Using Amazon Simple Storage Service (S3) as a primary storage for Enterprise Vault

14.0 or later

arctera™

Using Amazon Simple Storage Service (S3) 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 Amazon Simple Storage Service (S3) primary partition

Enterprise Vault supports Amazon Simple Storage Service (S3) as primary storage, letting you store primary archived data in the AWS public cloud. It supports Amazon S3-Managed Encryption that provides data security by encrypting the data at rest. It also provides support for AWS Identity and Access Management (IAM) Role that provides accessibility to cloud-native services with granular policies and permissions.

You can use the Amazon Simple Storage Service (S3) primary partition to archive, restore, and search data when Enterprise Vault is hosted in the on-premise and cloud. This guide shows how to configure the Amazon Simple Storage Service (S3) 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 S3 cloud storage concepts.

Chapter 2

Configuring Amazon Simple Storage Service (S3) primary partition

This chapter includes the following topics:

About configuring Amazon S3 primary partition

You need to perform the following steps to configure Amazon S3 primary partition:

- Get the Amazon S3 supported authentication
  See "Getting the Amazon S3 supported authentication" on page 8.
- Configure Amazon S3 primary partition
  See "Configuring Amazon S3 primary partition" on page 9.
- Configure and use replication with replicate to cloud and exit on the cloud option
  See "Configuring replication with the supported option" on page 27.
- Troubleshooting

See "Using the DTrace utility for enabling AWS SDK to view diagnostic logs" on page 29.

Getting the Amazon S3 supported authentication

You must have the following for using the Amazon S3 cloud storage:

- Enterprise Vault 14.0 or later
- AWS S3 bucket name
- Multiple AWS authentication types, which includes:
  - AWS standard authentication that makes use of Access Key ID and Secret Access Key, for AWS public cloud.
  - AWS IAM Role that makes use of AWS Identity and Access Management (IAM) Access Key ID and Secret Access Key, for AWS public cloud.
  - AWS Security Token Service (STS) authentication for AWS public cloud.
- Multiple AWS storage classes, including S3 Standard, S3 Standard-IA, S3 One Zone-IA, S3 Intelligent-Tiering, and S3 Glacier Instant Retrieval.
- Server-side encryption with Amazon S3-Managed Encryption Keys.
- Replication configure the bucket replication with the same region or cross region on the AWS portal to use.

For any authentication method that you are using to create a vault store partition or a smart partition, if you are specifying credentials of a user who has access to restricted AWS regions, then you should add the following permissions to the IAM policy attached to that user.

```
{
"Sid": "VisualEditor1",
"Effect": "Allow",
"Action": "s3:GetBucketLocation",
"Resource": "*",
"Condition": {
"StringEquals": {
"aws:RequestedRegion": "us-east-1"
}
```

In case of Enterprise Vault 14.0 or any of its hotfix, the following permission should be added to the IAM policy attached to the user:

```
{
"Sid": "VisualEditor1",
```

```
"Effect": "Allow",
"Action": "s3:GetBucketLocation",
"Resource": "*",
"Condition": {
"StringEquals": {
"aws:RequestedRegion": "us-west-1"
}
```

The following operations can be performed during configuration:

- Add a new Amazon S3 partition that uses Access Keys authentication
- Add a new Amazon S3 partition that uses IAM Role authentication
- Add a new Amazon S3 partition that uses STS Assume Role authentication
- View an Amazon S3 partition
- Edit an Amazon S3 partition
- Delete an Amazon S3 partition

Configuring Amazon S3 primary partition

This section includes the following topics:

Adding a new Amazon S3 partition that uses Access Keys authentication

Before configuring the Amazon S3 for primary partition with AWS Access Keys authentication, complete the following steps:

- Keep your AWS Access Key ID and Secret Access Key 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.

To add a new Amazon S3 partition that uses Access Keys 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 Simple Storage Service**.
8. Select the **Store data in WORM mode using S3 Object Lock** if you want to store data in WORM mode. By default, this option is cleared so that data is stored in non-WORM mode.

   Note: Ensure that the retention mode of S3 Object Lock for the AWS S3 bucket is configured in Compliance mode.

   The test functionality for the partition created for AWS S3 in WORM mode fails if the clock on the Enterprise Vault server is behind the universal clock in the same time zone for more than 2 minutes. In case 'Retain Until Date' is behind with respect to AWS S3 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.

   ---

9. Select the **Access Keys** option to authenticate with Amazon S3.
10. Provide the Amazon S3 connection settings:

Setting	Description
AWS PrivateLink	Select **Yes** to use the private interface S3 endpoint, or **No** to use the public S3 endpoint. By default, the public S3 endpoint is used to communicate with S3 and store archived files in the specified bucket. If you select **Yes**, ensure that you have provided the private interface S3 endpoint in the **S3 Endpoint** setting. Note: This setting is available in Enterprise Vault 14.3 and later.

Setting	Description
S3 Endpoint	Specify the URL of the AWS S3 endpoint. By default, the public AWS S3 endpoint URL - https://s3.amazonaws.com - is used. If you have selected **Yes** for the **AWS PrivateLink** setting, specify the private interface S3 endpoint. Note: This setting is available in Enterprise Vault 14.3 and later.
Access key ID	Specify the access key ID that is provided by Amazon.
Secret access key	Specify the secret access key that is provided by Amazon.
Bucket name	Specify the name of the AWS S3 bucket. Note: The bucket name cannot be modified once the partition is created. You must not delete the bucket after creating the partition. In case you need to delete the bucket for some reason, you must create a new partition.
Bucket Region	Enter the code of the region where the S3 bucket (specified in the **Bucket name** setting) resides. For more information about the region codes, see https://docs.aws.amazon.com/general/latest/gr/rande.html. Ensure that you have specified the correct region code to create the partition. Note: This setting is available in Enterprise Vault 14.3 and later.
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. ■ **S3 Glacier Instant Retrieval** - to store long-retention data that is rarely accessed and requires retrieval in milliseconds at the lowest cost. For more information, see https://aws.amazon.com/s3/storage-classes.

Setting	Description
Encryption	Specify encryption setting whether to encrypt archived files stored in bucket or not. Select **SSE-S3** to encrypt the archived files by using server-side encryption with Amazon S3-Managed Encryption Keys. By default, **None** is selected that does not use encryption.
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.

11 Click **Next**.

12 On the **Replication** page, select the appropriate option as **When archived files exist on the cloud storage** or **When archived files are replicated 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 archived data is replicated or exists on cloud based on the above options. 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 S3 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 AWS S3 service times go out of sync. The default value of 'RetentionPeriodInHours' is 1 hour. Refer to the Enterprise Vault Registry Values Guide for more information.

Adding a new Amazon S3 partition that uses IAM Role authentication

Before configuring the Amazon S3 for primary partition with AWS IAM Role authentication, complete the following steps:

- Ensure that the AWS S3 bucket that needs to be configured with the primary partition have been created with AWS, and that you know the name of your bucket.
- Ensure that the IAM roles and their managed policies have been defined for your AWS S3 buckets.

To create the AWS IAM Role with the policy using the IAM console, see http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user.html.

Using the AWS Management Console, create the IAM Role with the policy that must have the following permissions:

1 In the IAM role pane of the console, click **Roles**, and then click **Create role**.

2 Select the **AWS service** type of the trusted entity.

3 Click **Amazon EC2 Full Access**.

Create and attach the AWS IAM Role policy for Amazon S3 with the following access level permission:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
               "s3:DeleteObject",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:GetBucketObjectLockConfiguration"
                ],
            "Resource": "*"
       }
    ]
}
```

By default, the partition is created in non-WORM mode and you can use the above policy.

If you choose to create the partition in WORM mode, you need to set additional permissions for the IAM Role authentication method. In this case, create and attach the AWS IAM Role policy for Amazon S3 with the following access level permission:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "VisualEditor0",
"Effect": "Allow",
"Action": [
"s3:PutObject",
"s3:GetObject",
"s3:DeleteObject",
"s3:GetBucketLocation",
"s3:ListBucket",
"s3:PutObjectRetention",
```

```
"s3:GetBucketObjectLockConfiguration",
"s3:GetObjectVersion",
"s3:ListBucketVersions",
"s3:DeleteObjectVersion",
"s3:GetObjectRetention"
],
"Resource": "*"
}
]
}
```

4 For **Role name**, type a name for your role.

5 Review the role, and then click **Create role**.

To add a new Amazon S3 partition that uses Access Keys 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 Simple Storage Service.

8 Select the **Store data in WORM mode using S3 Object Lock** if you want to store data in WORM mode. By default, this option is cleared so that data is stored in non-WORM mode.

Note: Ensure that the retention mode of S3 Object Lock for the AWS S3 bucket is configured in Compliance mode.

The test functionality for the partition created for AWS S3 in WORM mode fails if the clock on the Enterprise Vault server is behind the universal clock in the same time zone for more than 2 minutes. In case 'Retain Until Date' is behind with respect to AWS S3 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.

---

9 Select the **IAM Role** option to authenticate with Amazon S3.

10 Provide the Amazon S3 connection settings:

Setting	Description
AWS PrivateLink	Select **Yes** to use the private interface S3 endpoint, or **No** to use the public S3 endpoint. By default, the public S3 endpoint is used to communicate with S3 and store archived files in the specified bucket. If you select **Yes**, ensure that you have provided the private interface S3 endpoint in the **S3 Endpoint** setting. Note: This setting is available in Enterprise Vault 14.3 and later.
S3 Endpoint	Specify the URL of the AWS S3 endpoint. By default, the public AWS S3 endpoint URL - https://s3.amazonaws.com - is used. If you have selected **Yes** for the **AWS PrivateLink** setting, specify the private interface S3 endpoint. Note: This setting is available in Enterprise Vault 14.3 and later.
Bucket name	Specify the name of the Amazon S3 bucket. Note: The bucket name cannot be modified once the partition is created. You must not delete the bucket after creating the partition. In case you need to delete the bucket for some reason, you must create a new partition.
Bucket Region	Enter the code of the region where the S3 bucket (specified in the **Bucket name** setting) '' resides. For more information about the region codes, see https://docs.aws.amazon.com/general/latest/gr/rande.html. Ensure that you have specified the correct region code to create the partition. Note: This setting is available in Enterprise Vault 14.3 and later.

Setting	Description
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. ■ **S3 Glacier Instant Retrieval** - to store long-retention data that is rarely accessed and requires retrieval in milliseconds at the lowest cost. 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. Select **SSE-S3** to encrypt the archived files by using server-side encryption with Amazon S3-Managed Encryption Keys. By default, **None** is selected that does not use encryption.
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.

11 Click **Next**.

12 On the **Replication** page, select the appropriate option as **When archived files exist on the cloud storage** or **When archived files are replicated 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 archived data is replicated or exists on cloud based on the above options. 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 S3 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 AWS S3 service times go out of sync. The default value of 'RetentionPeriodInHours' is 1 hour. Refer to the Enterprise Vault Registry Values Guide for more information.

Adding a new Amazon S3 partition that uses STS Assume Role authentication

Before configuring the Amazon S3 for primary partition with AWS STS Assume Role authentication, complete the following steps:

- 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 names of your bucket.
- Ensure that the IAM roles and their managed policies have been defined for your AWS S3 buckets, and that you know the roles' Amazon Resource Name (ARN).

For more information on Amazon STS (Security Token Service), see AWS Documentation.

Using the AWS Management Console, create a role that an IAM user can assume

1 In the IAM role pane of the console, click **Users**, and then click **Add User**. This user will be used to assume roles in your on-premise environment.

2 Create an IAM Role User policy which will be attached to the user added in the above step.

It allows the IAM user to list and assume roles. The following JSON document describes the IAM policy.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "sts:AssumeRole"
            ],
            "Resource": "*"
        }
    ]
}
```

3 Attach the policy to the IAM user.

4 The IAM user who is allowed to assume role has been created. Before you create the role, create an IAM policy which will be attached to the role.

5 Create AWS IAM Role policy for Amazon S3 with the following access levels permissions on the S3:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:GetBucketObjectLockConfiguration"
            ],
            "Resource": "*"
        }
    ]
}
```

By default, the partition is created in non-WORM mode and you can use the above policy.

If you choose to create the partition in WORM mode, you need to set additional permissions for the STS Assume Role authentication method. In this case, create and attach the AWS IAM Role policy for Amazon S3 with the following access level permission:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "VisualEditor0",
"Effect": "Allow",
"Action": [
"s3:PutObject",
"s3:GetObject",
"s3:DeleteObject",
"s3:GetBucketLocation",
"s3:ListBucket",
"s3:PutObjectRetention",
"s3:GetBucketObjectLockConfiguration",
"s3:GetObjectVersion",
```

```
"s3:ListBucketVersions",
"s3:DeleteObjectVersion",
"s3:GetObjectRetention"
],
"Resource": "*"
}
]
}
```

6 To create the IAM role, in the IAM role pane of the console, click **Roles**, and then choose **Create role**.

7 Select the **Another AWS account** role type of trusted identity.

8 Provide the **Account ID** of the IAM user created in step a.

9 Associate the policy created in step e.

10 For **Role name**, type a name for your role.

11 Review the role, and then click **Create role**.

To add a new Amazon S3 partition that uses Access Keys 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 Simple Storage Service.

8 Select the **Store data in WORM mode using S3 Object Lock** if you want to store data in WORM mode. By default, this option is cleared so that data is stored in non-WORM mode.

Note: Ensure that the retention mode of S3 Object Lock for the AWS S3 bucket is configured in Compliance mode.

The test functionality for the partition created for AWS S3 in WORM mode fails if the clock on the Enterprise Vault server is behind the universal clock in the same time zone for more than 2 minutes. In case 'Retain Until Date' is behind with respect to AWS S3 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.

---

9 Select the **STS Assume Role** option to authenticate with Amazon S3.

10 Provide the Amazon S3 connection settings:

Setting	Description
AWS PrivateLink	Select **Yes** to use the private interface S3 endpoint, or **No** to use the public S3 endpoint. By default, the public S3 endpoint is used to communicate with S3 and store archived files in the specified bucket. If you select **Yes**, ensure that you have provided the private interface S3 endpoint in the **S3 Endpoint** setting. Note: This setting is available in Enterprise Vault 14.3 and later.
S3 Endpoint	Specify the URL of the AWS S3 endpoint. By default, the public AWS S3 endpoint URL - https://s3.amazonaws.com - is used. If you have selected **Yes** for the **AWS PrivateLink** setting, specify the private interface S3 endpoint. Note: This setting is available in Enterprise Vault 14.3 and later.
Access key ID	Specify the access key ID that is provided by Amazon.
Secret access key	Specify the secret access key that is provided by Amazon.
ARN of IAM Role	Specify the Amazon Resource Name for the IAM role to be assumed for the specified IAM user.

Setting	Description
STS Endpoint	Depending on your Enterprise Vault version, perform one of the following actions: ■ If you are on Enterprise Vault versions 14.3 and later, enter the STS endpoint of the same region where the AWS S3 bucket also resides. ■ If you are on Enterprise Vault versions earlier than 14.3, select the STS endpoint of the same region where the AWS S3 bucket also resides. Note: Enterprise Vault recommends using the STS endpoint of the region where the AWS S3 bucket exists to reduce latency and improve response time. If the **AWS PrivateLink** setting is set to **Yes**, specify the private interface STS endpoint URL; otherwise specify the public STS endpoint URL available at: https://docs.aws.amazon.com/general/latest/gr/sts.html
Bucket name	Specify the name of the AWS S3 bucket. Note: The bucket name cannot be modified once the partition is created. You must not delete the bucket after creating the partition. In case you need to delete the bucket for some reason, you must create a new partition.
Bucket Region	Enter the code of the region where the S3 bucket (specified in the **Bucket name** setting) resides. For more information about the region codes, see https://docs.aws.amazon.com/general/latest/gr/rande.html. Ensure that you have specified the correct region code to create the partition. Note: This setting is available in Enterprise Vault 14.3 and later.

Setting	Description
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. ■ **S3 Glacier Instant Retrieval** - to store long-retention data that is rarely accessed and requires retrieval in milliseconds at the lowest cost. 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. Select **SSE-S3** to encrypt the archived files by using server-side encryption with Amazon S3-Managed Encryption Keys. By default, **None** is selected that does not use encryption.
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.

11 Click **Next**.

12 On the **Replication** page, select the appropriate option as **When archived files exist on the cloud storage** or **When archived files are replicated 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 archived data is replicated or exists on cloud based on the above options. 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 S3 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 AWS S3 service times go out of sync. The default value of 'RetentionPeriodInHours' is 1 hour. Refer to the Enterprise Vault Registry Values Guide for more information.

Viewing an Amazon S3 partition

To view a list of currently configured Amazon S3 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 Authentication type, Storage class, Encryption, Log level, and buffer size.

5 After viewing the destination information, click **Okay**.

Editing an Amazon S3 partition

To edit an existing Amazon S3 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 field, 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 or exists 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 Authentication type, Storage class, Encryption, Log level, and buffer size.
4. To edit a field, type directly in the field (for example, type a new Access key ID and Secret access key), or select another option from the drop-down list.

   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 S3 partition

To delete an existing Amazon S3 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 S3

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

Configuring replication with the supported option

To use the replication with Enterprise Vault, the AWS administrator needs to configure bucket replication on the AWS portal.

To configure the bucket replication, see the AWS Replication:
https://docs.aws.amazon.com/AmazonS3/latest/dev/replication.html

To change the configured AWS S3 bucket of an existing Amazon Simple Storage Service (S3) partition, see:
https://www.veritas.com/support/en_US/article.100048607

To enable delete marker from the source bucket to destination bucket, see:
https://www.veritas.com/support/en_US/article.100048606

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 Simple Storage Service (S3) primary and smart partition. For more information, refer to the tech note: https://www.veritas.com/support/en_US/article.100048604
- On the on-premise environment where the administrator has a partition configured with the STS Assume role, if the provided STS ARN is removed OR modification is done with the attached policy on the AWS Portal, then the EventViewer shows the following error:

  `"CCloudStreamerObject::Init method failed", Reason = 0x80070005`
- On the AWS environment EC2 instance where the administrator has a partition configured with the IAM role, if the attached IAM role to EC2 instance is removed OR modification is done with the IAM policy on the AWS Portal, the EventViewer shows the error:

  `"CCloudStreamerObject::Init method failed", Reason = 0x80070005`

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 Simple Storage Service (S3) 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 "Configuring Amazon S3 primary 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 Amazon Simple Storage Service (S3).
StorageOnlineOpns.exe	To get diagnostic logs for the retrieved and restored of files that are in the Amazon Simple Storage Service (S3).

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 Simple Storage Service (S3) 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*.