Using Microsoft Azure Blob Storage and Microsoft Azure Government Cloud as a primary storage for Enterprise Vault

14.0 or later

arctera™

Using Microsoft Azure Cloud as a primary storage for Enterprise Vault

Last updated: 2025-07-07.

Legal Notice

Arctera US LLC | www.arctera.io

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the company website:

https://www.veritas.com/docs/100040095

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

productdocs@arctera.io

You can also see documentation information or ask a question on the Arctera (formerly Veritas) community site:

https://vox.veritas.com/category/arctera-discussions/discussions/enterprise-vault

Technical Support

Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within the company to answer your questions in a timely fashion.

Our support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about our support offerings, you can visit our website at the following URL:

www.arctera.io/support

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contents

Chapter 1

Overview

This chapter includes the following topics:

About the Enterprise Vault primary partition for Microsoft Azure Cloud

Enterprise Vault now supports Microsoft Azure Blob Storage as primary storage, letting you store primary archived data in the following:

- Azure public cloud
- Azure Government cloud (for US Government Agencies)

You can use Hot and Cool access tier to store and access data. You can use this primary partition to archive, restore, search, and delete the data when Enterprise Vault is hosted in the on-premise and cloud network.

This guide shows how to configure the Enterprise Vault primary partition for both Microsoft Azure Blob Storage and Microsoft Azure Government Cloud. This guide assumes that you possess a working knowledge of Enterprise Vault tasks, such as creating and configuring vault store partitions and Microsoft Azure Cloud concepts.

Requirements for using Enterprise Vault primary partition

You must have the following for using the Microsoft Azure Cloud storage:

- Arctera Enterprise Vault 14.0
- If you are using Microsoft Azure Blob Storage, then Microsoft Azure public cloud account with the storage account rights
- If you are using Microsoft Azure Government Cloud, then Microsoft Azure Government Cloud account with the storage account rights

Prerequisites for configuring Enterprise Vault primary partition

Before you configure the Microsoft Azure Government Cloud or Microsoft Azure Blob Storage, make sure that you meet the following prerequisites:

- You have created a storage account on Microsoft Azure with the right replication type.
  See Azure Storage redundancy.
- You have the access keys of this storage account.
- You have created a container in the same storage account.
- You have a Vault Store Group and a Vault Store created.

Chapter 2

Configuring Enterprise Vault primary partition for Microsoft Azure Cloud

This chapter includes the following topics:

About configuration of Enterprise Vault primary partition

The following operations can be performed during configuration of Microsoft Azure Government Cloud or Microsoft Azure Blob Storage partition:

- Add a new partition
- View a partition
- Edit an existing partition
- Delete an existing partition
- Add a smart partition

Adding a new partition

To add a new Microsoft Azure Government Cloud or Microsoft Azure Blob Storage partition

1. In the left pane of the Administration Console, expand the Vault Store Groups container to view the existing vault store groups.
2. Expand the vault store group that contains the vault store for which you want to create the partition.
3. Expand the vault store in which you want to create the partition.
4. Right-click the Partitions container, and then click **New** > **Partition**. The New Partition wizard starts.
5. Click **Next**.
6. Enter all the details for new Vault Store Partition and then Click **Next**.
7. In the **Storage type** list, select the required storage type for Microsoft Azure Cloud.
   - **Microsoft Azure Blob Storage** to store primary archived data in the Azure public cloud.
   - **Microsoft Azure Government Cloud** to store primary archived data in the Azure Government cloud for US Government Agencies.
8. Click **Next**.
9. If you want to store data in WORM mode, select **Store data in WORM mode using Microsoft Azure Blob Immutable Storage**. This option is cleared by default so that data is stored in non-WORM mode.

   Note: WORM mode is not supported for Microsoft Azure China cloud and Microsoft Azure Government cloud.

   Ensure the VERSION-LEVEL IMMUTABILITY SUPPORT for the Microsoft Azure Blob Container is configured.

   The test functionality for the partition created for Microsoft Azure Blob in WORM mode fails if the clock on the Enterprise Vault server is more than 2 minutes behind the universal clock in the same time zone. If the 'Retention Period' is behind the Microsoft Azure Blob service time, the test functionality may fail to upload the object. You must synchronize the clock on your Enterprise Vault server with the universal clock.

   ---

10. Click **Next**.

11 Provide the Microsoft Azure Government Cloud or Microsoft Azure Blob Storage connection settings:

Setting	Description
Azure environment	(For Microsoft Azure Blob Storage) Specify an Azure environment that includes Azure for global Azure and Azure China for Azure operated in China. (For Microsoft Azure Government Cloud) Specify the Azure US Government Cloud environment.
Storage account name	Specify a general-purpose storage account or a Blob storage account. Note: The storage account name cannot be changed once the partition is created.
Access key	Specify the access key ID provided for the Azure storage account.
Container name	Specify where the data will be archived. Note: The container name cannot be modified once the partition is created.
Access tier	Specify the access tier that allows you to store data. The available access tiers include: ■ **Default** - used to infer account-level tiering. ■ **Hot** - used if the data is frequently accessed. ■ **Cool** - used if the data is infrequently accessed. For more information, refer to this article.
Write buffer size (MB)	Specify the write buffer size, in the range of 1 MB to 100 MB, to upload data in chunks.
Read buffer size (MB)	Specify the read buffer size, in the range of 1 MB to 100 MB, to download data in chunks.

Setting	Description

Log level	Specify the logging level for Azure SDK logs.
	■ **Off** - Enterprise Vault does not log any Azure SDK logs.
	■ **Error** - Logs all exceptions that are not handled internally and thrown to the user.
	■ **Warning** - Logs all exceptions that are handled internally.
	■ **Informational** - Logs the following information:
	  ■ Request details, such as URI and client request ID
	  ■ A timestamp for all important milestones, such as Send Request, Upload Data, Receive Response, and Download Data.
	  ■ Response details, such as request ID and HTTP status code.
	  ■ Reason for retrying a failed operation, and schedule of the next retry.
	  ■ All client-side timeouts about an aborted pending request.
	■ **Verbose** - Logs extra details about operations, and the String-to-sign for each request.
	Note: DTrace logs will include the Azure C#.NET SDK log statements, which can be easily found prefixed with **AzureSDKTrace:**.

12 Click **Next**.

13 On the Replication page, select the required option from the following:

- **When archived files are replicated on the cloud storage**
- **When archived files exist on the cloud storage**

For more information, see the *Administration Console help*.

Note: If you choose the option **When archived files are replicated on the cloud storage**, it is crucial to ensure that replication is enabled in the specified storage account and that the replication policy does not exclude any objects. Disabling replication or using filters can significantly increase the number of unsecured items.

---

14 Choose the scan interval for checking if files are replicated on cloud or not.

By default, every 60 minutes, Enterprise Vault checks whether archived data is replicated. If required, you can change the scan interval. If you set the scan interval to 0 minutes, partitions are checked only when the backup mode is cleared from the vault store, and when the storage service starts.

15 Click **Next**.

16 Click **OK** on the warning message box.

17 The summary page provides the information for the newly created partition.

Note: For write operations, you can configure the 'RetentionPeriodInHours' registry key to add hours to the Universal current time, creating a new retention period. This registry key is used only when the Enterprise Vault server and Microsoft Azure Blob service times go out of sync. The default value of 'RetentionPeriodInHours' is 1 hour. For more information, see the *Enterprise Vault Registry Values Guide*.

Viewing a partition

To view a configured Microsoft Azure Government Cloud or Microsoft Azure Blob Storage partition

1 On **Vault Store Groups** > **Vault Store Group** > **Partition**, select the partition.

2 Right-click the partition, and then select **Properties**.

3 There are three tabs: **General**, **Replication**, **Advanced**.

4 Click each tab to view the relevant information.

Editing an existing partition

To edit an existing Microsoft Azure Government Cloud or Microsoft Azure Blob Storage partition

1 On **Vault Store Groups** > **Vault Store Group** > **Partition**, and select the partition.

2 Right-click the partition, and then select **Properties**.

3 Click the **Advanced** tab. The editable fields on the screen are the Access key, Access tier, Log level, Write buffer size (MB) and Read Buffer Size (MB).

4 To edit a field, double-click or click **Modify**, then type directly in the field, or select another option from the drop-down list.

5 Click **Test** or **Apply** to save your changes. The **Apply** will initiate the Test configuration with the Azure Container automatically.

6 On the successful Test configuration, if you are prompted, restart the storage service.

7 Click the **Replication** tab.

8 You can change the scan interval.

9 Click **Apply**, if you are prompted, restart the storage service.

10 Click **Ok**.

Deleting a partition

To delete an existing Microsoft Azure Government Cloud or Microsoft Azure Blob Storage partition

1 On **Vault Store Groups** > **Vault Store Group** > **Partition**, and select the partition.

2 Right-click the partition, and then select **Delete**.

Note: Only Ready and Closed partitions can be deleted.

3 When a confirmation message appears, click **Yes** to proceed with the deletion or **No** to abort the deletion.

Smart partition for Microsoft Azure Cloud

You can create a new smart partition, and view, edit, or delete an existing smart partition.

Chapter 3

Verifying replication on Microsoft Azure Cloud storage

This chapter includes the following topics:

Replication verification on Microsoft Azure Cloud storage

Enterprise Vault checks whether archived data in the Microsoft Azure Government Cloud or Microsoft Azure Blob Storage has been replicated. Based on the replication status, Enterprise Vault marks the items in partition as secured and the post-processing of the items will be done. Enterprise Vault supports replication verification for the following Microsoft Azure replication types:

- Locally redundant storage (LRS)
- Zone-redundant storage (ZRS)
- Geo-redundant storage (GRS)
- Geo-zone-redundant storage (GZRS)
- Read-access geo-redundant storage (RA-GRS)
- Read-access geo-zone-redundant storage (RA-GZRS)

Note: In case of GRS and GZRS, Enterprise Vault checks whether the archived data in the Microsoft Azure Blob Storage is replicated in the primary region only. Enterprise Vault cannot check the replication status of the archived data in the secondary region due to the limitation of Microsoft Azure SDK

Please refer this link for more information about replication at Microsoft Azure Storage Account.

Chapter 4

Troubleshooting

This chapter includes the following topics:

Using the DTrace utility for enabling Azure SDK to view diagnostic logs

If you encounter issues when you store or retrieve archived data with the Enterprise Vault Microsoft Azure Government Cloud or Microsoft Azure Blob Storage primary partition, you can run the DTrace utility to identify the cause for issues.

You can also add Azure SDK-provided log level on partition, which has been incorporated in the DTrace utility as an additional support for troubleshooting. To enable Azure SDK logs for troubleshooting purpose, see See "Adding a new partition" on page 9.

The DTrace utility lets you monitor multiple services simultaneously, write the trace to a file, filter for specific words, and trigger tracing based on the filters.

The following table lists the processes for which you can get the diagnostic logs with DTrace.

Note: Arctera Enterprise Vault recommends setting the monitoring level to **Verbose** in all cases.

Monitor this process	To do this
StorageArchive.exe	To get diagnostic logs for archived files that are written in the Microsoft Azure Government Cloud or Microsoft Azure Blob Storage.

Monitor this process	To do this
StorageOnlineOpns.exe	To get diagnostic logs for the retrieved and restored of files that are in the Microsoft Azure Government Cloud or Microsoft Azure Blob Storage.
StorageFileWatch.exe	To get the diagnostic logs to know whether items is secure or not based on the replication setting configured on Microsoft Azure Government Cloud or Microsoft Azure Blob Storage partition.
StorageManagement.exe	To view the information that is logged when Enterprise Vault checks whether the partition has been configured correctly and validates the configured settings. Enterprise Vault logs this information when you click the **Test** button on the **Advanced** page of the vault store partition **Properties** page and the vault store partition creation wizard.

Note: For more information on DTrace, see the *Enterprise Vault™ Utilities Guide*.