Using Amazon Commercial Cloud Services (C2S) as a primary storage for Enterprise Vault

14.0 or later

VERITAS™

Using Amazon Commercial Cloud Services (C2S) as a primary storage for Enterprise Vault

Last updated: 2021-03-19.

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

https://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Before you contact Technical Support, run the Veritas Quick Assist (VQA) tool to make sure that you have satisfied the system requirements that are listed in your product documentation. You can download VQA from the following article on the Veritas Support website:

https://www.veritas.com/support/en_US/vqa

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 Veritas 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:

evdocs@veritas.com

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

https://www.veritas.com/community

Contents

Chapter 1

Overview

This chapter includes the following topics:

About the Amazon Commercial Cloud Services (C2S) primary partition

Enterprise Vault supports Amazon Commercial Cloud Services (C2S) as primary storage, letting you store primary archived data in the AWS Government cloud for US Federal Agencies. It also supports Amazon SSE-S3-Managed Encryption that provides data security by encrypting the data at rest.

You can use this partition to archive, restore, and search data when Enterprise Vault is hosted in the C2S cloud network. This guide shows how to configure the Amazon C2S as a primary partition.

This guide assumes that you possess a working knowledge of Enterprise Vault tasks, such as creating and configuring vault store partitions and Amazon C2S cloud storage concepts.

Chapter 2

Configuring Amazon Commercial Cloud Services (C2S) primary partition

This chapter includes the following topics:

About configuring Amazon C2S primary partition

You need to perform the following steps to configure Amazon Commercial Cloud Services (C2S) primary partition:

- Get the Amazon C2S-supported CAP authentication
  See "Getting the Amazon C2S-supported authentication" on page 7.
- Configure Amazon C2S primary partition
  See "Configuring Amazon C2S primary partition" on page 7.
- Troubleshooting
  See "Using the DTrace utility for enabling AWS SDK to view diagnostic logs" on page 14.

Getting the Amazon C2S-supported authentication

Before you migrate Enterprise Vault files to the Amazon C2S cloud storage, you must have the information about Amazon Commercial Cloud (C2S) S3 endpoint, CAP URL, Agency, Mission Name, Role, Configure Certificate, AWS S3 bucket created in the supported region, and Storage Class to used.

You must have the following for using the Amazon C2S cloud storage:

- Enterprise Vault 14.0
- Amazon C2S authentication
- Amazon Simple Storage Service (S3) bucket name
- Multiple AWS storage classes, including S3 Standard, S3 Standard - IA, S3 One Zone – IA, or S3 Intelligent-Tiering.
- Server-side encryption with Amazon S3-Managed keys

The following operations can be performed during configuration:

- Add a new Amazon C2S partition that uses CAP authentication
- View an Amazon C2S partition
- Edit an Amazon C2S partition
- Delete an Amazon C2S partition

Configuring Amazon C2S primary partition

This section includes the following topics:

Adding a new Amazon C2S partition that uses CAP Authentication

Before configuring the Amazon C2S primary partition with CAP authentication, complete the following steps:

- Keep your AWS CAP URL, Agency, Mission Name, Role, and Configure Certificate ready.
- Ensure that the AWS S3 bucket that needs to be configured with the primary partition has been created with AWS, and that you know the name of your bucket.

- Update the `cacert.pem` file with the provided certificate on location `C:\Program Files (x86)\Enterprise Vault\CloudStreamer`.

To add a new Amazon C2S partition that uses CAP authentication

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 **Amazon Commercial Cloud Service (C2S)**.
8. Click **Next**.
9. Provide the Amazon C2S connection settings:

Setting	Description
AWS C2S S3 endpoint	Specify the endpoint for the AWS region based on the AWS S3 bucket.
CAP URL	Specify the URL for the C2S access portal.
Agency	Specify the agency that is associated with the target C2S account.
Mission Name	Specify the mission name that is assigned to the target C2S account.
Role	Specify the IAM Role in the target C2S account.

Setting	Description
Certificate name	Specify the client certificate for the C2S access portal authentication. You cannot remove a certificate that is currently in use. To configure the Certificate name for the C2S access portal authentication: **1** Click **Add**. **2** Enter the certificate name. **3** Provide the certificate `.cert.pem` file. **4** Provide the private key `.key.pem` file. **5** Configure **Passphrase**, if required. **6** Click **OK**. You can use the same screen for removing and viewing the configured certificate.
Storage class	Specify the storage class for storing objects into the AWS S3 bucket. ■ **S3 Standard** - to store frequently accessed data. ■ **S3 Standard-IA** - to store infrequently accessed data that requires rapid access when needed. Data is stored in a minimum of three Availability Zones (AZs). ■ **S3 One Zone-IA** - to store infrequently accessed data in a single Availability Zone. ■ **S3 Intelligent-Tiering** - to move data across most cost-effective access tier. For more information, see https://aws.amazon.com/s3/storage-classes.
Encryption	Specify encryption setting whether to encrypt archived files stored in bucket or not. By default, **SSE-S3** is selected that encrypts the archived files by using server-side encryption with Amazon S3-Managed Encryption Keys.

Setting	Description
Log level	Specify the logging level for AWS SDK logs. ■ **No logging** - Enterprise Vault does not log any AWS SDK logs. ■ **Fatal** - Logs only fatal errors. ■ **Error** - Logs all errors. ■ **Warn** - Logs warning and errors. ■ **Info** - Logs every information, including warnings and errors. ■ **Debug** - Logs debug messages, including info, warnings, and errors. ■ **Everything** - Logs everything. **Note:** DTrace logs will include the AWS SDK log statements, which can be easily found prefixed with **AwsSdk:**.
Write buffer size (MB)	Specify the write buffer size, in the range of 5 MB to 200 MB, to upload data in chunks.
Read buffer size (MB)	Specify the read buffer size, in the range of 1 MB to 1024 MB, to download data in chunks.

10 Click **Next** to check the configuration.

11 New Partition configuration shows the Amazon Commercial Cloud Services success message. Click **Next**.

12 The **Replication** page shows the selected option as **When archived files exist on the cloud storage**.

Please see the Administration Console Help pages for more information.

13 Choose the scan interval for checking if files exist on the cloud. The supported scan interval is from 0 minute to 1440 minutes. By default, every 60 minutes, Enterprise Vault checks whether the archived data exists on the cloud. 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.

14 Click **Next**.

15 The summary page provides the information for the newly created Amazon C2S partition.

Viewing an Amazon C2S partition

To view a list of currently configured Amazon C2S partition

1. On the Configuration Vault Store partition, right-click and select **Properties**.
2. Click the **Replication** tab. The screen displays the appropriate replication option selected during new partition creation, set/edit scan interval time along with the status for secured, unsecured items with the last scan started and items secured in the last scan.
3. Click the **Details** button. The screen displays the information for the Last item secured, Last scan, Summary and Unsecured items information.
4. Click the **Advance** tab. The screen displays the C2S endpoint, CAP URL, Agency, Mission, Role, Certificate, Storage class, Encryption, Log level, and buffer size.
5. After viewing the destination information, click **Okay**.

Editing an Amazon C2S partition

To edit an existing Amazon C2S partition

1. On the Configuration Vault Store partition, right-click and select **Properties**.
2. Click the **Replication** tab. The screen display the option to select **When archived files are replicated on the cloud storage** and **When archived files exist on the cloud storage**, and an editable field for scan interval. To edit the scan interval, type directly in the field. The supported scan interval is from 0 minute to 1440 minutes. By default, Enterprise Vault checks whether archived data is replicated every 60 minutes. 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.
3. Click the **Advance** tab. The screen displays the CAP URL, Agency, Mission, Role, Certificate, Storage class, Encryption, Log level, and buffer size.
4. To edit a field, type directly in the field. For example, select Storage Class and select the required option, S3 Standard, S3 Standard-IA, S3 One Zone-IA, or S3 Intelligent-Tiering.

   Note: To return to the last saved configuration, click **Reset**.

5. Click **Test** or **Apply** to save your changes. The **Apply** will initiate the Test configuration with the AWS S3 bucket automatically.

6 On the successful Test configuration, restart the storage service.

7 Click **Ok**.

Deleting an Amazon C2S partition

To delete an existing Amazon C2S partition

1 On the Configuration Vault Store partition, right-click and select **Delete**.

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

Smart partition for Amazon Commercial Cloud Service (C2S)

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

Chapter 3

Known Issues

This chapter includes the following topics:

Known Issues

Below are the know issues:

- Enterprise Vault fails to upload archived files with a size greater than 4 GB to the AWS S3 bucket mentioned in an Amazon Commercial Cloud Service (C2S) primary and smart partition. For more information, refer to the tech note: https://www.veritas.com/support/en_US/article.100048604

Chapter 4

Troubleshooting

This chapter includes the following topics:

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

If you encounter issues when you store or retrieve archived data with the Enterprise Vault Amazon C2S primary partition, you can run the DTrace utility to identify the cause for issues.

You can also add AWS SDK-provided log level on partition, which has been incorporated in the DTrace utility as an additional support for troubleshooting. To enable AWS SDK logs for troubleshooting purpose, see See "Adding a new Amazon C2S partition that uses CAP Authentication" on page 7.

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: Veritas 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 (DVS, DVSSP, DVSCC, and so on) that are written in the Amazon C2S.
StorageOnlineOpns.exe	To get diagnostic logs for the retrieved and restored of files that are in the Amazon C2S.

Monitor this process	To do this
StorageFileWatch.exe	To get the diagnostic logs to know whether items is secure or not based on the replication setting configured on Amazon C2S 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*.