  connection: local
  vars:
    dr_target_host: secondary
    dr_source_map: primary
  vars_files:
    - disaster_recovery_vars.yml
    - passwords.yml
  roles:
    - oVirt.disaster-recovery

```

创建以下 Ansible playbook 以返回环境：

```

---
- name: Failback RHV
  hosts: localhost
  connection: local
  vars:
    dr_target_host: primary
    dr_source_map: secondary
  vars_files:
    - disaster_recovery_vars.yml
    - passwords.yml
  roles:
    - oVirt.disaster-recovery

```

3.4.4. 创建 Playbook 以清理主要站点

在返回到主站点前，您必须确保清理要导入的所有存储域的主站点。您可以在 Manager 上手动执行此操作，也可以选择创建 Ansible playbook 来为您完成此操作。

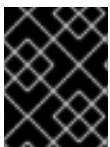
清理主站点的 Ansible playbook 示例中名为 **dr-cleanup.yml**，它使用由另一个 Ansible playbook 生成的映射文件：

```
---
- name: clean RHV
  hosts: localhost
  connection: local
  vars:
    dr_source_map: primary
  vars_files:
    - disaster_recovery_vars.yml
  roles:
    - oVirt.disaster-recovery
```

3.5. 执行故障

先决条件

- 第二个站点中的 Manager 和主机正在运行。
- 复制存储域处于读/写模式。
- 没有复制存储域连接到次要站点。
- 运行 Red Hat Ansible Engine 的机器，可以通过 SSH 连接到主站点和次要站点中的 Manager，其中包含所需的软件包和文件：
 - **oVirt.disaster-recovery** 软件包。
 - 映射文件和所需的故障切换 playbook。



重要

在故障转移过程开始前，Sanlock 必须从复制存储域释放所有存储锁定。这些锁应当在灾难发生后约 80 秒后自动释放。

本例使用先前创建的 **dr-rhv-failover.yml** playbook。

流程

1. 使用以下命令运行故障切换 playbook：

```
# ansible-playbook dr-rhv-failover.yml --tags "fail_over"
```

2. 当主站点变为活动状态时，请确保在失败前清理环境。如需更多信息，[请参阅清理主站点](#)。

3.6. 清理主站点

故障转移后，您必须在主站点中清理环境后，才能返回它：

- 重新引导主站点中的所有主机。
- 确保次要站点的存储域处于读/写模式，并且主站点的存储域处于只读模式。
- 将次要站点的存储域中的复制同步到主站点的存储域。
- 清理要导入的所有存储域的主站点。这可以在管理器中手动完成，也可以通过创建并运行 Ansible playbook 来完成。有关手动说明，请参阅 [管理指南中的 分离存储域](#)，或者创建 [Playbook 以清理主要站点](#) 的信息以创建 Ansible playbook。

本示例使用之前创建的 **dr-cleanup.yml** playbook 来清理环境。

流程

1. 使用以下命令清理主站点：

```
# ansible-playbook dr-cleanup.yml --tags "clean_engine"
```

2. 现在，您可以将环境恢复到主站点。如需更多信息，请参阅 [执行 Failback](#)。

3.7. 执行故障转移

故障转移后，当主站点处于活动状态并且已执行必要的步骤清理环境时，可以切换回主站点。

先决条件

- 主站点中的环境正在运行并已清理，请参阅 [清理主站点](#) 以了解更多信息。
- 第二个站点中的环境正在运行，并且具有活动存储域。
- 运行 Red Hat Ansible Engine 的机器，可以通过 SSH 连接到主站点和次要站点中的 Manager，其中包含所需的软件包和文件：
 - **oVirt.disaster-recovery** 软件包。
 - 映射文件和所需的故障恢复 playbook。

本例使用先前创建的 **dr-rhv-failback.yml** playbook。

流程

1. 使用以下命令运行 failback playbook:

```
# ansible-playbook dr-rhv-failback.yml --tags "fail_back"
```

2. 启用从主存储域到次要存储域的复制。

附录 A. 映射文件属性

下表描述了映射文件中用于故障转移和恢复主动灾难恢复解决方案的两个站点之间的属性。

表 A.1. 映射文件属性

映射文件部分	描述
网站详情	<p>这些属性映射主站点和次要站点中的管理器详细信息。例如：</p> <pre> dr_sites_primary_url: https://manager1.example.redhat.com/ovirt-engine/api dr_sites_primary_username: admin@internal dr_sites_primary_ca_file: /etc/pki/ovirt-engine/ca.pem # Please fill in the following properties for the secondary site: dr_sites_secondary_url: https://manager2.example.redhat.com/ovirt-engine/api dr_sites_secondary_username: admin@internal dr_sites_secondary_ca_file: /etc/pki/ovirt-engine/ca.pem </pre>
存储域详情	<p>这些属性映射主站点和次要站点之间的存储域详细信息。例如：</p> <pre> dr_import_storages: - dr_domain_type: nfs dr_primary_name: DATA dr_master_domain: True dr_wipe_after_delete: False dr_backup: False dr_critical_space_action_blocker: 5 dr_warning_low_space: 10 dr_primary_dc_name: Default dr_discard_after_delete: False dr_primary_path: /storage/data dr_primary_address: 10.64.100.xxx # Fill in the empty properties related to the secondary site dr_secondary_dc_name: Default dr_secondary_path: /storage/data2 dr_secondary_address: 10.64.90.xxx dr_secondary_name: DATA </pre>

映射文件部分	描述
集群详情	<p>这些属性在主站点和次要站点之间映射集群名称。例如：</p> <pre>dr_cluster_mappings: - primary_name: cluster_prod secondary_name: cluster_recovery - primary_name: fc_cluster secondary_name: recovery_fc_cluster</pre>
关联性组详情	<p>这些属性映射虚拟机所属的关联性组。例如：</p> <pre>dr_affinity_group_mappings: - primary_name: affinity_prod secondary_name: affinity_recovery</pre>
关联性标签详情	<p>这些属性映射虚拟机所属的关联性标签。例如：</p> <pre>dr_affinity_label_mappings: - primary_name: affinity_label_prod secondary_name: affinity_label_recovery</pre>
域 AAA 详情	<p>域身份验证、授权和帐户(AAA)属性映射主站点和次要站点之间的授权详细信息。例如：</p> <pre>dr_domain_mappings: - primary_name: internal-authz secondary_name: recovery-authz - primary_name: external-authz secondary_name: recovery2-authz</pre>
角色详情	<p>Role 属性提供特定角色的映射。例如，如果虚拟机注册了具有 VmCreator 角色的用户，则管理器可以使用同一用户但具有不同角色为该虚拟机注册权限。例如：</p> <pre>dr_role_mappings: - primary_name: VmCreator Secondary_name: NewVmCreator</pre>

映射文件部分	描述
网络详情	<p>网络属性映射主站点和次要站点之间的 vNIC 详情。例如：</p> <pre>dr_network_mappings: - primary_network_name: ovirtmgmt primary_profile_name: ovirtmgmt primary_profile_id: 0000000a-000a-000a-000a-0000000000398 # Fill in the correlated vnic profile properties in the secondary site for profile 'ovirtmgmt' secondary_network_name: ovirtmgmt secondary_profile_name: ovirtmgmt secondary_profile_id: 0000000a-000a-000a-000a-0000000000410</pre> <p>如果您有多个网络或多个数据中心，您必须在映射文件中使用空网络映射，以确保所有实体在故障转移过程中在目标上注册。例如：</p> <pre>dr_network_mappings: # No mapping should be here</pre>
外部 LUN 磁盘详情	<p>故障转移和故障后，外部 LUN 属性允许虚拟机注册到适当的外部 LUN 磁盘。例如：</p> <pre>dr_lun_mappings: - primary_logical_unit_id: 460014069b2be431c0fd46c4bdce29b66 primary_logical_unit_alias: Fedora_Disk primary_wipe_after_delete: False primary_shareable: False primary_logical_unit_description: 2b66 primary_storage_type: iscsi primary_logical_unit_address: 10.35.xx.xxx primary_logical_unit_port: 3260 primary_logical_unit_portal: 1 primary_logical_unit_target: iqn.2017-12.com.prod.example:444 secondary_storage_type: iscsi secondary_wipe_after_delete: False secondary_shareable: False secondary_logical_unit_id: 460014069b2be431c0fd46c4bdce29b66 secondary_logical_unit_address: 10.35.x.xxx secondary_logical_unit_port: 3260 secondary_logical_unit_portal: 1 secondary_logical_unit_target: iqn.2017-12.com.recovery.example:444</pre>

附录 B. 测试主动配置

配置后您必须测试灾难恢复解决方案。本节提供了多个选项来测试主动 - 被动灾难恢复配置。

1. 主站点保持活动状态且不会干扰主站点存储域中的虚拟机测试故障转移。请参阅 [Discreet Failover Test](#)。
2. 使用连接到主站点的特定存储域测试故障转移和故障恢复，从而允许主站点保持活动状态。请参阅 [Discreet Failover](#) 和 [Failback Test](#)。
3. 当您有切换到次要站点的宽限期或主站点计划外关闭时，为即将到来的灾难测试故障转移和故障恢复。请参阅 [Full Failover](#) 和 [Failback test](#)。



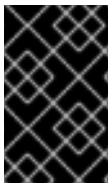
重要

在运行其中任何一个测试之前，确保您完成了配置主动 - 被动配置的所有步骤。

B.1. 磁盘故障切换测试

此测试模拟故障转移，同时主站点及其所有存储域仍保持活动，允许用户继续在主站点中工作。要启用此场景，您必须禁用主存储域和复制（次要）存储域之间的复制。在此测试期间，主站点不知道次要站点上的故障转移活动。

此测试将不允许您测试故障恢复功能。



重要

确保故障转移后未执行任何生产任务。例如，确保电子邮件系统被阻止向真实用户发送电子邮件，或将电子邮件重定向到其他位置。如果使用系统直接管理系统，请禁止访问系统或确保其访问次要站点中的并行系统。

执行磁盘故障转移测试：

1. 禁用主存储域和复制存储域之间的存储复制，并确保所有复制存储域都处于读/写模式。
2. 运行该命令切换到第二个站点：

```
# ansible-playbook playbook --tags "fail_over"
```

如需更多信息，请参阅[执行失败](#)。

3. 验证所有相关存储域、虚拟机和模板是否已成功注册并在运行。

将环境恢复到其主动 - 被动状态：

1. 将存储域从次要站点分离。
2. 启用主存储域和辅助存储域之间的存储复制。

B.2. 磁盘故障切换和反馈测试

对于此测试，您必须定义将用于测试故障转移和故障恢复的可测试存储域。必须复制这些存储域，才能将复制存储域连接到次要站点。这允许您在用户继续在主站点中运行时测试故障转移。



注意

您应该在单独的存储服务器上定义可测试存储域，这些存储域可以脱机，而不影响主站点中用于生产的主要存储域。

有关环境中失败的更多信息，清理环境并执行故障恢复，请参阅 [执行故障转移](#)、[对主站点](#) 和 [执行执行](#)。

流程：Discreet 故障切换测试：

1. 停止主站点中的测试存储域。例如，您可以关闭服务器主机或使用防火墙规则阻止它。
2. 禁用可测试存储域之间的存储复制，并确保用于测试的所有复制存储域都处于读/写模式。
3. 将测试主存储域置于只读模式。
4. 运行该命令切换到第二个站点：

```
# ansible-playbook playbook --tags "fail_over"
```

5. 验证所有相关存储域、虚拟机和模板是否已成功注册并在运行。

步骤：Discreet failback test*

1. 运行命令清理主站点并删除所有不活跃存储域及相关的虚拟机和模板：

```
# ansible-playbook playbook --tags "clean_engine"
```

2. 运行 failback 命令：

```
# ansible-playbook playbook --tags "fail_back"
```

3. 启用从主存储域到次要存储域的复制。
4. 验证所有相关存储域、虚拟机和模板是否已成功注册并在运行。

B.3. 完全故障和反馈测试

此测试在主站点和次要站点之间执行完全故障转移和故障恢复。您可以通过关闭主站点的主机或添加防火墙规则来阻止写入存储域来模拟灾难。

有关环境中失败的更多信息，清理环境并执行故障恢复，请参阅 [执行故障转移](#)、[对主站点](#) 和 [执行执行](#)。

步骤：故障切换测试

1. 禁用主存储域和复制存储域之间的存储复制，并确保所有复制存储域都处于读/写模式。
2. 运行该命令切换到第二个站点：

```
# ansible-playbook playbook --tags "fail_over"
```

3. 验证所有相关存储域、虚拟机和模板是否已成功注册并在运行。

步骤：失败测试

1. 同步次要站点的存储域与主站点存储域之间的复制。第二个站点的存储域必须处于读/写模式，并且主站点的存储域必须处于只读模式。
2. 运行命令清理主站点并删除所有不活跃存储域及相关的虚拟机和模板：

```
# ansible-playbook playbook --tags "clean_engine"
```

3. 运行 failback 命令：

```
# ansible-playbook playbook --tags "fail_back"
```

4. 启用从主存储域到次要存储域的复制。
5. 验证所有相关存储域、虚拟机和模板是否已成功注册并在运行。

附录 C. 法律通知

Copyright © 2022 Red Hat, Inc.

Licensed under the ([Creative Commons Attribution–ShareAlike 4.0 International License](#)).从(oVirt Project)的文档衍生而来。如果您发布本文档或对其进行改编，您必须提供原始版本的 URL。

修改后的版本必须删除所有红帽商标。

Red Hat、Red Hat Enterprise Linux、Red Hat 商标、Shadowman 商标、JBoss、OpenShift、Fedora、Infinity 商标以及 RHCE 都是在美国及其他国家的注册商标。

Linux® 是 Linus Torvalds 在美国和其他国家/地区的注册商标。

Java® 是 Oracle 和/或其附属公司的注册商标。

XFS® 是 Silicon Graphics International Corp. 或其子公司在美国和/或其他国家的商标。

MySQL® 是 MySQL AB 在美国、欧盟和其他国家/地区的注册商标。

Node.js® 是 Joyent 的官方商标。Red Hat Software Collections 与官方 Joyent Node.js 开源或商业项目没有正式关联或被正式认可。

The OpenStack® Word Mark 和 OpenStack 标识是 OpenStack Foundation 在美国及其他国家的注册商标/服务标记或商标/服务标记，可根据 OpenStack Foundation 授权使用。我们不附属于 OpenStack Foundation 或 OpenStack 社区。

所有其他商标均由其各自所有者所有。