Migrate volumes to Azure NetApp Files

09/09/2025

With Azure NetApp Files' migration assistant, you can peer and migrate volumes from on-premises ONTAP or Cloud Volumes ONTAP to Azure NetApp Files. The feature is currently only available with the REST API.

Requirements

- In ONTAP or Cloud Volumes ONTAP, you must be running ONTAP 9.10.0 or later.
- SnapMirror license entitlement needs to be obtained and applied to the on-premises ONTAP or Cloud Volumes ONTAP cluster. Work with your account team to involve an Azure Technology Specialist in applying the license to the on-premises storage cluster.
- Snapshot locking must be turned off for volumes in the source cluster. If snapshot locking is enabled, you receive a `Last transfer error`. To disable snapshot locking, see ONTAP documentation .
- Ensure your network topology is supported for Azure NetApp Files. Ensure you have established connectivity from your on-premises storage to Azure NetApp Files.
- The delegated subnet address space for hosting the Azure NetApp Files volumes must have at least seven free IP addresses: six for cluster peering and one for data access to the migration volumes.
- The delegated subnet address space should be sized appropriately to accommodate more Azure NetApp Files network interfaces. Review Guidelines for Azure NetApp Files network planning to ensure you meet the requirements for delegated subnet sizing.
- With the migration assistant, Azure NetApp Files volumes must be using Standard networking features. For more information about setting network features, see Configure network features.
- After issuing the peering request, the request must be accepted within 60 minutes of making the request. Peer requests expire if not accepted within 60 minutes.
- You should complete migrations from a single source cluster using one Azure subscription before migrating volumes destined for another subscription. Cluster peering fails when using a second Azure subscription and the same external source clusters.
- If you use Azure RBAC to separate the role of Azure NetApp Files storage management with the intention of separating volume management tasks where volumes reside on the same network sibling set, be aware that externally connected ONTAP systems peered to that sibling set don't adhere to these Azure-defined roles. The external storage administrator

might have limited visibility to all volumes in the sibling set showing storage level metadata details.

- When creating each migration volume, the Azure NetApp Files volume placement algorithm attempts to reuse the same Azure NetApp Files storage system as any previously created volumes in the subscription to reduce the number of network interface cards (NICs) or IPs consumed in the delegated subnet. If this isn't possible, an additional seven NICs are consumed.
- You should ensure that there are no external FlexGroup volumes as they cannot be migrated to Azure NetApp Files large volumes.
- When the migration is in progress, don't enable features such as backup. Only enable features once the migration has completed.

> **Tip**
>
> For help creating a migration volume and peering clusters for the migration assistant, see the PowerShell migration assistant workflow sample script .

Register the feature

You need to register the feature before using it for the migration assistant for the first time. After registration, the feature is enabled and works in the background.

1. Register the feature:

   Azure PowerShell

   ```
   Register-AzProviderFeature -ProviderNamespace Microsoft.NetApp -FeatureName ANFMigrationAssistant
   ```

2. Check the status of the feature registration:

   > **Note**
   >
   > The **RegistrationState** may be in the `Registering` state for up to 60 minutes before changing to `Registered`. Wait until the status is **Registered** before continuing.

   Azure PowerShell

```
Get-AzProviderFeature -ProviderNamespace Microsoft.NetApp -FeatureName
ANFMigrationAssistant
```

You can also use Azure CLI commands `az feature register` and `az feature show` to register the feature and display the registration status.

Before you begin

You must create Express Route or VPN resources to ensure network connectivity from the external NetApp ONTAP cluster to the target Azure NetApp Files cluster. There are multiple ways to ensure network connectivity. Connectivity includes this set of firewall rules (bidirectional for all):

- ICMP
- TCP 11104
- TCP 11105
- HTTPS

The network connectivity must be in place for all intercluster (IC) LIFs on the source cluster to all IC LIFs on the Azure NetApp Files endpoint.

> **Note**
>
> The migration assistant copies all volume contents including directories, files, file metadata (for example owner, creation date, modified date), and existing snapshots. You are responsible for ensuring that the Azure NetApp Files target volume is configured with LDAP or Active Directory.

Migrate volumes

1. Authenticate with Azure Active Directory to retrieve an OAuth token. This token is used for subsequent API calls.

2. Create a migration API request to create Azure NetApp Files volumes for each on-premises volume you intend to migrate.

   > **Important**

> Ensure the size and other volume properties on the target volumes match with the source.
>
> You should create the Azure NetApp Files volume with 20% or more quota than the source volume. Azure NetApp Files volumes use raw capacity size. The source volume might be smaller due to deduplication and compression. You can shrink Azure NetApp Files nondisruptively after the migration to prevent over-provisioning.

The "remote path" values are the host, server, and volume names of your on-premises storage.

rest

```
PUT: https://<region>.management.azure.com/subscriptions/<subscription-
ID>/resourceGroups/<resource-group-name>/providers/Microsoft.NetApp/net-
AppAccounts/<account-name>/capacityPools/<capacity-pool-
name>/volumes/Migvolfinal?api-version=2025-06-01
Body: {
   "type":"Microsoft.NetApp/netAppAccounts/capacityPools/volumes",
   "location":"<LOCATION>",
   "properties":{
      "volumeType":"Migration",
      "dataProtection":{
         "replication":{
            "endpointType":"Dst",
            "replicationSchedule":"Hourly",
            "remotePath":{
               "externalHostName":"<external-host-name>",
               "serverName":"<server-name>",
               "volumeName":"<volume-name>"
            }
         }
      },
      "serviceLevel":"<service-level>",
      "creationToken":"<token>",
      "usageThreshold":<value>,
      "exportPolicy":{
         "rules":[
            {
               "ruleIndex":1,
               "unixReadOnly":false,
               "unixReadWrite":true,
               "cifs":<true|false>,
               "nfsv3":<true|false>,
               "nfsv41":<true|false>,
               "allowedClients":"0.0.0.0/0",
               "kerberos5ReadOnly":<true|false>,
               "kerberos5ReadWrite":<true|false>,
               "kerberos5iReadOnly":<true|false>,
               "kerberos5iReadWrite":<true|false>,
               "kerberos5pReadOnly":<true|false>,
               "kerberos5pReadWrite":<true|false>,
               "hasRootAccess":<true|false>
            }
         ]
      },
      "protocolTypes":[
         "<protocols>"
      ],
      "subnetId":"/subscriptions/<subscription-
ID>/resourceGroups/<resource-group-name>/providers/Microsoft.Network/vir-
tualNetworks/<virtual-network-name>/subnets/<subnet>",
      "networkFeatures":"Standard",
      "isLargeVolume":"false"
   }
}
```

3. Issue a cluster peering API request for each of the target Azure NetApp Files migration volumes to the on-premises cluster. Repeat this step for each migration volume. Each call must provide a list of the on-premises cluster intercluster LIFs. The peer IP Addresses must match your on-premises networking.

> **Note**
>
> Every node in your ONTAP system needs an IC LIF. Each IC LIF needs to be listed here.

rest

```
    PUT https://<region>.management.azure.com/subscriptions/<subscrip-
tion-ID>/resourceGroups/<resource-group-
name>/providers/Microsoft.NetApp/netAppAccounts/<account-name>/capacity-
Pools/<capacity-pool-name>/volumes/<volume-names>/peerExternalCluster?
api-version=2025-06-01

    Body: {
       "PeerAddresses":[
          "<LIF address>",
          "<LIF address>",
          "<LIF address>",
          "<LIF address>"
       ]
    }
```

4. View the result header. Copy the `Azure-AsyncOperation` ID.

5. In your ONTAP or Cloud Volumes ONTAP system, accept the cluster peer request from Azure NetApp Files by sending a GET request using Azure-AsyncOperation ID.

rest

```
POST https://<region>.management.azure.com/subscriptions/<subscription-ID>/providers/Microsoft.NetApp/locations/<location>/operationResults/<Azure-AsyncOperation>?api-version=2025-06-01...
```

> ⓘ **Note**
>
> This operation can take time. Check on the request status. It's complete when that status reads "Succeeded." If the `Azure-AsyncOperation` doesn't respond successfully after an hour or it fails with an error, run the `peerExternalCluster` command again. Ensure the network configuration between your external ONTAP or Cloud Volumes ONTAP system and your Azure NetApp Files delegated subnet is working before continuing.

JSON

```
{
    "id": "/subscriptions/<subscriptionID>/providers/Microsoft.NetApp/locations/southcentralus/operationResults/00000-aaaa-1111-bbbb-22222222222",
    "name": "<name>",
    "status": "Succeeded",
    "name": "<name>",
    "status": "Succeeded",
    "startTime": "2023-11-02T07:48:53.6563893Z",
    "endTime": "2023-11-02T07:53:25.3253982Z",
    "percentComplete": 100.0,
    "properties": {
        "peerAcceptCommand": "cluster peer create -ipspace <IP-SPACE-NAME> -encryption-protocol-proposed tls-psk -peer-addrs <peer-addresses-list>",
        "passphrase": "<passphrase>"
    }
}
```

6. Once you receive the succeeded status, copy and paste the `peerAcceptCommand` string into the command line for your on-premises volumes followed by the passphrase string.

> ⓘ **Note**
>
> If the `peerAcceptCommand` string in the response body is empty, peering is already established. Skip this step for the corresponding migration volume.

7. Issue an `authorizeExternalReplication` API request for your migration volumes. Repeat this request for each migration volume.

rest

```
POST:
https://<region>.management.azure.com/subscriptions/<subscription>/re-
sourceGroups/<resource-
group>/providers/Microsoft.NetApp/netAppAccounts/<account-name>/capacity-
Pools/<capacity-pool-name>/volumes/<volume-names>/authorizeExternalRepli-
cation?api-version=2025-06-01
```

8. Accept the storage virtual machine (SVM) peer request from Azure NetApp Files by sending a GET request using the Azure-AsyncOperation ID in step 4.

rest

```
GET https://<region>.management.azure.com/subscriptions/<subscription-
ID>/providers/Microsoft.NetApp/locations/<location>/operationResults/<>?
api-version=2025-06-01&...
```

An example response:

JSON

```
{
    "id": "/subscriptions/00000000-aaaa-0000-aaaa-
0000000000000/providers/Microsoft.NetApp/locations/southcentralus/opera-
tionResults/00000000-aaaa-000-aaaa-000000000000"
    "name": "00000000-aaaa-000-aaaa-000000000000",
    "status": "Succeeded",
    "name": "00000000-aaaa-0000-aaaa-0000000000000",
    "status": "Succeeded",
    "startTime": "2023-11-02T07:48:53.6563893Z",
    "endTime": "2023-11-02T07:53:25.3253982Z",
    "percentComplete": 100.0,
    "properties": {
        "svmPeeringCommand": "vserver peer accept -vserver on-prem-svm-
name -peer-vserver destination-svm-name",
    }
}
```

Allow the baseline data transfer to complete. You can monitor the status of the replication using the Azure portal or the REST API.

9. After receiving the response, copy the CLI command from `svmPeeringCommand` into the ONTAP CLI.

10. Once baseline transfers have completed, select a time to take the on-premises volumes offline to prevent new data writes.

11. If there were changes to the data after the baseline transfer, send a "Perform Replication Transfer" request to capture any incremental data written after the baseline transfer was completed. Repeat this operation for *each* migration volume.

rest

```rest
    POST https://<region>.management.azure.com/subscriptions/<subscription-ID>/resourceGroups/<resource-group-names>/providers/Microsoft.NetApp/netAppAccounts/<account-name>>/capacityPools/<capacity-pool>/volumes/<volumes>/performReplicationTransfer?api-version=2024-06-01
```

12. Break the replication relationship. To break replication in the portal, navigate to each volume's **Replication** menu then select **Break peering**. You can alternately submit an API request:

rest

```rest
POST https://<region>.management.azure.com/subscriptions/<subscription-ID>/resourceGroups/<resource-group>/providers/Microsoft.NetApp/netAppAccounts/<NetApp-account>/capacityPools/<capacity-pool-name>>/volumes/<volumes>/breakReplication?api-version=2025-06-01
```

> **Note**
>
> Once you break the replication relationship, don't run any `snapmirror` commands (such as `snapmirror delete` or `snapmirror release`); these commands render the Azure NetApp Files volumes unusable.

13. Delete the migration replication relationship. If the deleted replication is the last migration associated with your subscription, the associated cluster peer and intercluster LIFs are deleted.

    rest

    ```
    POST https://<region>.management.azure.com/subscriptions/<subscription-ID>/resourceGroups/<resource-group-name>/providers/Microsoft.NetApp/netAppAccounts/<NetApp-account>/capacityPools/<capacity-pool>/volumes/<volume-names>/finalizeExternalReplication?api-version=2025-06-01
    ```

    Finalizing replication removes all the peering information on Azure NetApp Files. Manually confirm that all replication data is removed on the ONTAP cluster. If any peering information remains, run the `cluster peer delete` command.

More information

- Guidelines for Azure NetApp Files network planning
- Migrating data to Azure NetApp Files volumes