Storage Foundation and High Availability Solutions [7.3.1] HA and DR Solutions Guide for Microsoft SharePoint 2013 - Windows

VERITAS™

Last updated: 2017-11-05

Legal Notice

Copyright © 2017 Veritas Technologies LLC. All rights reserved.

Veritas and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third party software for which Veritas is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the third party legal notices document accompanying this Veritas product or available at:

https://www.veritas.com/about/legal/license-agreements

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. VERITAS TECHNOLOGIES LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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

Contents

Chapter 1 Introducing the VCS agent for SharePoint Server 2013 6

About high availability support for SharePoint Server 6
About the [VCS] agent for Microsoft SharePoint Server 2013 7
SharePoint Server agent functions 7
SharePoint Server agent state definitions 8
SharePoint Server agent resource type definition 8
SharePoint Server agent attribute definitions 9

Chapter 2 Installing and configuring the [InfoScale Enterprise] product 13

About installing the product 13
About configuring the cluster 13

Chapter 3 Installing and configuring SharePoint Server 2013 for high availability 15

About installing and configuring [SharePoint] 15
Configuring 64-bit Perl for [SharePoint] 16
About configuring [SharePoint] service groups 16
Before you configure a SharePoint service group 17
Creating a SharePoint service group 18
Verifying the [SharePoint] cluster configuration 20
Considerations when modifying a SharePoint service group 21

Appendix A Using Veritas AppProtect for vSphere 23

About Just In Time Availability 24
Prerequisites 28
Setting up a plan 30
Deleting a plan 32
Managing a plan 32
Viewing the history tab 34
Limitations of Just In Time Availability 34
Getting started with Just In Time Availability 35

Supported operating systems and configurations 37
Viewing the properties 38
Log files 38
Plan states 39
Troubleshooting Just In Time Availability 41

Chapter 1

Introducing the VCS agent for SharePoint Server 2013

This chapter includes the following topics:

- About high availability support for SharePoint Server
- About the [VCS] agent for Microsoft SharePoint Server 2013
- SharePoint Server agent functions
- SharePoint Server agent state definitions
- SharePoint Server agent resource type definition
- SharePoint Server agent attribute definitions

About high availability support for SharePoint Server

The high availability (HA) solution for SharePoint Server is a combination of monitoring and recovery support for SharePoint applications and high availability support for SQL Server databases used by SharePoint Server.

The SharePoint high availability configuration components are as follows:

- [VCS] provides an agent for SharePoint that performs the task of managing the SharePoint Web Applications, Service Applications, and services configured in the server farm. Depending on the configuration, the agent monitors, starts, and stops the SharePoint components in the cluster.

- SharePoint Web Applications are configured in a [VCS] parallel service group. A parallel service group runs simultaneously on multiple nodes in a cluster. The parallel service group manages the Web Applications configured in the farm. The state of the parallel service group represents the state of the Web Applications configured in the farm. If a Web Application becomes unavailable, the agent attempts to restart the application in the farm.
- SharePoint Service Applications and services are configured in a separate service group that is created locally on each cluster node. The service group manages the components configured on the local node only. If any of the components become unavailable, the agent attempts to restart the component on the local node.
- The [VCS] agents for [SQL Server] database agents are used to configure high availability for the SharePoint databases. The agents monitor the health of the SharePoint databases as well as underlying resources and hardware. If a failure occurs, predefined actions bring up [SQL Server] on another node in the cluster.

About the [VCS] agent for Microsoft SharePoint Server 2013

The [VCS] application agent for Microsoft SharePoint Server manages SharePoint Server Service Applications, Web Applications, and services in a [VCS] cluster. The agent provides monitoring support in making a SharePoint Server applications highly available in a [VCS] environment.

Depending on the configuration, the agent performs the following operations:

- Monitors, starts, and stops the configured SharePoint services.
- Monitors the configured Web Applications, brings them online, and takes them offline.
- Monitors the configured Service Applications, brings them online, and takes them offline.

If any of the configured SharePoint component fails or is unavailable, the agent attempts to restart the component on the local node. If the component fails to start, the agent declares the resource as faulted.

SharePoint Server agent functions

Agent functions include the following

Online	Starts the configured Web Applications, Service Applications, or services.
Offline	Stops the configured Web Applications and Service Applications. The agent also stops monitoring the configured services on the node.
Monitor	Verifies the status of the configured Web Application, Service Application or service. If the components are running, the agent reports the resource as online. If any of the components are not running, the agent reports the resource as `FAULTED`.
Clean	Forcibly stops the configured Web Applications and Service Applications. The agent also stops monitoring the configured services on the node.

SharePoint Server agent state definitions

Agent state definitions are as follows:

`Online`	Indicates that the configured Web Applications, Service Applications, or services are running on the cluster node.
`Offline`	Indicates that the configured Web Applications and Service Applications are stopped on the cluster node. It also indicates that the monitoring for the services is also stopped.
`Faulted`	Indicates that the agent is unable to start the configured Web Applications, Service Applications, or services on the cluster node.
`Unknown`	Indicates that the agent is unable to determine the status of the configured SharePoint components on the cluster node.

SharePoint Server agent resource type definition

The resource type represents the [VCS] configuration definition of the agent and specifies how the agent is defined in the cluster configuration file, main.cf.

The SharePoint Server agent is represented by the SharePointServer resource type.

```
type SharePointServer (
static i18nstr ArgList[] = { AppType, AppName, Description, AppPoolMon,
FarmAdminAccount, FarmAdminPassword, ServiceIDList, StopSPSService }
str AppType
i18nstr AppName
```

```
i18nstr Description
str AppPoolMon = NONE
i18nstr FarmAdminAccount
str FarmAdminPassword
i18nstr ServiceIDList[]
boolean StopSPSService = 0
)
```

SharePoint Server agent attribute definitions

Review the tables of required and optional attributes to familiarize yourself with the agent attributes for a SharePointServer resource type. This information will assist you during the agent configuration.

Table 1-1 SharePoint Server agent required attributes

Required Attributes	Definition
AppType	Defines whether the agent is configured to monitor a SharePoint Web Application, Service Application, or service. This attribute can take one of the following values: ■ WebApp ■ ServiceApp ■ SPSService The default value is WebApp. If this attribute value is set to WebApp or ServiceApp, then you must specify a value for the AppName attribute. If this attribute value is set to SPSService, the AppName attribute value is ignored. Type and Dimension: string-scalar

Table 1-1 SharePoint Server agent required attributes *(continued)*

Required Attributes	Definition
AppPoolMon	Defines the monitoring modes for the application pool associated with the Web site being monitored. Configure this attribute only if AppType attribute value is set to WebApp and IIS is configured to run in the Worker Process Isolation mode. The attribute can take one of the following values: ■ NONE: Indicates that the agent does not monitor the application pool associated with the Web site. ■ DEFAULT: Indicates that the agent monitors the root application pool associated with the Web site. If this attribute is set, the agent starts, stops, and monitors the root application pool associated with the Web site. If the root application pool is stopped externally, the service group faults; the agent then attempts to restart the root application pool. ■ ALL: Indicates that the agent starts all the application pools associated with the Web site, but monitors and stops the root application pool only. If any application pool is stopped externally, the service group faults; the agent then attempts to restart the application pool. The default value is NONE. Type and Dimension: string-scalar
ServiceIDList	Defines the service IDs of the SharePoint services that are managed by the agent. This attribute is always local. This attribute can take the following values: ■ If AppType attribute value is set to WebApp, specify the service ID of the Microsoft SharePoint Foundation Web Application service. ■ If AppType attribute value is set to ServiceApp, specify the service ID of the service on which the Service Application depends. ■ If AppType attribute value is set to SPSService, specify the service IDs of the SharePoint services. **Note:** If you are configuring this attribute manually, use the [VCS] hadiscover command or the SharePoint server cmdlets to retrieve the service IDs. Type and Dimension: string-vector

Table 1-2 SharePoint Server agent optional attributes

Optional Attribute	Definition
AppName	The name of the SharePoint Web Application or Service Application that is managed by the agent. The value of this attribute depends on the value of the AppType attribute. This attribute can take the following values: ■ If AppType attribute value is set as WebApp, specify the Web Application name. ■ If AppType attribute value is set as ServiceApp, specify the application pool ID for the SharePoint Service Application. **Note:** This attribute is ignored if AppType attribute value is set as SPSService. Type and Dimension: string-scalar
Description	The display name of the service ID specified in the ServiceIDList attribute Type and Dimension: string-scalar
FarmAdminAccount	A user account that has the SharePoint Server Farm Admin privileges. User name can be of the form username@domain.com, domain\username, or domain.com\username. The agent uses the Farm Admin user account context to manage the services specified in the ServiceIDList attribute value. Type and Dimension: string-scalar
FarmAdminPassword	The password of the user specified in the FarmAdminAccount attribute value. The password is stored in the [VCS] configuration in an encrypted form. Type and Dimension: string-scalar

Table 1-2 SharePoint Server agent optional attributes *(continued)*

Optional Attribute	Definition
StopSPSService	When a resource in the [VCS] cluster is taken offline: ■ If the value of this attribute is set to true, the agent stops all the SharePoint services in its ServiceIDList. ■ If the value of this attribute is set to false, the agent does not change the state of the SharePoint services in its ServiceIDList, but it stops monitoring the services. The default value of this attribute is false. Type and Dimension: boolean

Chapter 2

Installing and configuring the [InfoScale Enterprise] product

This chapter includes the following topics:

- About installing the product
- About configuring the cluster

About installing the product

Install [InfoScale Enterprise] on all the systems where you want to configure the agent.

Refer to the appropriate guide for instructions:

- *[Veritas InfoScale] Installation and Upgrade Guide*

About configuring the cluster

Open the [VCS] Cluster Configuration Wizard (VCW) to set up the cluster infrastructure. The [VCS] Cluster Configuration Wizard (VCW) sets up the cluster infrastructure, including LLT and GAB, the user account for the [VCS] Helper service. VCW also provides an option for configuring the [VCS] Authentication Service in the cluster. The wizard also configures the ClusterService group, which contains resources for notification and global clusters (GCO). You can also use VCW to modify or delete cluster configurations.

Refer to the appropriate guide for instructions:

- *[Cluster Server] Administrator's Guide*
- *[Storage Foundation and High Availability Solutions], Solutions Guide*

Chapter 3

Installing and configuring SharePoint Server 2013 for high availability

This chapter includes the following topics:

- About installing and configuring [SharePoint]
- Configuring 64-bit Perl for [SharePoint]
- About configuring [SharePoint] service groups
- Verifying the [SharePoint] cluster configuration
- Considerations when modifying a SharePoint service group

About installing and configuring [SharePoint]

Install and configure [SharePoint] on all the nodes that will be part of the [SharePoint] service group and configure the farm.

Note the following before you proceed:

- [Veritas] recommends that you first configure [SQL Server] for high availability before configuring [SharePoint].
- While installing [SharePoint], ensure that you select **Server Farm** installation and then select **Complete** Server Type installation (Microsoft SharePoint Server installer > Server Type tab).

Note: The **Stand-alone** Server Type installation is not supported.

- [VCS] does not require you to install the [SharePoint] components on shared storage. You can install [SharePoint] on the local system disks.
- During configuration, for the database server name for the farm configuration database, specify the [SQL Server] that you configured for high availability earlier.

For installation and configuration instructions, see the Microsoft SharePoint documentation.

Note: For Perl scripts related to the [SharePoint] solution to work properly, use 64-bit Perl instead of the default version that is provided with the product installation.

See "Configuring 64-bit Perl for [SharePoint] " on page 16.

Configuring 64-bit Perl for [SharePoint]

Perl scripts are used to update DNS entries pertaining to the Network Load Balancer (NLB) name for the [SharePoint] DR solution. The scripts fail to execute when VERITAS Perl is used, because it is a 32-bit version of Perl.

By default, when a 32-bit process tries to access a 64-bit component in the `C:\Windows\System32` directory, Windows File System Redirector redirects it to the `C:\Windows\SysWOW64` directory. When `C:\Windows\System32\dnscmd.exe` is used, Windows is unable to locate the 64-bit file, because `dnscmd.exe` is only installed in the `System32` directory.

To configure 64-bit Perl

1. Install a 64-bit version of Perl.
2. Copy the `ag_i18n_inc.pm` file from `%vcs_home%\VRTSPerl\lib` to *`64-bit_Perl_install_dir`*`\lib`.
3. Make sure that you add the file path of 64-bit Perl to the process resource attribute in the [SQL Server] service group for configuring the web servers.

For further information about process resources,

About configuring [SharePoint] service groups

Configuring the [SharePoint] service group involves the following tasks:

- Creating a parallel service group for the [SharePoint] Web Applications running on the front-end Web servers.

- Creating service groups for [SharePoint] Service Applications or services locally on the application servers.

Use the SharePoint 2013 Configuration Wizard to create the required service groups and its resources and define the attribute values for the configured resources.

Note the following before you proceed:

- The wizard discovers the Web Applications, Service Applications, and services in the farm where the local node resides and then configures them in the service groups.
- The wizard automatically configures all the discovered [SharePoint] applications and services configured in the local cluster farm. With the new [SharePoint] 2013 wizard, you can also select the stopped services which you want to configure in the service application service group. If you do not want to configure an application or a service, host it on a server outside the local cluster.
- The wizard has a single workflow that performs service group creation as well as modification tasks. If you wish to add or remove a [SharePoint] component from the configuration, you must run the wizard again. If you run the wizard after configuring the [SharePoint] service groups, the wizard modifies the existing service group configuration. The wizard rediscovers the [SharePoint] configuration in the farm and then adds or removes resources depending on the changes made.

  For example, if you add a node to the server farm, the wizard adds the required resources and service groups to the configuration. If an application is removed from the server farm, the wizard removes the corresponding resources from the service group and also updates the [VCS] configuration.
- If you have configured the Web Applications and Service Applications in different clusters, then you must run the configuration wizard once from a node in each cluster.
- After configuring the [SharePoint] service groups, you can add custom resources such as IP or NIC to monitor the network availability of the cluster nodes in the configuration. You can add these resources manually from the Cluster Manager (Java Console).

  If you run the wizard again, these custom resources are ignored.

Before you configure a SharePoint service group

Before you configure a SharePoint service group, do the following:

- Verify that you have configured a cluster using the [VCS] Cluster Configuration Wizard (VCW).

- Verify that you have installed and configured SharePoint Server on all the nodes that will be part of the SharePoint service groups.
- Ensure that the SharePoint Server Timer service is running on all the nodes that will be part of the SharePoint service groups.
- Ensure that the Veritas Command Server service is running on all the nodes that will be part of the SharePoint service groups.
- Verify that the Veritas High Availability Engine (HAD) is running on the system from where you run the [VCS] SharePoint Server 2013 Configuration Wizard.
- Ensure that you have [VCS] Cluster Administrator privileges. This privilege is required to configure service groups.
- Ensure that the logged-on user has SharePoint Server Farm Administrator privileges on the SharePoint Server.
- Ensure that you run the wizard from a node where SharePoint Server is installed and configured.
- If you have configured a firewall, add the required ports and services to the Firewall Exception list.
  For a detailed list of services and ports used by the product, refer to the *[Veritas InfoScale] Installation and Upgrade Guide*.

Creating a SharePoint service group

Complete the following steps to create a service group for SharePoint Server.

To create the SharePoint Server service group

1. Launch the [VCS] SharePoint Server 2013 Configuration Wizard.

   Launch SharePoint Server 2013 Configuration Wizard from **Start > All Programs > Veritas > Veritas Cluster Server > Configuration tools > SharePoint Server 2013 Configuration Wizard** or, on Windows 2012 operating systems, from the **Apps** menu in the **Start** screen.
2. Review the information in the Welcome panel and click **Next**.

3 On the Farm Admin User Details panel, specify the SharePoint Farm Admin user credentials and then click **Next**.

Farm Name	Displays the name of the farm configuration database where the nodes reside.
Farm Admin User Name	Specify a user account that has Farm Admin privileges in the SharePoint farm where the current node resides. Click the ellipsis button to launch the Windows Select User dialog box and then specify the appropriate user account. The Farm Admin user account is used to manage the SharePoint applications and services configured in the SharePoint service groups in the cluster.
Password	Type the password of the user account specified in the Farm Admin User Name field. The wizard stores the user password in the [VCS] configuration in an encrypted form.

4 On the Web Applications Details panel, review the list of Web Applications that the wizard discovers in the farm and then click **Next**.

The wizard configures these Web Applications in a parallel service group. The wizard configures only those components that are part of the local cluster.

5 On the Service Applications Details panel, review the list of Service Applications and running services that the wizard discovers in the farm. You can also select the stopped services that you want to configure as part of the service group. Click **Next**.

The wizard configures these Service Applications and services in a local service group on each node. The wizard configures only those components that are part of the local cluster.

The wizard configures resources for the services currently running on the system. To configure a resource for a service stopped on the system and which can be started independently, click **Advanced Service Configuration**. The Service Selection dialog box appears.

In the Service Selection dialog box, select a system to view the list of services stopped on it. Select the services to be configured as resources in the service group. Click **OK**.

6 On the Service Groups Summary panel, review the service group configuration, edit the service group and resource names if required, and then click **Next**.

Resources	Displays a list of configured service groups and its resources. The wizard assigns unique names to service group and resources. ■ For parallel service groups, the wizard uses the following naming convention: FarmConfigurationDatabaseName-WebApplications ■ For local service groups, the wizard uses the following naming convention: FarmConfigurationDatabasename-NodeName-ServiceApps You can edit resource names only in the create mode. You cannot modify names of service groups and resources that already exist in the configuration. To edit a name, select the resource name and either click it or press the F2 key. Edit the resource name and then press the Enter key to confirm the changes. To cancel editing a resource name, press the Esc key.
Attributes	Displays the attributes and their configured values, for a resource selected in the Resources list.

7 Click **Yes** on the message that informs that the wizard will run commands to modify the service group configuration. The wizard starts running commands to create the service groups. Various messages indicate the status of these commands.

8 On the completion panel, check **Bring the service group online** check box to bring the SharePoint service groups online in the cluster, and then click **Finish**.

This completes the SharePoint service group configuration.

Verifying the [SharePoint] cluster configuration

Failover simulation is an important part of configuration testing. To verify the configuration in the cluster, you can take the service groups offline, or manually stop the configured applications on the active cluster node.

You can also simulate a local cluster failover for the [SQL Server] databases configured in the [SQL Server] service group. Refer to the application-specific documentation for instructions.

Use Veritas Cluster Manager (Java Console) to perform all the service groups operations.

To take the service groups offline and bring them online

1. In the Veritas Cluster Manager (Java Console), click the cluster in the configuration tree, click the Service Groups tab, and right-click the service group icon in the view panel.
   - Click **Offline** and then choose the local system.
   - In the dialog box, click **Yes**. The service group you selected is taken offline on the node.
     If there is more than one service group, you must repeat this step until all the service groups are offline.
2. Verify that the applications and services configured in the service groups are in the stopped state.
3. To start all the stopped services, bring all the services groups online on the node.

To manually stop the configured applications and services

1. To verify that the [SharePoint] applications and services are properly configured with [VCS], manually stop these components either from the SharePoint Central Administration console or from the IIS Manager.
2. From the IIS Manager, in the Connections pane on the left, select a configured Web site and then in the Actions pane on the right, click Stop. The status of the Web Site will show as stopped.
3. In the Cluster Manager (Java Console) the corresponding service group resource state may temporarily show as faulted as the [SharePoint] agent attempts to start the stopped application.
4. When the resource comes online, refresh the IIS Manager view to verify that the IIS site is in the started state.

Considerations when modifying a SharePoint service group

Note the following while modifying SharePoint service groups:

- The wizard has a single workflow that performs service group creation as well as modification tasks. If you wish to add or remove a SharePoint component from the configuration, you must run the wizard again.
  If you run the wizard after configuring the SharePoint service groups, the wizard modifies the existing service group configuration. The wizard rediscovers the SharePoint configuration in the farm and then adds or removes resources depending on the changes made.

For example, if you add a node to the server farm, the wizard adds the required resources and service groups to the configuration. If an application is removed from the server farm, the wizard removes the corresponding resources from the service group and also updates the [VCS] configuration.

- When you run the wizard after configuring the SharePoint service groups, the wizard ignores any custom resources that you may have added to the service groups. If you wish to add, remove, or modify those custom resources, you must do so manually. The wizard does not provide any options to modify custom resources.

Appendix A

Using Veritas AppProtect for vSphere

This appendix includes the following topics:

- About Just In Time Availability
- Prerequisites
- Setting up a plan
- Deleting a plan
- Managing a plan
- Viewing the history tab
- Limitations of Just In Time Availability
- Getting started with Just In Time Availability
- Supported operating systems and configurations
- Viewing the properties
- Log files
- Plan states
- Troubleshooting Just In Time Availability

About Just In Time Availability

The Just In Time Availability solution provides increased availability to the applications on a single node InfoScale Availability cluster in VMware virtual environments.

Using the Just In Time Availability solution, you can create plans for:

- Planned Maintenance
- Unplanned Recovery

Planned Maintenance

In the event of planned maintenance, the Just In Time Availability solution enables you to clone a virtual machine, bring it online, and fail over the applications running on that virtual machine to the clone on the same ESX host. After the maintenance procedure is complete, you can fail back the applications to the original virtual machine. Besides failover and failback operations, you can delete a virtual machine clone, view the properties of the virtual machine and its clone, and so on.

Unplanned Recovery

When an application encounters an unexpected or unplanned failure on the original or primary virtual machine on the primary ESX host, the Just In Time Availability solution enables you to recover the application and bring it online using the unplanned recovery feature.

With **Unplanned Recovery Policies**, the Just In Time Availability solution enables you to set up recovery policies to mitigate unplanned failures that are encountered by an application. Just In Time Availability solution provides the following recovery policies; you may select one or all the recovery policies as per your need:

Unplanned Recovery Policies	Description
Restart Application	Just In Time Availability (JIT) solution attempts to restart the service group (SG), and bring the application online on the original virtual machine on primary ESX. Maximum three retry attempts are permitted under this policy. **Note:** If all the three attempts fail, application continues to remain in faulted state or continues with the next policy as selected while creating a plan.

Unplanned Recovery Policies	Description
Restart virtual machine (VM)	Just In Time Availability (JIT) solution performs the following subsequent tasks: ■ take the service group offline ■ shut down the virtual machine ■ power on the virtual machine ■ bring the service group online on the original virtual machine on primary ESX You are provided with **Last attempt will be VM reset** option to reset the virtual machine. By default, this checkbox is selected and the default retry attempt value is one. If you retain the default settings, then VM reset operation is performed on the virtual machine at the first attempt itself. Maximum three retry attempts are permitted for this operation. If you deselect the checkbox, then the virtual machine reset (VM Reset) operation is not performed.
Restart VM on target ESX	Using this policy, you can recover the faulted application on the virtual machine. In this policy, the original virtual machine is unregistered from the primary ESX; registered on the target ESX; and the faulted application is brought online on the target ESX.
Restore VM on target ESX	Using this policy, you can recover the faulted application on the virtual machine using a boot disk backup copy of the original virtual machine. In this policy, the original virtual machine is unregistered from the ESX and the boot disk backup copy of the original virtual machine is registered on target ESX. The faulted application is then brought online on the virtual machine.

Unplanned Recovery Policies	Description
Unplanned Failback	The **Unplanned Failback** operation lets you fail back the application from the boot disk backup copy of virtual machine on the target ESX to the original virtual machine on primary ESX. If you have selected either **Restart VM on target ESX** or **Restore VM on target ESX** or both the recovery policies, you can perform the **Unplanned Failback** operation. On the **Plans** tab, in the plans table list, right-click the virtual machine and click **Unplanned Failback**. **Note: Unplanned Failback operation** operation is disabled and not available for the plans and the virtual machines which have **Restart Application** and **Restart VM** policies as the only selected options.

Based on the selected recovery policy for a plan, Just In Time Availability (JIT) solution performs the necessary operations in the sequential order.

For example, if you have selected **Restart Application** and **Restart VM** as the recovery policy, then in the event of unplanned application failure, first it performs tasks for **Restart Application** policy and if that fails, it moves to the next policy.

You may select one or all the recovery policies based on your requirement.

Table A-1 lists the sequence of tasks that are performed for each Unplanned Recovery policy.

Table A-1 Tasks performed for each Unplanned Recovery policy

Unplanned Recovery Policy	Tasks Performed
Restart Application	◆ Make an attempt to restart the application.
Restart virtual machine (VM)	**1** Takes the service group(s) offline **2** Shuts down the virtual machine **3** Power on the virtual machine **4** Brings the service group(s) online

Table A-1 Tasks performed for each Unplanned Recovery policy *(continued)*

Unplanned Recovery Policy	Tasks Performed
Restart VM on target ESX	**1** Takes the service group(s) offline **2** Shuts down the original virtual machine **3** Detaches the data disks from the original virtual machine **4** Unregisters the virtual machine from the primary ESX **5** Registers the original virtual machine on target ESX **6** Attaches the data disks back to the virtual machine **7** Power on the virtual machine **8** Brings the service group(s) online
Restore VM on target ESX	**1** Takes the service group(s) offline **2** Shuts down the virtual machine **3** Detaches the data disks from the virtual machine **4** Unregisters the original virtual machine from the target ESX **5** Registers the boot disk backup copy of the original virtual machine to the target ESX **6** Attaches the data disks back to the virtual machine **7** Power on the virtual machine **8** Brings the service group(s) online
Unplanned Failback	**1** Takes the service group(s) offline **2** Shuts down the virtual machine **3** Detaches the data disks from the virtual machine **4** Unregisters the virtual machine from the target ESX **5** Registers the virtual machine using the original boot disk backup copy to the primary ESX **6** Attaches the data disks to the virtual machine **7** Power on the virtual machine on primary ESX **8** Brings the service group(s) online on the virtual machine

Scheduler Settings

While creating a plan for unplanned recovery, with **Scheduler Settings**, you can set up a schedule for taking a back up of boot disk of all the virtual machines that are a part of the plan.

To use the Just In Time Availability solution, go to **vSphere Web Client > Home view > Veritas AppProtect**.

See "Setting up a plan" on page 30.

Prerequisites

Before getting started with Just In Time Availability, ensure that the following prerequisites are met:

- The Just In Time (JIT) solution feature cannot co-exist with VMware HA, VMware FT, and VMware DRS. This pre-requisite is applicable for **Unplanned Recovery**only.
- VIOM 7.2 version must be installed and configured using fully qualified domain name (FQDN) or IP.
- Make sure that you have the admin privileges for vCenter.
- VMware Tools must be installed and running on the guest virtual machine.
- VIOM Control Host add-on must be installed on VIOM server or machine.
- The virtual machines must be added in VIOM. The virtual machines, vSphere ESX servers, and VIOM must have the same Network Time Protocol (NTP) server configured.
- Make sure to specify VIOM Central Server FQDN or IP in the SNMP Settings of the vCenter Server.
- vCenter Server and VIOM must be configured using the same FQDN or IP address. Make sure that if FQDN is used to configure vCenter in VIOM Server that is used during the configuration.
- If raw disk mapping (RDM) disks are added to the virtual machine, then make sure that the virtual machine is in the physical compatibility mode. Veritas AppProtect does not support the virtual compatibility mode for RDM disks.
- For Microsoft Windows operating system, make sure that you have the Microsoft Windows product license key. The key is required to run the Sysprep utility, which enables customization of the Windows operating system for a clone operation.

- For RHEL7 and SUSE12 operating system, install the deployPkg plug-in file on the virtual machine.
  For more information on installing the plug-in, see https://kb.vmware.com/kb/2075048
- Make sure that the InfoScale Availability service group is configured with one of the storage agents such as Mount, DiskGroup, LVMVolumeGroup, VMNSDg (for Windows), or DiskRes (for Windows), for the data disks. This configuration enables Veritas AppProtect to discover data disks for the applications. Also, ensure that the service group is online to determine data disk mapping.
- Virtual machines which have snapshots associated with them are not supported.
- Virtual machines with SCSI Bus Sharing are not supported.
- Make sure that the SNMP Traps are configured for the following from vCenter server to VIOM:
  - Registered virtual machine
  - Reconfigured virtual machine
  - Virtual machine which is getting cloned
- Make sure that the boot disk of VM's (vmdk) does not have spaces.
- For HA console add on upgrade from VIOM 7.1 to VIOM 7.2, refer *Veritas InfoScale Operations Manager 7.2 Add-ons User's Guide* for more details.
- Make sure to set the vSphere DRS Automation Level to manual, if you want to configure **Restart VM on target ESX** or **Restore VM on target ESX** policies for your plan.
- Ensure to update or edit the plan, when a virtual machine is migrated or if there are any modifications made to the settings of the virtual machines which are configured for that plan.
- Ensure to increase the tolerance limit of DiskRes resource to two, if you want to create a plan for unplanned recovery with **Restore VM on target ESX** as the unplanned recovery policy.

Note: This prerequisite is applicable for Windows operating system.

Setting up a plan

Plan is a template which involves a logical grouping of virtual machines so as to increase the availability of the application in the event of a planned failover and recovery of the application in the event of an unexpected application failure.

To set up a plan

1. Launch Veritas AppProtect from the **VMware vSphere Web Client > Home view > Veritas AppProtect** icon.
2. Click **Configure Plan**.

   The **Plan Configuration** wizard appears.
3. Specify a unique **Plan Name** and **Description**, and then click **Next**.

   The wizard validates the system details to ensure that all prerequisites are met.
4. Select the virtual machines that you want to include in the plan, review the host and operating system details, and then click **Next**.

   The **Unplanned Recovery Settings** page appears.
5. On the **Unplanned Recovery Settings** page, you can configure the selected virtual machines for **Unplanned Recovery** as well.

   Deselect the **Configure selected VMs for Unplanned Recovery as well** check box, if you do not want to include the selected virtual machines for unplanned recovery.

   If you have selected the virtual machines for unplanned recovery, then set up the unplanned recovery policies as appropriate from the available options. You can set up policies to restart applications, restart virtual machines, restart virtual machine on target ESX, and restore a virtual machine on target ESX.

   If you have selected **Restore VM on target ESX** as the unplanned recovery policy, then you can set up a schedule to create a boot disk back up copy of the virtual machine within the configured plan. You can set the frequency as daily, weekly, monthly, or manual as per your requirement.

   After you have finished making necessary settings for Unplanned Recovery, Click **Next**.
6. The wizard validates the prerequisite attributes of the virtual machine and the ESX host, and adds the qualified virtual machines to the plan.

   Click **Next** after the validation process completes.

7 In the **Disks** tab, you can view the selected application data disks. Just In Time Availability solution uses the selected data disks to perform detach-attach operation during a planned failover and unplanned recovery.

Note: If the disks are not auto-marked as selected to perform detach-attach operation, then first refresh the VIOM server and then the VCenter server in VIOM and then create a plan.

---

8 In the **Network Configuration** tab, specify the network interface configuration details for the cloned virtual machine. Make sure to specify at least one public interface and valid IP details.

9 In the **Unplanned Recovery Target** tab, specify the target ESX server to restore the virtual machine, and the target ESX port details.

Note: The **Unplanned Recovery Target** tab is visible only when **Restart VM on target ESX** or **Restore VM on target ESX** is selected.

---

10 In the **Windows Settings** tab, specify the domain name, Microsoft Windows product license key, domain user name, domain password, admin password, and time zone index.

Note: The **Windows Settings** tab is visible only when a Windows virtual machine is selected in the plan.

---

11 Click **Next**. The **Summary** wizard appears.

12 In the **Summary** wizard, review the plan details such as the plan name, unplanned recovery policies, schedule, and so on.

Deselect the **Start backup process on finish** checkbox if you do not want to initiate a backup process when the plan creation procedure is finished. This checkbox is selected by default.

Click **Create**. The plan is created and saved.

13 Click **Finish** to return to the plans tab and view the created plans.

See “Managing a plan” on page 32.

See “Deleting a plan” on page 32.

Deleting a plan

After you have finished performing failback operations from the clone to the primary virtual machine in case of planned maintenance and recovery operations in case of unplanned recovery, you may want to delete the plan.

To delete a plan

1. Launch **Veritas AppProtect** from the VMware vSphere Web Client Home view.
2. In the **Plans** tab, select the plan that you want to delete.
3. Click **Delete Plan**.

Note: The **Delete plan** icon is enabled only when the selected plan is in **Ready For Failover**, **Failed to Revert**, and **Failed to Failback** state.

Managing a plan

Planned Maintenance

After the maintenance plan is created, you can fail over the applications to the clone virtual machine and fail back the applications from the clone to the virtual machine. When the scheduled maintenance is complete, you can delete the cloned virtual machine or retain it for future use.

To perform failover, failback, revert, or delete clone operations, go to **Plans**, and select a plan. Based on the enabled operation, perform the following tasks:

To fail over the applications to the cloned virtual machine

- Click the **Failover** icon.

  Just In Time Availability (JIT) performs the sequence of failover tasks, which includes taking the application offline, detaching the disks, cloning the virtual machine, attaching the disks, and so on.

To fail back the applications from the clone to the primary virtual machine

- Click the **Failback** icon.

  Just In Time Availability (JIT) performs the sequence of failback tasks, which includes taking the application offline, detaching the disks, attaching the disks, and so on.

To revert a failover or a failback operation

- Click the **Revert** icon.

  If the failover or a failback operation fails, the revert operation restores the applications on the virtual machine, and deletes the clone if created.

To delete a clone

- Click the **Delete Clone** icon.

  After the failback operation is complete, you can delete the clone. By default, the revert operation deletes the clone.

Note: Alternatively, right-click **Plan** in the **Plans** table on the **Plans** wizard to perform failover, failback, revert, delete plan, and delete clone operations.

Unplanned Recovery

Once you have set up a plan for unplanned recovery during **Configure Plan** operation, based on the recovery policies selected for the plan, the application is recovered accordingly.

You can manage unplanned recovery policies settings by performing the following operations on the plan and its associated virtual machines.

Managing unplanned recovery settings

On the **Plans** tab, in the plans table which lists all the existing plans, navigate to the required plan and use the right-click option on the selected plan.

- **Edit**: Use this option to modify the configured plans settings such as adding or removing a virtual machine from the plan, and so on.
  The same **Configuration Plan** wizard using which you had set up or configured a plan is displayed with pre-populated details.
  See “Setting up a plan” on page 30.
- **Disable Unplanned Recovery**: Use this option to disable the Unplanned Recovery settings.
- **Enable Unplanned Recovery**: Use this option to enable the Unplanned Recovery settings.
- **Disable Scheduler**: Use this option to disable the scheduler settings.
- **Enable Scheduler**: Use this option to enable the scheduler settings.
- **Delete Plan**: Use this option to delete the created plan.
- **Properties**: Use this option to view the properties for unplanned recovery. It displays details such as the selected unplanned recovery policies and the

associated operations for the selected policies. It also provides information about the selected scheduler mode for performing boot disk back up operation for the selected virtual machines.

Managing virtual machines settings

On the **Plans** tab, in the plans table which lists all the existing plans and its associated virtual machines, navigate to the required virtual machine. Select the required virtual machine and use the right-click option on the selected virtual machine.

- **Remove VM From Plan**: Use this option to delete the virtual machine from the selected plan.
- **Create Clone Backup**: Use this option to create a boot disk backup copy of the virtual machine.
- **Unplanned Failback**: Use this option to fail back the application from the boot disk backup copy of the virtual machine on target ESX to the original virtual machine on primary ESX.

  Note: This option is available only if you have set unplanned recovery policies as **Restart VM on target ESX** or **Restore VM on target ESX**.

- **Properties**: Use this option to view properties such as the last run time for backup operation, last successful backup attempt time and the target ESX details.

See "Plan states" on page 39.

Viewing the history tab

On the **History** tab, you can view the detailed summary of the operations that are performed on the virtual machine. The details include the plan name, virtual machine name, operation, the status of the operation, the start and the end time of the operation, and the description of the operation status.

To view the summary

1. Launch **Veritas AppProtect** from the VMware vSphere Web Client Home view.
2. Click the **History** tab.

Limitations of Just In Time Availability

The following limitations are applicable to Just In Time Availability:

- On a single ESX host only ten concurrent failover operations are supported. Across ESX hosts, twenty concurrent failover operations are supported.
- Linked mode vCenter is not supported.
- Only three backup operations per data store are active , the rest will be queued. Only five backup operations per ESX host are active, the rest will be queued.

See "Supported operating systems and configurations" on page 37.

Getting started with Just In Time Availability

You can access the Just In Time Availability solution from the **vSphere Web Client > Veritas AppProtect** interface.

The **Veritas AppProtect** is registered with Veritas InfoScale Operations Manager (VIOM), and is accessed from the **vSphere Web Client > Home** view.

Figure A-1 describes the Veritas AppProtect interface in detail.

Figure A-1 Elements of the Veritas AppProtect interface

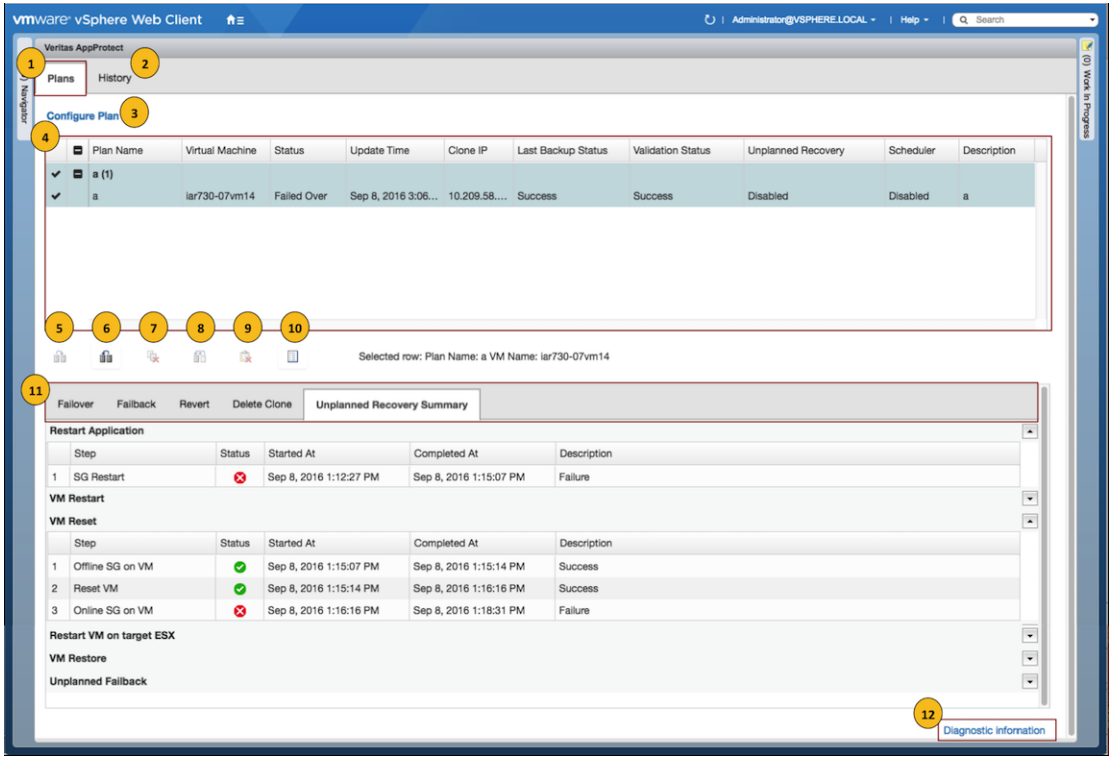


Table A-2 Elements of the Veritas AppProtect interface and the description

Label	Element	Description
1	**Plans** tab	Enables setting up a plan for a planned failover and unplanned recovery. Displays the plan attributes, and the virtual machines that are added to the plan. Displays the status of virtual machines for unplanned recovery and schedule for virtual machine back up operation based on the criteria set while configuring or editing the plan. Shows the enabled or disabled failover, failback, delete clone, revert, delete plan, and properties operations icons based on the state of the selected plan for planned failover.
2	**History** tab	Displays the status and the start and the end time of the specific operation performed on the created plans.
3	**Configure Plan** link	Opens the **Plan Configuration** wizard.
4	**Plans** table	Displays the attributes of the plan.
5	**Failover** icon	Fails over the applications from the original virtual machine to the clone.
6	**Failback** icon	Fails back the applications from the clone to the original virtual machine.
7	**Delete Clone** icon	Deletes the cloned virtual machine.
8	**Revert State** icon	Reverts the failed operation, restores the applications to the original virtual machines, and delete the clone virtual machines.
9	**Delete Plan** icon	Deletes the plan.
10	**Properties** icon	Displays the attributes of each virtual machine and the clone.

Table A-2 Elements of the Veritas AppProtect interface and the description *(continued)*

Label	Element	Description
11	Operation-specific tabs	Displays the sequence of the tasks that are performed for the selected operation. Based on the operation that is executed, the associate tab opens. **For Planned Maintenance** **1** Failover **2** Failback **3** Revert **4** Delete Clone **For Unplanned Recovery** ◆ Unplanned Recovery Summary
12	**Diagnostic information**	Displays the logs that are reported for the Veritas AppProtect interface.

See "Plan states" on page 39.

Supported operating systems and configurations

Just In Time Availability supports the following operating systems:

- On Windows: Windows 2012, and Windows 2012 R2.
- On Linux: RHEL5.5, RHEL6, RHEL7, SUSE11, SUSE12.

Just In Time Availability supports the following configurations:

- Veritas Cluster Server (VCS) 6.0 or later, or InfoScale Availability 7.1 and later.
- Veritas InfoScale Operations Manager managed host (VRTSsfmh) 7.1 and 7.2 version on the virtual machines.
  For more information about VRTSsfmh, see the *Veritas InfoScale Operations Manager 7.2 User Guide*.
- Veritas InfoScale Operations Manager (VIOM) 7.2 as a central or managed server.
- VMware vSphere 5.5 Update 2, Update 3, or 6.0 and 6.0 Update 1 version.

Viewing the properties

Virtual Machine Properties

The **Virtual Machine Properties** window displays information about the virtual machine and its clone such as name, operating system, cluster name, service groups, DNS server, domain, IP addresses, and data disks.

To view the properties

1. On the **Plans** tab, select the virtual machine.
2. Click the **Properties** icon or right-click the virtual machine.

   The**Virtual Machine Properties** window opens and displays the attributes of the virtual machine and its clone.

Plan Properties

The **Plan Properties** window displays information about the unplanned recovery policies selected; scheduler mode set; and the time when the last backup operation was run and was successful for a virtual machine.

To view properties for the plan

1. In the Plan Name table, select the plan.
2. Right-click the selected plan. A window with a list of options is displayed.
3. Click **Properties**

   The **Plan Properties** window opens and displays the unplanned recovery policies selected and the schedule mode for virtual machine backup operation.

Log files

The following log files are helpful for resolving the issues that you may encounter while using Veritas AppProtect:

- Console related logs:

  ```
  /var/opt/VRTSsfmcs/logs/*
  ```

  These log files show console messages and are useful for debugging console issues.

- Operations logs:

  ```
  /var/opt/VRTSsfmh/logs/vm_operations.log
  ```

  This log file shows the messages pertinent to the Veritas AppProtect interface.

- VMware vSphere 6.0 logs:

  ```
  C:\ProgramData\VMware\vCenterServer\logs\vsphere-client\logs\*
  ```

  These log files show the messages that are reported for the VMware vSphere Web Client version 6.0.

- VMware vSphere 5.5 U2 and U3 logs:

  ```
  C:\ProgramData\VMware\vSphere Web Client\serviceability\logs\*
  ```

  These log files show the messages that are reported for the VMware vSphere Web Client version 5.5 U2 and U3.

- Veritas AppProtect interface logs:
  The log file shows the logs that are reported for the Veritas AppProtect interface. To view the log files, on the **Planned Maintenance** tab or the **History** tab **> Diagnostic Information**.

Plan states

Based on the state of the plan, the operation icons are enabled and disabled on the **Plans** tab.

Table A-3 List of plan and operation states

Plan state	Failover	Failback	Revert	Delete clone	Delete Plan	Unplanned Failback	Create Clone backup	Properties
Ready For Failover	✓	–	–	✓ **Note:** Enabled when the selected maintenance plan has an associate clone.	✓ **Note:** Enabled when the selected maintenance plan does not have an associate clone.	–	✓	✓
Failed Over	–	✓	–	–	–	–	–	✓
Failed To Failover	–	–	✓	–	–	–	–	✓

Table A-3 List of plan and operation states *(continued)*

Plan state	Failover	Failback	Revert	Delete clone	Delete Plan	Unplanned Failback	Create Clone backup	Properties
Failed To Failback	–	–	✓	–	–	–	–	✓
Failed To Revert	–	–	✓	–	✓	–	–	✓
Unknown	–	–	✓	–	–	✓	–	✓
Failed To Delete Clone	–	–	–	✓	–	–	–	✓
Failover In Progress	–	–	–	–	–	–	–	✓
Failback In Progress	–	–	–	–	–	–	–	✓
Revert In Progress	–	–	–	–	–	–	–	✓
Delete Clone In Progress	–	–	–	–	–	–	–	✓
Application Faulted	–	–	–	–	–	–	–	✓
Failed To Restart VM	–	–	–	–	–	–	–	✓
Failed To Move VM	–	–	–	–	–	✓	–	✓
Failed To Restore VM	–	–	–	–	–	✓	–	✓
Unplanned	–	–	–	–	–	✓	✓	–
Unplanned Restored VM	–	–	–	–	–	✓	–	✓
Unplanned Failed to Failback	–	–	–	–	✓	–	–	–

Troubleshooting Just In Time Availability

Table A-4 lists the issues and the recommended solutions.

Table A-4 Issues and the corresponding resolutions

Issue	Recommended Solution
When setting up a maintenance plan, the registered virtual machine is not listed on the wizard.	To troubleshoot the issue, make sure the following: ■ ESX host on which the virtual machine resides, is connected to the vCenter. ■ The virtual machine is added as a managed host to Management Server. ■ On the virtual machine, at least one application is configured for monitoring, along with VCS. ■ The virtual machine is registered in VIOM. ■ VCS is configured on the virtual machine. ■ The virtual machine does not contain RHEL7 and SUSE 12, which are not supported. **Note:** Windows 2012 R2 and 2008 R2 are supported. ■ VCS is configured with the service groups.
When setting up a maintenance plan, the listed virtual machine is not available for selection.	To troubleshoot the issue, make sure the following: ■ The virtual machine is not configured for Global Cluster option (GCO). ■ Agents that support SAN are configured.
When Veritas AppProtect executes an operation, the timeout message is reported.	To troubleshoot the issue, perform the following: ■ If the failover or the failback operation fails, then click **Planned Maintenance > Revert** icon. Retry the operation. ■ If the delete plan or the delete clone operation fails, then retry the operation.
The revert operation failed.	Manually revert the virtual machine to its original state.