# Storage Services - Files (File Services)

[ PDF generated August 10 2026. For all recent updates please see the Nutanix Bible releases notes located at https://nutanixbible.com/release_notes.html. Disclaimer: Downloaded PDFs may not always contain the latest information. ]

The Nutanix Files feature allows users to leverage the Nutanix platform as a highly available file server. This allows for a single namespace where users can store home directories and files.

## Supported Configurations

The solution is applicable to the configurations below (list may be incomplete, refer to documentation for a fully supported list):

Core Use Case(s):

- Home folders / user profiles
- File storage
- Media repository
- Persistent container storage

Management interfaces(s):

- Prism Element (PE)
- Prism Central (PC)

Hypervisor(s):

- AHV
- ESXi

Upgrades:

- Prism

Compatible Features:

- Nutanix Snapshots and DR
- File share level replication and DR (Smart DR)
- File tiering to S3 compliant storage (Smart Tier)
- File level snapshots including Windows Previous Version (WPV)
- Self Service Restore
- CFT Backups

File Protocols:

- SMB 2
- SMB 3
- NFS v4
- NFS v3

## Files Constructs

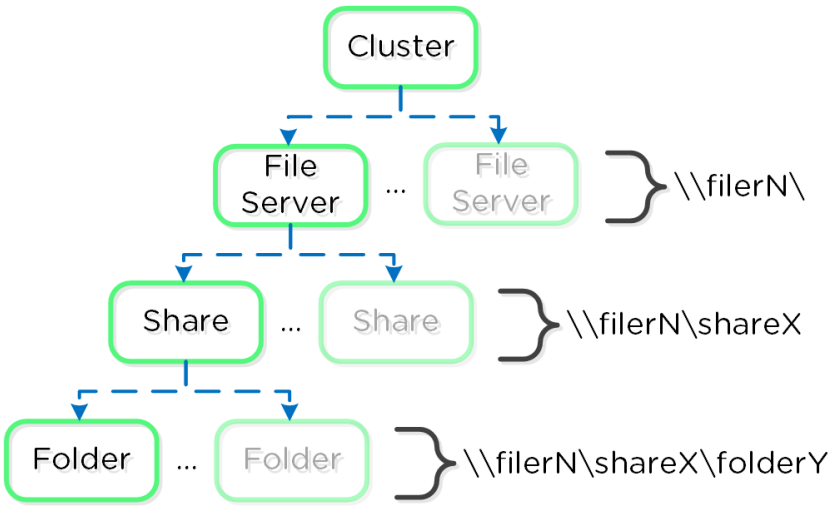
This feature is composed of a few high-level constructs:

- File Server
  - High-level namespace. Each file server will have its own set of Files VMs (FSVM) which are deployed

- Share
  - Share exposed to users. A file server can have multiple shares (e.g. departmental shares, etc.)

- Folder
  - Folders for file storage. Folders are sharded across FSVMs

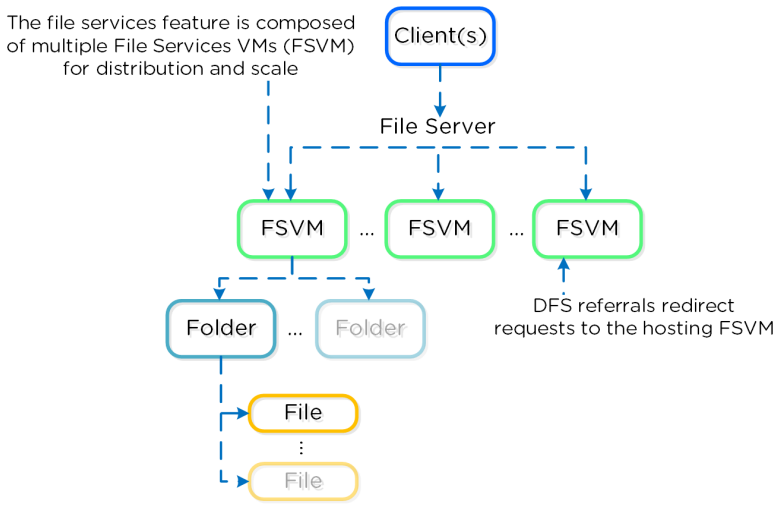
The figure shows the high-level mapping of the constructs:




Files Mapping

The Nutanix Files feature follows the same methodology for distribution as the Nutanix platform to ensure availability and scale. A minimum of 3 FSVMs will be deployed as part of the File Server deployment.

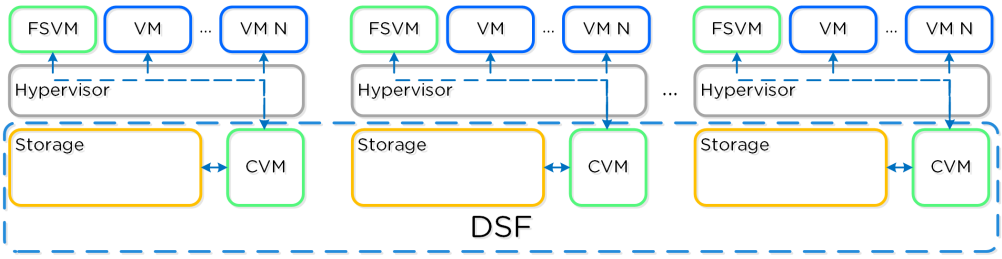
The figure shows a detailed view of the components:




Files Detail

The FSVMs are combined into a logical file server instance sometimes referred to as a Files cluster. You can create multiple Files clusters within a single Nutanix cluster. The FSVMs are transparently deployed as part of the configuration process.

The figure shows a detailed view of FSVMs on the AOS platform:




FSVM Deployment Arch

## Authentication and Authorization

The Nutanix Files feature is fully integrated into Microsoft Active Directory (AD) and DNS. This allows all of the secure and established authentication and authorization capabilities of AD to be leveraged. All share permissions, user and group management is done using the traditional Windows MMC for file management.

As part of the installation process the following AD / DNS objects will be created:

- AD Computer Account for File Server
- AD Service Principal Name (SPN) for File Server and each FSVM
- DNS entry for File Server pointing to all FSVM(s)
- DNS entry for each FSVM

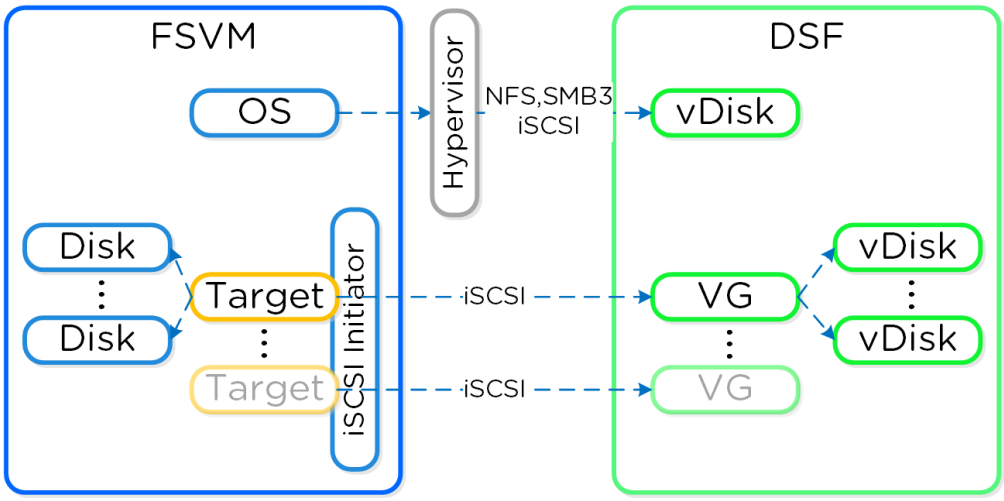
### AD Privileges for File Server Creation

A user account with the domain admin or equivalent privileges must be used to deploy the File Service feature as AD and DNS objects are created.

## High-Availability (HA)

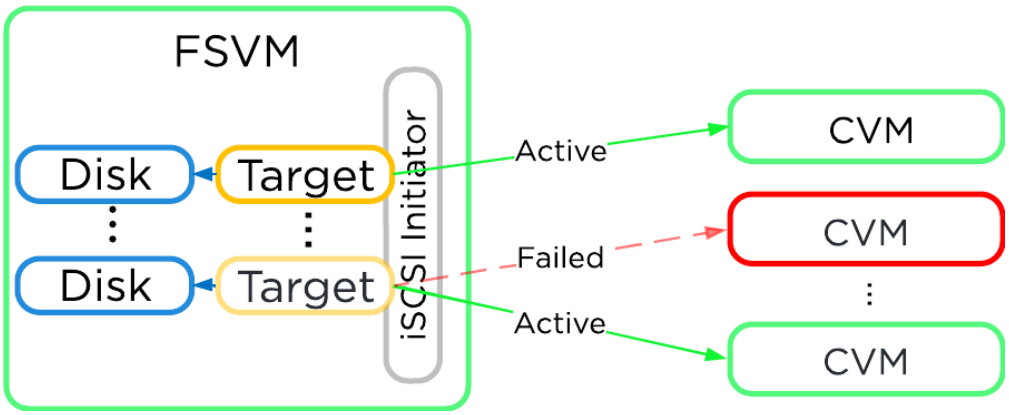
Each FSVM leverages the Volumes API for its data storage which is accessed via in-guest iSCSI. This allows any FSVM to connect to any iSCSI target in the event of a FSVM outage.

The figure shows a high-level overview of the FSVM storage:




FSVM Storage

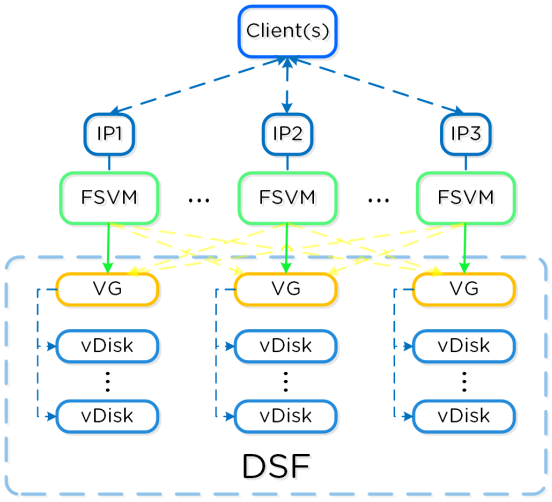
In the event a CVM becomes unavailable (e.g. active path down), iSCSI redirection is used to failover targets to another CVM which will then takeover IO.




FSVM Storage Failover

When the original CVM comes back and is healthy it will be marked as the active path to provide for IO.

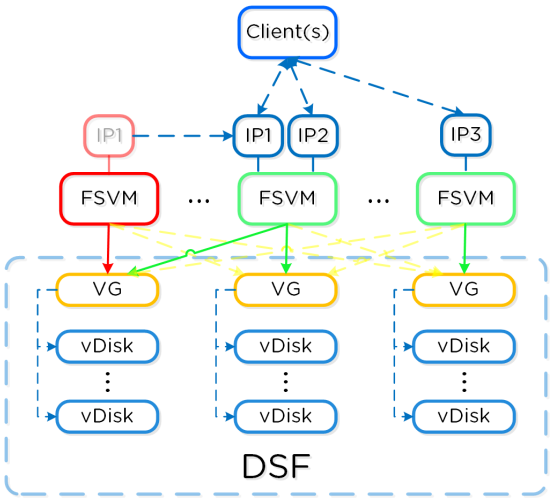
In a normal operating environment each FSVM will be communicating with its own VGs for data storage with passive connections to the others. Each FSVM will have an IP which clients use to communicate with the FSVM as part of the DFS referral process. Clients do not need to know each individual FSVM's IP as the DFS referral process will connect them to the correct IP hosting their shares and folder(s).




FSVM Normal Operation

In the event of a FSVM "failure" (e.g. maintenance, power off, etc.) the VG and IP of the failed FSVM will be taken over by another FSVM to ensure client availability.

The figure shows the transfer of the failed FSVM's IP and VG:




FSVM Failure Scenario

When the failed FSVM comes back and is stable, it will re-take its IP and VG and continue to serve client IO.