SailPoint IdentityIQ

Version: 8.0

File Access Manager Disaster Recovery Plan Configuration Plan

Table of Contents

List of Figures

List of Tables

No table of figures entries found.

Table of Revisions

Ver. #	Description	Date
0.1	Initial release	June 2019

Chapter 1: Overview

Disaster recovery Plan scope

Terms used throughout this document:

Disaster: Time when the IdentityIQ File Access Manager servers and / or services are not actively monitoring due to a planned or unplanned unavailability of the servers or services.

Production environment (PRD): The ongoing working environment that includes the IdentityIQ File Access Manager servers, services and databases.

Disaster Recovery environment (DR): A preconfigured secondary datacenter with IdentityIQ File Access Manager servers and databases configured to run most of the IdentityIQ File Access Manager services as a temporary solution while the Production environment encounters a disaster.

The SailPoint IdentityIQ File Access Manager Disaster Recovery Plan describes a method to minimize the loss of information during a disaster (as defined above).

In case of a disaster in the Production environment, this procedure enables configuring the system to run the IdentityIQ File Access Manager services from the Disaster Recovery environment.

Note: The Windows File Server activity monitor runs on the same server as the Windows File Server, so it cannot have a disaster recovery installation.

The IdentityIQ File Access Manager accesses customer servers and databases. These include the identity stores, such as Active Directory and Azure, Target applications, such as NAS Storage, mail systems, and directories, and the IdentityIQ File Access Manager SQL database. In case these sources are moved due to the customer's disaster recovery procedures, (or any other reason) the IdentityIQ File Access Manager configuration must be updated to point to the new sources, as per regular resource configuration.

High level solution

The SailPoint disaster recovery plan assumes the following:

The SailPoint disaster recovery plan follows this high-level flow:

1. Create a Disaster Recovery environment
    a. Allocate servers for the Disaster Recovery environment.
    b. Using the IdentityIQ File Access Manager Server Installer, Configure a parallel IdentityIQ File Access Manager system on the Disaster Recovery environment for all services (except for the Windows file server activity monitors). For each service allocate the Production server, and Disaster Recovery server you want this service to run on.
2. When identifying a disaster:
    a. Identify the Production servers that are down
    b. Using the IdentityIQ File Access Manager Server Installer, Select these servers in the Server Configuration window and set them to **Inactive**. This will set the corresponding server on the Disaster Recovery environment to **Active**.

Note: Identifying a corresponding Disaster Recovery server is done automatically when setting a Prod server to Inactive, per service.

3. Once the disaster condition on the Production environment has ended:

    a. Select the Production servers that are back in action and set them to **Active** in the server configuration screen. This will set the corresponding server on the Disaster Recovery environment to **Inactive**.

Chapter 2: Creating the Disaster Recovery environment

Server designation and configuration

The server designation as Production or Disaster Recovery, as well as the configuration of the services in these servers is performed using the IdentityIQ File Access Manager Server Installer.

Initial configuration

When configuring the servers in the initial setup, mark Disaster Recovery (DR) servers, by ticking the **Disaster Recovery** tick box.

Disaster recovery configuration: Setting the active servers

You can set the servers to be active or inactive in the Server Installer. If a server is set to be "Toggle UP", the twin DR Server will be in "Sleep State" (idle). if the Production server is in "Toggle Down" Mode the Twin DR server will be in running state.

the user can set server up and down from any machine.

To set a production server Active\Inactive

1. Open the Server Installer and connect to an existing DB.
2. Select the Production server which will be activated / deactivated and click the Edit button 

   This will enable the server status buttons

   - **Deactivate** / **Activate** – Toggle the server status. This will automatically toggle the corresponding DR server as well
   - **Reset** – mark the services running on this server as uninstalled (This is necessary when a server should be reinstalled or replaced)

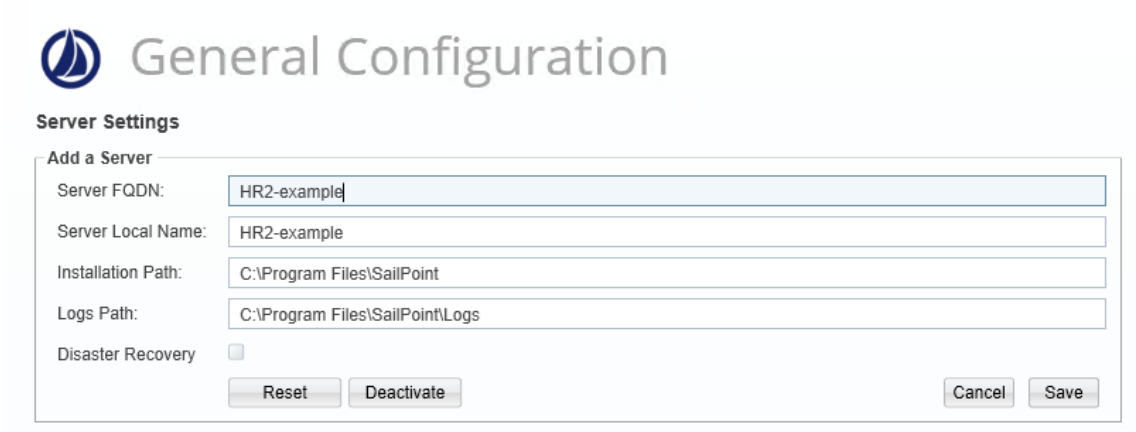

Figure 1. Server Configuration Panel

3. Click **Activate** / **deactivate** to change the server state
4. Click **save**

Chapter 3: Disaster Recovery Flow

Switching on Disaster Recovery mode

Select the production servers and set them back to **Inactive** (See Toggle above).

This will set the corresponding DR servers to **Active**.

Note: Only the Production servers have the Active / Inactive button enabled.

If the web site and/or API servers are down

If the web site and/or API servers are down, a manual action will be required for the clients to connect.

There are two possibilities to recover:

- In the DNS server, change the target URL of the web site/API to point to the disaster recovery environment, this is the recommended action and will be the simplest.

  or

- Browse directly to the disaster recovery environment address.

Disaster Recovery Fallback to the Production environment

Select the production servers and set them back to **Active** (See Toggle above).

This will set the corresponding DR servers to **Inactive**.

If the return to Production requires installing the services

1. Press **Reset** on the server configuration screen
2. Reinstall the services
3. After completing the installation wait at least 2 minutes to allow all IdentityIQ File Access Manager services to update their configuration
4. Set the Production servers to **Active**

If the production server cannot be restored and a new one is required

1. In the Server Installer add a new server in the server list
2. Continue until the end and press **save configuration**.
3. Restart the server installer
4. Select the new server in the Server Configuration list, click **edit**, then **deactivate** (the new server is not yet ready to be live)

5. Configure the required services on the new server and install them
6. Wait for at least 2 minutes after the installation has completed
7. Turn the new server to **active**

If the fallback includes the Production server of the Web site/API server

In case the fallback includes the production server of the Web site/API server, a manual action will be required for the clients to connect.

The action will be according to the recovery action taken in section “Switching on Disaster Recovery mode”.

- If the DNS server was changed, it should be changed back to point to the Production environment.
- If the DNS server was not changed, you should browse directly to the Production environment address.

Chapter 4: Troubleshooting

The Reindex task marked as cancelled following a DR transfer

In the following scenario, the Reindex task might fail. In this case, run the Reindex manually.

1. Prod Elasticsearch server goes down
2. The user marks the server **Inactive** in the server installer. This will toggle the parallel server in the DR environment to **Active.**
3. Reindex activities task starts automatically (which is run by the Scheduled Task Handler service).
4. The server where the Scheduled Task Handler service goes down.
5. The reindex task automatically gets canceled.

In this specific scenario and only if the reindex task was cancelled, create a new reindex task manually.

This is done from the Administartive client Health Center screen

Admin Client System → Health Center.