Veritas Enterprise Vault™

Best Practice for Implementing Enterprise Vault in AWS and Microsoft Azure Cloud

14.1

VERITAS

Veritas Enterprise Vault™: Best Practice for Implementing Enterprise Vault in AWS and Microsoft Azure Cloud

Last updated: 2021-03-19.

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

https://www.veritas.com

Contents

Chapter 1 About this document 7

Purpose 7
Intended Audience 7
Supporting documents 7

Chapter 2 Enterprise Vault Deployment in AWS 9

Choosing the right EC2 instance 10
Considerations for Enterprise Vault Amazon S3 partitions 10
Authentication 10
Storage class 11
Replication 11

Chapter 3 Enterprise Vault Deployment in Azure Cloud 13

Choosing the right Azure virtual machine 13
Considerations for Enterprise Vault Azure Cloud partition 14

Chapter 1

About this document

Purpose

This document aims to provide guidance on designing and deploying Enterprise Vault in Amazon Web Services (AWS) and Microsoft Azure Cloud. The purpose of this guide is to recommend best practices for creating Enterprise Vault partition to store archived files on Cloud storage.

This document should be used in conjunction with other performance and best practice guides, as outlined in the “Supporting documents” section of this document.

This guide also assumes you are familiar with how to configure and administer Enterprise Vault and associated products. You can obtain more detailed installation and configuration information from the Enterprise Vault documentation.

Intended Audience

This document is aimed at system administrators, solutions architects, and consultants. It is assumed that the reader has a thorough understanding of the architecture and operational aspects of Enterprise Vault. It is also assumed that the reader has experience and knowledge of AWS or Azure Cloud concepts.

Supporting documents

Use this guide in conjunction with the following documents:

- Enterprise Vault Performance Guide, which is available from the following page of the Veritas Support website:

  http://www.veritas.com/docs/100000918

- Enterprise Vault Compatibility Charts, which is available from the following page of the Veritas Support website:

  http://www.veritas.com/docs/000097605
- Enterprise Vault 14.1: SQL Best Practices Guide, which is available at the following location: http://www.veritas.com/docs/000021697
- Using Amazon Simple Storage Service (S3) as a primary storage for Enterprise Vault, which is available at the following location: https://www.veritas.com/support/en_US/doc/143662178-143662181-0
- Using Amazon Commercial Cloud Services (C2S) as a primary storage for Enterprise Vault, which is available at the following location: https://www.veritas.com/support/en_US/doc/143662328-143662331-0
- Using Microsoft Azure Blob Storage and Microsoft Azure Government Cloud as a primary storage for Enterprise Vault, which is available at the following location: https://www.veritas.com/support/en_US/doc/143662369-143662372-0

Chapter 2

Enterprise Vault Deployment in AWS

Enterprise Vault 14.1 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 cloud.

Enterprise Vault 14.1 supports Amazon S3 as a primary storage within Amazon Commercial Cloud Services (C2S), 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.

Veritas recommends deploying Enterprise Vault in AWS to get all the benefits that AWS provides for IaaS by using Cloud Native services.

For hybrid environments where Enterprise Vault is deployed on-premise and primary storage resides in the cloud, there would be a significant impact on archiving, indexing, and retrieval performance. Additionally, any retrieval will incur higher costs making the hybrid environment less optimal for Supervision and Discovery.

Choosing the right EC2 instance

Instance types comprise varying CPU combinations, memory, storage, and networking capacity and provide the flexibility to choose the appropriate mix of resources for your applications. Each instance type has one or more size options that address different workload sizes.

Amazon Elastic Compute Cloud (EC2) gives you the option of choosing between multiple instance types, distributed across instance families. You have the flexibility to select the combination of instance types and sizes most appropriate for your current application, and you can always change the type you use later as your business and application requirements change.

Several factors should be considered before choosing an EC2 instance for Enterprise Vault:

- Enterprise Vault is dependent on CPU resources. It is not unusual for the CPU to run at 90% or higher utilization while archiving is being performed in a typical server configuration—generally, the more powerful the processor, the better the ingestion and retrieval rates.
- The recommended CPU and memory configuration for Enterprise Vault is 8 CPU cores and 16 GB of RAM.

Based on the above considerations, Enterprise Vault recommends using the EC2 instance C5.2xlarge or higher.

Considerations for Enterprise Vault Amazon S3 partitions

You need to consider authentication methods and storage classes while creating Enterprise Vault partitions for Amazon S3.

Authentication

The following authentication methods are available for Amazon Simple Storage Service (S3) authentication:

- **Access Keys**: The Access Keys option is selected by default. Authentication is done using access key ID and secret access key that is provided by Amazon for programmatic (API) access to AWS services. This authentication mechanism is less recommended as access keys are long-term security credentials and stored with Enterprise Vault for a longer duration.
- **IAM Role**: Authentication is done using the IAM Role. This authentication method uses short-term security credentials obtained

using the role attached to the EC2 instance. This authentication method is highly recommended when Enterprise Vault runs on EC2 instance.

- **STS Assume Role**: Authentication is done using IAM user, IAM Role and STS service. This authentication method uses short-term credentials obtained using the role attached to specified IAM user. This authentication method is highly recommended when Enterprise Vault runs an on-premise server.

It is recommended using the IAM Role for partition on Amazon S3.

Note: When you create a partition for Amazon Simple Storage Service (S3), the data is stored in non-WORM mode by default. You can choose to create the partition for Amazon Simple Storage Service (S3) in WORM mode using S3 Object Lock feature of Amazon. In this case, you need to set additional permissions for the IAM Role and STS Assume Role authentication methods. For details, refer to Using Amazon Simple Storage Service (S3) as a primary storage for Enterprise Vault.

Storage class

Amazon S3 uses the following storage classes 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.

You can optimize the Amazon S3 storage cost by selecting an appropriate storage class for objects. You can also configure appropriate lifecycle management rules to move objects to different storage classes and expire them.

It is recommended using Standard storage class for best performance.

Replication

Archived files on cloud storage should be replicated so that there will be one more copy of archived files that could be used in disaster recovery.

It is recommended to use "When archived files are replicated on the cloud storage" option on Amazon S3 partition.

Ensure that replication is kept enabled on the cloud storage. If replication is disabled on cloud storage, there will be a significant increase in the number of unsecured items.

Note: Additional costs associated with replication will apply based on pricing by your cloud storage provider.

Chapter 3

Enterprise Vault Deployment in Azure Cloud

Enterprise Vault 14.1 supports Microsoft Azure Blob Storage as primary storage, letting you store primary archived data in the Azure public cloud and the 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 cloud network.

Veritas recommends deploying Enterprise Vault in Microsoft Azure Cloud to get all the benefits that Azure Cloud provides for IaaS by using Cloud Native services.

For hybrid environments where Enterprise Vault is deployed on-premise and primary storage resides in the cloud, there would be a significant impact on archiving, indexing, and retrieval performance. Additionally, any retrieval will incur higher costs making the hybrid environment less optimal for Supervision and Discovery.

Choosing the right Azure virtual machine

Azure virtual machine (VM) types comprise varying CPU combinations, memory, storage, and networking capacity and provide the flexibility to choose the appropriate mix of resources for your applications. Each VM type has one or more size options that address different workload sizes.

Azure gives you the option of choosing between multiple VM types, distributed across VM families. You have the flexibility to select the combination of VM types and sizes most appropriate for your application today, and you can always change the type you use later as your business and application requirements change.

Several factors should be considered before choosing a VM for Enterprise Vault:

- Enterprise Vault is dependent on CPU resources. It is not unusual for the CPU to run at 90% or higher utilization while archiving is being performed in a typical server configuration—generally, the more powerful the processor, the better the ingestion and retrieval rates.
- The recommended CPU and memory configuration for Enterprise Vault is 8 CPU cores and 16 GB RAM.

Based on the above considerations, it is recommended to use the F8s_v2 instance or higher.

Considerations for Enterprise Vault Azure Cloud partition

You need to consider access tier while creating Enterprise Vault partitions for Microsoft Azure Blob Storage and Microsoft Azure Government Cloud.

Access Tier

You can use the following access tier to store data:

- **Default** - used to infer account-level tiering.
- **Hot** - used if the data is frequently accessed.
- **Cool** - used if the data is infrequently accessed.

You can choose the access tier based on your business requirement. It is recommended to use Hot access tier for better performance.