Disaster Recovery

The Frame Disaster Recovery (DR) feature provides Frame administrators with the ability to backup a Frame account on an AHV cluster or Azure public cloud region to a separate AHV cluster or Azure public cloud region, respectively.

Primary Infrastructure	Secondary Infrastructure
Nutanix AHV cluster 1	Nutanix AHV cluster 2
Microsoft Azure region A	Microsoft Azure region B

> Currently, the Frame Disaster Recovery feature set consists of backup, replication, and restore functionality for AHV and Azure only. Support for AWS and GCP infrastructure and Failover to a secondary Frame account is in development.

All persistent resources of the primary Frame account are backed up in the primary location and replicated to the secondary location. Frame administrators can then either use the backups in the primary location or the replicas in the secondary location to recover the Frame account in the event of a disaster.

This document discusses how to configure AHV and Azure infrastructure with Frame to back up and recover a Frame account's persistent resources.

Prerequisites

When enabled, the DR backup and replication feature is triggered when any persistent resource is backed up. Frame administrators can manually trigger a backup, schedule backups on a

regular interval, and have Frame back up the resource after a user has closed their session.

Considerations

Customers will need to consider several factors when deciding how often to perform these back ups:

- Desired Recovery Point Objective (RPO)
- Amount of backup data that must be replicated to the secondary location
- Network bandwidth allowed between primary and secondary locations
- Delay for end users waiting for their user volumes (Persistent Desktops, Enterprise Profile disks, Personal drives) to be backed up (if the “Enable post-session backup” and optionally “Stop server before post-session backup” are enabled).
- Cost of data egress from the primary region to a different region (for public cloud infrastructure)

Return to Operation (RTO) will then depend on:

- Amount of backup data that must be restored from either the primary or secondary location
- Network bandwidth allowed between primary and secondary locations, if restoration is from replicas from the secondary location

Requirements

- The Backup and Recovery feature is only supported on Bring Your Own (BYO) infrastructure. This feature set is not available with Dizzion IaaS.
- For Frame accounts on AHV infrastructure, the backups must be on a second AHV cluster. The second AHV cluster must be registered on the customer's Frame Customer or Organization entity as a second AHV Cloud Account.
- For Frame accounts on public cloud infrastructure, the backups must be in the same public cloud account, registered on the customer's Frame Customer or Organization entity, and in a region different from the primary Frame account.
- The instance types that are used in the Primary AHV Cloud account must be configured with the same vCPU/Core and RAM values in the second AHV cluster for the Backup and Recovery feature. This prerequisite will be eliminated when the Failover feature is released with a user interface to map instance types from primary to secondary Frame accounts.
- For Frame accounts on AHV infrastructure, a user with Prism Element administrator privileges to both AHV clusters to setup protection domains is required.
- For Frame accounts on Azure, the Azure instance type must be supported in both the region of the Frame account and the region of the backups.
- To configure the Backup and Recovery feature for a Frame account, the Frame administrator must have the role of Customer Administrator or Organization

Administrator, depending on where the Cloud Account is registered in the Frame Platform Hierarchy and the relative location of the Frame Account within the hierarchy. Account Administrators do not have permission to view the list of Cloud Accounts when setting up the Frame account's DR configuration.

Persistent Resources

The following Frame account resources are considered “persistent” for the purposes of backup, replication, and recovery for the Frame Backup and Recovery feature. These persistent resources are backed up and replicated to the backup AHV Cloud Account or public cloud region.

Resource	Description
Sandbox	One disk per Sandbox (gold image, associated with the account)
Utility Server	One disk per Utility Server
Persistent Desktop	One disk per persistent workload VM that has been assigned to a user
Enterprise Profile	One profile disk per user
Personal Drive	One personal drive per user

Template images are not backed up as they are not part of a Frame account. Customers are responsible for backing up template images separately.

The customer is responsible for backup and recovery of any data not explicitly defined in the table above. For example, the customer must have a backup and disaster recovery plan for data stored in third-party profile solutions, external file servers, and database servers.

Infrastructure

Select an supported infrastructure below for instructions on how to prepare your underlying infrastructure *before* configuring a Frame account for use with the Frame DR feature.

To use the Backup and Recovery feature, the AHV cluster hosting the Primary Frame Account must be configured with a Remote Site. This enables the primary AHV cluster to replicate to and recover from the secondary AHV cluster. Both the primary and secondary AHV Clusters must be added as AHV Cloud Accounts.

Refer to the Nutanix AHV Remote Site documentation for further details on the AHV Remote Site feature.

The following step-by-step procedure must be completed before the Frame account can be enabled for Frame DR.

1. Login to Prism Element on your Primary AHV Cluster and go to Data Protection.

2. Switch to table view. In the upper right corner, click + Remote Site and select Physical Cluster.

3. Complete the form for the new Remote Site.

- **Remote Site Name**: Select a Name for the Secondary Site (Remote Site)
- **Enable Proxy**: Enable if a proxy server is required to communicate with the secondary site.
- **Capabilities**: Select Disaster Recovery
- **Cluster Virtual IP**: Enter the virtual IP of your Remote Site Cluster (can be found in Prism Element/Cluster details of your secondary cluster.

> By default, tcp/2009 and tcp/2020 are used for AHV cluster to AHV cluster communication.

4. After the above information has been added, click on **Add Site**.

5. Next, under the Settings, configure the parameters for how the persistent data will be replicated.

- **Bandwidth Throttling**: The bandwidth throttling policy provides you with an option to set the maximum limit of the network bandwidth. You can specify the policy depending on the usage of your network. For example, you can define a policy that a Nutanix cluster should replicate data from site A to site B at less than 10 MBps between 9 a.m. to 5 p.m. on weekdays because there might be other critical traffic between the two sites then
- **Compression**: Enable this option to compress the replicated data on wire (network compression).

6. Then, map the storage containers. Typically, there would be two storage containers:

- Storage container #1 holds the template image(s) and the workload VMs created for the Frame accounts. This storage container is the same storage container where the original template image was stored when the primary AHV cluster was added to Frame.
- Storage container #2 stores the Volume Groups containing profile disks and personal drives. During the initial Frame setup of the primary AHV cluster, this storage container gets selected in the CCA Wizard.

If the customer has multiple primary AHV cluster storage containers that have Frame template images and workload VMs, each storage container would need to be mapped.

Under vStore Name Mapping:

- Source vStore: the storage container where your Frame resources are located on the Primary AHV cluster.
- Destination vStore: the storage container where the replicates/backups will be stored on the remote (Secondary) AHV cluster.

> It is possible to have both primary containers mapped to only one container on the Remote Site.

In the above figure, the first row defines the mapping of the Primary Site SelfServiceContainer to the Remote Site SelfServiceContainer. The SelfServiceContainer was specified to hold the

Volume Groups of the Enterprise Profile and Personal Drive volumes. The second row defines the mapping of the Primary Site storage container default-container-77107 (containing the persistent Frame resources for all Frame Accounts on the AHV cluster) to the Remote Site storage-container-112133 (storing all the backup replicas).

> When the Failover feature is added and the Frame Administrator configures Frame to do so, the Remote Site storage container will also store the persistent workload VMs provisioned from the replicas, at the point the replicas are copied to the secondary site. This will reduce the Return to Operation time as the VMs will not have to be provisioned the moment the Failover is enabled.

7. Click on Save to finish the setup. You can now see your new Remote Site within the Data Protection section in Prism.

8. To confirm that both clusters can communicate with each other, click on the “Test Connection” option to verify the settings and network response.

9. To complete the preparation of the two AHV clusters, the AHV administrator must add the Primary Site as a Remote Site on your secondary AHV cluster. You do this by logging in to Prism Element on your second AHV Cluster and performing the same steps as described previously with the Primary Site as the Remote Site for your secondary AHV Cluster.

For Frame accounts on Azure infrastructure, no infrastructure configuration work is required. Frame administrators must use the same Azure Cloud Account when specifying the cloud account where the persistent resources of the Frame account are to be stored. Persistent resource backups must be stored in a different datacenter (region).

Monitor your Azure resource usage to ensure you do not exceed your Azure resource limits in your secondary region.

Configuration

Once the infrastructure is prepared, follow the step-by-step guide below to enable Frame DR on your Frame account.

1. Login to your Frame Account as a Customer or Organization Administrator
2. Navigate to the Account Settings tab, and select the *Disaster recovery* tab. Enable the **Enable Frame DR** option.

3. The following configuration information needs to be provided.

- **Backup cloud account**: Select the cloud account that has been setup during the Remote Site configuration
- **Backup data center**: Select the region for the Cloud Account (only for public cloud infrastructure)
- **Enable post-session backup**: After a user session is closed, the resource is backed up. For Sandbox/utility/persistent desktop, Frame will create a backup of the respective server. The VM will stay powered on during the backup which will allow users to start new sessions faster, but also add a risk of inconsistency of the backup depending on the workload. If user volumes (enterprise profile disk, personal drive) are used, when the session closes, the user volume is detached and Frame will create a user volume backup.
- **Stop server before post-session backup**: If enabled, after a Frame session closes, the VM will be stopped before the backup task is executed to ensure the backup is in a consistent state. Enabling this option will increase the time for the VM to be available for the next session, since the VM must be powered on.

> There is no option currently to set the post-session backup policy specifically for Sandbox or Utility Server(s).

4. After all configuration parameter values are set, click Save to save the settings to complete the setup. You can go to the account Notification Center to confirm that Frame has completed the DR configuration for your account.

Backup and Restore

When the Frame DR is enabled, backups are replicated to the secondary AHV cluster or secondary cloud region. Refer to Backups for details on the different ways Frame administrators can backup the persistent resources and restore from backups on the primary site or from replicas on the secondary site.

Revision #6
Created 1 October 2025 04:53:01
Updated 14 January 2026 05:58:44 by Nikola Savic