Veritas InfoScale 7.3.1 What's New Guide - Windows

VERITAS™

Last updated: 2017-11-05

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

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:

doc.feedback@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

What's new in this release of Veritas InfoScale

This document includes the following topics:

About this document

The Veritas InfoScale products are used for enterprise data management and protection, high availability, and disaster recovery. This document describes the new features, enhancements, and changes that are introduced in the 7.3.1 release of the Veritas InfoScale products.

The following documents provide further information that is common to all the InfoScale products:

- *Veritas InfoScale Getting Started Guide*
- *Veritas InfoScale Release Notes*
- *Veritas InfoScale Installation and Upgrade Guide*

For information about the InfoScale product components and their capabilities, refer to the corresponding administrator's guides and agent guides.

For information about configuring and administering your applications with the InfoScale products, refer to the application-specific implementation guides and solutions guides.

New features and changes in this release

This section describes the new features and changes that are introduced in this release.

Change in upgrade path

You can upgrade to Veritas InfoScale 7.3.1 only if the base version of your currently installed product is 6.1 or later.

For more information, see *Veritas InfoScale Installation and Upgrade Guide - Windows*.

256-bit encryption for enhanced security

The Cluster Server component now provides 256-bit encryption for enhanced security. The `vcsencrypt` utility, which you use to generated encrypted VCS and agent passwords, now generates 256-bit encrypted passwords.

For more information, see the *Cluster Server Administrator's Guide*.

The NIC and the IP agents can monitor network adapters based on GUID

The NIC and the IP agents can now use the network adapter GUID to monitor the NIC and the IP resources. This enhancement is useful in the following scenario where the public network is used for a VCS cluster:

- The NIC interface name is used for the **MACAddress** attribute on the physical systems that use NIC teaming.
- A tenant controls the NIC interface name, and it may be changed for various reasons without knowing how it affects VCS clusters.
- Enforcing the use of a naming convention for the interface or preventing a person or a system from renaming the NIC is not possible.

You can now set the MACAddress attribute of the NIC and the IP agents to the GUID of the network adapter. The agents can then monitor the resource based on the GUID. In scenarios like the one mentioned earlier, you can use the GUID, instead of the interface name, to monitor the public network in a VCS cluster.

Updated auto-import functionality of dynamic disk groups

The auto-import functionality of dynamic disk groups was modified in the InfoScale 7.2 release. This functionality is now re-modified.

Prior to 7.2 release the vxboot driver was used to auto-import the dynamic disk groups when a machine was restarted. The vxboot driver was deprecated in the 7.2 release, and the Veritas DG Delayed Import Service (VxDgDI) was used to manage the auto-import of dynamic disk groups. VxDgDI service is an automatic service and starts as soon as an operating system restarts. It imports the dynamic disk groups after an operating system restarts.

With this release, the vxboot driver is re-included and it auto-imports the dynamic disk groups when a machine restarts. In the event of a scenario where the dynamic disk groups are not imported during the machine restart, the VxDgDI service import them after the operating system restarts.

The vxboot driver has been re-included to address the cases where service dependencies are not defined for an application that is installed on VxVM volumes. In such cases, it was observed that after a system restart the services may fail to start and a manual intervention may be required to start the services.

VxVM support for hardware cloning

Advanced disk arrays provide methods to create clones or copies of physical volumes (disks or LUNs) from the hardware-side. Using the hardware cloning technology, you can create a hardware snapshot (such as an EMC BCV™ or Hitachi ShadowImage™), a hardware mirror, or a hardware clone.

If a disk that you plan to clone is under SFW control, the data that is stored in the private region of the disk is also copied. As a result, the disk id in the private region of the original disk and the cloned disk remains same. Also, the VxVM disk group becomes a duplicate of the original disk group.

In order to identify a cloned disk, a unique and persistent attribute called the Veritas Device Identifier (VDID) is added to the private region of every disk. For a disk in which the original VDID differs from the one in the private region, a vdid_mismatch flag or a "shadow" flag is added to the private region. Such a disk is considered as a cloned disk.

Now, if standard (non-cloned) disks in a disk group are already imported, you cannot simultaneously import the cloned disks in the same disk group. VxVM does not support a disk group with both clone and non-clone disks. If you want to import the cloned disks, you must specify a new disk group name for the disk group containing the cloned disks. During the import process, the vdid_mismatch flag and the shadow flag are cleared from the disks in the new disk group. The new disk group becomes a standard disk group, and the disks become the standard disks.

Notes:

- The functionality to import a cloned disk group is disabled by default. To enable the functionality, you must set the SupportVDIDTOC registry key value to 1, and then restart the vxsvc service.
  The SupportVDIDTOC registry key is located under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vxboot\VDID.
- Currently, you cannot import a cloned disk group if your disk groups contains volume layout type Mirrored with Stripped.
- If the process to import a cloned disk group fails or if you intend to import a cloned disk group on a new host, you must first update the VDID in the private region and then import the disk group.

For more details about importing a cloned disk group and updating the VDID, see *Storage Foundation 7.3.1 Administrator's Guide-Windows*.

Added support for DMP DSMs

Veritas InfoScale provides support for the following arrays:

- KMNRIO(VKMNRIO)
- NexentaStor(VNEXENTA)
- NIMBLE(VNIMBLE)

The product installer lists these DSMs as selectable options, on the **System Selection** page.

Note: These options are available only if you are installing InfoScale Foundation, Veritas InfoScale Storage,or InfoScale Enterprise.

If your deployment setup includes any of these arrays, then you must select the respective option during the product installation. The installer installs the required drivers for the selected array.

Support for Veritas InfoScale Storage deployments on Amazon Web Services (AWS) cloud

Veritas InfoScale can now be deployed in AWS cloud environment. The Veritas replication technology in tandem with cloud services offer scalable, cost-effective disaster recovery options for your business.

With Veritas Volume Replicator (VVR), you can leverage the cloud as a DR site and replicate data to or within cloud without incurring the infrastructural costs that are needed to maintain a second physical site.

Veritas InfoScale deployments in cloud support the following scenarios to replicate data:

- Replication from an on-premise data center to an on-cloud data center
- Replication within a region
- Replication across regions

For more details about configuring replication in cloud environments, refer to *Volume Replicator Administrator's Guide*.

Support for setting up replication across clouds

Veritas replication technology can now be used to set up replication across AWS and Azure cloud.

With Veritas Volume Replicator (VVR), you can leverage one of the cloud setup as an on-premise data center and the other cloud as a DR site to replicate data across the two clouds.

For details about setting up replication across cloud, refer to *Volume Replicator Administrator's Guide*.

Support for configuring applications for HA in Azure cloud using InfoScale Enterprise

InfoScale Enterprise lets you configure applications for HA and disaster recovery (DR) in Azure cloud environment.

The following scenarios are supported:

- Failover within the same subnet using a private IP
- Failover across the subnets using an overlay IP
- Public access to the cluster nodes in an Azure environment using a public IP
- DR across Azure Regions or VNets, and from the on-premises cluster to Azure

For more information, refer to the following documents:

- *Cluster Server Bundled Agents Reference Guide - Windows*
- *Cluster Server Administrator's Guide - Windows*
- *Volume Replicator Administrator's Guide -Windows*

New High Availability agents for Azure environment

Veritas has introduced the following high availability agents for Azure:

- AzureDisk agent
- AzureIP agent
- AzureDNSZone agent
- AzureAuth agent

These agents are bundled with the product.

AzureDisk agent

The AzureDisk agent brings online, takes offline, and monitors the managed and un-managed Azure data disks. It attaches the managed and un-managed data disks to a virtual machine of the same or different resource group. The AzureDisk agent uses Azure Python SDK to determine whether the Azure data disks are attached to the Azure virtual machines or not.

AzureIP agent

The AzureIP agent manages the networking resources in an Azure environment. The agent uses Azure Python APIs to associate IP resources in an Azure VM.

The agent does the following:

- Gets the NIC details, creates the configuration, and associates or disassociates the private IP address.
- Associates or disassociates the public IP address, with the private IP address.
- Manages the route table entries of overlay IP, for failing over across the subnets.

AzureDNSZone agent

The AzureDNSZone agent monitors and updates the host name to resource record mapping. This agent does the mapping for the Azure DNS domain when failing over to the nodes across the subnets or the regions.

AzureDNSZone agent provides DNS-based traffic routing and failover.

Use this agent, if the resource records need to be dynamically added and deleted from the domain during failover. This agent updates the new resource record mappings while failing over, and allows the clients to connect to the failed over instance of the application.

AzureAuth agent

AzureAuth agent authenticates the Azure subscription using the Service Principal credentials. This agent is a persistent resource that monitors the validity of Service Principal credentials.

Support for configuring applications for HA in AWS cloud using InfoScale Enterprise

InfoScale Enterprise lets you configure applications for HA and disaster recovery (DR) in AWS cloud environment.

The following scenarios are supported:

- Failover within the same subnet of an availability zone (AZ) using a virtual private IP
- Failover across the subnets within a single AZ using an overlay IP
- Failover across the multiple AZs using an overlay IP

For more information, see the following documents:

- *Cluster Server Bundled Agents Reference Guide - Windows*
- *Cluster Server Administrator's Guide - Windows*
- *Volume Replicator Administrator's Guide - Windows*

New High Availability agent for Amazon Web Services (AWS)

Veritas has introduced the AWSIP agent for AWS. This agent is bundled with the product.

AWSIP agent

The AWSIP agent manages the networking resources in an Amazon Web Services (AWS) cloud environment. The agent uses AWS CLIs to associate IP resources in an AWS cloud environment. The agent does the following:

- Assigns or un-assigns the private IP address.
- Associates or disassociates the Elastic IP address, and assigns or un-assigns the private IP address.
- Manages the route table entries of overlay IP, for failing over across the subnets.