Red Hat Enterprise Linux 8

准备身份管理的灾难恢复

有关影响身份管理部署的缓解方案文档

Last Updated: 2023-03-21

Red Hat Enterprise Linux 8 准备身份管理的灾难恢复

有关影响身份管理部署的缓解方案文档

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

摘要

本文档描述了 IdM 部署中常见的灾难情况,以及通过复制、虚拟机快照和备份来缓解这些情况的方法。

目录

使开源包含更多

红帽致力于替换我们的代码、文档和 Web 属性中存在问题的语言。我们从这四个术语开始：master、slave、黑名单和白名单。由于此项工作十分艰巨，这些更改将在即将推出的几个发行版本中逐步实施。有关更多详情，请参阅我们的首席技术官 Chris Wright 提供的消息。

在身份管理中，计划中的术语变化包括：

- 使用 ***block list*** 替换 *blacklist*
- 使用 ***allow list*** 替换 *whitelist*
- 使用 ***secondary*** 替换 *slave*
- *master* 会根据上下文被替换为其他更适当的术语:
  - 使用 ***IdM server*** 替换 *IdM master*
  - 使用 ***CA renewal server*** 替换 *CA renewal master*
  - 使用 ***CRL publisher server*** 替换 *CRL master*
  - 使用 ***multi-supplier*** 替换 *multi-master*

对红帽文档提供反馈

我们感谢您对文档提供反馈信息。请让我们了解如何改进文档。

- 关于特定内容的简单评论：
  1. 请确定您使用 *Multi-page HTML* 格式查看文档。另外，确定 **Feedback** 按钮出现在文档页的右上方。
  2. 用鼠标指针高亮显示您想评论的文本部分。
  3. 点在高亮文本上弹出的 **Add Feedback**。
  4. 按照显示的步骤操作。
- 要通过 Bugzilla 提交反馈，请创建一个新的 ticket：
  1. 进入 Bugzilla 网站。
  2. 在 Component 中选择 **Documentation**。
  3. 在 **Description** 中输入您要提供的信息。包括文档相关部分的链接。
  4. 点 **Submit Bug**。

第 1 章 IDM 中的灾难恢复工具

好的灾难恢复策略合并了以下工具，以便尽快从灾难中恢复并使数据丢失最少：

复制

在 IdM 服务器之间复制数据库内容。如果一个 IdM 服务器出现问题，您可以根据一个剩余的服务器来创建一个新副本来替换出现问题的服务器。

虚拟机(VM)快照

快照是虚拟机在任何或所有可用磁盘上的操作系统和应用程序在一个特定时间点时的视图。在对虚拟机进行快照后，您可以使用它将虚拟机及其 IdM 数据返回到之前的状态。

IdM 备份

使用 **ipa-backup** 程序可以备份 IdM 服务器的配置文件及其数据。之后，在需要时您可以使用备份将 IdM 服务器恢复到以前的状态。

第 2 章 IDM 中的灾难情况

灾难情境主要有两种： *服务器丢失*和*数据丢失*。

表 2.1. 服务器丢失和数据丢失

灾难类型	原因示例	如何准备
服务器丢失 ：IdM 部署丢失了一个或多个服务器。	• 硬件故障	• 通过使用复制来为服务器丢失的情况做准备
数据丢失 ：一个服务器上的 IdM 数据被意外修改，其变化传播到其他服务器中。	• 用户意外删除数据 • 软件错误修改数据	• 使用虚拟机快照为数据丢失的情况做准备 • 准备使用 IdM 备份数据丢失

第 3 章 通过使用复制来为服务器丢失的情况做准备

按照以下步骤建立一个复制拓扑，从而使您可以对丢失服务器的情况做出响应。

本节涵盖了以下主题：

- 在拓扑中连接副本
- 副本拓扑示例
- 保护 IdM CA 数据

3.1. 在拓扑中连接副本

将每个副本连接到至少两个其他副本

配置额外的复制协议确保信息不仅在初始副本和您安装的第一个服务器之间复制，而且在其他副本之间复制。

将副本连接到最多四个其他副本（这并不是硬要求）

每个服务器有大量的复制协议不会带来很大的好处。接收副本一次只能被另外一个副本更新，而其他复制协议则处于闲置状态。每个副本有超过四个复制协议通常意味着资源不足。

注意

本建议适用于证书复制协议和域复制协议。

每个副本有四个复制协议的限制有两个例外：

- 如果某些副本没有在线或没有响应时，您需要使用故障切换路径。
- 在大型部署中，您需要特定节点间的其他直接链接。

配置大量复制协议可能会对整体性能造成负面影响：当拓扑中的多个复制协议正在发送更新时，某些副本可能会在进入更新和传出更新之间在更改日志数据库文件出现高竞争。

如果您决定每个副本使用更多复制协议，请确保您没有遇到复制问题和延迟。但请注意，但距离大及存在大量中间节点时也可能造成延迟问题。

相互连接数据中心中的副本

这样可保证数据中心中的域复制。

将每个数据中心连接到至少两个其他数据中心

这样可确保数据中心间的域复制。

至少使用一对复制协议连接数据中心

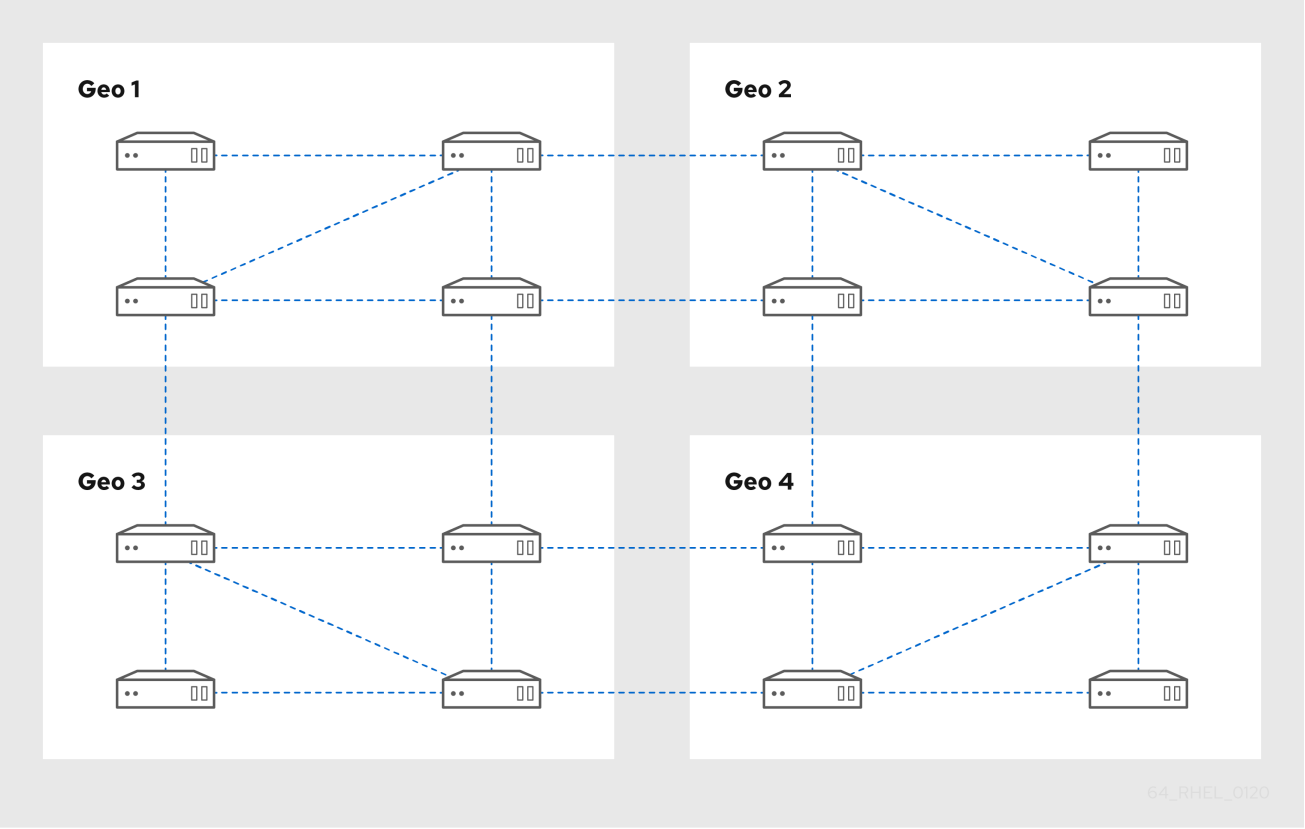
如果数据中心 A 和 B 有从 A1 到 B1 的复制协议，当存在从 A2 到 B2 的复制协议时，可确保其中一个服务器停止工作时复制可在两个数据中心之间继续。

3.2. 副本拓扑示例

下图显示了基于创建可靠拓扑指南的身份管理 (IdM) 拓扑示例。

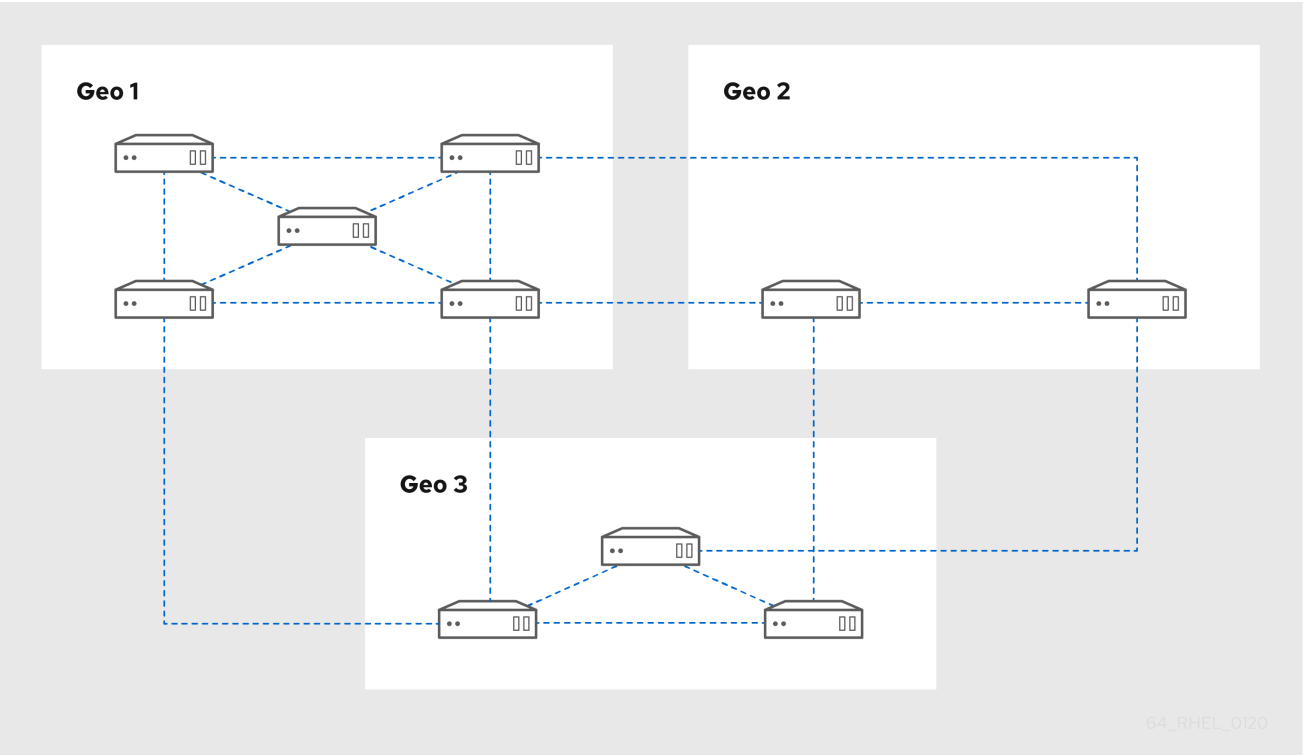
副本拓扑示例 1 显示了四个数据中心，每个数据中心有四个服务器。服务器与复制协议连接。

图 3.1. 副本拓扑示例 1



副本拓扑示例 2 显示三个数据中心，每个数据中心都有不同数量的服务器。服务器与复制协议连接。

图 3.2. 副本拓扑示例 2



3.3. 保护 IDM CA 数据

如果您的部署包含了集成的 IdM 证书颁发机构 (CA)，请安装多个 CA 副本，以便在其中一个丢失时创建额外的 CA 副本。

流程

1. 配置三个或更多副本来提供 CA 服务。
   a. 要安装一个带有 CA 服务的新副本，运行带有 **--setup-ca** 选项的 **ipa-replica-install** 命令。

   ```
   [root@server ~]# ipa-replica-install --setup-ca
   ```

   b. 要在一个预先存在的副本中安装 CA 服务，请运行 **ipa-ca-install**。

   ```
   [root@replica ~]# ipa-ca-install
   ```

2. 在 CA 副本之间创建 CA 复制协议。

```
[root@careplica1 ~]# ipa topologysegment-add
Suffix name: ca
Left node: ca-replica1.example.com
Right node: ca-replica2.example.com
Segment name [ca-replica1.example.com-to-ca-replica2.example.com]: new_segment
----------------------------
Added segment "new_segment"
----------------------------
  Segment name: new_segment
  Left node: ca-replica1.example.com
  Right node: ca-replica2.example.com
  Connectivity: both
```

警告

如果只有一个服务器提供 CA 服务，当这个服务器被损坏时，则整个环境将会丢失。如果您使用 IdM CA，红帽强烈建议安装三个或更多带有 CA 服务的副本，它们之间带有 CA 复制协议。

其他资源

- 规划您的 CA 服务。
- 安装 IdM 副本。
- 规划副本拓扑。

第 4 章 使用虚拟机快照为数据丢失的情况做准备

虚拟机(VM)快照是数据恢复策略中的一个重要组件，因为它们保留了 IdM 服务器的完整状态：

- 操作系统软件和设置
- IdM 软件和设置
- IdM 客户数据

通过准备 IdM 证书颁发机构(CA)副本的虚拟机快照，您可以在灾难后重建整个 IdM 部署。

警告

如果您的环境使用集成的 CA，*在没有 CA* 的情况下，没有 CA 的副本快照不足以重建部署，因为证书数据将无法保留。

同样，如果您的环境使用 IdM 密钥恢复授权(KRA)，请确保创建 KRA 副本的快照，否则可能会丢失存储密钥。

红帽建议，对一个带有安装了所以在您的部署中使用的 IdM 服务器角色（CA、KRA、DNS）的虚拟机进行快照。

先决条件

- 有一个可托管 RHEL 虚拟机的虚拟机管理程序。

流程

1. 在部署中至少配置一个 **CA 副本**，在虚拟机内运行。
   a. 如果环境中使用了 IdM DNS 或 KRA，请考虑在这个副本中安装 DNS 和 KRA 服务。
   b. （可选）将此虚拟机副本配置为隐藏的副本。
2. 定期关闭此虚拟机，生成完整的快照，并使其重新上线，以便继续接收复制更新。如果虚拟机是一个隐藏的副本，则以上过程不会影响 IdM 客户端的正常运行。

其他资源

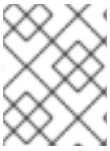
- 哪个虚拟机管理程序已经过认证可运行 Red Hat Enterprise Linux？
- 隐藏的副本模式。

第 5 章 准备使用 IDM 备份数据丢失

IdM 提供了 **ipa-backup** 程序来备份 IdM 数据，并可以使用 **ipa-restore** 程序从这些备份中恢复服务器和数据。

本节涵盖了以下主题：

- IdM 备份类型
- IdM 备份文件的命名惯例
- 创建备份时的注意事项
- 创建 IdM 备份
- 创建 GPG2 加密的 IdM 备份
- 创建 GPG2 密钥



注意

红帽建议，根据需要对安装了所有服务器角色的一个*隐藏的副本*进行频繁备份，特别是当环境使用了集成的 IdM CA 时的证书颁发机构 (CA) 角色。请参阅安装 IdM 隐藏的副本。

5.1. IDM 备份类型

使用 **ipa-backup** 工具，您可以创建两种类型的备份：

全服务器备份

- **包含**与 IdM 相关的所有服务器配置文件，以及 LDAP 数据交换格式 (LDIF) 文件中的 LDAP 数据
- IdM 服务必须**离**线。
- **适合**从头开始重建 IdM 部署。

只进行数据备份

- 在 LDIF 文件和复制更改日志中**包含** LDAP 数据
- IdM 服务可以为**在线或者离**线。
- **适用于** 将 IdM 数据恢复到一个过去的状态

5.2. IDM 备份文件的命名惯例

默认情况下，IdM 存储被备份为 **.tar** 存档，并保存在 **/var/lib/ipa/backup/** 目录的子目录中。

归档和子目录遵循以下命名约定：

全服务器备份

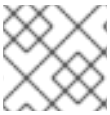
在名为 **ipa-full-*<YEAR-MM-DD-HH-MM-SS>*** 目录中的一个名为 **ipa-full.tar** 的归档，带有 GMT 时间。

```
[root@server ~]# ll /var/lib/ipa/backup/ipa-full-2021-01-29-12-11-46
total 3056
-rw-r--r--. 1 root root     158 Jan 29 12:11 header
-rw-r--r--. 1 root root 3121511 Jan 29 12:11 ipa-full.tar
```

只进行数据备份

在名为 **ipa-data-*<YEAR-MM-DD-HH-MM-SS>*** 目录中的一个名为 **ipa-data.tar** 的归档，带有 GMT 时间。

```
[root@server ~]# ll /var/lib/ipa/backup/ipa-data-2021-01-29-12-14-23
total 1072
-rw-r--r--. 1 root root     158 Jan 29 12:14 header
-rw-r--r--. 1 root root 1090388 Jan 29 12:14 ipa-data.tar
```



注意

卸载 IdM 服务器不会自动删除任何备份文件。

5.3. 创建备份时的注意事项

这部分论述了 **ipa-backup** 命令的重要行为和限制。

- 默认情况下，**ipa-backup** 工具以离线模式运行，这会停止所有 IdM 服务。该程序会在备份完成后自动重启 IdM 服务。
- 全服务器备份必须**始终**在 IdM 服务离线的情况下运行，但可通过在线服务执行仅数据备份。
- 默认情况下，**ipa-backup** 实用程序会在包含 **/var/lib/ipa/backup/** 目录的文件系统中创建备份。红帽建议在独立于 IdM 使用的生产文件系统的文件系统中定期创建备份，并将备份归档到固定介质，如磁带或光存储。
- 考虑对 隐藏的副本 执行备份。IdM 服务可在隐藏的副本中关闭，而不会影响到 IdM 客户端。
- 从 RHEL 8.3.0 开始，**ipa-backup** 实用程序检查您的 IdM 集群中使用的所有服务（如证书颁发机构(CA)、域名系统 (DNS) 和密钥恢复代理 (KRA) 是否安装在您要运行备份的服务器上。如果服务器没有安装所有这些服务，**ipa-backup** 实用程序会以警告方式退出，因为在该主机上进行的备份不足以完全恢复集群。
  例如，如果您的 IdM 部署使用集成证书认证机构（CA），非副本中运行的备份将无法捕获 CA 数据。红帽建议验证执行 **ipa-backup** 的副本是否在集群安装中使用了所有 IdM 服务。

  您可以使用 **ipa-backup --disable-role-check** 命令绕过 IdM 服务器角色检查，但生成的备份不会包含完全恢复 IdM 所需的所有数据。

5.4. 创建 IDM 备份

这部分论述了如何使用 **ipa-backup** 命令在离线和在线模式下创建完全服务器和仅数据备份。

先决条件

- 您必须具有 **root** 权限才能运行 **ipa-backup** 实用程序。

流程

- 要在离线模式中创建全服务器备份，请使用 **ipa-backup** 工具，而无需附加选项。

```
[root@server ~]# ipa-backup
Preparing backup on server.example.com
Stopping IPA services
Backing up ipaca in EXAMPLE-COM to LDIF
Backing up userRoot in EXAMPLE-COM to LDIF
Backing up EXAMPLE-COM
Backing up files
Starting IPA service
Backed up to /var/lib/ipa/backup/ipa-full-2020-01-14-11-26-06
The ipa-backup command was successful
```

- 要创建仅离线数据备份，请指定 **--data** 选项。

```
[root@server ~]# ipa-backup --data
```

- 要创建包含 IdM 日志文件的完整服务器备份，请使用 **--logs** 选项。

```
[root@server ~]# ipa-backup --logs
```

- 要在 IdM 服务运行时创建仅数据备份，请指定 **--data** 和 **--online** 选项。

```
[root@server ~]# ipa-backup --data --online
```

注意

如果因为 **/tmp** 目录中空间不足造成备份失败，请使用 **TMPDIR** 环境变量更改备份过程创建的临时文件的目标位置：

```
[root@server ~]# TMPDIR=/new/location ipa-backup
```

如需了解更多详细信息，请参阅 ipa-backup Command Fails to Finish 。

验证步骤

- 备份目录包含有备份的归档。

```
[root@server ~]# ls /var/lib/ipa/backup/ipa-full-2020-01-14-11-26-06
header  ipa-full.tar
```

5.5. 创建 GPG2 加密的 IDM 备份

您可以使用 GNU Privacy Guard (GPG) 加密来创建加密的备份。以下步骤创建了 IdM 备份并使用 GPG2 密钥对其进行加密。

先决条件

- 您已创建了 GPG2 密钥。请参阅创建 GPG2 密钥。

流程

- 通过指定 **--gpg** 选项创建 GPG 加密备份。

```
[root@server ~]# ipa-backup --gpg
Preparing backup on server.example.com
Stopping IPA services
Backing up ipaca in EXAMPLE-COM to LDIF
Backing up userRoot in EXAMPLE-COM to LDIF
Backing up EXAMPLE-COM
Backing up files
Starting IPA service
Encrypting /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00/ipa-full.tar
Backed up to /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00
The ipa-backup command was successful
```

验证步骤

- 确保备份目录包含带有一个 **.gpg** 文件扩展名的加密存档。

```
[root@server ~]# ls /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00
header  ipa-full.tar.gpg
```

其他资源

- 创建备份。

5.6. 创建 GPG2 密钥

下面的步骤描述了如何生成使用加密工具的 GPG2 密钥。

先决条件

- 您需要 **root** 权限。

流程

1. 安装并配置 **pinentry** 工具。

```
[root@server ~]# yum install pinentry
[root@server ~]# mkdir ~/.gnupg -m 700
[root@server ~]# echo "pinentry-program /usr/bin/pinentry-curses" >> ~/.gnupg/gpg-agent.conf
```

2. 创建一个 **key-input** 文件来生成附带您想要的详细信息的 GPG 密钥对。例如：

```
[root@server ~]# cat >key-input <<EOF
%echo Generating a standard key
Key-Type: RSA
Key-Length: 2048
Name-Real: GPG User
Name-Comment: first key
Name-Email: root@example.com
Expire-Date: 0
```

```
%commit
%echo Finished creating standard key
EOF
```

3. *（可选）*默认情况下，GPG2 在 **~/.gnupg** 文件中保存其密钥环。要使用自定义的密钥环位置，请将 **GNUPGHOME** 环境变量设置为只可由根用户访问的目录。

```
[root@server ~]# export GNUPGHOME=/root/backup

[root@server ~]# mkdir -p $GNUPGHOME -m 700
```

4. 根据 **key-input** 文件的内容生成一个新的 GPG2 密钥。

```
[root@server ~]# gpg2 --batch --gen-key key-input
```

5. 输入密码短语来保护 GPG2 密钥。您可以使用这个密码短语访问解密的私钥。

```
┌──────────────────────────────────────────────────────┐
│ Please enter the passphrase to                       │
│ protect your new key                                 │
│                                                      │
│ Passphrase: <passphrase>                             │
│                                                      │
│  <OK>                    <Cancel>                    │
└──────────────────────────────────────────────────────┘
```

6. 再输入一次来确认正确的密码短语。

```
┌──────────────────────────────────────────────────────┐
│ Please re-enter this passphrase                      │
│                                                      │
│ Passphrase: <passphrase>                             │
│                                                      │
│  <OK>                    <Cancel>                    │
└──────────────────────────────────────────────────────┘
```

7. 验证新 GPG2 密钥是否已成功创建。

```
gpg: keybox '/root/backup/pubring.kbx' created
gpg: Generating a standard key
gpg: /root/backup/trustdb.gpg: trustdb created
gpg: key BF28FFA302EF4557 marked as ultimately trusted
gpg: directory '/root/backup/openpgp-revocs.d' created
gpg: revocation certificate stored as '/root/backup/openpgp-
revocs.d/8F6FCF10C80359D5A05AED67BF28FFA302EF4557.rev'
gpg: Finished creating standard key
```

验证步骤

- 列出服务器中的 GPG 密钥。

```
[root@server ~]# gpg2 --list-secret-keys
gpg: checking the trustdb
```

```
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
/root/backup/pubring.kbx
------------------------
sec   rsa2048 2020-01-13 [SCEA]
      8F6FCF10C80359D5A05AED67BF28FFA302EF4557
uid           [ultimate] GPG User (first key) <root@example.com>
```

其他资源

- GNU Privacy Guard

第 6 章 使用 ANSIBLE PLAYBOOK 备份 IDM 服务器

使用 **ipabackup** Ansible 角色，您可以自动备份 IdM 服务器并在服务器和 Ansible 控制器之间传输备份文件。

本节涵盖了以下主题：

- 准备 Ansible 控制节点来管理 IdM
- 使用 Ansible 创建 IdM 服务器的备份
- 使用 Ansible 在 Ansible 控制器上创建 IdM 服务器的备份
- 使用 Ansible 将 IdM 服务器的备份复制到 Ansible 控制器
- 使用 Ansible 将 IdM 服务器的备份从 Ansible 控制器复制到 IdM 服务器
- 使用 Ansible 从 IdM 服务器中删除备份

6.1. 准备 ANSIBLE 控制节点来管理 IDM

作为管理身份管理 (IdM) 的系统管理员，在使用 Red Hat Ansible Engine 时，最好执行以下操作：

- 在您的主目录中，创建专用于 Ansible playbook 的子目录，如 **~/MyPlaybooks**。
- 将示例 Ansible playbook 从 **/usr/share/doc/ansible-freeipa/*** 和 **/usr/share/doc/rhel-system-roles/*** 目录以及它们的子目录复制到 **~/MyPlaybooks** 目录中并进行调整。
- 将清单文件包含在 **~/MyPlaybooks** 目录中。

按照这种做法，您可以在一个地方找到所有 playbook，您可以在不调用 root 特权的情况下运行 playbook。

注意

您只需要在受管节点上具有 **root** 权限来执行 **ipaserver**、**ipareplica**、**ipaclient** 和 **ipabackup ansible-freeipa** 角色。这些角色需要具有目录和 **dnf** 软件包管理器的特权访问权限。

本节论述了如何创建 **~/MyPlaybooks** 目录并进行配置，以便您可以使用它来存储和运行 Ansible playbook。

先决条件

- 您已在受管节点上安装了 IdM 服务器 *server.idm.example.com* 和 *replica.idm.example.com*。
- 您已配置了 DNS 和网络，以便您可以直接从控制节点登录到受管节点 *server.idm.example.com* 和 *replica.idm.example.com*。
- 您需要知道 IdM **admin** 密码。

步骤

1. 在主目录中为您的 Ansible 配置和 playbook 创建目录：

```
$ mkdir ~/MyPlaybooks/
```

2. 进入 **~/MyPlaybooks/** 目录：

```
$ cd ~/MyPlaybooks
```

3. 使用以下内容创建 **~/MyPlaybooks/ansible.cfg** 文件：

```
[defaults]
inventory = /home/your_username/MyPlaybooks/inventory

[privilege_escalation]
become=True
```

4. 使用以下内容创建 **~/MyPlaybooks/inventory** 文件：

```
[eu]
server.idm.example.com

[us]
replica.idm.example.com

[ipaserver:children]
eu
us
```

此配置定义了两个主机组，即 **eu** 和 **us**，用于这些位置中的主机。此外，此配置定义了 **ipaserver** 主机组，它包含来自 **eu** 和 **us** 组的所有主机。

5. [可选] 创建 SSH 公钥和私钥。要在测试环境中简化访问，请不要在私钥中设置密码：

```
$ ssh-keygen
```

6. 将 SSH 公钥复制到每个受管节点上的 IdM **admin** 帐户：

```
$ ssh-copy-id admin@server.idm.example.com
$ ssh-copy-id admin@replica.idm.example.com
```

输入这些命令时，您必须输入 IdM **admin** 密码。

其他资源

- 使用 Ansible playbook 安装身份管理服务器。
- 如何构建清单。

6.2. 使用 ANSIBLE 创建 IDM 服务器的备份

以下流程描述了如何在 Ansible playbook 中使用 ipabackup 角色来创建 IdM 服务器的备份并将其存储在 IdM 服务器中。

先决条件

- 您已配置了符合以下要求的 Ansible 控制节点：
  - 您使用 Ansible 版本 2.8 或更高版本。
  - 您已安装 **ansible-freeipa** 软件包。
  - 您已创建了带有您要配置这些选项的 IdM 服务器的完全限定域名 (FQDN) 的 Ansible 清单文件。
  - 您的 Ansible 清单文件位于 **~/MyPlaybooks/** 目录中。

流程

1. 进入 **~/MyPlaybooks/** 目录：

```
$ cd ~/MyPlaybooks/
```

2. 创建位于 **/usr/share/doc/ansible-freeipa/playbooks** 目录中的 **backup-server.yml** 文件的副本：

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/backup-server.yml backup-my-server.yml
```

3. 打开 **backup-my-server.yml** Ansible playbook 文件以进行编辑。

4. 通过将您的清单文件中的 **hosts** 变量设置为主机组来调整 文件。在本例中，将其设置为 **ipaserver** 主机组：

```
---
- name: Playbook to backup IPA server
  hosts: ipaserver
  become: true

  roles:
  - role: ipabackup
    state: present
```

5. 保存该文件。

6. 运行 Ansible playbook，指定清单文件和 playbook 文件：

```
$ ansible-playbook -v -i ~/MyPlaybooks/inventory backup-my-server.yml
```

验证步骤

1. 登录到您备份的 IdM 服务器。

2. 验证备份是否位于 **/var/lib/ipa/backup** 目录中。

```
[root@server ~]# ls /var/lib/ipa/backup/
ipa-full-2021-04-30-13-12-00
```

其他资源

- 有关使用 **ipabackup** 角色的更多 Ansible playbook 示例，请参阅：

- /**usr**/**share**/**doc**/**ansible-freeipa**/**roles**/**ipabackup** 目录中的 **README.md** 文件。
- /**usr**/**share**/**doc**/**ansible-freeipa**/**playbooks**/ 目录。

6.3. 使用 ANSIBLE 在 ANSIBLE 控制器上创建 IDM 服务器的备份

以下流程描述了如何使用 Ansible playbook 中的 **ipabackup** 角色创建 IdM 服务器的备份并在 Ansible 控制器中自动传输它。您的备份文件名以 IdM 服务器的主机名开头。

先决条件

- 您已配置了符合以下要求的 Ansible 控制节点：
  - 您使用 Ansible 版本 2.8 或更高版本。
  - 您已安装 **ansible-freeipa** 软件包。
  - 您已创建了带有您要配置这些选项的 IdM 服务器的完全限定域名 (FQDN) 的 Ansible 清单文件。
  - 您的 Ansible 清单文件位于 ~/**MyPlaybooks**/ 目录中。

流程

1. 若要存储备份，请在 Ansible 控制器上的主目录中创建一个子目录。

```
$ mkdir ~/ipabackups
```

2. 进入 ~/**MyPlaybooks**/ 目录：

```
$ cd ~/MyPlaybooks/
```

3. 在 /**usr**/**share**/**doc**/**ansible-freeipa**/**playbooks** 目录中生成 **backup-server-to-controller.yml** 文件的副本：

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/backup-server-to-controller.yml backup-my-server-to-my-controller.yml
```

4. 打开 **backup-my-server-to-my-controller.yml** 文件进行编辑。
5. 通过设置以下变量来调整文件：
   a. 将 **hosts** 变量设置为清单文件中的主机组。在本例中，将它设置为 **ipaserver** 主机组。
   b. *（可选）*若要在 IdM 服务器中维护备份副本，请取消注释以下行：

```
# ipabackup_keep_on_server: yes
```

6. 默认情况下，备份存储在 Ansible 控制器的当前工作目录中。要指定在第 1 步中创建的备份目录，请添加 **ipabackup_controller_path** 变量并将其设置为 /**home**/**user**/**ipabackups** 目录。

```
---
- name: Playbook to backup IPA server to controller
  hosts: ipaserver
```

```
  become: true
  vars:
    ipabackup_to_controller: yes
    # ipabackup_keep_on_server: yes
    ipabackup_controller_path: /home/user/ipabackups

  roles:
  - role: ipabackup
    state: present
```

7. 保存该文件。

8. 运行 Ansible playbook，指定清单文件和 playbook 文件：

```
$ ansible-playbook -v -i ~/MyPlaybooks/inventory backup-my-server-to-my-controller.yml
```

验证步骤

- 验证备份是否位于 Ansible 控制器的 **/home/user/ipabackups** 目录中：

```
[user@controller ~]$ ls /home/user/ipabackups
server.idm.example.com_ipa-full-2021-04-30-13-12-00
```

其他资源

- 有关使用 **ipabackup** 角色的更多 Ansible playbook 示例，请参阅：
  - **/usr/share/doc/ansible-freeipa/roles/ipabackup** 目录中的 **README.md** 文件。
  - **/usr/share/doc/ansible-freeipa/playbooks/** 目录。

6.4. 使用 ANSIBLE 将 IDM 服务器的备份复制到 ANSIBLE 控制器

以下流程描述了如何使用 Ansible playbook 将 IdM 服务器的备份从 IdM 服务器复制到 Ansible 控制器。

先决条件

- 您已配置了符合以下要求的 Ansible 控制节点：
  - 您使用 Ansible 版本 2.8 或更高版本。
  - 您已安装 **ansible-freeipa** 软件包。
  - 您已创建了带有您要配置这些选项的 IdM 服务器的完全限定域名 (FQDN) 的 Ansible 清单文件。
  - 您的 Ansible 清单文件位于 **~/MyPlaybooks/** 目录中。

流程

1. 若要存储备份，请在 Ansible 控制器上的主目录中创建一个子目录。

```
$ mkdir ~/ipabackups
```

2. 进入 **~/MyPlaybooks/** 目录：

```
$ cd ~/MyPlaybooks/
```

3. 在 **/usr/share/doc/ansible-freeipa/playbooks** 目录中生成 **copy-backup-from-server.yml** 文件的副本：

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/copy-backup-from-server.yml copy-backup-from-my-server-to-my-controller.yml
```

4. 打开 **copy-my-backup-from-my-server-to-my-controller.yml** 文件进行编辑。

5. 通过设置以下变量来调整文件：

   a. 将 **hosts** 变量设置为清单文件中的主机组。在本例中，将它设置为 **ipaserver** 主机组。

   b. 将 **ipabackup_name** 变量设置为 IdM 服务器上的 **ipabackup** 的名称，以复制到您的 Ansible 控制器。

   c. 默认情况下，备份存储在 Ansible 控制器的当前工作目录中。要指定在第 1 步中创建的目录，请添加 **ipabackup_controller_path** 变量并将其设置为 **/home/user/ipabackups** 目录。

```
---
- name: Playbook to copy backup from IPA server
  hosts: ipaserver
  become: true
  vars:
    ipabackup_name: ipa-full-2021-04-30-13-12-00
    ipabackup_to_controller: yes
    ipabackup_controller_path: /home/user/ipabackups

  roles:
  - role: ipabackup
    state: present
```

6. 保存该文件。

7. 运行 Ansible playbook，指定清单文件和 playbook 文件：

```
$ ansible-playbook -v -i ~/MyPlaybooks/inventory copy-backup-from-my-server-to-my-controller.yml
```

注意

要将**所有** IdM 备份复制到控制器，请将 Ansible playbook 中的 **ipabackup_name** 变量设置为 **all** ：

```
  vars:
    ipabackup_name: all
    ipabackup_to_controller: yes
```

例如，请参阅 **/usr/share/doc/ansible-freeipa/playbooks** 目录中的 **copy-all-backups-from-server.yml** Ansible playbook。

验证步骤

- 验证备份是否位于 Ansible 控制器上的 **/home/user/ipabackups** 目录中：

```
[user@controller ~]$ ls /home/user/ipabackups
server.idm.example.com_ipa-full-2021-04-30-13-12-00
```

其他资源

- **/usr/share/doc/ansible-freeipa/roles/ipabackup** 目录中的 **README.md** 文件。
- **/usr/share/doc/ansible-freeipa/playbooks/** 目录。

6.5. 使用 ANSIBLE 将 IDM 服务器的备份从 ANSIBLE 控制器复制到 IDM 服务器

以下流程描述了如何使用 Ansible playbook 将 IdM 服务器的备份从 Ansible 控制器复制到 IdM 服务器。

先决条件

- 您已配置了符合以下要求的 Ansible 控制节点：
  - 您使用 Ansible 版本 2.8 或更高版本。
  - 您已安装 **ansible-freeipa** 软件包。
  - 您已创建了带有您要配置这些选项的 IdM 服务器的完全限定域名 (FQDN) 的 Ansible 清单文件。
  - 您的 Ansible 清单文件位于 **~/MyPlaybooks/** 目录中。

流程

1. 进入 **~/MyPlaybooks/** 目录：

```
$ cd ~/MyPlaybooks/
```

2. 在 **/usr/share/doc/ansible-freeipa/playbooks** 目录中生成 **copy-backup-from-controller.yml** 文件的副本：

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/copy-backup-from-controller.yml copy-backup-from-my-controller-to-my-server.yml
```

3. 打开 **copy-my-backup-from-my-controller-to-my-server.yml** 文件进行编辑。
4. 通过设置以下变量来调整文件：
   a. 将 **hosts** 变量设置为清单文件中的主机组。在本例中，将它设置为 **ipaserver** 主机组。
   b. 将 **ipabackup_name** 变量设置为 Ansible 控制器上 **ipabackup** 的名称，以复制到 IdM 服务器。

```
---
- name: Playbook to copy a backup from controller to the IPA server
```

```
hosts: ipaserver
become: true

vars:
  ipabackup_name: server.idm.example.com_ipa-full-2021-04-30-13-12-00
  ipabackup_from_controller: yes

roles:
- role: ipabackup
  state: copied
```

5. 保存该文件。

6. 运行 Ansible playbook，指定清单文件和 playbook 文件：

```
$ ansible-playbook -v -i ~/MyPlaybooks/inventory copy-backup-from-my-controller-to-my-server.yml
```

其他资源

- **/usr/share/doc/ansible-freeipa/roles/ipabackup** 目录中的 **README.md** 文件。
- **/usr/share/doc/ansible-freeipa/playbooks/** 目录。

6.6. 使用 ANSIBLE 从 IDM 服务器中删除备份

以下流程描述了如何使用 Ansible playbook 从 IdM 服务器中删除备份。

先决条件

- 您已配置了符合以下要求的 Ansible 控制节点：
  - 您使用 Ansible 版本 2.8 或更高版本。
  - 您已安装 **ansible-freeipa** 软件包。
  - 您已创建了带有您要配置这些选项的 IdM 服务器的完全限定域名 (FQDN) 的 Ansible 清单文件。
  - 您的 Ansible 清单文件位于 **~/MyPlaybooks/** 目录中。

流程

1. 进入 ~/MyPlaybooks/ 目录：

```
$ cd ~/MyPlaybooks/
```

2. 在 **/usr/share/doc/ansible-freeipa/playbooks** 目录中生成 **remove-backup-from-server.yml** 文件的副本：

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/remove-backup-from-server.yml remove-backup-from-my-server.yml
```

3. 打开 **remove-backup-from-my-server.yml** 文件以进行编辑。

4. 通过设置以下变量来调整文件：

   a. 将 **hosts** 变量设置为清单文件中的主机组。在本例中，将它设置为 **ipaserver** 主机组。

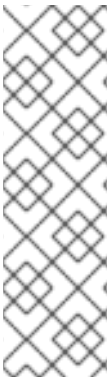
   b. 将 **ipabackup_name** 变量设置为 **ipabackup** 的名称，以从 IdM 服务器中删除。

```
---
- name: Playbook to remove backup from IPA server
  hosts: ipaserver
  become: true

  vars:
    ipabackup_name: ipa-full-2021-04-30-13-12-00

  roles:
  - role: ipabackup
    state: absent
```

5. 保存该文件。

6. 运行 Ansible playbook，指定清单文件和 playbook 文件：

```
$ ansible-playbook -v -i ~/MyPlaybooks/inventory remove-backup-from-my-server.yml
```



注意

要从 IdM 服务器中删除**所有** IdM 备份，将 Ansible playbook 中的 **ipabackup_name** 变量设置为 **all** ：

```
  vars:
    ipabackup_name: all
```

作为一个示例，请参阅 **/usr/share/doc/ansible-freeipa/playbooks** 目录中的 **remove-all-backups-from-server.yml** Ansible playbook。

其他资源

- **/usr/share/doc/ansible-freeipa/roles/ipabackup** 目录中的 **README.md** 文件。
- **/usr/share/doc/ansible-freeipa/playbooks/** 目录。