Veritas InfoScale™ Enterprise AMI/CFT Deployment Guide - Linux

VERITAS™

Last updated: 2022-10-20

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054
http://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

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://sort.veritas.com/documents

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:
infoscaledocs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:
http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:
https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Veritas InfoScale Enterprise in the Amazon Web Services cloud

This document includes the following topics:

About Veritas InfoScale Enterprise

Veritas InfoScale Enterprise enables organizations to provision and manage storage, and provides high availability for business critical applications. Storage provisioning is independent of hardware types or locations with predictable quality-of-service by identifying and optimizing critical workloads. It increases storage agility enabling

you to work with and manage multiple types of storage to achieve better ROI without compromising on performance and flexibility. For application high availability, InfoScale Enterprise monitors an application to detect any application or node failure, and brings the application services up on a target system in case of a failure.

With Veritas InfoScale, you can now extend your workloads to the cloud with Amazon Web Services delivering resiliency, flexibility and performance at scale.

Some of the key features of Veritas InfoScale Enterprise include:

- Accelerated I/O performance using Veritas SmartIO technology. SmartIO uses instance store—SSD storage, the closest to compute as a data caching device to improve performance. You can use the SmartAssist tool to determine cache size and forecasting of performance gains for custom workloads.
- Efficient and cost-effective method to migrate data to cloud using Veritas SmartMove technology. SmartMove analyzes storage usage by looking up the file system (VxFS) metadata, and moving only relevant data to the cloud. This helps you to save on bandwidth and storage costs.
- Redefined storage performance and scalability potential using Veritas' Flexible Storage Sharing (FSS) technology. FSS enables to provision shared volumes or file systems on shared nothing architectures that redefine the storage, performance and scalability potential of your cloud infrastructure. FSS leverages Amazon Elastic Block Storage (EBS) volumes or instance store volumes to create shared storage in the cloud. By using FSS, you can form a cluster that can be configured within or across AZs in a single region. In the event of failures—node, storage, or Availability Zone— data will always be available. Organizations can even run multiple applications in a single FSS cluster and set up SLAs to ensure isolation among applications. This type of deployment unlocks valuable use cases such as running real time analytics on incoming transactional data, or fraud detection on credit card transactions.
- Availability of consistent copy of application data at a remote site to address data center break down using Veritas Volume Replicator (VVR). VVR provides volume and file level replication capabilities that ensures application data is replicated to a remote site (that includes AWS Availability Zones or regions) to protect against large-scale infrastructure outages. Using VVR data can be replicated from premise to cloud and from cloud to premise. With the help of VVR, you can leverage the cloud as a DR site.
- Increased application availability using Cluster Server (VCS). Cluster Server (VCS) connects multiple, independent systems into a management framework for increased availability. Each system, or node, runs its own operating system and cooperates at the software level to form a cluster. VCS links commodity hardware with intelligent software to provide application failover and control.

When a node or a monitored application fails, other nodes can take predefined actions to take over and bring up services elsewhere in the cluster.

VCS detects failure of an application by issuing specific commands, tests, or scripts to monitor the overall health of an application. VCS also determines the health of underlying resources by supporting the applications such as file systems and network interfaces. VCS uses a redundant network heartbeat to differentiate between the loss of a system and the loss of communication between systems. VCS can also use SCSI3-based membership coordination and data protection for detecting failure on a node and on fencing.

About the InfoScale Enterprise AMI and its deployment using AWS CFTs

Veritas InfoScale provides an Amazon Machine Image (AMI) that can be used to deploy InfoScale Enterprise in an Amazon Web Services (AWS) cloud. The InfoScale Enterprise AMI consists of Red Hat Enterprise Linux (RHEL) 8.4 and InfoScale Enterprise 8.0 binaries. The deployment requires you to bring your own licenses for RHEL and InfoScale Enterprise.

Using this version of InfoScale Enterprise (available on AWS Marketplace) you can deploy an InfoScale Enterprise cluster using any of the following fulfillment methods:

- Amazon Machine Image (AMI)
  For configuring InfoScale Enterprise using AMI, use the Veritas Product Installer. For more details, refer to the product documentation.
  https://sort.veritas.com/documents
- AWS CloudFormation Template
  The CloudFormation template provides an automated deployment of Veritas InfoScale Enterprise on Amazon Web Services (AWS) cloud. The templates set up and configure the AWS environment for Veritas InfoScale with essential AWS resources— Amazon Elastic Compute Cloud (EC2) instances, Amazon Virtual Private Cloud (VPC), Elastic Network Interfaces (ENICs), and Elastic Block Storage (EBS).

  The templates perform the following configuration tasks:

  - Deploys the Amazon Elastic Compute Cloud (EC2) instances on the selected number of Availability Zones (AZs) on the cloud.
  - Configures the necessary storage and network resources in the Virtual Private Cloud
  - Configures an Veritas InfoScale Enterprise cluster (up to 8 nodes) on the cloud

This deployment guide provides instructions for deploying Veritas InfoScale Enterprise on the AWS cloud by using AWS CloudFormation templates.

The intended audience for this guide includes storage administrators, architects, and system administrators who are planning to deploy the Veritas InfoScale Enterprise solution on the AWS cloud.

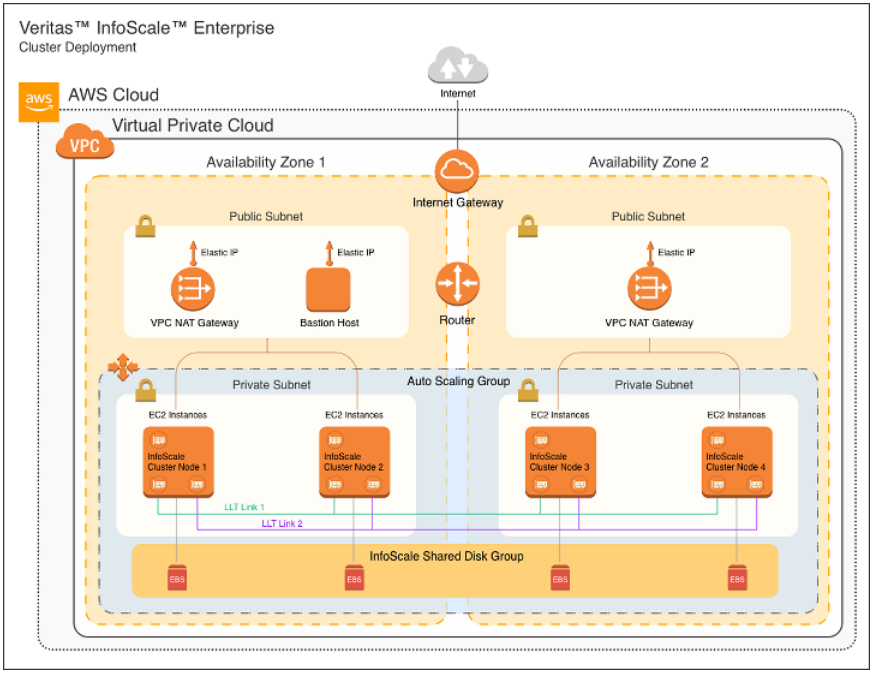
About the deployment scenarios and architecture

You can deploy Veritas InfoScale Enterprise using the AWS CFT to set up an InfoScale cluster in a same AZ or across two AZs. In case of two AZs, the AZs selection will be done automatically and from the same region.

This deployment can be implemented in an existing VPC or a new VPC.

The following diagram depicts the Veritas InfoScale Enterprise deployment in an AWS cloud for an InfoScale cluster.

Figure 1-1 Illustrates Veritas InfoScale Enterprise in AWS environments (without disaster recovery setup)



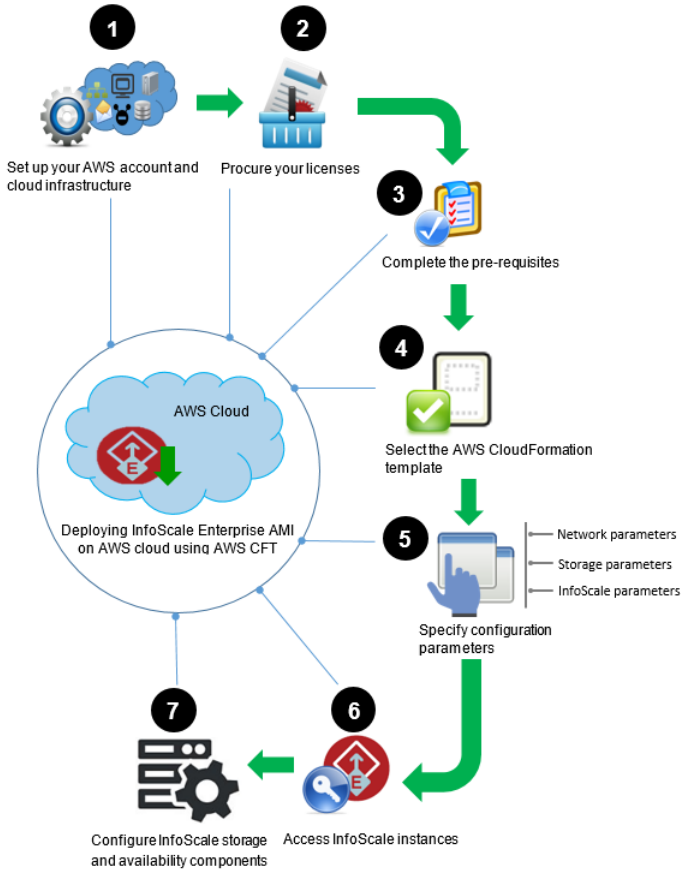
Deploying InfoScale cluster in a same AZ or across two AZs

Use the CFT to deploy an InfoScale cluster across AZs, in an existing VPC or a new VPC. For this deployment, the AZs from the same region gets selected.

Deployment of InfoScale cluster requires you to set various Network, Storage, and Security parameters. Depending on whether you are deploying the cluster in an existing VPC or a new VPC, the parameters may change.

The end-to-end workflow for deploying the cluster consists of the following steps:

Figure 1-2 Workflow for deploying InfoScale Enterprise in a same AZ or across AZ



Deployment steps

The procedure for an end-to-end deployment of Veritas InfoScale on AWS consists of the following steps:

1. See “Step 1: Complete the pre-requisites” on page 9.
2. See “Step 2: Prepare your AWS account” on page 12.
3. See “Step 3: Launch the stack” on page 12.
4. See “Step 4: Access Veritas InfoScale nodes” on page 24.
5. See “Step 5: Perform post-deployment tasks” on page 25.

The InfoScale AMI is currently available in the following regions:

Bahrain	Ohio
Canada (Central)	Oregon
Franfurt	Osaka
Hong Kong	Paris
Ireland	Seoul
London	Singapore
Mumbai	South America
N. California	Stockholm
N. Virgina	Sydney
	Tokyo

Step 1: Complete the pre-requisites

To deploy Veritas InfoScale Enterprise on an AWS cloud requires you to set up the cloud infrastructure, and the storage and network infrastructure as a pre-requisite.

The following table lists the basic requirements that must be satisfied to deploy InfoScale Enterprise, on an AWS cloud:

Table 1-1 Pre-requisites for deploying Veritas InfoScale Enterprise on an AWS cloud

Settings type	Requirement
Network	When you set up your cloud network, ensure that you consider the following requirements: ■ Configure EBS-optimized instances for better performance. This optimization provides the best performance for your EBS volumes by minimizing contention between Amazon EBS I/O and other traffic from your instances. ■ Enable enhanced networking on EC2 instances for high network performance and reduced latencies. ■ If you are deploying InfoScale Enterprise in an existing VPC, when you configure a hostname, select **Yes** to enable DNS hostname.
Storage	For efficient and fast storage, you use IO1 or instance store volumes. Keep in mind the limitations and specific use cases of these storage types.
Security	If you are deploying InfoScale Enterprise in an existing VPC, enable the SSH (22) and ALL UDP protocol types with the existing VPC CIDR as the source.
Resource Management	Plan to increase any instance or storage-related limit in advance.
Permissions	Ensure that your user account has all the required permissions on the available resources. See Table 1-2 on page 10.

Table 1-2 Resource and required permissions

Resource	Required permissions
s3	All permissions (*)
ec2	All permissions (*)
autoscaling	All permissions (*)

Table 1-2 Resource and required permissions *(continued)*

Resource	Required permissions
cloudformation	■ DescribeStacks ■ DescribeStackEvents ■ DescribeStackResource ■ DescribeStackResources ■ GetTemplate ■ List* ■ CreateStack ■ UpdateStack
events	■ PutRule ■ PutTargets ■ ListRules ■ ListTargetsByRule
iam	■ CreatePolicy ■ CreateRole ■ AttachRolePolicy ■ PassRole
ssm	■ DescribeAssociation ■ GetDeployablePatchSnapshotForInstance ■ GetDocument ■ GetParameters ■ ListAssociations ■ ListInstanceAssociations ■ PutInventory ■ UpdateAssociationStatus ■ UpdateInstanceAssociationStatus ■ UpdateInstanceInformation
ec2messages	■ AcknowledgeMessage ■ DeleteMessage ■ FailMessage ■ GetEndpoint ■ GetMessages ■ SendReply

Step 2: Prepare your AWS account

This involves signing up for an AWS account, choosing a region, creating a key pair, and requesting increases for account limits, if necessary.

To prepare your AWS account

1. If you don't already have an AWS account, create one at http://aws.amazon.com by following the on-screen instructions. Part of the sign-up process involves receiving a phone call and entering a PIN using the phone keypad.
2. Use the region selector in the navigation bar to choose the Amazon EC2 region where you want to deploy Veritas InfoScale Enterprise on AWS.

   Amazon EC2 locations are composed of Regions and Availability Zones. Regions are dispersed and located in separate geographic areas.

   Note: Consider choosing a region closest to your data center or corporate network to reduce network latency between systems running on AWS and the systems and users on your corporate network.

3. Create a key pair in your preferred region. To do this, in the navigation pane of the Amazon EC2 console, choose **Key Pairs**, **Create Key Pair**, type a name, and then choose **Create**.

   Amazon EC2 uses public-key cryptography to encrypt and decrypt login information. To be able to log into your instances, you must create a key pair. On Linux, we use the key pair to authenticate SSH login.
4. (Production deployments only): If necessary, request a service limit increase for the instance type you're using. If you already have an existing deployment that uses this instance type, and you think you might exceed the default limit with this reference deployment you will need to request an increase. To do this, in the AWS Support Center, choose **Create Case**, **Service Limit Increase**, **EC2 instances**, and then complete the fields in the limit increase form. It might take a few days for the new service limit to become effective.

   For more information, see Amazon EC2 Service Limits in the AWS documentation.

Step 3: Launch the stack

This section contains general instructions for deploying Veritas InfoScale in AWS cloud.

Note: To create the stack in the cloud, you must first subscribe to *Veritas InfoScale Enterprise for AWS BYOL* on the AWS Marketplace.

To launch the stack

1. Go to AWS Marketplace at https://aws.amazon.com/marketplace.
2. Browse the products or search to find **Veritas InfoScale Enterprise for AWS BYOL**.
3. Click the product link to view the product details page.
4. Click **Continue to Configure**.
5. In the **Fulfillment Option** list, select **Cloud Formation**.
6. In the drop-down list that appears, you can choose to deploy the cluster in a new VPC or an existing VPC.

   Note that this selection impacts the URL for the AWS CloudFormation template.

   The **Software version** and **Region** fields display the version of Veritas InfoScale Enterprise software and the region of the network infrastructure where InfoScale will be deployed.
7. (Optional) Change the region.
8. Click **Continue to Launch**.
9. On the Launch this software page, select **Launch CloudFormation** to launch your configuration through AWS CloudFormation console.
10. Click **Launch**.

    The appropriate URL for the AWS CloudFormation template is automatically populated in the **Specify an Amazon S3 template URL** field.
11. Click **Next**.

12 On the **Specify Details** page, change the stack name if needed. Review the parameters for the template. Provide values for the parameters that require input. For all other parameters, review the default settings and customize them as necessary. When you finish reviewing and customizing the parameters, choose **Next**.

The parameters are grouped by category.

Deployment type	Parameters
New VPC	See "Network configuration parameters for a new VPC" on page 15.
	See "Server, storage, and security configuration parameters for a new VPC" on page 17.
	See "Veritas InfoScale cluster configuration parameters- New VPC" on page 18.
Existing VPC	See "Network configuration parameters for an existing VPC" on page 20.
	See "Server, storage, and security configuration parameters for an existing VPC" on page 21.
	See "Veritas InfoScale cluster configuration parameters- Existing VPC" on page 23.

13 On the **Options** page, specify tags (key-value pairs) for resources in your stack and set additional options. When you're done, click **Next**.

14 On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the checkbox to acknowledge that the template will create IAM resources.

15 Click **Create** to deploy the stack.

16 Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the resources defined in the CFT are configured and the cluster configuration script is triggered.

To verify if the cluster configuration is complete, log on to any of the cluster node and run the following command:

```
gabconfig -a
```

Parameters for deploying Veritas InfoScale Enterprise on a new VPC

Provide the following information for deploying Veritas InfoScale Enterprise in a new VPC.

Table 1-3 Parameters for deploying Veritas InfoScale Enterprise in a new VPC

Network configuration parameters	See "Network configuration parameters for a new VPC" on page 15.
Server and storage configuration parameters	See "Server, storage, and security configuration parameters for a new VPC" on page 17.
Veritas InfoScale configuration parameters	See "Veritas InfoScale cluster configuration parameters- New VPC" on page 18.

Network configuration parameters for a new VPC

Table 1-4 Network configuration parameters for deploying InfoScale Enterprise using AWS CFT- New VPC

Parameter name	Parameter label	Default value	Description
VPC CIDR	VPCCIDR	Requires user input	Specify a New VPC CIDR block for Veritas InfoScale cluster.
NumberOfAZs	NumberOfAZs	1	Select the number of AvailabilityZones required for InfoScale product deployment. Allowed values are 1 and 2.
First Availability Zone (AZ1) network parameters			
DMZ subnet CIDR	AZ1DMZCIDR	Requires user input	CIDR Block for DMZ subnet in AZ1.
eth0 subnet CIDR	AZ1PubCIDR0	Requires user input	CIDR Block for Public Subnet of EC2 in the AZ1. For example, x.x.x.0/24

Table 1-4 Network configuration parameters for deploying InfoScale Enterprise using AWS CFT- New VPC *(continued)*

Parameter name	Parameter label	Default value	Description
LLT link1 subnet CIDR	AZ1PrivCIDR1	Requires user input	CIDR Block for Private Subnet1 for EC2. For example, x.x.x.0/24
LLT link2 subnet CIDR	AZ1PrivCIDR2	Requires user input	CIDR Block for Private Subnet2 for EC2. For example, x.x.x.0/24
Second Availability Zone (AZ2) network parameters **Note:** These parameters are required only if you are deploying the cluster across two AZs. For cluster deployment in a single AZ, you must not specify these parameters.			
DMZ subnet CIDR	AZ2DMZCIDR	Requires user input	CIDR Block for DMZ subnet in AZ2.
eth0 subnet CIDR	AZ2PubCIDR0	Requires user input	CIDR Block for Public Subnet in AZ2. For example, x.x.x.0/24
LLT link1 subnet CIDR	AZ2PrivCIDR1	Requires user input	CIDR Block for Private Subnet1 in AZ2. For example, x.x.x.0/24
LLT link2 subnet CIDR	AZ2PrivCIDR2	Requires user input	CIDR Block for Private Subnet2 in AZ2. For example, x.x.x.0/24

Server, storage, and security configuration parameters for a new VPC

Table 1-5 Server, storage, and security parameters for deploying InfoScale Enterprise using AWS CFT in a new VPC

Parameter name	Parameter label	Default value	Description
Management server instance type	BastionInstanceType	t2.micro	Amazon EC2 instance type for the management server.
EC2 instance type for InfoScale cluster	VeritasInstanceType	m4.4xlarge	Amazon EC2 instance type for the Veritas InfoScale cluster node.
EC2 instances in InfoScale cluster	HostCount	2	Number of hosts in Veritas InfoScale cluster.
Volume type	VolumeType	standard	Select volume type. ■ gp2, for General Purpose SSD ■ st1, for Throughput Optimized HDD ■ sc1, for Cold HDD ■ standard, for Magnetic volumes
Volume size (in GB)	VolumeSize	1	Volume size for each instance in GB. MinValue=0, MaxValue = 16384
Number of volumes	VolumeCount	2	Number of volumes for each cluster node. The permitted number of volumes for each node is 0 to 8.

Table 1-5 Server, storage, and security parameters for deploying InfoScale Enterprise using AWS CFT in a new VPC *(continued)*

Parameter name	Parameter label	Default value	Description
Security key-pair	KeyPairName	Requires user input	Public/private key pair, which allows you to connect securely to the instances. The key-pair is created when you create your AWS account.
CIDR block for remote access	RemoteAccessCIDR	Requires user input	CIDR block from where you can access the management server. For example, x.x.x.x/32

Veritas InfoScale cluster configuration parameters- New VPC

Table 1-6 Veritas InfoScale cluster configuration parameters for deploying InfoScale Enterprise using AWS CFT- New VPC

Parameter name	Parameter label	Default value	Description
InfoScale component	Component	SFCFSHA	InfoScale component to be configured: VCS, SFHA, and SFCFSHA. **Note:** SF Oracle RAC and SF Sybase CE are not supported in AWS.

Table 1-6 Veritas InfoScale cluster configuration parameters for deploying InfoScale Enterprise using AWS CFT- New VPC *(continued)*

Parameter name	Parameter label	Default value	Description
InfoScale cluster name	ClusName	Requires user input	A unique cluster name. The cluster name must begin with any letter between a-z or A-Z. Only letters, numbers, hyphens (-), and underscores (_) are allowed in a cluster name.
Virtual IP address	AWSIP	Requires user input	Vitual IP (VIP) address for InfoScale cluster. **Note:** If you are deploying the cluster in the same AZ, VIP must be in the same subnet as eth0. However, if the cluster deployment spans across two AZs, the VIP must be beyond the VPC range.
License key	InfoScaleLicense	Keyless	A valid Veritas InfoScale Enterprise permanent license. Keyless license will be applied if no input is provided.

Parameters for deploying Veritas InfoScale Enterprise in an existing VPC

Provide the following information for deploying Veritas InfoScale Enterprise in an existing VPC.

Table 1-7 Parameters for deploying Veritas InfoScale Enterprise in an existing VPC

Network configuration parameters	See "Network configuration parameters for an existing VPC" on page 20.
Server and storage configuration parameters	See "Server, storage, and security configuration parameters for an existing VPC" on page 21.
InfoScale configuration parameters	See "Veritas InfoScale cluster configuration parameters-Existing VPC" on page 23.

Network configuration parameters for an existing VPC

Table 1-8 Network configuration parameters for deploying InfoScale Enterprise using AWS CFT- Existing VPC

Parameter name	Parameter label	Default value	Description
VPC	VPCCIDR	Requires user input	Choose a VPC ID.
NumberOfAZs	NumberOfAZs	1	Select the number of AvailabilityZones required for InfoScale product deployment. Allowed values are 1 and 2.
First Availability Zone (AZ1) network parameters			
DMZ subnet ID	AZ1DMZCIDR	Requires user input	CIDR Block for DMZ subnet in AZ1.
eth0 subnet CIDR	AZ1PubCIDR0	Requires user input	CIDR Block for eth0 in AZ1. For example, x.x.x.0/24
LLT link1 subnet CIDR	AZ1PrivCIDR1	Requires user input	CIDR Block for LLT link 1 AZ1. For example, x.x.x.0/24
LLT link2 subnet CIDR	AZ1PrivCIDR2	Requires user input	CIDR Block for LLT link 2 in AZ1. For example, x.x.x.0/24

Table 1-8 Network configuration parameters for deploying InfoScale Enterprise using AWS CFT- Existing VPC *(continued)*

Parameter name	Parameter label	Default value	Description
Second Availability Zone (AZ2) network parameters **Note:** These parameters are required only if you are deploying the cluster across two AZs. For cluster deployment in a single AZ, you must not specify these parameters.			
DMZ subnet CIDR	AZ2DMZCIDR	Requires user input	CIDR Block for DMZ subnet in AZ2.
eth0 subnet CIDR	AZ2PubCIDR0	Requires user input	CIDR Block for eth0 in AZ2. For example, x.x.x.0/24
LLT link1 subnet CIDR	AZ2PrivCIDR1	Requires user input	CIDR Block for LLT link 1 in AZ2. For example, x.x.x.0/24
LLT link2 subnet CIDR	AZ2PrivCIDR2	Requires user input	CIDR Block for LLT link 2 in AZ2. For example, x.x.x.0/24

Server, storage, and security configuration parameters for an existing VPC

Table 1-9 Server, storage, and security configuration parameters for deploying InfoScale Enterprise using AWS CFT

Parameter name	Parameter label	Default value	Description
Management server instance type	BastionInstanceType	t2.micro	EC2 instance type for the management server.
EC2 instance type for InfoScale cluster	VeritasInstanceType	m4.4xlarge	EC2 instance type for the Veritas InfoScale cluster node.
EC2 instances in InfoScale cluster	HostCount	2	Number of hosts in InfoScale cluster.

Table 1-9 Server, storage, and security configuration parameters for deploying InfoScale Enterprise using AWS CFT *(continued)*

Parameter name	Parameter label	Default value	Description
Volume type	VolumeType	standard	Select volume type. ■ gp2, for General Purpose SSD ■ st1, for Throughput Optimized HDD ■ sc1, for Cold HDD ■ standard, for Magnetic volumes
Volume size (in GB)	VolumeSize	1	The volume size for each instance in GB; MinValue=0, MaxValue = 16384.
Number of volumes	VolumeCount	2	Number of volumes for each cluster node. The permitted number of volumes for each node is 0 to 8.
Security key-pair	KeyPairName	Requires user input	Public/private key pair, which allows you to connect securely to the instance. The key pair is created when you create your AWS account.
Security group	SecurityGroupID	Requires user input	Choose a Security Group ID.

Veritas InfoScale cluster configuration parameters- Existing VPC

Table 1-10 Veritas InfoScale configuration parameters for deploying InfoScale Enterprise using AWS CFT- Existing VPC

Parameter name	Parameter label	Default value	Description
InfoScale component	Component	SFCFSHA	InfoScale component to be configured: VCS, SFHA, and SFCFSHA. **Note:** SF Oracle RAC and SF Sybase CE are not supported in AWS.
InfoScale cluster name	ClusName	Requires user input	A unique cluster name. The cluster name must begin with any letter between a-z or A-Z. Only letters, numbers, hyphens (-), and underscores (_) are allowed in a cluster name.
Virtual IP address	AWSIP	Requires user input	Vitual IP (VIP) address for the InfoScale cluster. **Note:** If you are deploying the cluster in the same AZ, VIP must be in the same subnet as eth0. However, if the cluster deployment spans across two AZs, the VIP must be beyond the VPC range.

Table 1-10 Veritas InfoScale configuration parameters for deploying InfoScale Enterprise using AWS CFT- Existing VPC *(continued)*

Parameter name	Parameter label	Default value	Description
License key	InfoScaleLicense	Keyless	A valid Veritas InfoScale Enterprise permanent license. Keyless license is used if you do not enter a valid license.

Step 4: Access Veritas InfoScale nodes

Perform the following steps to access the Veritas InfoScale Enterprise instances.

To access the Veritas InfoScale Enterprise instances

1 Transfer PEM/Private key file to the management server.

```
# scp -i pem_file -r pem_file
ec2-user@managementServerEIP:/home/ec2-user
```

2 Log in to the management server.

Specify the following SSH command with the path to the private key (`.pem`) file and the appropriate user name. The user name is `ec2-user`.

```
# ssh -i pem_file ec2-user@managementServerEIP.
```

3 From the management server login to any of the cluster nodes:

```
# ssh -i pem_file ec2-user@clusterHostEth0IP
```

Note: For a new VPC, the management server is accessible only from “Remote Access CIDR” host(s) that was entered during CFT deployment.

For Existing VPC, a management server is accessible as per rules of the “Security Group” selected during CFT deployment.

4 Change the ownership of the login session to `root`.

```
# sudo su
```

5 Verify the GAB port membership.

```
# gabconfig -a
```

6 Verify the status of the cluster.

```
# hastatus -summary
```

Step 5: Perform post-deployment tasks

After you have successfully deployed InfoScale Enterprise, you must proceed to configure the storage resources and the other required components.

Refer to the InfoScale Enterprise product documentation for details about configuring the storage and application availability resources:

https://sort.veritas.com/documents/

Adding or deleting nodes from an InfoScale cluster

Use the AWS Autoscaling feature to add or delete nodes from an InfoScale cluster, that is deployed using AWS CFT.

You can add or delete nodes from an existing InfoScale cluster, using any of the following method:

- Defining autoscaling policies
  Autoscaling policies enable you to automate the process of adding or deleting nodes to the InfoScale cluster. AWS provides various metric types to define a custom policy. When the policy criteria is met, specified number of nodes are added to the cluster.
  Use this method to add or delete the desired number of nodes, only when a certain criterion is met.
  For details about Autoscaling and creating scaling policies, refer to AWS documentation.
- Manually updating the instance count
  Using the AWS Autoscaling feature, you can manually specify the number of nodes that you may want to add or delete from an InfoScale cluster.
  Use this method to add or delete nodes at any given point in time.

To add or delete a node from an InfoScale cluster using autoscaling policies:

1 Open the Cloud Formation Console page.

2 Select the region in which you have deployed the CFT.

3 From the left menu, select Auto Scaling Groups.

4 On the right hand side, in the upper pane, select the CFT that you had created.

5 In the lower pane, select the Details tab and click **Edit**.

6 Edit the Desired and the Max number of instances to a desired value.

7 Select the Scaling Policies tab.

8 Specify the required details in the available fields.

For details about the available fields, refer to AWS documentation.

9 Click **Create**.

When the specified criteria is met, the policy is triggered and the specified number of nodes are added to the cluster.

To add or delete a node from an InfoScale cluster, by manually updating the instance count

1 Open the Cloud Formation Console page.

2 Select the region in which you have deployed the CFT.

3 From the left menu, select Auto Scaling Groups.

4 On the right hand side, in the upper pane, select the CFT that you had created.

5 In the lower pane, select the Details tab and click **Edit**.

6 Edit the Desired, Min, and the Max number of instances to a desired value.

7 Click **Save**.

Deleting an InfoScale cluster

Perform the following steps to delete an InfoScale cluster

1 Open the Cloud Formation Console page.

2 Select the stack to be deleted.

3 From the Actions drop-down list, select **Delete Stack**.

4 Delete the non-root volumes created, if any.

To delete the non-root volumes, open the EC2 Console page, and from the left menu select **Volumes**. From the list of volumes displayed in the right pane, select the non-root volumes that are applicable for the deleted stack, and from the Actions drop-down list, select **Delete Volumes**.

5 Delete the CloudWatch rules created, if any.

To delete the CloudWatch rules, open the CloudWatch Console page, and from the left menu select **Rules**. From the list of rules displayed in the right pane, select the ones that are applicable for the deleted stack, and from the Actions drop-down list, select **Delete**.

Troubleshooting

If you run into issues while deploying Veritas InfoScale Enterprise, contact Veritas Technical Support at:

https://www.veritas.com/support

Resources

AWS Services

- AWS CloudFormation documentation
- Amazon EBS
  User Guide
  Volume types
  Optimized instances
- Amazon EC2 user guide for Linux
- Amazon VPC

Veritas InfoScale documents

Documentation

Quick Start reference deployments

AWS Quick Start

Feedback

We welcome your questions and comments. Please post your feedback on the AWS Quick Start Discussion Forum.