Red Hat Enterprise Linux 10

Preparing for disaster recovery with Identity Management

Mitigating the effects of server and data loss scenarios in IdM environments

Last Updated: 2025-06-06

Red Hat Enterprise Linux 10 Preparing for disaster recovery with Identity Management

Mitigating the effects of server and data loss scenarios in IdM environments

Legal Notice

Abstract

Server and data loss scenarios, for example due to a hardware failure, are the highest risks in IT environments. In a Red Hat Identity Management (IdM) topology, you can configure replication with other servers, use virtual machine (VM) snapshots, and IdM backups to mitigate the effects of these situations.

Table of Contents

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your feedback on our documentation. Let us know how we can improve it.

Submitting feedback through Jira (account required)

1. Log in to the Jira website.
2. Click **Create** in the top navigation bar
3. Enter a descriptive title in the **Summary** field.
4. Enter your suggestion for improvement in the **Description** field. Include links to the relevant parts of the documentation.
5. Click **Create** at the bottom of the dialogue.

CHAPTER 1. DISASTER RECOVERY TOOLS IN IDM

A good disaster recovery strategy combines the following tools to recover from a disaster as soon as possible with minimal data loss:

Replication

Replication copies database contents between IdM servers. If an IdM server fails, you can replace the lost server by creating a new replica based on one of the remaining servers.

Virtual machine (VM) snapshots

A snapshot is a view of a VM's operating system and applications on any or all available disks at a given point in time. After taking a VM snapshot, you can use it to return a VM and its IdM data to a previous state.

IdM backups

The **ipa-backup** utility allows you to take a backup of an IdM server's configuration files and its data. You can later use a backup to restore an IdM server to a previous state.

CHAPTER 2. DISASTER SCENARIOS IN IDM

Prepare and respond to various disaster scenarios in Identity Management (IdM) systems that affect servers, data, or entire infrastructures.

Table 2.1. Disaster scenarios in IdM

Disaster type	Example causes	How to prepare	How to respond
Server loss: The IdM deployment loses one or several servers.	• Hardware malfunction	• Preparing for server loss with replication	• Recovering a single server with replication
Data loss: IdM data is unexpectedly modified on a server, and the change is propagated to other servers.	• A user accidentally deletes data • A software bug modifies data	• Preparing for data loss with VM snapshots • Preparing for data loss with IdM backups	• Recovering from data loss with VM snapshots • Recovering from data loss with IdM backups • Managing data loss
Total infrastructure loss: All IdM servers or Certificate Authority (CA) replicas are lost with no VM snapshots or data backups available.	• Lack of off-site backups or redundancy prevents recovery after a failure or disaster.	• Preparing for data loss with VM snapshots	This situation is a total loss.

WARNING

A total loss scenario occurs when all Certificate Authority (CA) replicas or all IdM servers are lost, and no virtual machine (VM) snapshots or backups are available for recovery. Without CA replicas, the IdM environment cannot deploy additional replicas or rebuild itself, making recovery impossible. To avoid such scenarios, ensure backups are stored off-site, maintain multiple geographically redundant CA replicas, and connect each replica to at least two others.

CHAPTER 3. PREPARING FOR SERVER LOSS WITH REPLICATION

Follow these guidelines to establish a replication topology that will allow you to respond to losing a server:

- Guidelines for connecting IdM replicas in a topology in the *Planning RHEL Identity Management* documentation.
- Replica topology examples in the *Planning RHEL Identity Management* documentation.
- Protecting IdM CA data.

3.1. PROTECTING IDM CA DATA

If your deployment contains the integrated IdM Certificate Authority (CA), install several CA replicas so you can create additional CA replicas if one is lost.

Procedure

1. Configure three or more replicas to provide CA services.
   a. To install a new replica with CA services, run **ipa-replica-install** with the **--setup-ca** option.

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

   b. To install CA services on a preexisting replica, run **ipa-ca-install**.

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

2. Create CA replication agreements between your CA replicas.

```
[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
```

WARNING

If only one server provides CA services and it is damaged, the entire environment will be lost. If you use the IdM CA, Red Hat **strongly recommends** having three or more replicas with CA services installed, with CA replication agreements between them.

Additional resources

- Planning your CA services
- Installing an IdM replica
- Planning the replica topology

CHAPTER 4. PREPARING FOR DATA LOSS WITH VM SNAPSHOTS

Virtual machine (VM) snapshots are an integral component of a data recovery strategy, since they preserve the full state of an IdM server:

- Operating system software and settings
- IdM software and settings
- IdM customer data

Preparing a VM snapshot of an IdM Certificate Authority (CA) replica allows you to rebuild an entire IdM deployment after a disaster.

WARNING

If your environment uses the integrated CA, a snapshot of a replica *without a CA* will not be sufficient for rebuilding a deployment, because certificate data will not be preserved.

Similarly, if your environment uses the IdM Key Recovery Authority (KRA), make sure you create snapshots of a KRA replica, or you might lose the storage key.

Red Hat recommends creating snapshots of a VM that has all of the IdM server roles installed which are in use in your deployment: CA, KRA, DNS.

Prerequisites

- A hypervisor capable of hosting RHEL VMs.

Procedure

1. Configure at least one **CA replica** in the deployment to run inside a VM.
   a. If IdM DNS or KRA are used in your environment, consider installing DNS and KRA services on this replica as well.
   b. Optional: Configure this VM replica as a hidden replica.
2. Periodically shutdown this VM, take a full snapshot of it, and bring it back online so it continues to receive replication updates. If the VM is a hidden replica, IdM Clients will not be disrupted during this procedure.

Additional resources

- Which hypervisors are certified to run Red Hat Enterprise Linux?
- The hidden replica mode

CHAPTER 5. PREPARING FOR DATA LOSS WITH IDM BACKUPS

IdM provides the **ipa-backup** utility to backup IdM data, and the **ipa-restore** utility to restore servers and data from those backups.

NOTE

Run backups as often as necessary on a *hidden replica* with all server roles installed, especially the Certificate Authority (CA) role if the environment uses the integrated IdM CA. See Installing an IdM hidden replica .

For details how to perform IdM backups, see the following chapters in the RHEL Identity Management documentation:

- Backing up and restoring IdM
- Backing up and restoring IdM servers using Ansible playbooks