



NetApp Data Migrator documentation

NetApp Data Migrator

NetApp
May 06, 2026

This PDF was generated from <https://docs.netapp.com/us-en/data-migrator/index.html> on May 06, 2026.
Always check docs.netapp.com for the latest.

Table of Contents

- NetApp Data Migrator documentation 1
- Release notes 2
 - What's new in NetApp Data Migrator 2
 - 22 April 2026 2
- NetApp Data Migrator support for features, file servers, and protocols 2
 - Supported and unsupported features 2
 - Supported file servers 3
 - Supported NFS and SMB migration protocols 4
- Known issues for NetApp Data Migrator 4
 - Configuration 4
 - Reporting 6
 - Validation 7
 - Workflows 7
- Known limitations for NetApp Data Migrator 8
 - NFS and SMB discovery and migration limitations 8
 - Feature limitations 8
- Get started 10
 - Learn about NetApp Data Migrator 10
 - Decide whether to use NetApp Data Migrator 13
 - Quick start for NetApp Data Migrator 14
 - Networking requirements 15
 - Verify NFS and SMB networking access in NetApp Data Migrator 15
 - Port requirements for NetApp Data Migrator 15
- Install, set up, and upgrade 17
 - Learn about installing NetApp Data Migrator 17
 - Register for an account to access NetApp Data Migrator 17
 - Deploy the control plane and Linux worker VMs for NetApp Data Migrator 18
 - Create the control plane and worker VMs to access NetApp Data Migrator 21
 - Optionally, validate the control plane VM deployment for NetApp Data Migrator 23
 - Access the NetApp Data Migrator UI 24
 - Configure NetApp Data Migrator 24
 - Log in to NetApp Data Migrator 24
 - Log out of NetApp Data Migrator 25
 - Upgrade the control plane and workers in NetApp Data Migrator 25
 - Step 1: Upload the upgrade bundle 26
 - Step 2: Upgrade the control plane and workers 26
 - Step 3: View logs and troubleshoot 27
- Use NetApp Data Migrator 28
 - Create and manage projects in NetApp Data Migrator 28
 - Create a project 28
 - Edit a project 28
 - Switch between projects 28
 - Manage users 29

| | |
|---|----|
| Add and manage users in NetApp Data Migrator | 29 |
| Manage access control for NetApp Data Migrator | 30 |
| Add and manage file servers | 31 |
| Add a new file server | 31 |
| Manually upload export and directory paths | 34 |
| Edit file server details | 34 |
| Configure real-time notifications for NetApp Data Migrator | 35 |
| Manage migration options | 36 |
| Plan data migration in NetApp Data Migrator using Bulk Discover | 36 |
| Perform data migration using NetApp Data Migrator | 37 |
| Configure Bulk Cutover in NetApp Data Migrator | 40 |
| Manage jobs and job runs in NetApp Data Migrator | 41 |
| View Job Config List | 42 |
| Activate or deactivate a Job | 42 |
| Edit job configurations | 43 |
| Re-run errored files and directories | 43 |
| Delete a Job | 43 |
| View Job Details | 44 |
| View Job Run History | 44 |
| Manage Job Run operations | 44 |
| Access Job Run Details | 45 |
| View Migration Activity | 46 |
| Generate a job error report | 46 |
| Generate a NetApp Data Migrator support bundle | 46 |
| FAQ for NetApp Data Migrator | 48 |
| Get help | 49 |
| Register for NetApp Data Migrator support | 49 |
| Troubleshoot NetApp Data Migrator | 49 |
| SMB mount failure when using host name | 49 |
| Troubleshoot application access | 50 |
| Use the "kubect!" reference commands | 50 |
| Unseal OpenBao | 51 |
| Troubleshoot Azure VM access | 51 |
| Windows worker fails to switch user on SMB file server | 52 |
| Legal notices | 53 |
| Copyright | 53 |
| Trademarks | 53 |
| Patents | 53 |
| Privacy policy | 53 |
| Open source | 53 |

NetApp Data Migrator documentation

Release notes

What's new in NetApp Data Migrator

Learn about what's new in NetApp Data Migrator.

22 April 2026

NetApp Data Migrator 2026.04.0 offers a new solution for migrating data files. You can use NetApp Data Migrator to migrate data from on-premises or third-party storage systems to NetApp cloud storage services. NetApp Data Migrator supports the NFS and SMB file transfer protocols.

[Learn more about NetApp Data Migrator](#)

NetApp Data Migrator support for features, file servers, and protocols

NetApp Data Migrator supports certain features, file servers, and protocols.

Supported and unsupported features

NetApp Data Migrator supports a range of features for NFS and SMB migrations. Some features are not supported.

Supported features

| Description | Supported feature |
|--------------------------------|--|
| Permissions and audit handling | <ul style="list-style-type: none">• Chain of custody reporting• Discretionary Access Control List (DACL)• Preserve Access Control List (ACL)• User Identifier (UID) and Security Identifier (SID) remapping |
| File system objects and links | <ul style="list-style-type: none">• Hard link handling <p>NetApp Data Migrator migrates objects and links as separate files.</p> <ul style="list-style-type: none">• Symbolic links <p>Note: Supported for NFS migrations</p> |
| File metadata preservation | <ul style="list-style-type: none">• Preserve access time• Preserve creation time• Preserve modified time• Preserve permissions |

| Description | Supported feature |
|---|---|
| Migration behavior and data consistency | <ul style="list-style-type: none"> • Delete propagation • Incremental migration • Support for open files • Switchover support |
| Migration control and execution | <ul style="list-style-type: none"> • File pattern exclusions • Scheduling for migration |

Unsupported features

| Description | Unsupported feature |
|---|--|
| Permissions and audit handling | <p>System Access Control List (SACL)</p> <p>Note: Unsupported for SMB migrations</p> |
| File system objects and links | <ul style="list-style-type: none"> • Follow NTFS junctions • Symbolic links <p>Note: Unsupported for SMB migrations</p> <ul style="list-style-type: none"> • Alternate data streams <p>NetApp Data Migrator can discover but not migrate alternate data streams.</p> |
| File metadata preservation | Selective file attributes |
| Migration behavior and data consistency | Migration of snapshots |

Supported file servers

NetApp Data Migrator supports certain file servers as source and destination for data migration.

| Description | Supported file server |
|-------------|---|
| Source | Any NAS server, for example, Dell Isilon, ONTAP, Vanilla Linux, Windows, Cloud Volumes ONTAP |
| Destination | All service levels of Azure NetApp Files (ANF), Google Cloud NetApp Volumes (GCNV), Amazon FSx for NetApp ONTAP (FSxN), Cloud Volumes ONTAP |

Supported NFS and SMB migration protocols

NetApp Data Migrator supports certain NFS and SMB protocol versions for data migration.

| Protocol | Supported versions |
|----------|--------------------|
| NFS | 4.1, 3.0 |
| SMB | 3.1, 3.0, 2.0 |

Known issues for NetApp Data Migrator

Known issues identify problems that might prevent you from using this release of the product successfully. Read these known issues carefully.

Configuration

Access permission mismatch when using SID mapping

NetApp Data Migrator might report a `Missing ACE in target` error when using SID mapping. This error indicates an access permission mismatch between the source and target systems because SID mapping was not performed at the root level.

Workaround

Provide the CSV mapping for the SID source and target as shown in the following two scenarios:

Scenario 1

Provide the SID in the CSV mapping sheet for users or groups deleted or removed from the source Active Directory, as shown in the following example:

| sid_source | sid_target |
|--|---|
| S-1-5-21-2444020195-1862089444-1769087368-1000 | S-1-5-21-3481156262-2863848796-4292454742-512 |

Scenario 2

For active users or groups in Active Directory, provide the usernames or group names in the CSV mapping sheet exclusively in lowercase. Include the domain prefix (domain\username), as shown in the following example:

| sid_source | sid_target |
|------------------|------------------|
| rootdomain\user1 | rootdomain\user2 |

Bulk migration limitation for same level directories

When using the Bulk Migrate feature, you cannot create multiple migration jobs together for directories that are

at the same level in the source and destination directory hierarchy. For example, sibling folders in the same share operation for a source and destination. Attempting to include such directories in a single bulk migration configuration causes the job creation to fail.

Workaround

Create migration jobs one at a time for directories that are at the same level, instead of adding them together.

Directory level migration inherited permission stamping

In directory level migrations, inherited permissions on a selected root directory are not stamped on the destination. Because NetApp Data Migrator does not apply the inherited permissions for the root directory, child directories and files that rely on inheritance also do not receive the inherited permissions.

This issue affects only inherited permission propagation from the root directory. NetApp Data Migrator correctly stamps explicit permissions set directly on files and directories (noninherited permissions) during migration.

Workaround

After the migration completes, manually reapply or reset the inherited permissions on the root directory at the destination. This allows the correct inherited permissions to propagate to all child directories and files

Validation of manual upload of UID and GID mapping in NFS

During NFS migrations, if the UID and GID mapping CSV file contains numeric user IDs or group IDs that do not exist on the destination system, NetApp Data Migrator applies (stamps) these values as is. NetApp Data Migrator does not validate whether the specified UID or GID exists on the destination and does not report any error or warning in the UI. This can result in file migration with incorrect ownership. You need to provide the correct UID and GID mapping.

Workaround

Ensure that all UID and GID values specified in the mapping CSV correspond to valid and existing users and groups on the destination system before starting the migration. Manually verify user and group existence on the destination to avoid NetApp Data Migrator applying incorrect ownership during migration.

Migration precheck displays false insufficient space warning

During migration prechecks, you might see the following warning, even if the destination has sufficient space:

```
Insufficient destination space for selected path. Do you still want to
proceed with the migration?
```

This can happen if you skip the discovery step and NetApp Data Migrator uses a general command that reads the entire block device size instead of the actual dataset size.

Workaround

Run Discovery before a Migration run. This ensures that the disk usage information is available for the pre-check operation. If you still see the warning:

1. Confirm that discovery has completed.
2. Manually verify the destination volume has enough space.
3. If there is sufficient space, you can safely proceed with data migration.

Reporting

Excel displays incorrect permissions in COC report file

When opening the Chain of Custody (CoC) report CSV file in Microsoft Excel, some file or folder permissions might appear as #NAME?, for example, -rwxrwxrwx, instead of the actual values.

This happens because Excel mistakenly treats certain permission strings (starting with - or =) as formulas, leading to display errors. The CSV file itself is correct, this is only a display issue.

Workaround

To view correct file and folder permissions open the CSV file using one of the following applications:

- Google Sheets
- Apple Numbers
- Online CSV viewer
- Text editor, for example, Notepad++

No error message when Bulk Discovery job fails due to network issues

If the host or destination server goes down during a Bulk Discovery job, NetApp Data Migrator might not show an error message. This can give the impression that the job is still running normally.

Discovery jobs refresh every 30 seconds. If you notice that the file count, directory count, or data size is not updating, this might indicate a network issue.

Workaround

1. Check the network connectivity:
 - a. Open the worker VM terminal.
 - b. Ping the IP address of the destination server.

If there is no response, the destination might be unreachable.

2. Restore the network interface:
 - a. Use SSH to connect to the destination server:

```
ssh <destination_IP>
```

- b. Find the interface name, for example, eth0:

```
ipconfig
```

- c. Bring the network interface back online:

```
ifup <interface_name>
```

3. If required, repeat the Steps 1 and 2 for the source server.

Unable to switch user on Windows worker

Switching to a different user account on Windows worker might fail due to existing network connections. This can prevent access to the file server.

Workaround

1. Remove the previous connection by opening Command Prompt on the Windows worker and running the following commands:

```
net use
```

```
net use <IP address> /delete
```

2. Switch to the new user account and access the file server.

Validation

File sizes might differ after migration even if counts match

After data migration completes, the total number of files is correct, but some files might have a different size compared to the original source. This can happen if the network is interrupted or if there are problems with the server during file transfer.

Workaround

1. Review the migration COC report to identify files marked as errored.
2. Re-run the migration until the errors are resolved.

Workflows

Job paused or stalled for more than 20 minutes

You might need to intervene when you observe network connectivity issues, issues with source or destination volume stability, or both. The job might be in the Paused or Running state without any visible progress. This might happen if the source or destination services go down, or if the worker service experiences downtime.

Workaround

1. Check the source and destination.

If they are offline, restart to restore connectivity.

2. Check the worker status.

If the worker is offline, use SSH to connect to the VM and run the following command:

```
systemctl restart datamigrator-worker.service
```

3. Reboot the VM:

If issue persists, restart the worker VM.

Job run status is confusing when errors occur

Some Migration job runs encounter errors and show a Completed or Errored status. This can cause confusion when interpreting the Migration job run status.

Status definitions:

- Completed: A job run has finished, but might contain errors.
- Errored: A job run failed due to a critical issue.

Workaround

Verify the job run outcome by checking the job run details for any errors, especially if the status is Completed. Do not rely only on the status label until after you address this issue.

Known limitations for NetApp Data Migrator

NFS and SMB migration limitations and features that do not work or do not work well with this version are listed here. Read these limitations carefully.

NFS and SMB discovery and migration limitations

| Description | NFS | SMB |
|--|--------------------------|---------------------------|
| Number of export paths that can run simultaneously | 4 | 2 |
| Maximum number of files in a directory | 1 million | 1 million |
| Worker sizing | 4 core CPU, 16 GB memory | 16 core CPU, 64 GB memory |
| Control plane sizing | 8 core CPU, 64 GB memory | 8 core CPU, 64 GB memory |
| Maximum number of files in an export path | 20 million | 20 million |

Feature limitations

| Description | Limits |
|----------------------------|---|
| Active destination support | NetApp Data Migrator does not support an active destination (when a target storage is actively used or written before Cutover). |

| Description | Limits |
|--------------------------------|---|
| Case sensitive files | For SMB, NetApp Data Migrator migrates only one of the case-differing files created using NFS in a folder and errors out the other file. This occurs because SMB can't accept both files. You can run discovery using NFS to identify these case-sensitive files. |
| Network accessibility | NetApp recommends using NetApp Data Migrator in private networks. |
| NFSv4 ACLs | NetApp Data Migrator does not stamp access control lists (ACLs) with NFSv4, it only applies basic permissions in the destination. This behavior is similar to NFSv3. |
| Protocol migration - Type | Cross-protocol migration is not supported, for example, NFS to SMB. |
| Protocol migration - Version | Cross-version migration within the same protocol is not supported, for example, NFSv3 to NFSv4. |
| SMB permissions | NetApp Data Migrator does not support migration of SMB System Access Control List (SACL) (audit permissions). |
| SMB files with trailing spaces | When migrating over SMB, NetApp Data Migrator errors out files with names that contain trailing spaces because SMB does not permit these file names. |
| SMB special files | NetApp Data Migrator discovers redirects (symbolic links, hard links, junction points, Alternate Data Streams (ADS), and volume mount points) and reports them after discovery. Migration of ADS, sparse files, and SMB redirects is not supported. |
| Security | NetApp Data Migrator uses self-signed certificates to encrypt web traffic with SSL/TLS. |
| Sparse files | Sparse files become full-size files when they migrate, NetApp Data Migrator doesn't preserve sparsity. You need extra storage for these files. |
| System files | NetApp Data Migrator cannot migrate system-generated files that the source owns. |
| User interface | NetApp Data Migrator is optimized for Google Chrome and Firefox browsers using 1920 x 1080 screen resolution; mobile displays are not supported. |
| Windows worker deployment | The Windows worker must be part of the same root domain as the destination. |

Get started

Learn about NetApp Data Migrator

NetApp Data Migrator is an enterprise grade, multicloud, data migration software application that simplifies the migration of unstructured file data from on-premises or third-party storage systems to public cloud storage services powered by NetApp. NetApp Data Migrator is an independent application that runs on user-managed virtual machines and eliminates the need for complex custom scripts and disjointed tools.

You can use NetApp Data Migrator to discover your existing storage environments, generate a quick inventory of files, and create plans to migrate your data from a source storage server to NetApp cloud storage services. After data migration starts, you can monitor migration jobs using the UI. You can also generate Chain of Custody (CoC) reports that use checksums to help verify your data migration operations.

NetApp Data Migrator supports NFS and SMB file transfer protocols. You deploy worker nodes in your environment to maintain control and security during migration. The workers facilitate parallel data transfers, which improves performance and scalability. NetApp Data Migrator includes features such as pre-checks and incremental sync to provide smooth and efficient migration with minimal downtime. You can keep your source systems active for most of the migration process, then perform a final cutover when ready. NetApp Data Migrator also offers robust logging and error handling, allowing you to troubleshoot and recover from issues without having to restart the entire migration process.

Before you start working with NetApp Data Migrator, it's helpful to first be familiar with the key terminology.

Control plane

The control plane gives you access to the migration activities. From the control plane, you can perform the following tasks:

- Manage projects, users, jobs, and file servers.
- Schedule and dispatch job runs to available workers.
- Monitor job runs, collect logs, and report status.
- Enforce access control and user permissions.
- Configure an SMTP email server for real-time notifications.

Cutover

A Cutover job is the last migration step. It is required for the final sync between source and destination systems. A Cutover job performs the following actions:

- Stops ongoing migrate jobs for selected paths
- Performs a final sync to ensure that data is consistent
- Generates a Chain of Custody (CoC) report for validation
- Requires your approval to mark the migration as complete

Discover

A Discover job scans and inventories data on a source or destination file server. It creates a report with details about the files and directories in selected export paths in a source or destination file server, which helps you to understand the scope and complexity of your data before starting migration. A Discover job

performs the following actions:

- Analyzes the structure and contents of export paths
- Collects metadata such as file names, sizes, permissions, and timestamps
- Generates detailed reports and histograms for planning and auditing

Export path

An export path represents the location of the data to be included in a Discover, Migrate, or Cutover operation. Export paths are the fundamental units of data being copied in any migration workflow and have the following characteristics:

- Protocol-specific (NFS exports or SMB shares)
- Validated for accessibility and permissions
- Used as input for job creation (Discovery, Migrate, Cutover)

Job

A job is a logical construct of a data migration task. It specifies what to do, where to do it, and how it should be executed. You can reuse jobs and schedule or trigger them manually.

A job includes two main components:

- **Job definition:** A predefined sequence of steps, for example, scan, sync, or report.
- **Job configuration:** User-defined parameters such as source or destination paths, exclusion rules, and scheduling.

NetApp Data Migrator supports three main job types:

- **Discovery job:** Inventories and analyzes source and destination data.
- **Migrate job:** Transfers data from source to destination.
- **Cutover job:** Finalizes the migration and switches to the destination system.

Job run

A job run is a single execution instance of a job. Job runs allow you to monitor, manage, and troubleshoot the execution of migration tasks in real time. A job run includes the following details:

- Has a unique timestamp and execution ID
- Can be in one of several states: Ready, Running, Paused, Stopped, Errored, Blocked, or Completed
- Generates logs, metrics, and task-level details

Migrate

A Migrate job migrates your data from a source to a destination file server, securely, efficiently, and with minimal disruption. It has the following features:

- Performs baseline migration (initial full copy)
- Supports incremental sync (updates based on changes)
- Allows you to configure options such as exclusion patterns, permission remapping, and access time preservation
- Includes pre-checks of permissions, capacity, and connectivity

Project

A Project is a logical workspace that includes all components and activities related to a specific data migration activity. It serves as the top-level organizational unit within NetApp Data Migrator. A project has the following characteristics:

- A unique name and description
- Associated users with defined roles (Project Admin, Project Viewer)
- Linked file servers, jobs, workers, and configurations

Projects help you to isolate migration efforts, making it easier to manage multiple migrations simultaneously across different teams, departments, or clients.

Storage server (file server)

A storage (file) server is a critical component in the migration workflow. It stores the data to be migrated or serves as the destination for migrated data.

- NetApp Data Migrator supports NFS and SMB file servers
- Each file server is configured with the following details:
 - A name and server type
 - Authentication credentials
 - Associated workers for executing migration tasks

Users

Users manage data migration activities. App Admin users (administrators) assign roles to other users that determine their level of access and control.

NetApp Data Migrator supports three user roles:

- **App Admin:** Provides full administrative privileges that allow you to manage other users, projects, and system settings
- **Project Admin:** Provides permission to manage specific projects and configure, create, and monitor jobs
- **Project Viewer:** Provides read-only access to view project details, job statuses, and reports

You authenticate with an email and password, and Role-Based Access Control (RBAC) governs your permissions. This provides secure, role-appropriate access to sensitive data and operations. NetApp Data Migrator uses RBAC to manage permissions and helps secure access to resources.

Worker

A worker is a virtual machine that performs actual data operations, for example, copying data from source to destination.

- Workers are responsible for executing tasks such as scanning directories, copying files, and syncing metadata.
- Workers enable distributed processing, allowing NetApp Data Migrator to scale across large datasets and multiple environments efficiently.
- Workers relay high-level statistical information about data migration to the control plane.
- You install and register a worker using NetApp Data Migrator.

- Each worker has the following characteristics:
 - Is associated with one or more file servers
 - Reports system metrics such as CPU, memory, and status (online or offline) to the control plane
 - Reports high-level statistical information about data migration to the control plane

What's next?

After learning about NetApp Data Migrator, you can [decide whether to use the software for your data migration operations](#).

Decide whether to use NetApp Data Migrator

Use the decision matrix to determine whether to use NetApp Data Migrator or SnapMirror for your NFS and SMB data migration operations from an ONTAP on-premises storage system. For example, if you are migrating NFS and SMB files from an ONTAP on-premises source running ONTAP 9.12.1 to a Google Cloud NetApp Volumes Flex service destination, you should use NetApp Data Migrator.

| On-premises or third-party storage system source | Amazon FSx for NetApp ONTAP | Azure NetApp Files hardware | Cloud Volumes ONTAP | Google Cloud NetApp Volumes hardware | Google Cloud NetApp Volumes Flex | Google Cloud NetApp Volumes Flex (VSA based) |
|--|-----------------------------|-----------------------------|----------------------|--------------------------------------|----------------------------------|--|
| ONTAP on-premises Beginning with ONTAP 9.10.1 | SnapMirror | SnapMirror | SnapMirror | SnapMirror | NetApp Data Migrator | SnapMirror |
| ONTAP on-premises For ONTAP 9.9.1 and earlier | NetApp Data Migrator | NetApp Data Migrator | NetApp Data Migrator | NetApp Data Migrator | NetApp Data Migrator | NetApp Data Migrator |
| Non-NetApp storage systems and arrays | NetApp Data Migrator | NetApp Data Migrator | NetApp Data Migrator | NetApp Data Migrator | NetApp Data Migrator | NetApp Data Migrator |
| Cloud Volumes ONTAP Beginning with ONTAP 9.10.1 | SnapMirror | SnapMirror | SnapMirror | SnapMirror | NetApp Data Migrator | SnapMirror |
| Cloud Volumes ONTAP For ONTAP 9.9.1 and earlier | NetApp Data Migrator | NetApp Data Migrator | NetApp Data Migrator | NetApp Data Migrator | NetApp Data Migrator | NetApp Data Migrator |
| Google Cloud NetApp Volumes Flex | Not applicable | Not applicable | NetApp Data Migrator | NetApp Data Migrator | Not applicable | NetApp Data Migrator |

| On-premises or third-party storage system source | Amazon FSx for NetApp ONTAP | Azure NetApp Files hardware | Cloud Volumes ONTAP | Google Cloud NetApp Volumes hardware | Google Cloud NetApp Volumes Flex | Google Cloud NetApp Volumes Flex (VSA based) |
|--|-----------------------------|-----------------------------|----------------------|--------------------------------------|----------------------------------|--|
| Migrating data without permissions | NetApp Data Migrator | NetApp Data Migrator | NetApp Data Migrator | NetApp Data Migrator | NetApp Data Migrator | NetApp Data Migrator |

Related information

Learn about [SnapMirror volume replication](#)

Quick start for NetApp Data Migrator

Getting started with NetApp Data Migrator includes a few steps.

1

Learn about NetApp Data Migrator

NetApp Data Migrator supports NFS and SMB file transfer protocols. Determine that NetApp Data Migrator supports your data migration needs and choose the deployment option that suits your environment:

- AWS
- Azure
- Google Cloud services
- Open Virtual Appliance (OVA) templates

Review [Decide whether to use NetApp Data Migrator](#) and the [Networking requirements](#).

2

Install and set up

NetApp Data Migrator uses a control plane and worker nodes. First you deploy the control plane VM and worker VMs based on your migration needs. For NFS, you deploy a Linux worker and for SMB, you deploy a Windows worker. You can use NFS or SMB, or both protocols. After deployment, you create the control plane VM and worker VMs and access the NetApp Data Migrator UI.

[Learn about installing NetApp Data Migrator](#)

Learn how to:

1. [Deploy the control plane VM and Linux worker VM](#)
2. [Create the control plane VM and worker VMs](#)
3. [Access the NetApp Data Migrator UI](#)

3

Configure and manage

You first log in as an administrator using the default credentials and update your username and password.

Then you can create your first project and add the file servers to initiate migration workflows.

Learn how to:

1. [Configure NetApp Data Migrator](#)
2. [Create and manage projects in NetApp Data Migrator](#)

Networking requirements

Verify NFS and SMB networking access in NetApp Data Migrator

You need to ensure that the IP address and subnet for both the control plane and workers are allowed in the export policy on the storage system. This is required to support NFS and SMB migrations using NetApp Data Migrator.

Verify NFS access

For NFS, the control plane and worker nodes need permission to access the storage system as root clients.

Steps

1. Perform a manual mount from a worker node to verify volume accessibility:

```
sudo mount -t nfs <storage-ip>:/<volume-path> /mnt/test
ls -la /mnt/test
```

2. Ensure that root access is enabled by verifying that the export policy rule allows superuser access. If necessary, enable root access (no root squash) by modifying the export policy rule.

Verify SMB access

For SMB access, the control plane and worker nodes need permission to access the storage system using the SMB credentials. The SMB user must be part of the Backup operators and Administrators groups.

Step

1. Perform a manual mount from a worker node to verify volume accessibility:

```
net use Z: \\<storage-ip>\<share> /user:<domain>\<username> <password>
```

Port requirements for NetApp Data Migrator

You need to ensure that certain TCP ports are open to allow communication between the control plane virtual machines (VMs) and worker VMs in NetApp Data Migrator.

Control plane ports

| Service | TCP port | From | To |
|--------------------------------------|--------------|--|---------------|
| Temporal Server | 7233 or 7234 | Workers and clients | Control plane |
| Temporal UI | 8080 | Default port, if enabled | Control plane |
| PostgreSQL (Temporal database) | 5432 | Temporal Services (from the control plane) | Control plane |
| Redis | 6379 | Worker or control plane services | Control plane |
| API or UI ingress (your application) | 80 or 443 | Browser or any external client | Control plane |
| Grafana | 3000 | Browser | Control plane |

Worker ports

| Service | TCP port | From | To |
|---------------------------|-----------|-------------------------------|--|
| Outbound to control plane | 7233 | Services in the control plane | Temporal frontend |
| Outbound to control plane | 6379 | Services in the control plane | Redis |
| Outbound to control plane | 80 or 443 | Browser | API or UI (if you call it) |
| Outbound to storage | 2049 | Worker | NFS servers Note: Include TCP or UDP port 111 if you need the portmapper service for Remote Procedure Calls. |
| Outbound to storage | 445 | Worker | SMB servers |

Install, set up, and upgrade

Learn about installing NetApp Data Migrator

NetApp Data Migrator consists of a control plane and one or more workers that work together to perform data migration jobs using the NFS and SMB transport protocols.

- **Control plane:** The control plane acts as the central management and control layer. You deploy the control plane on a Linux virtual machine (VM), then you deploy the workers.
- **Workers:** Workers are virtual machines that perform the actual data migration. You can deploy multiple workers based on scale and your requirements. The worker type depends on the protocol:
 - A Linux worker supports NFS migrations.
 - A Windows worker supports SMB migrations.

First you deploy the control plane virtual machine (VM) and Linux worker VM using the AWS, Azure, or Google Cloud service or using Open Virtual Appliance (OVA) templates. You download the NetApp Data Migrator images required for deployment from the NetApp Support Site.

After deployment, create the control plane VM and worker VMs to access NetApp Data Migrator. Create the control plane VM and Linux worker VM using the deployed images. Create the Windows worker VM using the Windows Worker Installer, which you download from the NetApp Support Site. You can then optionally validate the control plane VM or proceed to access the NetApp Data Migrator UI and connect to the control plane and workers.

What's next?

After learning about installing NetApp Data Migrator, you can [register for an account](#) on the NetApp Support Site if you are a new customer or proceed to [deploy the control plane and Linux worker VMs](#) if you already have an account.

Register for an account to access NetApp Data Migrator

If you are a new NetApp customer, you need to register for an account on the NetApp Support Site before you can download NetApp Data Migrator. If you already have an account, you can proceed to [Deploy the control plane and Linux worker VMs for NetApp Data Migrator](#).



It can take up to one business day for your new account to be upgraded from **Guest access** to **Full access**.

Steps

1. Register for an account on the [NetApp Support Site](#) using your business email.
2. Select **Submit**.
3. Authenticate the registration initiation by entering the onetime password sent to your email.
4. On the registration completion page, provide the required details:
 - a. For User Access Level, select **NetApp Customer/End User**.
 - b. In the Serial Number field, enter NDMSSREG.

5. Select **Submit**. A confirmation window appears indicating that the user registration has been submitted successfully.

If you encounter any issues during registration or want to check the status of your registration, [open a support ticket](#).

What's next?

After learning about registering for an account, you can [deploy the control plane and Linux worker VMs](#).

Deploy the control plane and Linux worker VMs for NetApp Data Migrator

Deploy the control plane virtual machine (VM) and Linux worker VM for NetApp Data Migrator using AWS, Azure, or Google Cloud services or Open Virtual Appliance (OVA) templates. The Linux worker supports NFS data migrations.

Before you begin

Download the NetApp Data Migrator images from the [NetApp Support Site](#):

1. Select **NetApp Data Migrator**.
2. Follow the instructions on the NetApp Data Migrator downloads page to access the NetApp Data Migrator images.

About this task

Choose the AWS, Azure, Google Cloud tab, or OVA tab depending on your deploy option.

AWS

Repeat the following steps for the control plane and Linux worker Amazon Machine Images (AMIs).

Steps

1. Use the AMI IDs provided to locate the AMIs in your AWS account under **EC2 > AMIs > Private images**.
2. Copy the AMIs into your account:
 - a. Select the AMI, then select **Actions > Copy AMI**
 - b. Choose the target region (if needed).
 - c. Enable encryption and select your own KMS key.
 - d. Wait for the AMI status to show **Available**.

Azure

Repeat the following steps for the control plane and Linux worker VHDs.

Steps

1. Copy the VHD files to Azure Blob Storage:

```
az storage blob copy start \  
  --source-uri "<PROVIDED_SAS_URL>" \  
  --destination-blob "<VHD_FILE_NAME>.vhd" \  
Group 1065216673, Grouped object --destination-container \  
<YOUR_CONTAINER_NAME> \  
  --account-name <YOUR_STORAGE_ACCOUNT> \  
  --account-key <YOUR_STORAGE_ACCOUNT_KEY>
```

2. Create a new Azure image from the copied VHD file:

```
az image create \  
  --resource-group <your_resource_group> \  
  --name <your_image_name> \  
  --source \  
https://<your_storage_account>.blob.core.windows.net/<your_container_name>/<VHD_file_name>.vhd \  
  --os-type linux \  
  --location <your_Azure_region>
```

Google Cloud

Steps

1. Verify that the Google Cloud APIs required to import images and deploy the control plane and worker VMs are enabled. For more information, refer to the [Google Cloud documentation](#).
2. Create a Google Cloud Storage bucket if one does not already exist. This bucket is used to store the image archives (.tar.gz) during the import operation.

Learn how to [create a Google Cloud Storage bucket](#).

3. Set up the IAM roles and permissions. This ensures that the VM migration API has the required access permissions and the VM migration service can access the Google Cloud Storage bucket and create images.

- a. Assign the service account `objectViewer` access to your destination Cloud Storage bucket:

```
gcloud storage buckets add-iam-policy-binding
gs://<Google_Cloud_Storage_bucket> \
  --member=serviceAccount:service-<project_number>@gcp-sa
-vmmigration.iam.gserviceaccount.com \
  --role=roles/storage.objectViewer
```

The service account needs `roles/storage.objectViewer` permission to read the VM image files from your Cloud Storage bucket during the migration process.

When the VM Migration API is enabled, Google Cloud automatically provisions a service account with the following format:

```
service-<project_number>@gcp-sa-vmmigration.iam.gserviceaccount.com
```

- ++ `gcp-sa` is the Google Cloud service account
- `vmmigration` is the VM Migration service identifier
- `iam.gserviceaccount.com` is the standard domain for Google Cloud service accounts

- b. Make yourself an admin user on the `vmmigration` service:

```
gcloud projects add-iam-policy-binding <project_ID> \
  --member=user:<your_email> \
  --role=roles/vmmigration.admin
```

This gives you VM migration administrative permissions at the project level.

4. Obtain and upload the image files:

- a. Download the control plane `.tar.gz` image file and the Linux worker `.tar.gz` image file from the [NetApp Support Site](#).
- b. Upload the `.tar.gz` files to your Google Cloud Storage bucket.

5. After the image archives are uploaded to Google Cloud Storage, create VM images using the VM Migration Service by running the following command for each image (control plane and Linux worker).

```
gcloud migration vms image-imports create <image_name> \  
  --source-  
file=gs://<Google_Cloud_Storage_bucket>/<image_name>.tar.gz \  
  --image-name=<image_name> \  
  --location=<region> \  
  --target  
-project=projects/<project_ID>/locations/global/targetProjects/<proj  
ect_ID> \  
  --project=<project_ID>
```

This command creates a new Google Cloud Platform VM image from the provided archive in the specified region.

6. List image import operations and confirm completion:

```
gcloud migration vms image-imports list --location=<region>  
--project=<project_ID>
```

OVA

Step

Download the control plane .ova image file and the Linux worker .ova image file from the [NetApp Support Site](#).

What's next?

After learning about deploying a control plane VM and Linux worker VM, you can [create the control plane and worker VMs](#).

Create the control plane and worker VMs to access NetApp Data Migrator

Create the control plane virtual machine (VM) and Linux and Windows worker VMs to access NetApp Data Migrator.

Before you begin

For SMB migrations only, download the Windows Worker Installer from the [NetApp Support Site](#).

About this task

You create the control plane VM and Linux worker VM using the images that you deployed using AWS, Azure, or Google Cloud service or OVA templates. You create the Windows worker VM using the Windows Worker Installer. The Linux worker VM supports NFS migrations and the Windows worker VM supports SMB migrations. You can create multiple worker VMs based on your needs.

Steps

1. Use the deployed control plane image to create a control plane VM with the following recommended configuration:

| Description | Recommended setting |
|------------------|---|
| VM configuration | <ul style="list-style-type: none"> • Image: Custom imported image for the control plane • Network interface card type: gVNIC • Size: 8 vCPU, 64 GB RAM • Storage: 200 GiB <p>For storage planning, you should allocate approximately 1.1 GB of disk space for every one million files. You can estimate the total disk requirement by multiplying the expected number of files (in millions) by 1.1. For example, if you expect around 5 million files, the estimated disk space required for file metadata would be $5 \times 1.1 \text{ GB} = 5.5 \text{ GB}$.</p> <p>Additionally, you should allocate the following storage:</p> <ul style="list-style-type: none"> ◦ A extra 50 GB for Docker images, operating system storage, and other system level components ◦ Provision additional buffer space to accommodate future growth and operational overhead |
| Hyperscaler | <ul style="list-style-type: none"> • AWS: r7i.2xlarge instance • Azure VM size : Standard_E8ds_v5 • Google Cloud machine type : c3-highmem-8 |

2. Use the deployed Linux worker image to create the Linux worker VM to support NFS migration with the following recommended configuration:

| Description | Recommended setting |
|------------------|---|
| VM configuration | <ul style="list-style-type: none"> • Image: Custom imported image for the Linux worker • Network interface card type: gVNIC • Size: 4 vCPU, 16 GB RAM • Storage: 100 GB |
| Hyperscaler | <ul style="list-style-type: none"> • AWS: r7i.2xlarge • Azure VM size : Standard_E8ds_v5 • Google Cloud machine type : c3-highmem-8 |

3. Create a Windows worker VM to support SMB migrations using the Windows Worker Installer:

a. Create a Windows VM with the following recommended configuration settings:

- Image: Windows Server 2022 Base
- Architecture: 64bit
- Size: 16 vCPU, 64 GB RAM

- Network interface card type: gVNIC
 - Ensure Remote Desktop Protocol (RDP) (3389) is open
- b. Create a remote working session using RDP.

Learn about [RDP connections](#).

- c. Copy and run the Windows Worker Installer on the control plane VM.

What's next?

After learning about creating the control plane and worker VMs, you can do the following:

- Optionally [validate the control plane VM](#)
- [Access the NetApp Data Migrator UI and connect to the control plane and workers](#)

Optionally, validate the control plane VM deployment for NetApp Data Migrator

Optionally validate the control plane VM deployment for NetApp Data Migrator.

Steps

1. Use SSH to connect to your control plane server:

```
sudo su - datamigrator
```

2. Check the status of the boot service and logs:

```
sudo systemctl status boot-microk8s.service
```

Optionally, check the boot service logs:

```
tail -10f /opt/datamigrator/logs/ndm-first-boot.log
```

If the setup is complete, you see `Datamigrator Application Setup Complete` in the logs.

3. Verify that all the pods are up and running:

```
kubectl get pods -n datamigrator
```

What's next?

After learning about validating the control plane VM, you can [access the NetApp Data Migrator UI](#).

Access the NetApp Data Migrator UI

After you deploy the control plane VM and verify that the services and pods are running successfully, access the NetApp Data Migrator UI and connect to the control plane, Linux workers, and Windows workers.

Before you begin

Verify that you have the control plane VM private IP address, which you obtained when you [deployed the control plane VM](#). You use the control plane VM private IP address to access the UI.

Steps

1. Navigate to the control plane using a web browser:

```
https://<control-plane-private-ip-address>/
```

2. Use the default username and password to log in.
3. Based on your migration type, select one of the following tabs:

NFS: This option is for NFS migrations (Linux workers).

SMB: This option is for SMB migrations (Windows workers).

4. Follow the onscreen instructions to use the control plane to connect to the deployed worker VMs.

On the home page, select **View Instruction to Setup Worker**.

5. Check the status in the **Workers** section to verify that the worker is successfully connected.

After the workers are successfully connected, you can configure the NetApp Data Migrator environment and run migration jobs.

What's next?

After learning about accessing the NetApp Data Migrator UI, you can [configure NetApp Data Migrator](#).

Configure NetApp Data Migrator

After you install NetApp Data Migrator, you need to log in as an App Admin (administrator) using the default username and password.

Log in to NetApp Data Migrator

Log in to NetApp Data Migrator, then change your login credentials and create your first project.

Steps

1. Open a web browser and navigate to NetApp Data Migrator:

```
https://<private_IP_address>/
```

2. On the **Welcome** page, enter the default username in **Username/Email**.
3. Enter the default password in **Password**.

4. Select **Login**.

The **Reset Password** page opens.

5. Enter a new password that meets the following security requirements:

- Includes at least 8 characters
- Includes at least one uppercase letter
- Includes at least one lowercase letter
- Includes at least one number
- Includes at least one special character

6. Select **Reset Password**. The **Your Details** page opens.

7. Enter your **First Name**, **Last Name**, and **Email** address.

8. Select **Proceed**. The **Create a New Project** page opens.

9. Select **Create Project**, then enter the following details:

- **Project Name**: Enter a descriptive name for your project.
- **Project Description (Optional)**: You can provide additional details about your project.

10. Select **Create**.

The new project appears in the notification bar at the top of the NetApp Data Migrator control plane.

Log out of NetApp Data Migrator

After you log out of NetApp Data Migrator, you need to use your newly created credentials (email and password) the next time you log in.

Steps

1. Select the **User** icon (next to **Settings**).
2. Select **Logout**. The **Welcome** page opens.
3. In **Email** and **Password**, enter the email address and password that you registered when you [logged in](#).
4. Select **Login**.

What's next?

After learning about configuring NetApp Data Migrator, you can [use NetApp Data Migrator](#).

Upgrade the control plane and workers in NetApp Data Migrator

You can upgrade a control plane, Linux worker, or Windows worker in NetApp Data Migrator.

Before you begin

- Stop all job runs and make all jobs inactive.
- Download the upgrade bundle (tar.gz file) from the NetApp Support Site and save it in your local directory.

- Verify that the workers that are in use are online. Workers that are offline during an upgrade are not upgraded.

Step 1: Upload the upgrade bundle

Upload the upgrade bundle from your local directory.

Steps

1. Log in to the NetApp Data Migrator UI, then navigate to the home page.
2. Select the help icon in the top right corner.
3. Select the **Upgrade** tab.
4. Select **Select file**, then select the upgrade bundle tar.gz file.
5. Select **Upload** after selecting the file.

Wait for the message to appear that confirms that the upload and validation are complete.

6. Optionally, start the process again by selecting **Start Over** to upload a different file.

Step 2: Upgrade the control plane and workers

Upgrade the control plane followed by the Linux worker or Windows worker.

Steps

1. Select **Upgrade**. The system starts upgrading the control plane. This takes approximately five to ten minutes.

During the upgrade, the UI might become temporarily unavailable because the application is restarting with the new version. Log back in to the UI when it becomes accessible again.

2. After the upgrade completes, return to the **Upgrade** page.
3. Verify that the upgrade status is **Success**.
4. After a successful control plane upgrade, the worker upgrade starts automatically for all online workers.



The online workers automatically install and restart with the new version. Offline workers are not upgraded.

5. If a worker upgrade doesn't start automatically, use SSH to connect to the worker and start the upgrade:

Linux worker

```
sudo /opt/datamigrator/staging/<version>/upgrade.sh <version>
```

Windows worker

```
ExecutionPolicy Bypass -File  
C:\datamigrator\staging\<version>\upgrade.ps1 -Version <version>
```

Step 3: View logs and troubleshoot

View the virtual machine logs to support troubleshooting issues that you encounter during the upgrade.

Steps

1. Connect to the control plane VM using SSH and run the following command to view logs:

```
tail -f /upgrade/upgrade-<version>.log
```

2. Connect to the Linux worker or Windows worker VM using SSH and view the logs by using the following path:

Linux worker

```
/opt/datamigrator/upgrade.log
```

Windows worker

```
C:\datamigrator\upgrade.log
```

3. If the upgrade fails, the system automatically rolls back to the previous version and the UI shows the upgrade status as **Failed**.

Review the Ansible logs, then contact NetApp support and attach the Ansible logs to your communication.

Use NetApp Data Migrator

Create and manage projects in NetApp Data Migrator

You can use the Projects tab in the NetApp Data Migrator control plane to create, edit, or switch between projects.

Create a project

App Admin users can create a new project in NetApp Data Migrator and assign users with defined roles to that project.

Steps

1. Log in to NetApp Data Migrator.
2. Select **Settings** > **Projects** to view a list of existing projects.
3. Select **Add Project** and a new window appears.
4. Enter your **Project Name** and **Project Description (optional)**.
5. Add users to your project:
 - Select a **User** from the dropdown list.
 - Assign a **Role** to the user (**App Admin**, **Project Admin**, or **Project Viewer**).
 - Select **+Add**.
6. Select **Save and Confirm**.
7. Select **Submit** and a confirmation message appears, stating that the project has been successfully created.

Edit a project

You can quickly edit details about your project, if they need updating.

Steps

1. Select **Settings** in the top navigation bar.
2. Select the **Projects** tab to view a list of existing projects.
3. Select (;) next to the details of the project you want to edit, then select **Edit Project** from the dropdown menu.
4. Update the Project Name, Project Description, or add new users as required.
5. Select **Submit** to save the changes.

Switch between projects

If you are monitoring several projects at the same time, you can quickly switch between them.

Steps

1. Select the **Project** dropdown menu from the top navigation bar,
2. Select the current project name to open the **Project Selection** menu and a list of available projects appears.

3. Use the **Search Projects** bar to quickly find the project you want to switch to.
4. Select the checkbox next to the name of the project you want to switch to.
5. Select **Switch** to load the selected project.

Manage users

Add and manage users in NetApp Data Migrator

NetApp Data Migrator uses [Role-Based Access Control \(RBAC\)](#) to provide secure and efficient management of data migration activities. After setting up control and worker virtual machines (VMs), App Admin users can create and assign roles to new users. This allows new users to log in, view or manage projects, and perform other migration activities, depending on their permissions.

About this task

You need to be logged in as App Admin to add a new user, enable or disable an existing user, or reset a user password.

Add a new user

Create a new user and share the temporary password.

Steps

1. Log in to NetApp Data Migrator.
2. Select **Settings** > **Users** to view a list of registered users.
3. Select **Add User**.
4. Enter the **First Name**, **Last Name**, and **Email** address for the new user.
5. If the new user requires administrator permissions, select the **App Admin** checkbox.
6. Select **Submit**.
7. Select the **Copy** link (next to the password field) to copy the temporary password, which is displayed in a masked format.
8. Select **Close**.
9. Share the copied temporary password with the new user who can then use it to log in. At first login, they will be prompted to change their password.

Disable an existing user

Disable access to NetApp Data Migrator for other users. This prevents users from logging in but does not delete user data or previous migration jobs or logs associated with that user.

Steps

1. Select the **Settings** icon in the navigation bar.
2. Select the **Users** tab to view a list of registered users.
3. Select the (;) icon beside the details of the user who is being disabled, then select **Disable Access** from the dropdown menu.

The user status changes from **Active** to **Inactive** and they can't log in to NetApp Data Migrator.

Enable a user

Restore access to NetApp Data Migrator for a disabled user, allowing them to log in and perform actions based on their assigned permissions.

Steps

1. Select **Settings** icon in the navigation bar.
2. Select the **Users** tab to view a list of registered users.
3. Select the (:) icon beside the details of the user who is being enabled, then select **Enable Access** from the dropdown menu.

The user status changes from **Inactive** to **Active**. The user can now log in to NetApp Data Migrator.

Reset a user password

Reset the password for an existing user.



To reset the password for an App Admin user when there is no other App Admin available, contact ng-ndm-downloads@netapp.com to obtain the password reset script.

Steps

1. Select the **Settings** icon in the navigation bar.
2. Select the **Users** tab to view a list of registered users.
3. Select the (:) icon beside the details of the user whose password needs to be reset, then select **Reset Password** from the dropdown menu.

A message appears confirming that the password reset has been successful.

4. Select the **Copy** link (next to the password field) to copy the temporary password which is displayed in a masked format.
5. Share the copied temporary password with the user.

Manage access control for NetApp Data Migrator

NetApp Data Migrator uses role-based access control (RBAC) to manage user permissions. RBAC allows App Admin users (administrators) to assign any of the following three roles to other users, ensuring secure access control and efficient operations. App Admin users grant permissions to other users based on their responsibilities and access requirements.

- **App Admin:** This access level allows users to manage overall system settings, user roles, and access permissions.
- **Project Admin:** This access level allows users to manage specific migration projects, including job configuration and execution.
- **Project Viewer:** This access level provides users with read-only access to monitor migration progress, logs, and reports. This role is intended for users who need to monitor and observe the progress of data

migration projects but are not required to perform actions that could alter or interfere with a project.

The following table provides a summary of actions and user role permissions.

| Action | Description | App Admin | Project Admin | Project Viewer |
|----------------------|---|-----------|---------------|----------------|
| Agent deployment | User can access View Instruction To Setup Worker | Yes | Yes | No |
| Create a user | User can create new user accounts | Yes | No | No |
| List users | User can view a list of users | Yes | Yes | Yes |
| Manage configuration | User can manage configuration settings | Yes | Yes | No |
| Manage job | User can manage migration jobs | Yes | Yes | No |
| Reports | User can access options for downloading reports | Yes | Yes | Yes |
| Update project | User can edit a project | Yes | Yes | No |
| View a project | User can access the projects listing page | Yes | Yes | Yes |
| Create a project | User can create a project | Yes | No | No |
| Save SMTP | User can add or edit SMTP details | Yes | No | No |

Add and manage file servers

You can use NetApp Data Migrator to add, configure, and edit file servers that use the NFS or SMB protocols.

Add a new file server

Add a new NFS or SMB file server and configure the worker virtual machines.

Depending on your system configuration, use the Other NAS or Dell Isilon workflow option.

Other NAS

Steps

1. In the left navigation panel, select **Storage Servers**.
2. Select **File Servers > +Add**.

The **File Servers** page opens, followed by the **Server Type** page.

3. Enter the server name, then select **Server Type** as Other NAS.

The **Credentials** page opens.

4. Enter the **Host Name** (or IP address) of the NFS or SMB server.

5. If you are using an **NFS** file server:

- Enter a **Username** for accessing NFS file shares.
- Optionally, enter a **Password**.
- Select a **Protocol Version** for NFS.
- In the **Export Paths Retrieval Mechanism** panel select **Auto Discover** or **Manual Upload**:

Auto Discover automatically discovers export paths.

Manual Upload uploads export paths manually, or in environments where **Auto Discover** is not supported, such as the Google Cloud NetApp Volumes (GCNV) Flex service. After adding a file server, [you need to upload export paths manually](#).

6. If you are using an **SMB** file server:

- Enter a **Username** for accessing SMB file shares.
- Enter a **Password**.
- Select a **Protocol Version** for SMB.

7. Select the **Workers** tab.

- a. In the **Associated** column, select the toggle button next to each of the one or more workers you want to associate with a server.
- b. Select **Proceed** to initiate a pre-check operation that tests if the selected one or more workers have connectivity to NetApp Data Migrator.

8. When the pre-check is complete, you should resolve any errors that are flagged. (Refer to File Server Frequently Asked Questions (FAQ) for details on how to resolve errors).

If the pre-check completes without errors, select the **Job Config** tab, then select **Finish**. The name of your File Server appears under the list of **File Servers**.

The status of a file servers is listed in the **Status** column of the **File Servers** table. Status types include:

- **Active**: There are no errors, and all details have been validated.
- **In Progress**: Server validation is in progress.
- **Draft**: No workers have been associated with a file server.
- **Errored**: There are issues with permissions, no paths available, or only / is available as the export

path. These issues can occur if you select **Auto Discovery** for the export path during file server creation.

Dell Isilon

Steps

1. In the left navigation panel, select **Storage Servers**.
2. Select **File Servers > +Add**.

The **File Servers** page opens, followed by the **Server Type** page.

3. Enter a **Configuration Name** for your Isilon file server.
4. Select **Dell Isilon** from the **Server Type** dropdown.

The **Management Console** section opens:

5. Enter the **Management Host** (host name or IP address of the Isilon management console).
6. Enter the **Username** for accessing the Isilon management API.
7. Enter the **Password**.
8. Select **Proceed** to fetch the TLS certificate from the Isilon cluster.
9. Review the **TLS Certificate** details displayed in the modal:
 - a. Verify the certificate issuer, validity dates, and fingerprint.
 - b. Select **Accept** to trust the certificate and proceed.
 - c. Select **Reject** to cancel if you don't trust the certificate.
10. The **Zone Credentials** page opens:
 - a. Select one or more **Access Zones** from the available zones discovered.
 - b. For each selected zone, configure the protocol credentials:
 - a. Select the **NFS IP Address** from the dropdown.
 - b. Enter a **Username** for accessing NFS export paths.
 - c. Enter the **SMB IP Address**.
 - d. Enter a **Username** for accessing SMB file shares.
 - e. Enter a **Password**.



If a SmartConnect Service IP (SSIP) is configured on the Isilon cluster, you can select the SmartConnect zone domain name from the IP Address drop-down list. When using an SSIP-enabled domain name, the Isilon SmartConnect infrastructure manages connection load balancing and resolves it at the storage layer. NetApp Data Migrator does not perform additional load balancing in this configuration.

11. The **Workers** tab opens :

- a. For each zone and protocol combination, assign workers:

In the **Associated** column, select the toggle button next to each of the one or more workers you want to associate.

- b. Select **Proceed** to initiate a pre-check operation that tests if the one or more selected workers have connectivity to NetApp Data Migrator and the Isilon file server.

12. When the pre-check is complete, resolve any errors that are flagged.

If the pre-check completes without errors, the name of your file server appears under the list of file servers. The dropdown for the file servers displayed shows the zones configured.

Manually upload export and directory paths

NetApp Data Migrator allows you to manually upload export paths and directory paths for use in data migration operations for the NFS protocol. This feature is useful in environments where automatic NFS export path detection is unavailable. For example, for use with the GCNV Flex service or when migrating directory paths instead of the entire export path. If you select **Manual Upload** in the **Export Paths Retrieval Mechanism** panel, you need to download and complete the template file provided by NetApp Data Migrator after you finish creating a file server.



Use this option when you need to configure migration at the directory level. In cases where migration involves specific directories rather than entire exports, enter the directory paths directly into the Excel spreadsheet. This ensures that the migration workflow processes each directory individually, without requiring export level inputs.

Steps

1. In the left navigation panel, select **Storage Servers**.
2. Select **File Servers**.
3. Select **Click here to Upload Export Paths**.
4. Select **Download Template** to download a CSV file template.
5. Save your export paths and directory paths in the CSV file.
6. Select **Click here to Upload Export Paths**, then select the CSV file containing your export paths and directory paths.

The export paths and directory paths appear under **Paths**.

7. If you need to include more export paths or directory paths, add them to your file, then select **Re-Upload Export Paths**.

When upload is complete, export paths and directory paths can have one of the following status types:

- **Valid:** The path uploaded successfully and you can mount and unmount this path.
- **Invalid:** The path failed to upload.
- **Disabled:** The path is available, but not in the file you uploaded.

Edit file server details

If required, you can make changes to a previously configured file server.

Edit the file server details using the Other NAS or Dell Isilon workflow option.

Other NAS

Steps

1. Select the action menu beside the File Server you want to edit.
2. Select **Edit File Server**. If you selected the **Manual Upload** option for **Upload Export Path Retrieval**, only valid paths are displayed.
3. Select the **Server Type** tab, make your required edits, then select **Proceed**.
4. Select the **Credentials** tab, make any required edits, then select **Proceed**.
5. Select the **Workers** tab, make any required edits, then select **Submit**.

Dell Isilon

Steps

1. Select the action menu beside the Parent File Server you want to edit.
2. Select **Edit File Server**.
3. Select the **Server Type** tab:
 - a. Update the **Configuration Name** if needed.
 - b. Update **Username** or **Password** if needed.
 - c. Select **Proceed**.



You cannot change the **Server Type** (Dell Isilon) and **Management Host**.

4. Select the **Zone Credentials** tab:
 - a. Add new zones by selecting additional zones from the available list.
 - b. Update the protocol credentials for each zone:

Update the **NFS IP Address**, **Username**, or **Password** as needed.

Update the **SMB IP Address**, **Username**, or **Password** as needed.
 - c. Select **Proceed**.
5. Select the **Workers** tab:
 - a. Update worker assignments for each zone and protocol by toggling the workers on or off in the **Associated** column.
 - b. Select **Proceed** to run the pre-check validation on any newly assigned workers.
6. Select the **Job Config** tab:
 - a. Update the **Working Directory** if needed.
 - b. Select **Finish**.

Configure real-time notifications for NetApp Data Migrator

You can configure NetApp Data Migrator to email you real-time alerts about changes to the status of your projects.

Before you begin

Verify that you are logged in as an **App Admin** user. This user level is required to configure SMTP email server details.

Steps

1. Select **Settings** in the navigation bar.
2. Select the **SMTP** tab and complete the fields shown in the following table.

| Field | Description |
|------------|--------------------------------------|
| IP Address | SMTP server address |
| Port | SMTP port |
| Username | Server authentication username |
| Password | Server authentication password |
| From Email | Sender address for all notifications |
| To Email | Recipient address(es) for alerts |



After configuring SMTP, users are required to re-enter the password when editing SMTP settings.

Manage migration options

Plan data migration in NetApp Data Migrator using Bulk Discover

Configure Bulk Discover in NetApp Data Migrator to quickly generate an overview of your entire existing storage capacity before you begin migrating your data. Having a clear understanding of your stored files and system structures can help to streamline the data migration process.

Steps

1. Log in to NetApp Data Migrator.
2. Select **Storage Servers > File Servers** to view a list of available file servers.
3. Select the name of the server on which you want to perform a bulk discovery then, select **Bulk Discover**.
4. Select **Job Schedule**, then select one of the following options:
 - **Start Now** if you want the discovery to begin immediately.
 - **Schedule date and time (UTC)** if you want to schedule the discovery process. Enter the date and time when you want the job to start.
5. Choose one of the following options for **Scan Alternate Data Streams**:
 - Select **Yes** if you want NetApp Data Migrator to discover the Alternate Data Streams (ADS) associated with your files.

- Select **No** if you don't want NetApp Data Migrator to discover the ADS associated with your files.
6. In the **Excluded Path Patterns** text box, enter paths that you want to exclude from the discovery process. You should enter each path on a new line.
 7. Use the **Search bar** to find specific export paths (within the listed paths) that you want to include in the discovery process, then select the checkbox next to the **Export Path(s)**.

Export paths that are no longer reachable are disabled and cannot be used in the discovery process. For example, export paths that have been deleted or no longer appear in the output of `showmount -e` for NFS or paths which are not returned during SMB share enumeration are disabled.

8. Select **Submit** and a notification message appears confirming that the **Bulk Discover Job** has been created. Select the **View Job Listing** link in this message to view the **Job Config List** page, where your newly created job is listed in the **Job Listings** table.

Perform data migration using NetApp Data Migrator

Use the Bulk Migrate features in NetApp Data Migrator to transfer large volumes of data from a source to a destination location.

Step 1: Configure Bulk Migrate in NetApp Data Migrator

You need to define the servers for Bulk Migrate before you can use the Bulk Migrate features.

Steps

1. Log in to NetApp Data Migrator.
2. Select **Storage Servers > File Servers**.
3. Select the **File Server Name** for which you want to create the job.
4. Select **Bulk Migrate**.

Step 2: Add source and destination mappings

Add source and destination mappings to specify the source export paths and destination export paths for your migration.

Steps

1. Select the export path in the source that you want to migrate.
2. Optionally, select **Add Source Directory** if you want to perform a directory level migration.

After you select **Add Source Directory**, the directory explorer view appears. This view shows the list of directories at the root level. You can either navigate to the required directory or directly copy and paste the path of the required directory into the search bar of the explorer window to navigate to that folder.

3. After you select the source directory, select the destination file server and destination export path.
4. Optionally, select the directory in the destination export path.

If you don't select a directory in the destination export path, the migration takes place at the root level of the selected export path.

5. After you select the source and destination paths, select **Add Mapping** to add the selected mapping. You can create multiple mappings for different export paths and directories.

NetApp Data Migrator prevents you from selecting a mapping which has a parent or child connection with an existing mapping. This avoids conflicts during the migration.

6. Optionally, delete or edit a mapping by selecting the **Edit** or **Delete** option.
7. After you add the mappings, select **Proceed**.

Step 3: Customize the Bulk Migrate job

You can select various settings from the **Options** page to customize your Bulk Migrate job, according to your needs.

| Option | Description |
|-------------------------------|--|
| Excluded Path Patterns | <p>Defines the specific file paths or directories to be excluded from processing. This helps to optimize storage and performance by skipping unnecessary files.</p> <ul style="list-style-type: none"> • You can enter multiple path patterns, one per line. • You can enter a wildcard (*) to match multiple files or folders. • Example exclusions: <ul style="list-style-type: none"> ◦ /snapshots/: Excludes all files and folders inside any snapshots directory ◦ /logs/: Excludes log files ◦ /tmp/: Excludes temporary files |
| Incremental Sync Schedule | <p>Configures how often data syncs incrementally. This ensures that only the changes since the last sync are updated, which improves migration efficiency and reduces processing time.</p> <ul style="list-style-type: none"> • Select Off to disable incremental sync. • Select Set Schedule to specify a sync schedule. You can choose to sync data hourly, daily, or weekly. • Select Cron Expression if you are an advanced user and want to define a custom sync schedule using a cron expression, for more granular control over sync timing. |
| Migrate File | <p>Selects the files to migrate based on their last modified time.</p> <ul style="list-style-type: none"> • Select All to migrate all files, regardless of their modification date. • Select Exclude file older than (UTC) to exclude files older than a specified date. |
| Preserve a-time (Access Time) | <p>Retains the original file access timestamp, instead of updating it to the migration time.</p> |

| Option | Description |
|-----------------------------|---|
| Preserve permissions | <p>Retains the original source file and directory permissions on a destination.</p> <ul style="list-style-type: none"> • Select Enabled to preserve the original permissions, including owner, group, and access rights (access control lists for SMB, mode bits for NFS) from a source to a destination. • Select Disabled to skip permission preservation. NetApp Data Migrator migrates files with default destination permissions, which is useful when migrating between incompatible file systems. |
| Skip Files modified in last | <p>Specifies files from a time window (in minutes, hours, or days) to exclude from your migration. This helps prevent data inconsistency by ensuring that actively edited files are not transferred mid-update.</p> |
| Upload GID / UID mapping | <p>Uploads a Group ID (GID) or User ID (UID) mapping file to maintain correct file ownership during migration. The uploaded file must follow the format specified in the template provided.</p> <ol style="list-style-type: none"> 1. Select Download Template to download a sample file format. 2. Select Choose a file to select the mapping file from your local system. 3. Select Upload to apply the mapping. |
| Upload SID mapping | <p>Uploads a Security Identifier (SID) mapping file. SID mapping ensures that user and group permissions are retained accurately when migrating or syncing files between systems. The uploaded file must follow the format specified in the template provided for you to download.</p> <ol style="list-style-type: none"> 1. Select Download Template to download a sample file format. 2. Select Choose a file to select the mapping file from your local system. 3. Select Upload to apply the mapping. |

After selecting your options, select **Proceed** to open the **Review and Submit** page.

Step 4: Review and submit

Verify your settings, then proceed with a bulk migration job.

Steps

1. View the **Precheck Status** of your job. Ensure that the source path contains the correct data and confirm that the destination path has sufficient storage and access permissions.
2. Select **Submit** to create a new migration job.

The **Bulk Migrate job has been created** confirmation message appears.

3. Select the **View Job Listing** link next to the notification message to open the **Job Config List** page where your new job is listed.

Configure Bulk Cutover in NetApp Data Migrator

Use Bulk Cutover in NetApp Data Migrator to perform the final sync between your source and destination systems. When baseline migrations are complete and incremental syncs are running, you can merge multiple paths into one cutover job.

Start a Cutover Job

Follow these steps to start a cutover job.

Steps

1. Log in to NetApp Data Migrator.
2. Select **Storage Servers > File Servers**.
3. Select the name of the file server for which you want to create a Cutover Job.
4. Select **Bulk Cutover**.
5. On the **Select Path** page, select the checkbox next to **Source Path**.
6. Select the checkbox next to the source path (confirming the cutover job).
7. Select **Proceed**.
8. Select the checkbox next to a job name to confirm that you are starting a **Bulk Cutover** job.



You can select a job when a Bulk Migrate job is running in parallel.

9. Select **Submit** to start your Bulk Cutover job.

The **Cutover job has been created** confirmation message appears.

10. You can select the **View Job Listing** link next to this message to open the Job Config List page where your new job is listed.

Approve a Bulk Cutover job

Follow these steps to approve a cutover job.

Steps

1. On the **Jobs** page, select the **Job Run List** tab.
2. Select the action menu next to your Cutover job.
3. Select **Review**.

The **Cutover Confirmation** pop-up box appears.

4. Select the **Download CoC Report** link.

Review the report to verify if the cutover was successful and if all data has successfully migrated from source to destination.

5. Select the checkbox next to **I have reviewed and verified the Chain of Custody (CoC) document and all other essential information**.
6. If you are satisfied with the information in the Chain of Custody (CoC) report, select **Confirm** to approve the **Bulk Cutover**.

The status changes to **Complete**.

Resolve metadata update conflicts

Metadata update conflicts might arise during the cutover confirmation process for SMB migrations. To resolve the metadata update conflicts, run the metadata synchronization script for the impacted files.

Steps

1. Download the CoC report ZIP folder that was generated as part of the cutover process.
2. Extract the ZIP folder on the Windows worker machine that was involved in the cutover for the path pair.



The drive letters **S** and **T** are used to map the source and target volumes on the Windows worker. Do not use these drive letters for any other mounts when running this script.

3. Copy the required `metadata_conflict_errors.csv` file.
4. Open PowerShell as an administrator on the Windows worker machine.
5. Navigate to scripts directory:

```
cd C:\datamigrator\scripts
```

6. Run the metadata stamping script using placeholders for all parameters:

```
.\stamp-metadata.ps1 `
-SourceHost "<SourceFileServer_FQDN_or_IP>" `
-SourceShare "<Source_ShareName_Only (e.g., data)>" `
-DestHost "<DestinationFileServer_FQDN_or_IP>" `
-DestShare "<Destination_ShareName_Only>" `
-SourceUsername "<DOMAIN User_With_Read_Access_To_Source>" `
-SourcePassword "<Password_For_Source_User>" `
-DestUsername "<DOMAIN User_With_Write_Access_To_Destination>" `
-DestPassword "<Password_For_Destination_User>" `
-InputFile "<Full_Path_To_File_List_CSV (e.g., C:\Migration\files.csv)>" `
-SidMapFile "<Full_Path_To_SID_Mapping_CSV (OldSID_to_NewSID)>" `
-Domain "<ActiveDirectory_Domain (e.g., company.com_or_COMPANY)>"
```

The SID mapping and domain-related parameters (`SidMapFile` and `Domain`) are optional and can be included as needed.

Manage jobs and job runs in NetApp Data Migrator

Use job management features in NetApp Data Migrator to initiate and track your **Discovery**, **Migration**, and **Cutover** jobs and job runs.



Do not run Migration and Cutover jobs simultaneously. Ensure that only one job is active at a time.

View Job Config List

The **Job Config List** page provides a comprehensive overview of all migration related jobs. Use this page to monitor and manage the status and progress of **Discovery**, **Migration**, and **Cutover** jobs.

Steps

1. Log in to NetApp Data Migrator.
2. Select **Jobs > Job Config List**.

The **Jobs Listings** table appears, which includes the following information:

- **Source:** The location of source file server.
- **Destination:** The destination file server and export path details for Migration jobs.
- **Protocol:** The protocol used by the job (NFS or SMB).
- **Next Schedule:** The next scheduled execution time (if applicable).
- **Runs:** The number of times the job has been executed.
- **Type:** The job type (Discovery, Migration, or Cutover).
- **Status:** The current state of a job can be either Active or Inactive. Jobs that use manual export paths with an invalid or disabled status automatically become inactive. Refer to [Add and manage file servers](#) for more details.
- **Updated On:** Job update timestamp.

Jobs that use manual export paths or the export paths file are later re-uploaded. Any previously run jobs associated with a now invalid or disabled path automatically become inactive.

3. Select **Filters** to sort the jobs in the Jobs Listings table. You can choose a combination of filters based on the following options:
 - Source
 - Destination
 - Protocol
 - Type
 - Status
4. Select **Clear all** to remove filters already applied to your job listings.

Activate or deactivate a Job

From the Job Listings table, you can activate or deactivate a job.

Steps

1. Activate a job:
 - a. Select **Jobs > Job Config List**.
 - b. In the Job Listings table, select the action menu next to the job you want to activate.

- c. Select **Activate**. The job status changes to Active.
2. Deactivate a job:
 - a. Select **Jobs > Job Config List**.
 - b. In the Job Listings table, select the action menu next to the job you want to deactivate.
 - c. Select **Deactivate**. The job status changes to Inactive, and execution stops until you reactivate the job.

Edit job configurations

Steps

1. Select **Jobs > Job Config List**.
2. [Open the Job Details page](#) for the job you want to edit.
3. Select **View/Edit Configuration**.
4. Edit the job configuration:

Discovery Job

- Add or remove Excluded Path Patterns
- Schedule a job run

Migration Job

- Edit any job option
- Add or remove mappings
- Schedule a job run

5. Select **Save**. The new configuration affects future job runs.



Changing the configuration, for example, disabling preserve permissions, after baseline migration is completed might result in an inconsistent state during subsequent migrations. Instead of changing the configuration, you should delete the current job and start a new job.

Re-run errored files and directories

If a migration job run completes with errors due to transient issues such as network timeouts or permission problems, you can use the retry feature to re-process only the failed items without re-running the entire migration.

Steps

1. Select **Jobs > Job Config List**.
2. In the **Job Listings** table, select the action menu next to the job that has failed items.
3. Select **Details > Retry Recent Errors > Proceed with Retry** to start the retry operation.

Delete a Job

Steps

1. Select **Jobs > Job Config List**.

2. In the **Job Listings** table, select the action menu next to the job you want to delete.
3. Select **Delete > Delete**.



You can only delete a job if there is no active run.

View Job Details

From the **Job Config List** page, you can access the **Job Details** page to view additional details about individual jobs, such as:

- Job type (Discovery, Migration, or Cutover)
- Number of files and directories discovered
- Time elapsed
- Data discovered
- Job configuration

Steps

1. Select **Jobs > Job Config List**.
2. In the **Job Listings** table, select the action menu next to a job, then select **Details**.

View Job Run History

On the **Job Details** page, the **Run History** table provides you with the information about previous job runs and the job status.

The migration and discovery job status types include:

- **Ready:** A job is scheduled to run.
- **Running:** A job is in the running state.
- **Paused:** A job run has been paused manually or by NetApp Data Migrator. For example, a job can have a paused status if a worker goes down while the job is running.
- **Completed:** A job is complete.
- **Errored:** A job run triggers a fatal error.
- **Failed:** If a worker goes offline while a job is running, the job might enter a failed state.

The cutover job status types include:

- **Blocked:** The job is waiting for a user response.
- **Rejected:** The job has been reviewed and rejected by a user.
- **Approved:** The job has been reviewed and approved by a user.
- **Stopped:** The job has stopped running.

Manage Job Run operations

From the **Job Details** page, you can manage **Start**, **Stop**, **Pause**, and **Resume** operations for a job. Use the **Pause** feature to temporarily halt a running job, without canceling it. Then you can resume the job from the

point where it was paused. This is a useful feature in scenarios where you need to free up system resources or troubleshoot issues without losing progress.

Steps

1. On the **Job Details** page, in the **Run History** table, select the action menu next to a running job.
2. Pause or resume a job run:
 - a. Select **Pause**.
 - b. To Resume the job run, select **Resume**.

The job status changes to **Running** and the job continues to run from the step where it was paused.

3. Stop or start a job run:

You can use the stop option to permanently terminate a job run that is in progress. This action is useful when a job run is no longer required. You cannot resume a job run that is stopped but you have the option to start a new job run from the beginning.

- a. Select **Stop**.

The job run status changes to **Stopped**.

- b. To start a new job run, select **Adhoc Run**.

The job run status changes to **Running**.

Access Job Run Details

From the **Run History** table, access the **Job Run Details** page where you can view additional details about your job runs.

Steps

1. On the **Job Details** page, in the **Run History** table, select the action menu next to a job run.
2. Select **Details** to view the **Job Run Details** page, which includes the following information:
 - **Discovery/Migration**: The job run type and status.
 - **Files**: The number of files found during the discovery process.
 - **Directories**: The number of directories found during the discovery process.
 - **Elapsed Time**: How long the discovery process took.
 - **Data Discovered**: The total size of discovered files.
 - **Workers**: The number of workers assigned to the job.
 - **Tasks**: The number of tasks being executed.
 - **Task Status Indicators**:
 - **Pending**: The number of Tasks waiting to be executed.
 - **Running**: The number of Tasks currently in progress.
 - **Completed**: The number of tasks that have successfully completed.
 - **Errored**: The number of tasks that encountered issues during execution.
 - **Job Name**: The name assigned to the job.

- **Source Path:** The path to the file being used for data discovery.
- **Protocol:** The protocol being used for discovery (NFS or SMB).

The lower right tile on the **Job Run Details** page lists the number of errors that occurred during migration (if any). Select **View All** to access the **Errors** page, where you can find more detailed information about these errors.

3. Generate detailed reports that provide you with insights into job execution metrics including file counts, status, errors, and execution time. You can use these reports for review or auditing purposes.
 - Select **Discovery Report > Preview** to view a histogram of job report data.
 - Select **Download as CSV** to export a report in CSV format, which you can analyze using a spreadsheet application.
 - Select **Download as PDF** . This option is ideal for document sharing.
 - Select **View Logs** to view or download the log files using Grafana.

View Migration Activity

The Migration Activity page shows the ten oldest files currently being migrated. It also shows the total number of files in progress and provides an option to download a CSV file containing a complete list of these files.

Steps

1. From the **Run History** table, select **Job Run Details** for a running job.
2. Select **Migration Activity**.

Generate a job error report

You can generate an error report for jobs with an **Errored** status or for a previous job run. An error report can help you to understand why an error occurred.

Steps

1. Generate an error report for jobs with an **Errored** status:
 - a. On the **Job Details** page, in the Errors pane, select **View All**.
 - b. Select **Generate Error Report** to download details about errors in the latest job run.
2. Generate an error report for a previous job run:
 - a. On the **Job Details** page, in the **Run History** table, select the action menu next to the job run for which you want to generate an error report.
 - b. Select **Details**.
 - c. On the **Job Details** page, in the **Errors** panel, select **View All**.
 - d. Select **Generate Error Report** to download details about errors in the job run you selected.

Generate a NetApp Data Migrator support bundle

NetApp Data Migrator allows you to generate a support bundle to help troubleshoot any issues you experience. This bundle contains diagnostic information such as log files, error reports, and configuration data.

Steps

1. Log in to NetApp Data Migrator.
2. Select **Help** in the navigation bar then select the Support Bundle option.
3. Select **Date**. Enter the date range that you want to include in the support bundle.
4. Select **Other Metrics**. Enter the other metrics that you want to include in the support bundle.
5. Select **Generate Support Bundle**. When the bundle is ready, **Download Report** becomes active.
6. Select **Download Report**.

FAQ for NetApp Data Migrator

If you experience an issue while using NetApp Data Migrator, you might be able to resolve it quickly by reviewing these frequently asked questions (FAQ) by other users.

What can cause NT_STATUS_IO_TIMEOUT / NT_STATUS_ACCESS_DENIED / NT_STATUS_HOST_UNREACHABLE / NT_STATUS_UNSUCCESSFUL errors?

This error can occur if you enter incorrect host information. Ensure that the server hostname or IP address is correct and that the server is reachable. Verify your network connectivity and that your DNS can be resolved, if required.

What can cause a Wrong credentials - NT_STATUS_LOGON_FAILURE error?

Incorrect username or password entries can cause authentication and login failures. Ensure you have entered correct login details.

What does Unsupported protocol versions of NFS or SMB mean?

This means that the protocol version used by the file server is not supported. Check the compatibility of the protocol versions and upgrade or configure the file server as necessary.

What can cause an 'Invalid export path' error?

Ensure that the export path is correctly entered and exists on the server.

What can cause an 'Invalid working directory' error?

Check that you have entered correct working directory for the selected export path.

Why do I get a 'write permission' error on the working directory?

This error occurs when the correct export path and working directory are specified, but the necessary write permissions are not granted. Without the correct write access, the file server pre-check will fail, and the user will not be able to run jobs. Check that the user experiencing the error has the required write access.

Get help

Register for NetApp Data Migrator support

Register your NetApp Data Migrator product to access NetApp Support.

Steps

1. On the NetApp Data Migrator home page, select **Help (?) > About > Serial Number**
2. In the **About NDM** dialog box, record the NetApp Data Migrator instance ID.

This is a 20-digit number, starting with 975.

3. Go to the [NetApp Support Site registration page](#).
4. Select **I am not a registered NetApp Customer**.
5. Fill in the required product registration details:
 - a. Leave the **NetApp Reference SN** field blank.
 - b. From the Product Line dropdown, select **NDM**.
 - c. From the Billing Provider dropdown, select **NetApp**.



There is no billing for this product.

- d. Enter the 20-digit NetApp Data Migrator instance ID in the **NDM Serial #** field.
 - e. Complete the remaining required fields, then select **Submit**.
6. After submission, you receive a registration confirmation email. Follow the instructions in the email to confirm the registration.

Troubleshoot NetApp Data Migrator

If you experience issues while using NetApp Data Migrator, these troubleshooting steps and reference commands might be useful.

SMB mount failure when using host name

When configuring a directory level migration, the SMB mount might fail if the SMB file server host name is provided as a URL. This can occur when the control plane virtual machine (VM) does not have the correct DNS configuration to resolve the SMB file server host name. The mount failure might appear with an error similar to `mount failed: Resource temporarily unavailable`.

You can work around this issue by using the IP address of the SMB file server instead of the host name in the migration configuration.

Steps

1. Resolve the hostname to an IP address:

```
nslookup
```

2. Configure the SMB file server host name field using the resolved IP address.
3. Retry the directory level migration configuration.

After switching to the IP address, the mount operation should succeed.

Troubleshoot application access

All credentials are managed in OpenBao.

In the following steps, replace `<IP_ADDRESS>` with the IP address of your virtual machine (VM).

Steps

1. Fetch the OpenBao root token. Use SSH to connect to the control plane server from Bastion connect from the Azure portal:

```
sudo su - datamigrator
cat /opt/datamigrator/openbao/cluster-keys.json
```

2. Log in to the OpenBao UI: Use https://IP_ADDRESS/ui/ and enter the root token for login.
3. Navigate to secrets.
4. Keycloak UI: https://IP_ADDRESS/keycloak/
5. NetApp Data Migrator UI: https://IP_ADDRESS/

Log in to the NetApp Data Migrator UI using the default username and password.

6. Temporal UI: https://IP_ADDRESS/temporal/ui/
7. Postgres connection: Use the multipass IP address to connect to Postgres database. Get the username and password from OpenBao.

Keys: `POSTGRES_DMADMIN_USER` and `POSTGRES_DMADMIN_PASSWORD`

Use the "kubectl" reference commands

- To get the pods in datamigrator namespace:

```
kubectl get pods -n datamigrator
```

- To get the logs for a pod in datamigrator namespace:

```
kubectl logs <podname> -n datamigrator
```

- To describe a pod in datamigrator namespace:

```
kubectl describe <podname> -n datamigrator
```

- To get all namespaces:

```
kubectl get ns
```

- To get the pods in any namespace:

```
kubectl get pods -n <NAMESPACE>
```

Unseal OpenBao

If you encounter an issue where OpenBao is sealed, follow these steps to unseal.

Steps

1. Use SSH to connect to the control plane server using Bastion connect.
2. replace OPENBAO_UNSEAL_KEY with your key:

```
sudo su - datamigrator
export OPENBAO_UNSEAL_KEY=`jq -r ".unseal_keys_b64[]"
/opt/datamigrator/openbao/cluster-keys.json`
kubectl exec openbao-0 -n openbao -- bao operator unseal
$OPENBAO_UNSEAL_KEY
kubectl exec openbao-1 -n openbao -- bao operator unseal
$OPENBAO_UNSEAL_KEY
kubectl exec openbao-2 -n openbao -- bao operator unseal
$OPENBAO_UNSEAL_KEY
```

Troubleshoot Azure VM access

You should be able to successfully create and connect to your Azure VM. However, if you experience problems, try restarting your virtual machine or reset your SSH configuration.

Restart your virtual machine

Steps

1. Navigate to your Azure Portal.
2. Navigate to your VM and select **Restart**.

Reset SSH configuration

First refer to the instructions provided in this [Microsoft troubleshooting reference](#). However, sometimes issues can occur when opening the SSH Bastion portal, which you might be able to resolve in the following way.

Steps

1. Navigate to your Azure VM control plane.
2. Select **Help**.
3. Select **Reset password**.
4. From Mode, select **Add SSH Public Key**.
5. For the username, Enter ubuntu.
6. For the public key source, choose **Use existing key stored in Azure**.
7. For the Stored Key, choose **Select your existing created key**.
8. Select **Update**.

Windows worker fails to switch user on SMB file server

When a Windows worker attempts to connect to an SMB file server using a different set of credentials than those previously used for the same file server, the following error message might appear:

```
System error 1219: Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed.
```

This happens because Windows does not allow multiple simultaneous connections to the same network resource using different credentials. Even if the previous connection is inactive, it might still be cached or held by the system.

Follow these steps to resolve this issue:

1. List existing SMB connections:

```
net use
```

2. Delete any existing connection to the target server:

```
net use <share> /delete
```

3. Reboot to clear any remaining cached credentials or sessions.
4. Reconnect using your desired credentials.

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

<https://www.netapp.com/company/legal/copyright/>

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<https://www.netapp.com/company/legal/trademarks/>

Patents

A current list of NetApp owned patents can be found at:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Privacy policy

<https://www.netapp.com/company/legal/privacy-policy/>

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

[Notice for NetApp Data Migrator](#)

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.