Symantec™ Disaster Recovery Orchestrator Deployment Guide

Microsoft Azure

6.1

May 2014

Symantec™ Disaster Recovery Orchestrator Deployment Guide

Product version: 6.1

Document version: 6.1 Rev 1

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/index.jsp

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/contact_techsupp_static.jsp

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

About Symantec Connect

Symantec Connect is the peer-to-peer technical community site for Symantec's enterprise customers. Participants can connect and share information with other product users, including creating forum posts, articles, videos, downloads, blogs and suggesting ideas, as well as interact with Symantec product teams and Technical Support. Content is rated by the community, and members receive reward points for their contributions.

http://www.symantec.com/connect/storage-management

Documentation

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

doc_feedback@symantec.com

For information regarding the latest HOWTO articles, documentation updates, or to ask a question regarding product documentation, visit the Storage and Clustering Documentation forum on Symantec Connect.

https://www-secure.symantec.com/connect/storage-management/forums/storage-and-clustering-documentation

Contents

Chapter 1

Introduction to Disaster Recovery Orchestrator

This chapter includes the following topics:

Disaster Recovery Orchestrator overview

Disaster Recovery Orchestrator provides protection for the applications that are deployed in the IT setup of small and medium business (SMB) enterprises. The applications that are deployed on the on-premises site can be configured for monitoring and disaster recovery (DR). Such applications are migrated to or recovered at the Microsoft Azure cloud site for which the SMB has a subscription.

A monitoring configuration protects an application against internal faults. If an application stops responding, the monitoring configuration attempts to restart the application and bring it online again. A DR configuration protects an application against site failures. If an application stops responding because the on-premises site becomes unavailable, the DR configuration can be used to recover the application at the cloud site. An application that is configured with Disaster Recovery Orchestrator can also be migrated to the cloud.

About Disaster Recovery Orchestrator components

Disaster Recovery Orchestrator components are classified as follows:

- Console components
  These components reside on an Azure virtual machine that acts as a controller for the disaster recovery (DR) activities.
- Client components
  These components reside on an on-premises system and its counterpart Azure virtual machine that manage the application monitoring activities.

Disaster Recovery Orchestrator Console

The Console components are installed on a dedicated virtual machine in the Azure network, called the Console host.

The Console components and their functions are as follows:

- Disaster Recovery Orchestrator Authentication Service
  This service enables secure communication between the on-premises site and the Azure site. It uses digital certificates for authentication and SSL to encrypt communications. Disaster Recovery Orchestrator uses platform-based authentication; it does not store user passwords.
  The Console provides a single sign-on mechanism that uses this service so that an authenticated domain user does not have to:
  - Provide the user credentials associated with the virtual machine to manage application monitoring
  - Log on each time to connect to the virtual machine in Azure
- Role-based access control module
  This component manages the roles and users that are required for Disaster Recovery Orchestrator.
- Disaster Recovery Orchestrator Configuration Wizard
  This wizard is used to configure an application for DR. When an on-premises application fails, you can continue servicing it from the Azure cloud.
- Replication module
  This module manages the file replication mechanism that is used to synchronize the application data between the on-premises site and the Azure site.
- Symantec Storage Foundation Messaging Service (`xprtld`)
  The Console uses this service for the following functions:
  - Receive the application monitoring status, which is then displayed on the Dashboard and Application views

- Relay commands that act on an application monitoring configuration, for example, takeover

Disaster Recovery Orchestrator Client

Disaster Recovery Orchestrator Client is installed on the system where you wish to monitor an application. In your on-premises environment, the Client components can reside on a physical or a virtual machine. In Azure, the virtual machine on which you install the components is referred to as the cloud application host to differentiate it from the Console host.

The Client components and their functions are as follows:

- Application monitoring configuration wizard
  This wizard is used to configure application monitoring on the on-premises application host and on the corresponding cloud application host.
- Agents for configuring and monitoring applications
  - Infrastructure agents
    These agents manage resources such as heartbeats, NICs, storage, generic services, and so on.
  - Application-specific agents
    These agents manage the resources specific to those applications that are supported for monitoring, for example, Database Engine and FILESTREAM for SQL Server.
  - Replication agents
    These agents manage data replication between the on-premises site and the Azure site.
- Replication module
  This module ensures that application data at the on-premises site and the Azure site is in sync.
- Symantec Storage Foundation Messaging Service (`xprtld`)
  The infrastructure agents use this service to communicate the status of application monitoring to the Console.

Disaster Recovery Orchestrator licensing

Disaster Recovery Orchestrator follows a subscription-based licensing model. The licenses are metered on a per-instance basis, and the metering is done manually. An instance is defined as a 'protected application component'. If you change or renew the number of protected applications, you must report it to your Symantec Account Representative or your Symantec Certified Partner Reseller.

All licensing in Disaster Recovery Orchestrator is keyless. The Symantec product installer installs the embedded keys by default. A keyless license lets you use all the available product features.

For more information about the pricing, licensing, and the purchasing model, visit the Symantec website at:

https://licensing.symantec.com/

Deployment workflow

Deploying Disaster Recovery Orchestrator involves the following tasks:

1. Setting up the cloud infrastructure for disaster recovery (DR) readiness
   - Procuring a Microsoft cloud services subscription
   - Creating a virtual network for DR
   - (Optional) Creating a virtual network for performing fire drills
   - Creating a virtual machine to install Disaster Recovery Orchestrator Console (Console host)
   - Creating a virtual machines to host the applications (cloud application hosts)
   - Creating the management certificate and for authentication and uploading it to Azure
   - Creating the service certificate or the Personal Information Exchange (PFX) file for authentication
2. Installing the Disaster Recovery Orchestrator components
   - Allocating users and groups for installing and configuring Disaster Recovery Orchestrator
   - Installing Disaster Recovery Orchestrator Console on the Console host
   - Installing Disaster Recovery Orchestrator Client on the on-premises application hosts
   - Installing Disaster Recovery Orchestrator Client on the cloud application hosts
3. Configuring users and security settings
   - Copying the PFX file to the Console host
   - Creating users and assigning them privileges on the on-premises application hosts for the application configurations

- Creating users and assigning them privileges on the cloud application hosts to configure applications for monitoring and for recovery
  For more information, see the *Symantec Disaster Recovery Orchestrator Administration Guide*.

Common terms used in the context of Disaster Recovery Orchestrator

The Disaster Recovery Orchestrator solution caters to on-premises and cloud environments, and therefore, deals with a wide range of entities. Some of these entities may be referred to using multiple names. This section describes some common terms and conventions that are used throughout the Disaster Recovery Orchestrator user interface and documentation. These terms are listed in an alphabetical order.

Application Monitoring

A feature of Disaster Recovery Orchestrator that enables you to monitor applications running on a physical computer or a virtual machine. If the application components fail and cannot be recovered after a certain number of attempts, the application status is reported accordingly on the Health View or the Console UI.

Application Monitoring Configuration

An application that is configured for monitoring on the on-premises application host or the cloud application host. Disaster Recovery Orchestrator Client manages the application monitoring configuration on a system.

Application Recovery Configuration

An application that is configured for migration or for disaster recovery (DR) in the cloud in the event of a failure at the on-premises site. Disaster Recovery Orchestrator Console manages all the application recovery configurations. An application must be configured for monitoring before it can be configured for DR.

The following systems are associated with every application recovery configuration:

- On-premises application host
- Console host
- Cloud application host

These systems are also referred to as the systems that participate in the DR solution for an application.

Application Virtual Machine or Cloud Application Host

The Azure virtual machine on which Disaster Recovery Orchestrator Client is installed. This virtual machine acts as the Azure counterpart of on-premises system that hosts the application that is configured for recovery. The application is configured for monitoring on this virtual machine as well. If the on-premises application or its host becomes unavailable a recovery administrator performs Takeover. When Takeover is successful, this virtual machine begins processing the application.

Client

The Disaster Recovery Orchestrator client component that manages the authentication, file replication, application monitoring, and user interface modules.

Client Host

The on-premises system or the Azure virtual machine on which Disaster Recovery Orchestrator Client is installed. This system hosts the application and its monitoring configuration.

Cloud

The Microsoft Azure cloud service platform.

For more information, see the Microsoft article:

http://azure.microsoft.com/en-us/overview/what-is-azure/

Console

The Disaster Recovery Orchestrator server component that manages the authentication, file replication, DR, and user interface modules.

Console Host

The Azure virtual machine on which Disaster Recovery Orchestrator Console is installed. This virtual machine acts as controller for the DR activities.

Console UI

The Disaster Recovery Orchestrator Console user interface, which is browser-based.

Failback

The operation in which application processing is restored on the original on-premises system when it becomes available again. A recovery administrator manually triggers Failback, but the tasks involved in the operation are performed automatically in a predefined sequence.

File Replication

The replication mechanism that Disaster Recovery Orchestrator uses to synchronize application data between the on-premises site and the Azure site.

Firedrill

A feature of Disaster Recovery Orchestrator that lets you test your DR configuration. A fire drill operation tests the Takeover operations on an application configured for DR. When a fire drill is successful, the application comes online in a separate Azure virtual network, without disrupting the application in the production environment.

Journal file

The intermediate file that is used to store information about the updates made to the application data folders at the primary site. This information is further used to replicate those updates at the secondary site. This file is also referred to as the replication log.

On-Premises System or On-Premises Application Host

A physical computer or virtual machine that exists on the premises of an organization, rather than in the cloud. This system hosts the application that is configured for monitoring and then further configured for recovery.

Primary

The system or location that is the source for data replication, where data synchronization is required for recovery in the event of an operational failure. For example, while the application processes requests from the on-premises application host, that system is the primary and the Console host is the secondary.

Recovery or Disaster Recovery (DR)

A feature of Disaster Recovery Orchestrator that enables you to recover application processing in the cloud when your organization's on-premises site becomes unavailable. You can restore application processing back to the on-premises site when it is available again.

You can also perform a planned migration of the application from the on-premises site to the cloud site.

Recovery Administrator

A user who has the privileges to configure an application for recovery, perform recovery operations, and remove the application recovery configuration. A security administrator adds this user to the Privilege Settings tab of the Console UI.

Replication Log Volume

A dedicated volume on the storage that is attached to the systems that participate in the DR solution. This volume is used to store the journal file.

Secondary

The system or location that is the destination for data replication, where data synchronization is required for recovery in the event of an operational failure. For example, while the application processes requests from the cloud application host, that virtual machine is the primary and the on-premises application host is the secondary.

Security Administrator

A user who has the privileges to configure the recovery settings and other users for Disaster Recovery Orchestrator Console. The security administrator cannot directly work with application recovery configurations.

Takeover

The operation in which application processing is taken over by the cloud application host, when your on-premises application or its host or the site becomes unavailable. A recovery administrator manually triggers Takeover, but the tasks involved in the operation are performed automatically in a predefined sequence.

Virtualization Host

A host software that creates and manages virtual machines, for example, Microsoft Hyper-V Server.

Virtual Machine

A software-based computer that is provisioned to run certain processes or provide some specific services, like hosting an application.

Chapter 2

Requirements

This chapter includes the following topics:

System requirements

This section describes the hardware requirements for Disaster Recovery Orchestrator.

Processors

Disaster Recovery Orchestrator requires only a single CPU, and the minimum recommended processing speed is 1 GHz.

The following (or faster) processors are recommended:

- AMD Opteron
- AMD Athlon 64
- Intel Xeon with Intel EM64T support
- Intel Pentium IV with EM64T support

Memory

A minimum of 1 GB of RAM is required to install and use Disaster Recovery Orchestrator.

Storage

The following table lists the minimum disk space that is required to install each of the Disaster Recovery Orchestrator components.

Table 2-1 Disaster Recovery Orchestrator disk space requirements

Components	Minimum disk space required
Disaster Recovery Orchestrator Console	700 MB
Disaster Recovery Orchestrator Client	600 MB

Consider the following storage constraints:

- All the disks on the on-premises systems as well as the cloud virtual machines must be NTFS-formatted.

  Note: The recovery of applications depends on the file replication mechanism of Disaster Recovery Orchestrator, which does not work with the FAT or ReFS file systems.

- Dynamic disks and spanned volumes are not supported on the cloud virtual machines.
- Folder mounts are supported conditionally; a folder mount that points to a volume on a GPT disk is not supported.

Software requirements

This topic lists the software that Disaster Recovery Orchestrator requires for successful installation, configuration, and operation.

For the most recent information about the supported software, refer to the software compatibility list (SCL) at:

http://www.symantec.com/docs/TECH209011

Supported operating systems

The following table lists the operating systems on which you can install and use the Disaster Recovery Orchestrator components.

Table 2-2 Disaster Recovery Orchestrator supported operating systems

Operating Systems	Editions	Service Packs
Windows Server 2008 R2	Datacenter, Enterprise	Required: None Supported: SP1
Windows Server 2012	Datacenter, Enterprise	Required: None

Note: Your Azure subscription determines which platform versions and editions are available to create the virtual machines in the cloud.

You may create a virtual machine by uploading an image; there is no restriction on the operating system Edition in this case.

Supported applications

The following table lists the applications for which Disaster Recovery Orchestrator provides application monitoring and disaster recovery services.

Table 2-3 Disaster Recovery Orchestrator supported applications

Application	Architecture	Edition
Microsoft SQL Server 2008	64-bit	Enterprise, Standard
Microsoft SQL Server 2008 R2	64-bit	Datacenter, Enterprise, Standard
Microsoft SQL Server 2012	64-bit	Enterprise, Standard
Custom applications and generic services	32-bit, 64-bit	-

Supported browsers and other software

The following additional software is required:

- .NET framework 4.5 is required to install Disaster Recovery Orchestrator components.
- Adobe Flash Player 12 or later is required to use the Disaster Recovery Orchestrator Console UI.
- The following browsers are supported:
  - Internet Explorer 9 or later
  - Mozilla Firefox 19 or later

Network and security requirements

The network and security requirements for Disaster Recovery Orchestrator are as follows:

- Virtual private network (VPN) in the cloud for disaster recovery (DR)
  Create virtual network instance to be used as the failover network where application processing can continue if the on-premises becomes unavailable.
  See "Creating a virtual network in Azure to implement disaster recovery" on page 30.
- VPN in the cloud for fire drills
  Optionally, create a separate VPN instance in the cloud to test the DR configuration for your application without affecting the production environment.
  See "Creating a virtual network in Azure to perform fire drills" on page 32.
- Connectivity between the on-premises and the cloud networks
  Configure a site-to-site VPN connection to link your on-premises network to the cloud virtual network, so that resources in both the networks can communicate directly and securely.
- Firewall and ports
  If you have firewall, add exceptions for the ports that the applications need to use.
  See "Ports required for Disaster Recovery Orchestrator" on page 22.
- Network protocol usage restriction
  Disaster Recovery Orchestrator does not support the use of IPv6; disable IPv6 on all the systems on which you plan to install the product.
- Domain configuration
  The DNS server records must be up-to-date at all times so that the Disaster Recovery Orchestrator services do not encounter communication issues.
  See "Domain configuration recommendations" on page 28.
- Users and privileges
  Make sure that the existing users have the necessary privileges to install the Disaster Recovery Orchestrator components. Create users with the appropriate privileges so that they can configure applications for monitoring and DR, and perform operations on those configurations.
  See "Users and privileges required for Disaster Recovery Orchestrator" on page 24.
- The following exceptions must be added to the sites that can be accessed from your browser:
  - For the Disaster Recovery Orchestrator Console UI:

`https://ConsoleHost:14155/draas/login.html`

Replace the *ConsoleHost* variable with the name of the virtual machine that hosts the Console.

- For managing application monitoring configurations using Disaster Recovery Orchestrator Client:

  `https://ClientHost:5634/vcs/admin/application_healthview.html`

  Replace the *ClientHost* variable with the names of the systems that host the Client components.

- The following exceptions must be added to the pop-up blocker on your browser:
  - To enable pop-ups from the Console UI on a system within the private network:

    `ConsoleHost:14155`

    Replace the *ConsoleHost* variable with the name of the virtual machine that hosts the Console.
  - To enable pop-ups from the Console UI on a system over the public Internet:

    `ConsoleHostDNSName.cloudapp.net:14155`

    Replace the *ConsoleHostDNSName* variable with the DNS name of the virtual machine that hosts the Console.

    Note: This applicable only if the appropriate endpoint is added to the Console host.

Ports required for Disaster Recovery Orchestrator

Disaster Recovery Orchestrator and its related services need to use some dedicated ports on the systems that participate in the DR solution. If you have configured a firewall, ensure that the firewall settings allow access to the required services and ports.

The following table provides information about the required ports.

Table 2-4 Ports required by Disaster Recovery Orchestrator services

Port	Service	Protocol & Binding	Action Required
5634	Symantec Storage Foundation Messaging Service (`xprtld.exe`)	HTTPS: Bidirectional	Add exception to firewall
14141	Symantec High Availability Engine (`had.exe`)	TCP: Inbound	Ensure availability

Table 2-4 Ports required by Disaster Recovery Orchestrator services *(continued)*

Port	Service	Protocol & Binding	Action Required
14151	Symantec DRaaS Service listens on this port for a shutdown request	TCP: Inbound	Ensure availability
14153	Symantec DRaaS Authentication Service (`vxatd.exe`)	TCP: Inbound	Add exception to firewall
14154	Disaster Recovery Orchestrator Console Database (`dbsrv11.exe`)	HTTPS: Bidirectional	Add exception to firewall
14155	Symantec DRaaS Service (`draasctlsvc.exe`)	TCP: Inbound	Add exception to firewall
14159	Symantec File Replication (`vxrepservice.exe`)	TCP: Bidirectional	Add exception to firewall
49452 – 49652	DCOM Required for ports used by the Symantec File Replication service	TCP: Bidirectional	Add exception to firewall

After adding the necessary exceptions to the firewall, perform the following activities to make the dynamic ports range for DCOM (49452 – 49652) available:

- Make changes to the registry as described in the Microsoft article: http://support.microsoft.com/kb/154596
- Enable the following predefined firewall rules:
  - COM+ Network Access
  - COM+ Remote Administration

Additionally, the following system service ports need to be opened:

25, 53, 67, 88, 123, 135, 137, 138, 139, 389, 445 , 464, 636, 1433, 2148, 2535, 3268, 3269, 3389, 5722, 9389, 14152

For further information about these ports and their usage, see the Microsoft article:

http://support.microsoft.com/kb/832017

Users and privileges required for Disaster Recovery Orchestrator

The following table describes the required users and privileges.

Table 2-5 User and privileges required for Disaster Recovery Orchestrator

Roles	Functions	Privileges
-	Disaster Recovery Orchestrator Console installation	■ Domain user ■ Local administrator on the Console host
-	Disaster Recovery Orchestrator Client installation	■ Local administrator on the Client host ■ May or may not be a domain user

Security administrator	■ Manages the recovery settings on Disaster Recovery Orchestrator Console
	■ Manages privilege settings:
	  ■ Designates users as recovery administrators and guests on the on-premises application hosts
	  ■ Edits Admin or Guest privileges for a user
	  ■ Removes user privileges
		■ Domain user or domain administrator
		■ Local administrator on the Console host

■ Recovery administrator ■ Guest user	Recovery administrators can: ■ Create application monitoring configurations and application recovery configurations. ■ Perform operations on these configurations. ■ Remove these configurations. Guest users can only view the applications, the status of operations that are performed on the application configurations, and the corresponding reports.	Local administrator on the on-premises application host, or the corresponding cloud application host, or both For information about the Console users, refer to the *Symantec Disaster Recovery Orchestrator Administration Guide*.

Table 2-5 User and privileges required for Disaster Recovery Orchestrator *(continued)*

Roles	Functions	Privileges
-	This user's credentials are sought as input when a recovery administrator configures an application for recovery in the cloud (Disaster Recovery Orchestrator Configuration Wizard, Virtual Computer Name panel). The Lanman agent uses these credentials to access data and the application on an application host.	■ DNS administrator ■ Local administrator on all the systems that are associated with each application recovery configuration (the on-premises application host, the corresponding cloud application host, and the Console host) For information about the considerations for a DR configuration, refer to the *Symantec Disaster Recovery Orchestrator Administration Guide*.

Requirements for file replication

Disaster Recovery Orchestrator uses file-level replication to ensure that the application data at the on-premises site and at the cloud site is in sync.

For more information about file replication, refer to the *Symantec Disaster Recovery Orchestrator Administration Guide*.

The following requirements must be met for file replication to work:

- If a firewall is enabled on a system that hosts the file replication service, add exceptions to allow traffic across the firewall. These exceptions should include the default file replication port (14159) and any user-configured ports.
- The disks on which application data is stored must be NTFS-formatted. File replication does not work with the FAT or ReFS file systems.
- The following types of files are are not replicated:
  - Reparse points
  - Compressed files
  - Encrypted files

  If such files exist in your application data folders, make sure that you manage them appropriately.
- The minimum required journal file size is 1 GB, and the Disaster Recovery Orchestrator Configuration Wizard sets this by default. However, Symantec

recommends that you set the journal file size to 10 GB so that you do not encounter performance issues.

You can specify the journal file size at the following locations:

- On the Replication Settings page of the Symantec Disaster Recovery Orchestrator Configuration Wizard
  The wizard does not let you proceed with configuring an application for DR if you specify a size less than 1030 MB.
- On the Settings page of an application on the Console UI
  If you change the size to a smaller value, Disaster Recovery Orchestrator displays an error and does not let you save the change.

- The journal file must *not* be stored at the following locations:
  - The system volume
  - A temporary storage
  - The volume where the application data is stored

  Also, each time a recovery operation is performed on an application, the volume that contains the journal file in the cloud is moved as follows:
  - During the takeover operation, the volume is detached from the Console host and attached to the cloud application host.
  - During the failback operation, the volume is detached from the cloud application host and attached to the Console host.

  Therefore, the journal file for an application configuration at the cloud site must be stored on an independent volume.

Chapter 3

Preparing the cloud environment

This chapter includes the following topics:

Setting up the cloud infrastructure for disaster recovery readiness

Before you can install the Disaster Recovery Orchestrator components, you need to set up the Azure infrastructure. This involves creating virtual networks, enabling firewalls and ports, creating virtual machines, and using certificates to establish secure communication between your on-premises and the cloud networks.

Note: If you already have an Azure setup in place, you may not need to perform the tasks described in the following topics.

To set up the Azure infrastructure

1. Procure a Microsoft cloud services subscription.

To perform any activity in the Azure cloud, you must sign in to the Azure Management Portal. The Microsoft cloud services subscription provides you with Microsoft account credentials that you can use to sign in to the portal.

For further information, visit the Microsoft website at:

http://azure.microsoft.com/

2. Create virtual networks for the following purposes:
   - To create and administer application recovery configurations
   - (Optional) To test whether the on-premises applications can be successfully recovered in the cloud

   See "About creating virtual networks in Azure" on page 29.
3. Create virtual machines for the following purposes:
   - To manage the DR configurations, on which Disaster Recovery Orchestrator Console must be installed later
   - To host applications, on which Disaster Recovery Orchestrator Client must be installed later

   See "About creating virtual machines in Azure" on page 33.
4. Create a management certificate and a service certificate for authentication

   See "About using certificates for Azure authentication" on page 37.

Domain configuration recommendations

Symantec recommends that you configure a domain controller in Azure to locally autenticate the users, applications, and services in the cloud. While creating the domain, make the following ports available for the cloud domain controller:

Table 3-1 Ports to be made available for the cloud domain controller

Name	Protocol	Public Port	Private Port	Load-Balanced Set Name
DNS	TCP	53	53	-
LDAP	TCP	389	389	-

These ports are required for Microsoft's site management feature of the domain controller to work.

For more information about the required ports, refer to the Microsoft article:

http://technet.microsoft.com/en-us/library/dd772723%28v=ws.10%29.aspx

For more information about creating a cloud domain controller, refer to the Microsoft article:

http://azure.microsoft.com/en-us/documentation/articles/virtual-networks-install-replica-active-directory-domain-controller/#subnets

For information about the other ports required for Disaster Recovery Orchestrator:

See "Ports required for Disaster Recovery Orchestrator" on page 22.

Test the domain controller configuration using the following command:

```
nltest /DSGETDC:DomainName
```

Make sure that the following output string points to the local site:

```
Our Site Name: LocalSiteName
```

If it points to a non-local site, the issue might be one of the following:

- The site-level domain controller configuration is not done.
- The sites are unable to communicate with each other using the aforementioned ports.

To fix this issue, take the following actions:

1. Create a subnet-based site; refer to the Microsoft article:

   http://azure.microsoft.com/en-us/documentation/articles/virtual-networks-install-replica-active-directory-domain-controller/#subnets
2. Enable `SYSVOL` sharing; refer to the Microsoft article:

   http://support.microsoft.com/kb/947022
3. Reboot the domain controller system.

About creating virtual networks in Azure

Keep the following information ready when you create virtual networks in Azure:

- The IP addresses and subnet range of the on-premises network
- The IP addresses and subnet range planned for the Azure network
- An external IP address for the virtual private network (VPN) device

Refer to the following topics about creating the virtual networks that are required for configuring and testing application recovery configurations:

- See "Creating a virtual network in Azure to implement disaster recovery" on page 30.
- See "Creating a virtual network in Azure to perform fire drills" on page 32.

Creating a virtual network in Azure to implement disaster recovery

Azure lets you create a virtual network and securely link it to your on-premises network. The following procedure describes how to create a custom virtual network for Disaster Recovery Orchestrator.

To create a custom virtual network

1. Sign in to the Azure Management Portal using your Microsoft account credentials.
2. On the navigation pane, select **Networks** and click **New** on the command bar.
3. On the Virtual Network Details pages, specify the following:
   - Provide a name to identify the virtual network.
     For example, use **DRO_VPN**
   - Either select an existing affinity group or create a new one.
     If you choose to create a new affinity group, provide the following information:
     - Select an appropriate region.
       The virtual network is created in a datacenter in this region.
     - Provide a name to identify the affinity group.
       For example, use **DRO_Console_Aff_Grp**.

   Click the Next icon to proceed to the next page.
4. On the DNS Servers and VPN Connectivity page, select the **Configure site-to-site VPN** check box. You may enter the DNS name and IP address later.

   Click the Next icon to proceed.
5. On the Site-to-Site Connectivity page, specify the following:
   - Provide a name for the VPN device.
     For example, use **DRO_VPN_Device**.
   - Provide an external IP address for the VPN device.
   - Specify the IP addresses and subnet range of the on-premises network in the Starting IP and CIDR fields.

   Click the Next icon to proceed.
6. On the Virtual Network Address Spaces page, specify the following:
   - Specify the IP addresses and subnet range of the Azure network in the Starting IP and CIDR fields.
   - Add the required subnets and a gateway subnet.

Click the Complete icon to configure your network.

Upon completion, the new virtual network appears on the Networks page with its status as Created. You can further the edit the network settings using the Dashboard, Configure, and Certificates pages for the virtual network.

To edit the virtual network settings

1. On the Networks page of the Azure Management Portal, click the **DRO_VPN** network that you created.
2. On the Dashboard page, click **Create Gateway** and select the routing based on the VPN device.

   For example, select **Dynamic Routing**.

   Note: Choose the routing (static or dynamic) based on the VPN device capability. For the relevant information, refer to the Microsoft and the VPN device documentation.

   ---

3. When prompted, click **Yes** to confirm that you want to create a gateway for the selected network.

   This tasks takes a few minutes to complete.
4. On the Download a VPN Device Configuration Script dialog box, select the appropriate **Vendor**, **Platform**, and **Operating System**.

   Click the Complete icon to download the script.
5. When prompted, click **Keep** to confirm that the script should be saved.

   A visual representation of the virtual network appears on the Dashboard page.
6. Click **Connect** to complete creating the gateway by establishing the connection between the on-premises network and the new DR virtual network.
7. Select the Gateway IP Address value and click **Manage Key**.

   The Manage Shared Key dialog box displays the key, which you must use to configure your local network VPN device to connect to the virtual network.

Gather the following information and provide it to the IT or firewall implementation engineer for further configuration:

- On-premises IP addresses and subnet range
- Azure IP addresses and subnet range
- Gateway IP address
- Shared key

- VPN device script
- List of ports that need to be opened across the firewall
  See "Network and security requirements" on page 21.

For more information, see the Microsoft articles:

- http://msdn.microsoft.com/library/azure/jj156074.aspx
- http://msdn.microsoft.com/en-us/library/azure/dn133795.aspx

Creating a virtual network in Azure to perform fire drills

To perform disaster recovery (DR) fire drills, you need to create a bubble network in Azure. This network must be separate from the network in which Disaster Recovery Orchestrator Console is installed. The fire drill operation simulates the takeover and failback operations using this bubble network.

The following procedure describes how to create a custom virtual network for performing DR fire drills. This is an optional task. You need to create a fire drill network only if you plan to perform fire drills for any application configuration.

To create a custom virtual network

1. Sign in to the Azure Management Portal using your Microsoft account credentials.
2. On the command bar, click **New**.
3. From the menu, select **Network Services > Virtual Network > Custom Create**.
4. On the Virtual Network Details pages, specify the following:
   - A name to identify the virtual network.
     For example, use **DRO_FD_VPN**
   - Either select an existing affinity group or create a new one. You could select the same affinity group that is used for the network in which the Console component is installed. If you choose to create a new affinity group, provide the following information:
     - Select a region.
       The virtual network is created in a Datacenter in this region.
     - Provide a name to identify the affinity group.
       For example, use **DRO_FD_Aff_Grp**.

   Click the Next arrow in the bottom right corner to continue.

5 On the DNS Servers and VPN Connectivity page, click the Next icon to proceed to the next page.

6 On the Virtual Network Address Spaces page, specify the following:

- Specify the address space with a private address range.
- Add the required subnets.

Click the checkmark on the lower right to configure your network.

You can further the edit the network settings using the Dashboard, Configure, and Certificates pages for the virtual network in the Azure Management Portal.

For more information, see the Microsoft articles:

- http://msdn.microsoft.com/library/azure/jj156074.aspx
- http://msdn.microsoft.com/en-us/library/azure/dn133795.aspx

About creating virtual machines in Azure

An Azure virtual machine is a server that you can create and manage in the cloud. You must sign in to the Azure Management Portal to create a virtual machine in the cloud.

To implement the disaster recovery (DR) solution, you need to create the following virtual machines in Azure:

- A dedicate virtual machine on which to install Disaster Recovery Orchestrator Console

  This virtual machine is referred to as the Console host, which is used to configure applications for DR. It manages the DR operations and the replication that is required to keep the data in sync between the on-premises and the Azure sites. After the Console is installed, you can access the Console UI from any system within the network using the following URL:

  `https://ConsoleHost:14155/draas/login.html`

  Replace the *ConsoleHost* variable with the name of the virtual machine that hosts the Console. On the Console host itself, you may replace *ConsoleHost* with **localhost**.

  To access the Console UI from outside the network, add the port 14155 to the endpoints of the Console host. Thereafter, you can access the Console UI using the following URL:

  `https://ConsoleHostDNSName.cloudapp.net:14155/draas/login.html`

  Replace the *ConsoleHostDNSName* variable with the DNS name of the Console host.

- One virtual machine corresponding to each on-premises system that hosts an application that you want to configure for DR
  Install and configure Disaster Recovery Orchestrator Client and the appropriate application on each such virtual machine.

You can create an Azure virtual machine in one the following ways:

- Using a standard Azure template
  See "Creating an Azure virtual machine using a standard template" on page 34.
- Using a custom virtual machine template
  See "Creating a virtual machine in Azure using a custom template" on page 36.

The following storage is required:

- An operating system disk (or system volume) for the Console virtual machine
- An operating system disk (or system volume) for the virtual machine that hosts the application in the cloud
- A separate volume to store the journal file for each application recovery configuration
- As many application data volumes as required for the configured application

Creating an Azure virtual machine using a standard template

Use this method to create an Azure virtual machine when you do not need to replicate an existing system by using its image.

To create a virtual machine using the Azure image gallery

1. On the command bar, click **New**.
2. From the menu, select **Compute > Virtual Machine > From Gallery**.
3. On the Virtual Machine Image Selection page, select a platform image and click the forward arrow to continue.

   The platform must be among those supported for Disaster Recovery Orchestrator.

   See "Software requirements" on page 19.
4. On the Virtual Machine Configuration pages, specify the following:
   - If multiple versions of the image are available, select the one that you want to use.
   - Provide a meaningful name for the virtual machine.
     For example, use **DRO_Console** for the virtual machine on which you plan to install Disaster Recovery Orchestrator Console.

- Select a virtual machine size that would satisfy your storage requirement for disaster recovery (DR).

  For example, if you want to attach more than 8 disks, select **Extra Large (8 cores, 14 GB memory)**.

  The number of disks that can be attached to a virtual machine depends on the size of a virtual machine.

  Symantec recommends using the **Extra Large** or **Large** size for a virtual machine where you plan to install Disaster Recovery Orchestrator Console.

  In a DR configuration, all the disks are attached to the Console virtual machine. Therefore, the size of the Console virtual machine should be such that the maximum number of disks can be attached to it.

  For further recommendations about the virtual machine size, see the Microsoft article:

  http://msdn.microsoft.com/library/azure/dn197896.aspx

- Provide the credentials of the user who is identified to manage this server. For example, use **DRO_Console_User** for the administrative user.

Click the forward arrow to continue.

- Select the **Create a new cloud service** option.
- Provide a DNS name, which is used to contact the virtual machine through the cloud service. Make sure that the text is between 3 and 24 characters in length and contains only lower case letters and numbers.
- Select the network and subnet in which to make the virtual machine available.

  For example, select the site-to-site virtual network that you created earlier, **DRO_VPN**.

  See "Creating a virtual network in Azure to perform fire drills" on page 32.

- Use the default settings in **Storage Account** and **Availability Set**.

Click the forward arrow to continue.

The only endpoint that is required is 3389, which is the default port for the Remote Desktop.

If you plan to host the Console on this virtual machine and to make the Console UI accessible over the public Internet, add the 14155 port to the endpoints.

Click the forward arrow to finish creating the virtual machine.

For more information, see the Microsoft article:

http://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-tutorial/

Now, test whether the virtual machine is accessible.

See "Testing the connection to an Azure virtual machine" on page 37.

After creating the virtual machine in this manner, make sure to do the following:

- If you plan to use this virtual machine as the Console host, install and configure Disaster Recovery Orchestrator Console.

  Note: Make a note of the virtual machine name and the cloud service name. You may need these values later to create a new virtual machine and restore the Console component, if it gets corrupted.

- If you plan to use this virtual machine as an application host, install and configure Disaster Recovery Orchestrator Client and the application that you want to configure for recovery.

Creating a virtual machine in Azure using a custom template

Use this method to create a virtual machine in Azure based on a custom template. A custom template is the image of a system whose configuration you want to replicate. The image is stored as a VHD file, which is uploaded to Azure.

To create a virtual machine using a custom image, perform the following tasks:

1. Prepare the image to be uploaded.
2. Create a storage account in Azure.
3. Prepare the connection to Azure.
4. Upload the `.vhd` file.

For information about how to perform these tasks, see the Microsoft article:

http://azure.microsoft.com/en-us/documentation/articles/virtual-machines-create-upload-vhd-windows-server/

Now, test whether the virtual machine is accessible.

See "Testing the connection to an Azure virtual machine" on page 37.

Note: Check the Name and the Host Name values on the virtual machine details page of the Azure Management Portal. These values must match exactly for the application recovery configurations to work. If they are different, change the Host Name to match the Name and restart the virtual machine.

After creating a virtual machine in this manner, make sure to do the following:

- If you plan to use this virtual machine as the Console virtual machine, install Disaster Recovery Orchestrator Console.
  Skip this task if the Console component was installed on the system whose image was used to create the virtual machine.

  Note: If you create a Console virtual machine using this method, make a note of the virtual machine name and the cloud service name. You may need these values later to create a new virtual machine and restore the Console component, if it gets corrupted.

- If you plan to use this virtual machine as an application host, install and configure Disaster Recovery Orchestrator Client and the application that you want to configure for recovery.
  Skip this task if the Client component, or the application, or both were installed on the system whose image was used to create the virtual machine.

Testing the connection to an Azure virtual machine

After creating a virtual machine in Azure, you might want to test whether the virtual machine is accessible. You must sign in to the Azure Management Portal to test the connection.

To test the connection to a new Azure virtual machine

1. Sign in to the Azure Management Portal with the appropriate credentials.
2. On the Virtual Machine Instances page, select the virtual machine.
3. On the command bar, click **Connect**.
4. Click the `.rdp` file that the portal retrieves to connect to the virtual machine.
5. On the Remote Desktop Connection window, click **Connect**.
6. Provide the administrative user credentials that you specified when creating the virtual machine, and click **OK** to log on.

About using certificates for Azure authentication

Azure uses certificates to authenticate individuals, computers, and other entities on a network. For Disaster Recovery Orchestrator, you need to create a management certificate and a service certificate. The management certificate is associated with an Azure subscription. Disaster Recovery Orchestrator Console uses the service certificate to authenticate the requests that are sent to Azure.

Azure authorizes it to perform operations on the resources in the cloud, like creating or deleting virtual machines, attaching or detaching disks, and so on.

To use certificates for Azure authentication, perform the following tasks:

1. Create a management certificate.

   See "Creating a management certificate" on page 38.
2. Create a service certificate.

   See "Creating a service certificate" on page 39.
3. Create the encoded management certificate.

   See "Creating the encoded management certificate" on page 40.
4. Associate the management certificate with the Azure subscription.

   See "Associating the management certificate with the Azure subscription" on page 40.
5. Copy the service certificate to the Console virtual machine.

   See "Copying the service certificate to the Console virtual machine" on page 41.
6. Import the Chinese management certificate to the Console virtual machine if the Chinese Azure network is used.

   See "Importing the Chinese management certificate" on page 46.

Creating a management certificate

Azure requires a management certificate (CER file) to authenticate the Disaster Recovery Orchestrator services that manage the subscription resources.

For more information about management certificates, see the Microsoft article:

http://msdn.microsoft.com/en-us/library/azure/gg551722.aspx

To create a management certificate

- Open a Visual Studio command prompt and run the following command to create the certificate file:

  ```
  makecert -sky exchange -r -n "CN=CertificateName" -pe -a sha1
  -len 2048 -ss My "CertificateName.cer"
  ```

  For example:

  ```
  makecert -sky exchange -r -n "CN=SDRO" -pe -a sha1
  -len 2048 -ss My "SDRO.cer"
  ```

  The `makecert` command creates the management certificate and stores it in the default **Personal** certificate store for the current user.

Creating a service certificate

Azure requires a service certificate of the Personal Information Exchange (PFX) type to verify the authenticity and security of the Disaster Recovery Orchestrator services.

For more information about service certificates, see the Microsoft article:

http://msdn.microsoft.com/en-us/library/azure/gg432987.aspx

To create a service certificate (PFX file)

1. Open the certificate manager using the following command:

   ```
   certmgr.msc
   ```

2. Expand **Personal > Certificates**, and select the management certificate (CER file) that you created earlier.
3. From the Action menu, click **All Tasks > Export** to launch the Certificate Export Wizard.
4. On the Welcome page, click **Next**.
5. On the Export Private Key page, choose the option to export the private key and click **Next**.
6. On the Export File Format page, select **Personal Information Exchange** but do not select any of the related options, and click **Next**.
7. On the Password page, specify a password to protect the private key and click **Next**.

8 On the File to Export page, click **Browse** to navigate to an appropriate location and specify a name for the PFX file.

For example:

```
SDRO.pfx
```

Click **Next**.

9 Verify the export settings that you provided and click **Finish**.

Creating the encoded management certificate

To create an encoded management certificate (CER file)

1 Select the certificate that you created earlier and click **Action > All Tasks > Export** to launch the Certificate Export Wizard.

2 On the Welcome page, click **Next**.

3 On the Export Private Key page, choose not to export the private key and click **Next**.

4 On the Export File Format page, select **DER encoded binary** and click **Next**.

5 On the File to Export page, click **Browse** to navigate to an appropriate location and specify a name for the CER file, for example:

```
SDRO.cer
```

Click **Next**.

6 Verify the export settings that you provided and click **Finish**.

Associating the management certificate with the Azure subscription

Azure uses a management certificate to authenticate a client application that acts on behalf of a subscription owner to manage subscription resources. A management certificate is exported as a `CER` file, which does not contain its private key. This file is uploaded to the Azure Management Portal and stored at the subscription level. When the certificate is installed on the client system, it must contain its private key.

To associate the CER file with the Azure subscription

1 Navigate to the following URL, click on the Portal link at the top-right, and sign in using your Microsoft account:

http://azure.microsoft.com/

2 In the navigation pane, click **Settings**.

3 On the Management Certificates page, click **Upload**.

4 On the Upload a Management Certificate page, select the encoded management certificate (CER file) that you created earlier, and close the page.

Copying the service certificate to the Console virtual machine

Copy the service certificate (PFX file) to a folder on the Azure virtual machine that you plan to designate as the Console host. You need to provide this file path while installing Disaster Recovery Orchestrator Console.

See "Creating a service certificate" on page 39.

Note: The PFX file must be present on the local storage of the Console host at all times. The storage must not be detached from the virtual machine for as long as Disaster Recovery Orchestrator Console is installed.

After the installation, you may move the PFX file to any other location on the local storage of the Console host. Immediately after you move the PFX file, you must inform Disaster Recovery Orchestrator Console about this change. To do so, you must log on as a security administrator and update the **PFX File Path** on the Recovery Settings tab of the Console UI.

For more information, see the *Symantec Disaster Recovery Orchestrator Administration Guide*.

Note: Make a note of the PFX file location. You may need it later to create a new virtual machine and restore the Console component, if it gets corrupted.

See "Adding resiliency to Disaster Recovery Orchestrator Console" on page 47.

Chapter 4

Installing and configuring the product

This chapter includes the following topics:

About installing Disaster Recovery Orchestrator components

Installing Disaster Recovery Orchestrator involves the following tasks:

- Install Disaster Recovery Orchestrator Console on an Azure virtual machine. This virtual machine would then function as a controller for the disaster recovery (DR) activities.
- Optionally, configure a backup of the Console components. This adds resiliency to Disaster Recovery Orchestrator Console in case it fails due corruption in the operating system or the applications.
- Install Disaster Recovery Orchestrator Client on the on-premises application host and on the corresponding cloud application host. The application will be

available on the cloud application host when the on-premises application or its host becomes unavailable.

Considerations for installing Disaster Recovery Orchestrator Console

Consider the following before installing Disaster Recovery Orchestrator Console:

- Internet connectivity is required to access the Azure environment.
- A Microsoft account with an Azure subscription is required to sign in to the Azure Management Portal.
- A management certificate (CER file) and the corresponding service certificate (PFX file) is required for Azure authentication.
  See "About using certificates for Azure authentication" on page 37.
- Disaster Recovery Orchestrator Console can be installed only on an Azure virtual machine with one of the supported platforms.
  See "Software requirements" on page 19.
- The Azure virtual machine on which you install Disaster Recovery Orchestrator Console is referred to as the Console host. The installer must be launched locally on this virtual machine. Remote installation of the Console components is not allowed.
- An external disk should not be manually attached to the Console host.

  Note: Only Disaster Recovery Orchestrator manages the addition or removal of all storage devices on the Console host.

- The following user configurations are expected:
  - The user who installs Disaster Recovery Orchestrator Console must be a valid domain user and a member of the local Administrators group.
  - The User Access Control (UAC) feature of Windows must be disabled.
- A separate network is required to configure fire drills. It must not be a production network.
  Optionally, you can create this fire drill network later, and add its details to the Settings page of Disaster Recovery Orchestrator Console.
- Virtual Machines running Windows Server 2008 R2 must have .NET 4.5 installed. It is available by default with Windows Server 2012.

- The Name and the Host Name values of the virtual machine must match exactly. Check these values on the virtual machine details page of the Azure Management Portal. If these values are different, Disaster Recovery Orchestrator may fail to finalize an application recovery configuration or to restore the application processing from the cloud to the on-premises site.

Installing Disaster Recovery Orchestrator Console

Install Disaster Recovery Orchestrator Console on an Azure virtual machine that you plan to designate as a controller for the disaster recovery (DR) activities.

To install Disaster Recovery Orchestrator Console using the installation wizard

1. In Windows Explorer, browse to the Disaster Recovery Orchestrator software package directory, and double-click the `Setup.exe` file.
2. On the Symantec Product Installer screen, click **Install Disaster Recovery Orchestrator Console** to launch the installation wizard.
3. On the Welcome panel, review the list of prerequisites, make sure that they are met, and then click **Next**.
4. On the License panel, read the license terms, select **I accept the terms of License Agreement**, and click **Next**.

   The **Participate in the Symantec Product Improvement Program by submitting system and usage information anonymously** check box is selected by default. The Product Improvement Program allows the product installer to collect installation, deployment, and usage data, and anonymously submit it to Symantec. This information helps identify how customers deploy and use the product. If you do not want to participate in the product improvement program, clear this check box.
5. On the System Validation panel, verify the following:
   - The current system appears in the System field.
     Remote installation is not allowed.
   - The default installation directory is: `C:\Program Files\Veritas`. You can customize this location either by entering the path manually or by clicking **Browse...** and navigating to the desired location.
   - The wizard performs certain validation checks on the system and notes the details in the Verification Status field.
     If the system fails the validation checks, the wizard does not proceed with the installation. Review the details, rectify the issue, and then click **Re-Verify** to re-initiate the validation checks for this system.

   Click **Next**.

6 On the Cloud Authentication panel, provide the following information:

- Location of the Personal Information Exchange (PFX) file
- Password for the PFX file
- Azure subscription ID
- Cloud region
  This region indicates your Azure network location.

Note: For the China region, make sure to import the Chinese management certificate on this virtual machine after the Disaster Recovery Orchestrator Console installation is complete. If you import the certificate before the installation is complete, the wizard overwrites it.

See "Importing the Chinese management certificate" on page 46.

Note: Make a note of the PFX file name and its current path. You may need these values later to create a new virtual machine and restore Disaster Recovery Orchestrator Console, if it gets corrupted.

Click **Next**.

The wizard uses this information to authenticate the user credentials in the cloud environment.

For information about creating and using Azure certificate files:

See "About using certificates for Azure authentication" on page 37.

7 On the Fire Drill Network panel, provide the following information:

- Select the bubble network to be used for performing fire drills.
- Specify the subnet to be used.
  Alternatively, you may specify the subnet later on the DR Settings page of Disaster Recovery Orchestrator Console.

Click **Next**.

8 On the Domain Authentication panel, provide the credentials of the Active Directory user for authentication on the Windows domain.

9 On the Pre-install Summary panel, review the summary.

If you want to save this information for future reference, click **Save Report**. The default file name is `PreInstallReport`, and you can save it in a few different formats.

If any issues occur, review the log for details, and rectify the issues before proceeding.

Click **Next**.

10 On the Installation panel, review the progress of the installation.

If the installation fails, the details pane displays the status accordingly. You may click **Cancel** to exit the wizard. Perform the necessary troubleshooting tasks, and relaunch the wizard to complete the installation.

After the installation succeeds, click **Next** to begin the post-installation tasks.

11 On the Post-install Summary panel, review the installation results.

If you want to save this information for future reference, click **Save Report**. The default file name is `PostInstallReport`, and you can save it in a few different formats.

If the installation fails, refer to the log file for details. You may have to reinstall the software.

Click **Finish** to exit the wizard.

Importing the Chinese management certificate

If you install Disaster Recovery Orchestrator Console in a Chinese Azure network, you need to import the appropriate management certificate. This certificate is referenced and used when you select **China** in the **Cloud Region** field on the Cloud Authentication panel of the installation wizard.

Note: Import this certificate only after you complete the Disaster Recovery Orchestrator Console installation. Otherwise, the installation wizard overwrites the certificate entry.

To import the Chinese management certificate

1 Download the certificate from the following location:

http://www.cnnic.cn/download/cert/SHA2SSL.cer

Note: Save the `SHA2SSL.cer` file on a volume that is permanently attached to the Console host. Do not change the file name.

Make a note of the location where you save this file. You may need it later to create a new virtual machine and restore Disaster Recovery Orchestrator Console, if it gets corrupted.

See "Adding resiliency to Disaster Recovery Orchestrator Console" on page 47.

---

2 Open the command prompt in the **Run as administrator** mode at the following location:

```
C:\Program Files\Veritas\draasconsole\jre\lib\security
```

3 Import the certificate using the following command:

```
..\..\bin\keytool -keystore cacerts -importcert -alias chinaazure
-file CertificateFileLocation
```

Replace *CertificateFileLocation* with the appropriate file name and path.

4 Open the Services window, right-click **Symantec DRaaS Service**, and click **Restart** from the context menu.

Adding resiliency to Disaster Recovery Orchestrator Console

Disaster Recovery Orchestrator Console may be susceptible to corruption in the operating system or the applications. Symantec recommends that you back up the Console configuration to make it less susceptible to corruption. The following utilities enable you to add resiliency to the Console:

- `backup_console.pl`

  This utility performs the following actions:

  - Takes a one-time backup of the Disaster Recovery Orchestrator database and the authentication configuration
  - Schedules the periodic backups of the Disaster Recovery Orchestrator database

  You can specify the frequency and the location of the backup.

- `restore_console.pl`

  This utility restores the authentication configuration and database files, which includes attaching the appropriate data disks to the new Console host.

Note: You may perform the tasks that are listed in this topic after you have configured the applications for monitoring and recovery in the cloud. However, if you want to make the Console less susceptible to corruption right from the beginning, perform these tasks immediately after the installation.

To add resiliency to Disaster Recovery Orchestrator Console

1. Make a note of the following items:

   - Virtual machine name and cloud service name of the Console host

     These values are provided in the **Virtual Machine Name** and the **Cloud Service** fields when creating the virtual machine in Azure.

     See "About creating virtual machines in Azure" on page 33.

   - Name and path of the PFX file

     The PFX file is placed on a volume that is permanently attached to the Console host. This file is the service certificate that is used at the time of the Disaster Recovery Orchestrator Console installation.

     See "Installing Disaster Recovery Orchestrator Console" on page 44.

     On the Disaster Recovery Orchestrator Console UI, which is available after the installation is complete, the PFX file location is displayed on the Recovery Settings tab. Only a security administrator can access the Recovery Settings tab.

   - Names of the storage disks that are attached to the Console host

     The operating system disk can be deleted if the Console host needs to be re-created. The disks on which the journal file and the application data are stored must be retained.

2. Schedule a backup.

   Scheduling is a one-time activity that you can perform immediately after installing Disaster Recovery Orchestrator Console or after configuring applications for recovery.

   To schedule a backup

3. If a Disaster Recovery Orchestrator Console failure occurs, perform the following tasks sequentially:

   - Delete the Console host from the Azure Management Portal, and remember to select the **Keep the attached disks** option.

If the replication volume and the application data volumes are attached to the Console host, they are retained in the Azure storage account.
You may delete the operating system disk that was attached to the Console host.

- Create a new virtual machine with the same Virtual Machine Name and Cloud Service Name as the previous Console host.
- Install Disaster Recovery Orchestrator Console on the newly created virtual machine, and use the PFX file name and path that you noted earlier.
- Attach the disks on which the journal file and the application data are stored.

Note: Do so only if these disks were attached to the Console host (not the cloud application host) earlier.

---

4 Restore the Disaster Recovery Orchestrator Console configuration using the backup.

To restore the backup

To schedule a backup

1 Log on to the Console host.

2 Open the command prompt at the Console installation folder. For example:

```
C:\Program Files\Veritas\draasconsole\bin
```

3 Run the following command:

```
"C:\Program Files\Veritas\vrtssfmh\bin\perl.exe" backup_console.pl
/PATH NetworkLocation /USERNAME UserName [/PASSWORD Password]
[/PERIOD Period]
```

Here, the parameters take the following values:

- *NetworkLocation* is the location where the data is backed up.
- *UserName* and *Password* are the credentials of any user who has access permissions on the network location and the local system.
- *Period* is the duration (in hours) after which database is backed up; the default is 2 hours.

This utility stops the Symantec DRaaS Console Database Service, the Symantec DRaaS Service, and the Symantec DRaaS Authentication Service. It starts these services again immediately after the backup task is complete. This one-time activity is performed only at the first instance of the backup. These services are not stopped during the subsequent database backups.

To stop the periodic backup

1. Open the Task Scheduler window.
2. Expand **Task Scheduler Library > Symantec**.
3. Select the **DRaaS_Console_Backup** task, and click **Delete** from the Actions menu.

   The Console is no longer backed up.
4. If you want to schedule the periodic backups again, run `backup_console.pl`.

   To schedule a backup

To restore the backup

1. Log on to the Console host.
2. Open the command prompt at the Console installation folder. For example:

   ```
   C:\Program Files\Veritas\draasconsole\bin
   ```
3. Run the following command:

   ```
   restore_console.pl /PATH NetworkLocation
   ```

   Here, *NetworkLocation* is the location where the data is backed up.

Considerations for installing Disaster Recovery Orchestrator Client

Before you begin to install Disaster Recovery Orchestrator Client, consider the following:

- The user who performs the installation must have local administrator privileges. In case of remote installations, the user must have local administrator privileges on all the selected systems.
- On the systems where you plan to install these components:
  - The User Access Control (UAC) feature of Windows must be disabled.
  - The .NET 4.5 framework must be installed.
  - IPv6 must not be configured.
  - The Name and the Host Name values of the virtual machine must match exactly. Check these values on the virtual machine details page of the Azure Management Portal. If these values are different, Disaster Recovery Orchestrator may fail to migrate or to recover a configured application from the on-premises site to the cloud.

Installing Disaster Recovery Orchestrator Client

For each application that you want to configure for disaster recover (DR), install Disaster Recovery Orchestrator Client on the following systems:

- The on-premises system that hosts the application (on-premises application host)
- The Azure virtual machine (cloud application host) where the application will be available when the on-premises application or its host becomes unavailable

To install Disaster Recovery Orchestrator Client using the installation wizard

1. In Windows Explorer, browse to the Disaster Recovery Orchestrator software package directory, and double-click the `Setup.exe` file.
2. On the Symantec Product Installer screen, click **Install Disaster Recovery Orchestrator Client** to launch the installation wizard.
3. On the Welcome panel, review the list of prerequisites, make sure that they are met, and then click **Next**.
4. On the License panel, read the license terms, select **I accept the terms of License Agreement**, and click **Next**.

   The **Participate in the Symantec Product Improvement Program by submitting system and usage information anonymously** check box is selected by default. The Product Improvement Program allows the product installer to collect installation, deployment, and usage data, and anonymously submit it to Symantec. This information helps identify how customers deploy and use the product. If you do not want to participate in the product improvement program, clear this check box.
5. On the System Validation panel, select the systems and their installation directories as follows:

   The `localhost` information is populated by default; you can remove it if you do not want to install Disaster Recovery Orchestrator Client on it. You can install the product remotely on other systems in the domain. You can select more systems in the following ways:

   - In the **System Name or IP** field, type the name or IP address of a system, and click **Add**.

     Note: Disaster Recovery Orchestrator does not support Internet Protocol version 6 (IPv6), so do not add a system that uses IPv6.

   - Alternatively, click **Browse...** to select the systems.

The systems that belong to the domain to which you have logged on are listed in the **Available Systems** list. Select one or more systems and move them to the **Selected Systems** list. Click **OK**.

Once you add or select a system, the wizard performs certain validation checks, and notes the details in the Verification Details field. To review the details of a particular system, select it from the list on the left.

The default installation directory is: `C:\Program Files\Veritas`. For each system, you can customize this location either by entering the path manually or by clicking **Browse...** and navigating to the desired location.

To use the customized location for to multiple systems, click **Apply Install Options to Multiple Systems...**. On the dialog box that appears, select the systems on which to customize the location, and then click **OK**.

Unless all the selected systems pass the validation checks, the wizard does not proceed with the installation. For each system that might have failed the validation checks, review the details, rectify the issue, and then click **Re-Verify**.

When all the systems have been verified, click **Next** to proceed with the installation.

6 On the Pre-install Summary panel, review the summary and click **Next**.

If you want to save this information for future reference, click **Save Report**. The default file name used is `PreInstallReport`, and you can save it in a few different formats.

If any issues occur, review the log for details, and rectify the issues before proceeding.

7 On the Installation panel, review the progress of the installation.

If the installation fails, the details pane displays the status accordingly. You may click **Cancel** to exit the wizard. Perform the necessary troubleshooting tasks, and relaunch the wizard to complete the installation.

After the installation succeeds, click **Next** to begin the post-installation tasks.

8 On the Post-install Summary panel, review the installation results.

If you want to save this information for future reference, click **Save Report**. The default file name used is `PostInstallReport`, and you can save it in a few different formats.

If the installation fails, refer to the log file for details. You may have to reinstall the software.

Click **Finish** to exit the wizard.

Chapter 5

Repairing the product installation

This chapter includes the following topics:

Considerations for repairing a Disaster Recovery Orchestrator installation

Repairing an installation restores it to its original state, which includes replacing missing or corrupt files, shortcuts, and registry entries. Use the Disaster Recovery Orchestrator installer to perform a repair operation.

Before you begin to repair an installation, consider the following:

- Before repairing the Disaster Recovery Orchestrator installation, repair the **Veritas Operations Manager (Host Component)** on the system.
- The installer uses the logged-on user account context to perform the repair operation. Verify that the logged-on user has local administrator privileges on the system where you want to repair the installation.
- If you have configured application monitoring, it may be temporarily suspended while the installer performs the reparation tasks. Therefore, the Health View may not display the most current status of the configured application during this time.
- If you have configured an application disaster recovery (DR), it may be temporarily suspended while the installer performs the reparation tasks.

Therefore, the Disaster Recovery Orchestrator Console UI may not display the most current status of the DR configuration during this time.

- Any ongoing file replication activities must be paused before you repair the installation. You must also resume the activities after the repair operation completes successfully.
- You can repair a local installation only. Repairing an installation remotely is not supported.
- You cannot repair a failed installation. The Repair option is available only for an installation that has completed successfully.
- While repairing the product installation, you cannot modify the installation options.

Repairing a Disaster Recovery Orchestrator Console installation

The Disaster Recovery Orchestrator Console installer runs in the Repair mode to restore the installed components to their original state.

To repair a Disaster Recovery Orchestrator Console setup

1. Pause any ongoing file replication activities by running the following commands sequentially on the Console host:
   - `vxfradmin -viewconfig`
     A list of all the replicated file group (RFG) names, each associated with an application recovery configuation, is displayed.
   - `vxfradmin -pauserep` *`RFGName`*
     Run this command for each RFG to pause the file replication.
2. In the Programs and Features window, select Symantec Disaster Recovery Orchestrator 6.1 Console, and click **Change** to launch the installer.
3. On the Mode Selection panel, the **Repair** option is selected by default. Click **Next**.
4. On the System Validation panel, verify the following:
   - The current system appears in the System field.
     Remotely repairing an installation is not allowed.
   - The location in the Install Directory field is correct.
     You cannot specify a different location when repairing an installation.
   - The wizard performs certain validation checks on the system and notes the details in the Verification Status field.

If the system fails the validation checks, the wizard does not proceed with the repair operation. Review the details, rectify the issue, and then click **Re-Verify** to re-initiate the validation checks for this system.

Click **Next**.

5 On the Cloud Authentication panel, provide the following information:

- Location of the Personal Information Exchange (PFX) file
- Password for the PFX file
- Azure subscription ID
- Region that is applicable to your Azure network

Click **Next**.

The wizard uses this information to authenticate the user in the cloud environment.

For information about creating and using a PFX file:

See "About using certificates for Azure authentication" on page 37.

6 On the Firedrill Network panel, provide the following information:

- Select the bubble network to be used for performing fire drills.
- Specify the subnet to be used.
  Alternatively, you may specify the subnet later on the DR Settings page of Disaster Recovery Orchestrator Console.

Click **Next**.

7 On the Domain Authentication panel, provide the credentials of the Active Directory user for authentication on the Windows domain.

Note that the user must not be a member of the local Administrators group.

8 On the Pre-install Summary panel, review the summary.

If you want to save this information for future reference, click **Save Report**. The default file name used is `PreRepairReport`, and you can save it in a few different formats.

If any issues occur, review the log for details, and rectify the issues before proceeding.

Click **Next**.

9 On the Installation panel, review the progress of the repair operation.

If the repair operation fails, the wizard displays the status accordingly; click **Cancel** to exit the wizard. Then, perform the necessary troubleshooting tasks, and relaunch the wizard to complete the operation.

After the repair operation succeeds, click **Next** to perform the post-repair tasks.

10 On the Post-install Summary panel, review the results of the repair operation.

If you want to save this information for future reference, click **Save Report**. The default file name used is `PostRepairReport`, and you can save it in a few different formats.

If the repair operation fails, refer to the log file for details. You may have to reinstall the software.

Click **Finish** to exit the wizard.

11 Resume any file replication activities that were paused by running the following command on the Console host:

`vxfradmin -resumerep` *`RFGName`*

Run this command to resume the file replication for each RFG for which you paused the activity earlier.

Repairing a Disaster Recovery Orchestrator Client installation

The Disaster Recovery Orchestrator Client installer runs in the Repair mode to restore the installed components to their original state.

To repair a Disaster Recovery Orchestrator Client setup

1 Pause any ongoing file replication activity by running the following commands sequentially on the local system:

- `vxfradmin -viewconfig`
  If an application on the system is configured for disaster recovery (DR), the corresponding replicated file group (RFG) name is displayed.
- `vxfradmin -pauserep` *`RFGName`*
  Run this command to pause the file replication.

2 In the Programs and Features window, select Symantec Disaster Recovery Orchestrator 6.1 Client, and click **Change** to launch the installer.

3 On the Mode Selection panel, the **Repair** option is selected by default. Click **Next**.

4 On the System Validation panel, verify the following:

- Only the current system appears in the systems list.
  Remotely repairing an installation is not allowed.
- The installed options for this system are uneditable.
  You cannot specify a different location or a license key when repairing an installation.
- The wizard performs certain validation checks on the system and notes the details in the Verification Details field.
  If the system fails the validation checks, the wizard does not proceed with the repair operation. Review the details, rectify the issue, and then click **Re-Verify** to re-initiate the validation checks for this system.

Click **Next**.

5 On the Pre-install Summary panel, review the summary.

If you want to save this information for future reference, click **Save Report**. The default file name used is `PreRepairReport`, and you can save it in a few different formats.

If any issues occur, review the log for details, and rectify the issues before proceeding.

Click **Next**.

6 On the Installation panel, review the progress of the repair operation.

If the repair operation fails, the wizard displays the status accordingly; click **Cancel** to exit the wizard. Then, perform the necessary troubleshooting tasks, and relaunch the wizard to complete the operation.

After the repair operation succeeds, click **Next** to perform the post-repair tasks.

7 On the Post-install Summary panel, review the results of the repair operation.

If you want to save this information for future reference, click **Save Report**. The default file name used is `PostRepairReport`, and you can save it in a few different formats.

If the repair operation fails, refer to the log file for details. You may have to reinstall the software.

Click **Finish** to exit the wizard.

8 Resume any file replication activity that was paused by running the following command on the local system:

```
vxfradmin -resumeerep RFGName
```

Run this command to resume the file replication that you paused earlier.

Chapter 6

Uninstalling the product

This chapter includes the following topics:

About uninstalling Disaster Recovery Orchestrator components

Before you uninstall the Disaster Recovery Orchestrator components, consider the following:

- If application monitoring is configured on the system, you must remove the configuration.
  If the application is also configured for DR, you must remove the DR configuration.
  Use the Unconfigure menu of the Console UI to remove an application recovery configuration. Doing so also removes the corresponding monitoring configuration from the Client hosts.
  For more information, see the *Symantec Disaster Recovery Orchestrator Administration Guide*.
- The installer uses the logged-on user account context for uninstallation. Verify that the logged-on user has local administrator privileges on the system where you want to uninstall the product.
- Remote uninstallation is not supported.
- The Application Information service must be running on all the systems participate in the DR solution. To start the service type the following at the command prompt:

  ```
  net start appinfo
  ```

Note: Do not uninstall Veritas Operations Manager (Host Component) before uninstalling Disaster Recovery Orchestrator. This component is shared among multiple Symantec products that may be installed on the same system. Uninstall Veritas Operations Manager (Host Component) only after all Symantec products, including Disaster Recovery Orchestrator, are uninstalled from the system.

Uninstalling Disaster Recovery Orchestrator Client

To remove Disaster Recovery Orchestrator Client completely from your setup, perform this operation on each system where it was installed. Unlike the installation, you cannot perform an uninstallation on remote systems.

To uninstall Disaster Recovery Orchestrator Client

1. In the Programs and Features window, select Symantec Disaster Recovery Orchestrator 6.1 Client, and click **Uninstall** to launch the installer.
2. On the Welcome panel, review the prerequisites, make sure that they are met, and then click **Next**.
3. On the System Validation panel, perform the following actions:
   - Verify that the current system appears in the System field. Remote uninstallation is not allowed.
   - Verify that the correct path appears in the Install Directory field.
   - The wizard performs certain validation checks on the system and notes the details in the Verification Details field. If the system fails the validation checks, the wizard does not proceed with the uninstallation. Click **OK** to close the message box that appears.
   - Review the details, rectify the issue, and then click **Re-Verify**.
   - When the system has been verified, click **Next**.
4. On the Pre-install Summary panel, review the summary.

   If you want to save this information for future reference, click **Save Report**. The default file name used is `PreUninstallReport`, and you can save it in a few different formats.

   If any issues occur, review the log for details, and rectify the issues before proceeding.

   Click **Next**.

5 On the Uninstallation panel, review the progress of uninstallation.

If the uninstallation fails, the wizard displays the status accordingly; click **Cancel** to exit the wizard. Then, perform the necessary troubleshooting tasks, and relaunch the wizard to complete the operation.

After the uninstallation succeeds, click **Next** to perform the post-uninstallation tasks.

6 On the Post-install Summary panel, review the uninstallation results.

If you want to save this information for future reference, click **Save Report**. The default file name used is `PostUninstallReport`, and you can save it in a few different formats.

If the uninstallation fails, refer to the log file for details. You may have to attempt this operation again, or manually clean up uninstallation.

Click **Finish** to exit the wizard.

Uninstalling Disaster Recovery Orchestrator Console

Uninstall Disaster Recovery Orchestrator Console from the Console host in Azure.

To uninstall Disaster Recovery Orchestrator Console

1 In the Programs and Features window, select Symantec Disaster Recovery Orchestrator 6.1 Client, and click **Uninstall** to launch the installer.

2 On the Welcome panel, review the prerequisites, make sure that they are met, and then click **Next**.

3 On the System Validation panel, perform the following actions:

- Verify that the current system appears in the System field. Remote uninstallation is not allowed.
- Verify that the correct path appears in the Install Directory field.
- The wizard performs certain validation checks on the system and notes the details in the Verification Status field. If the system fails the validation checks, the wizard does not proceed with the uninstallation. Click **OK** to close the message box that appears.
- Review the details, rectify the issue, and then click **Re-Verify**.
- When the system is validated, click **Next**.

4 On the Pre-uninstall Summary panel, review the summary.

If you want to save this information for future reference, click **Save Report**. The default file name used is `PreUninstallReport`, and you can save it in a few different formats.

If any issues occur, review the log for details, and rectify the issues before proceeding.

Click **Next**.

5 On the Uninstallation panel, review the progress of uninstallation.

If the uninstallation fails, the wizard displays the status accordingly; click **Cancel** to exit the wizard. Then, perform the necessary troubleshooting tasks, and relaunch the wizard to complete the operation.

After the uninstallation succeeds, click **Next** to perform the post-uninstallation tasks.

6 On the Post-uninstall Summary panel, review the uninstallation results.

If you want to save this information for future reference, click **Save Report**. The default file name used is `PostUninstallReport`, and you can save it in a few different formats.

If the uninstallation fails, refer to the log file for details. You may have to attempt this operation again, or manually clean up uninstallation.

Click **Finish** to exit the wizard.

Appendix A

Troubleshooting

This appendix includes the following topics:

Disaster Recovery Orchestrator logging

Disaster Recovery Orchestrator provides the following logging information.

Installation logs

Disaster Recovery Orchestrator installer logs contain details about the installation tasks and the overall progress status. These logs are useful for identifying installation-related issues.

The installer creates the log directory as soon as you launch the wizard. The log files are located at:

`%AllUsersProfile%\Veritas\VPI\log\`

`%AllUsersProfile%` expands to `C:\ProgramData`.

Console logs

The Disaster Recovery Orchestrator Console logs are located at:

`%AllUsersProfile%\symantec\draasconsole\Logs`

`%AllUsersProfile%` expands to `C:\ProgramData`.

The Console logs are written to the `azuredraas.log` file.

The components of the Console logs are as follows:

- Timestamp

The date and time the message was generated

- Duration
  The number of milliseconds elapsed between the construction of the layout and the creation of the logging event
- Thread
  The name of the thread that generated this logging event
- Priority
  Levels in the increasing order of priority: TRACE, DEBUG, INFO, WARN, ERROR, and FATAL
- Object
  The logger object, which the fully qualified class name of the caller that issues the logging request
- Message
  The actual message that was generated by the thread

Additionally, the Disaster Recovery Orchestrator UI components create logs that are available only for the duration of their existence. For example, the Console UI logs are available only as long as you are signed in and the session is active. These logs are lost after the session ends. Similarly, the Disaster Recovery OrchestratorConfiguration Wizard creates a log file that is available from within the wizard. This information is lost when you exit the wizard.

Agent logs

The agent logs are located at:

```
C:\Program Files\Veritas\cluster server\log
```

The components of the agent logs are as follows:

- Timestamp
  The date and time the message was generated
- Mnemonic
  The string ID that represents the product, for example, SDRO
- Severity
  Levels in the increasing order of severity: INFO, NOTICE, WARNING, ERROR, and CRITICAL
- UMI
  A unique message ID
- Message
  The actual message generated by the agent

Collecting Disaster Recovery Orchestrator logs

Disaster Recovery Orchestrator provides the `hagetcf` utility, which you can use to collect logs. This utility retrieves detailed diagnostic information about your application monitoring and recovery configurations. You can use this information to troubleshoot configuration-related issues. You can also share these logs with Symantec Technical Support for further troubleshooting.

The `hagetcf` utility is available at the following locations:

- On the Console host (Azure virtual machine where Disaster Recovery Orchestrator Console is installed):

  `InstallDir\draasconsole\bin`

  Here, *InstallDir* is the Disaster Recovery Orchestrator Console installation directory, typically, `C:\Program Files\Veritas`.

- On a system where Disaster Recovery Orchestrator Client is installed:

  `%vcs_home%\bin`

  The `%vcs_home%` environment variable points to the product home directory, typically, `C:\Program Files\Veritas\Cluster Server`.

To collect Disaster Recovery Orchestrator logs

1. On the Console host, navigate to the location where the utility is installed.

   This step is not required on Disaster Recovery Orchestrator Client systems.

2. Collect the logs using the following command:

   `hagetcf [-Option]`

   You can limit the diagnostic information to specific components using the various available options.

   Use the `-?` or `-help` option to view the command's usage information.

   Note: If you do not specify any options, the command retrieves diagnostic information with the options: `-app`, `-sys`, `-ha`, `-log`, `-lock`, `-conf`, `-state`,`-islog`, and `-trigger`. On a Console host, it also includes the logs for the Disaster Recovery Orchestrator Console component.

   By default, `hagetcf` writes the output to the following locations:

   - On the Console host:

     `%AllUsersProfile%\Symantec\hagetcf\mmdd_hhmm`

     The `%AllUsersProfile%` environment variable points to the common program data location, typically, `C:\ProgramData`.

- On Disaster Recovery Orchestrator Client systems:
  %vcs_home%\hagetcf*mmdd_hhmm*

The *mmdd_hhmm* folder name indicates the date and time when the logs were collected, for example: `C:\Program Files\Veritas\Cluster Server\hagetcf\0428_1520`. The folder contains several subfolders and log files, which represent various components.

Disaster Recovery Orchestrator deployment issues and solutions

This section lists the issues that you might encounter when installing, repairing, or uninstalling the Disaster Recovery Orchestrator components. It also describes the tasks that you can perform to work around these issues.

'ERROR: Could not connect to server (err=167)' occurs during post-install configuration of Disaster Recovery Orchestrator Console

If you encounter this issue, take the following actions:

- Make sure that the Symantec Storage Foundation Messaging Service (`xprtld`) service is running on the system.
- If the `xprtld` service is running, check your domain controller configuration using the following command:

  `nltest /DSGETDC:`*`DomainName`*

  Make sure that the following output string points to the local site:

  `Our Site Name:` *`LocalSiteName`*

  If it points to a non-local site, fix the domain controller configuration as per Symantec recommendations.
  See "Network and security requirements" on page 21.

Cloud authentication for Disaster Recovery Orchestrator fails in the Chinese Azure environment

You might encounter authentication issues when working with a Disaster Recovery Orchestrator deployment installed in the China region. The Chinese management certificate might be not correctly installed on the Console host.

Workaround

Check whether the Chinese management certificate is imported.

Open the command prompt at the following location:

```
C:\Program Files\Veritas\draasconsole\jre\lib\security
```

List the certificates using the following command:

```
..\..\bin\keytool -list -keystore cacerts
```

Verify that the `SHA2SSL.cer` file is listed. If not, install the certificate.

See "Importing the Chinese management certificate" on page 46.

IPv4Monitor goes in the Unknown state after the Hyper-V virtual machine rebooted

You might encounter this issue with an on-premises virtual machine on which Disaster Recovery Orchestrator Client is installed.

If a Hyper-V virtual machine has its MAC Address set to Dynamic, it may change when the virtual machine restarts. This could occur in the following cases:

- After the virtual machine is migrated to a different Hyper-V server, the MAC address range of that new Hyper-V server is different from that of the previous Hyper-V server.
- When the virtual machine was switched off, the MAC address was reassigned to a different virtual machine, and now that MAC address is in use.

Workaround

To avoid such configuration changes, set the MAC Address to Static from the Advaced Features page of the Network Connection Settings of the virtual machine.

Uninstallation of Console or Client fails if the relevant services are not stopped

A Disaster Recovery Orchestrator Console or Client uninstallation may fail if any of the following services are not stopped:

- Symantec DRaaS Authentication Service
- Symantec DRaaS Console Database Service
- Symantec DRaaS Service
- Symantec File Replication

The Uninstallation panel displays a message that mentions the services that have not stopped as expected.

Workaround

Perform the following tasks:

1. Open the Services window, select the services that need to be stopped, and select **Action > Stop**.
2. On the Uninstallation panel, click **Back** and click **Next** again to proceed with the uninstallation.

   Alternatively, exit the wizard and launch the uninstallation program again from the Programs and Features window.

Index

S

T

U

V

W