Symantec™ Disaster Recovery Orchestrator Release Notes

Microsoft Azure

6.1

May 2014

Symantec™ Disaster Recovery Orchestrator Release Notes

Product version: 6.1

Document version: 6.1 Rev 0

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

Release Notes for Disaster Recovery Orchestrator 6.1

This document includes the following topics:

About this document

This document provides important information about Symantec Disaster Recovery Orchestrator 6.1. Review this entire document before you install or upgrade Disaster Recovery Orchestrator.

You can download the latest version of this document from the Symantec Operations Readiness Tools (SORT) website here:

https://sort.symantec.com

The information in the Release Notes supersedes the information provided in the product documents for Disaster Recovery Orchestrator.

For the latest patches available for this release, go to:

https://sort.symantec.com/patch/matrix

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.

Salient features

The salient features of Disaster Recovery Orchestrator are as follows:

- Protection of applications for small and medium business (SMB) enterprises
  For the list of supported applications, refer to:
  http://www.symantec.com/docs/TECH209011
- Elimination of the need to maintain additional on-premises systems for backup and recovery
- Reduction in cost and maintenance effort due to the use of cloud-based resources

- Simple workflow for installation and configuration
- Discretionary access control based on user privileges
- Ability to view component dependency of application monitoring configurations using the Health View
- Console UI that provides a consolidated view of the application recovery configurations and makes it easy for administrators to monitor and perform recovery operations
- Granular replication of application-specific data to avoid unnecessary usage of network and storage resources
- Ability to test the application recovery configurations without affecting the production environment
- Single-click migration of applications from the on-premises site to the cloud or vice versa
- Ability to review the RPO/RTO values of the recovery operations performed on the configured applications
- Continued updates and additional application support distributed via Symantec Agent Pack releases
- Online documentation available in the cloud-based SymHelp format

Supported software

For the latest information about the supported software, refer to the Software Compatibility List (SCL) at the following location:

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

Configurations not supported with this release

This section lists the configurations that are not supported with the current release of Disaster Recovery Orchestrator.

Applications configured using Symantec ApplicationHA

Symantec does not support the use of ApplicationHA with Disaster Recovery Orchestrator. You may configure applications for monitoring using ApplicationHA. However, such application monitoring configurations cannot be further configured for disaster recovery (DR) using Disaster Recovery Orchestrator.

You must install and use Disaster Recovery Orchestrator Client to configure application monitoring. Only such application monitoring configurations can be further configured for DR using Disaster Recovery Orchestrator Console.

Restoring data using backup and recovery software

Disaster Recovery Orchestrator components can coexist with backup and recovery software from Symantec or other vendors. However, Disaster Recovery Orchestrator does not support the restore operation of any such software on the volumes that it manages.

Disaster Recovery Orchestrator employs file-based replication to synchronize the application data between the on-premises site and the cloud site. The file replication configuration is stored on the replication volume itself. If the volume is restored, the most recent configuration data is replaced with the old configuration data, which causes the replication to fail.

Software limitations

This section lists the software limitations that apply to Disaster Recovery Orchestrator.

For information about China Azure, see:

http://msdn.microsoft.com/en-us/library/dn578439.aspx

If Hyper-V Live Migration is configured, virtual machines must use static MAC addresses

If Hyper-V Live Migration is configured, then the virtual machines in that environment must be configured to use static MAC addresses.

Failing this, the following issues may arise:

- After migrating to a new Hyper-V host, a different MAC address may be assigned to the virtual machine. This may occur because the range of MAC address is different for different hosts.
- While the virtual machine is rebooted as part of the recovery action, the existing MAC address may get reassigned to another system.

As a result of these issues, the IP and MAC address of the virtual machine may go in to an Unknown state and the application may fail.

For information about configuring a virtual machine to use static MAC Address, refer to the Microsoft documentation.

Open handles are not allowed on the secondary while initial sync is in progress

When an application is configured for recovery, Disaster Recovery Orchestrator performs an initial synchronization operation on the file replication targets. While this operation is in progress, the Dashboard view of the Console UI reports the replication status as Inconsistent. When the initial sync operation is completed, the Dashboard view displays the status as Consistent.

While the initial sync is in progress the data folders selected for replication at the secondary site must not have any open handles. The files in the configured folders at the secondary site should not be accessed by an application or a user, and they should not even be open in the Windows Explorer.

If there are any open handles at the secondary site, the initial sync operation fails, and the file replication cannot continue. If this happens, the DR configuration might fail.

Known issues

This section lists the known issues that exist in Disaster Recovery Orchestrator 6.1.

Deployment issues

This section lists the known issues that you might encounter when installing, repairing, or uninstalling the Disaster Recovery Orchestrator components.

Repairing the Console installation breaks the single sign-on configuration with the Client hosts

The repair operation re-creates the certificates that are required by the Disaster Recovery Orchestrator authentication service. As a result, the single sign-on connections with the Client hosts fail. Therefore, the heartbeat status of all the application recovery configurations appear out of sync on the Applications view. (3493575)

Workaround

Perform the following tasks for each on-premises application host and the corresponding cloud application host:

1. Launch any supported browser and enter the following URL:

   `https://`*`ConsoleHost`*`:14155/draas/ConfigureSSO.dr?hostName=`*`ClientHost`*`&userName=`*`Domain`*`\`*`UserName`*`&password=`*`Password`*

Replace the variables as follows:

ConsoleHost	Name of the Console host
ClientHost	Name of the Client host
Domain\UserName	Name of user in whose context the application monitoring helper service runs, prefixed with the domain name **Note:** Note: This value is provided on the Virtual Computer Name panel of the Disaster Recovery Orchestrator Configuration Wizard.
Password	Password of the user that was previously mentioned

2. When the browser prompts for authentication, provide the name (in the *Domain\Username* format) and password of any user who is authorized to access the Console.

To verify whether single sign-on is re-established, open the Applications view and check whether the heartbeats of all the application recovery configurations are in sync.

User interface issues

This section lists the known issues that you might encounter when working with the Disaster Recovery Orchestrator UI.

Console UI hangs if left idle for a few hours

If you log on to the Console UI and do not perform any actions on the UI for a few hours, it becomes unresponsive. (3371568)

Workaround: If you leave the Console UI idle for longer than 30 minutes, log on again to be able to use the UI.

Disaster Recovery Orchestrator Configuration Wizard becomes inactive after a session timeout

The default session timeout duration of a Console login is 30 minutes. If you launch the configuration wizard and leave it idle for longer than the session timeout duration, the wizard becomes unresponsive. The wizard also fails to display a session timeout error if you click any action button on it. (3414240)

This issue does not have a workaround. You need to log on to the Console and launch the configuration wizard again.

Launching multiple instances of the Disaster Recovery Orchestrator Configuration Wizard from the same browser gives unexpected results

If you launch the wizard from multiple tabs of a browser or from multiple instances of the same browser, the configuration operations return unexpected results. (3451977)

Workaround: If you need to run concurrent Configure operations, log on to the Console UI using different browsers or from different systems.

A recovery administrator is able to perform operations on an application even though the privileges are changed

A recovery administrator signs in to the Console UI to perform operations on an application. A security administrator who has signed in using a different browser or system may assign the Guest privileges to the signed-in recovery administrator. After the privilege settings are changed, the user should not be able to perform any operations on an application. However, the changed privilege settings are not communicated to a different browser session. Therefore, the user can perform operations as long as the current session lasts. (3436490)

Example: User1, who is configured with the Admin privileges, signs in to the Console UI and performs Takeover on a configured application. Now, the security administrator signs in from a different browser or system, changes the privileges for User1 from Admin to Guest, and saves the change. If User1 is still signed in, User1 can perform Failback on the application, even though the Admin privileges are no longer available. The change in privileges is reflected only when User1 signs out of the current session and signs in again.

This issue does not have a workaround.

Recommendation: The security administrator must not change a user's privilege settings from a different browser session while the user is signed in to the Console UI.

The option to dismiss a completed operation is not visible on the Applications view

Even though an operation is complete, the Dismiss link may not be visible on the Applications view of the Console UI. You might encounter this issue if the Operation column size is insufficient or if the horizontal scroll bar does not appear in the browser window. (3408994)

Workaround: Increase the size of the Operation column on the Applications view so that the **Dismiss** link is visible. Alternatively, open the view corresponding to the operation and use the **Dismiss** link in the Status column of the application.

Active directory user information is lost when the user name is changed and an incorrect password is entered

Log on to the Disaster Recovery Orchestrator Console as a security administrator and open the Recovery Settings tab. Select the **Change Non Admin AD User** check box, enter a different AD user name, and provide an incorrect password. The relevant error message is displayed when you click **Confirm**, but the AD User field no longer displays the original value. (3474672)

This issue does not have a workaround. The original AD User value is not displayed even after you log out and log on again. When you provide a wrong AD user name and password combination, the Disaster Recovery Orchestrator authentication configuration fails. You need to re-enter the original values or enter the correct information for a different user.

The AD User field on the Settings view does not accept the *username@domain* and other formats

Log on to the Disaster Recovery Orchestrator Console as a security administrator and open the Recovery Settings tab. Select the **Change Non Admin AD User** check box, enter an AD user name in the ***username@domain*** or any other format and provide the correct password. When you click **Confirm**, an error message is displayed. (3474694)

This issue does not have a workaround. The domain name or any other information is not required to be entered along with the user name. The user name must be single string without any spaces.

Configuration and operation issues

This section lists the known issues that you might encounter when performing the following tasks with the Disaster Recovery Orchestrator components:

- Configuring application recovery administrators and their privileges
- Configuring or unconfiguring applications for monitoring or for recovery
- Performing operations on the monitoring or the recovery configurations
- Changing the recovery settings of the Console or the applications

Retrying a failed task multiple times causes Symantec DRaaS Service to crash

When creating an application recovery configuration, you might encounter a failed task on the wizard. The **Retry** link appears next to the task. You can then troubleshoot the issue and click **Retry** to attempt the task again. If the task is still

not successful, the **Retry** link appears again. If you click **Retry** multiples times, the Symantec DRaaS Service might fail. (3414487)

Workaround: Keep the wizard open. For example, if you encountered the issue on the Disaster Recovery Orchestrator Configuration Wizard, keep the wizard open. Start the Symantec DRaaS Service from the Services window on the Console host. Then, retry the task again.

Configuring an application for recovery fails when 16 or more folders are selected for replication

If you select 16 or more folders on the Data Mapping for Replication panel of the Disaster Recovery Orchestrator Configuration Wizard, the application recovery configuration is not created. On the Implementation panel, the status of the 'Configure file replication' task appears as 'Failed'.

Disaster Recovery Orchestrator does not support replicating more than 15 folders simultaneously. However, a selected parent folder may have any number of subfolders. (3075014)

Workaround: To resolve this issue, you must close the wizard and launch it again. Then, select 15 or fewer folders on the Data Mapping for Replication panel and proceed with the next steps. The application recovery configuration completes successfully.

Cleanup fails if another Firedrill operation is in the Failed state

You can simultaneously perform fire drills on multiple applications. However, if one of the operations fails, you cannot run the Cleanup operation on any of the other fire drill configurations. The following error is displayed:

```
Unable to perform the operation on some or all of the selected
applications. For each application, do the following:
-Make sure that no other operation is in progress.
-If an operation has completed, make sure to clear its status using
the Dismiss link.
```

Workaround

Perform the following tasks to work around this issue:

1. On the Firedrill view of the Console UI, select the application for which the operation has failed.
2. Identify the task that has failed, resolve the issue, and return to this view. On the command bar, click **Retry**.

If you cannot resolve the issue, click the **mark as complete** link in the Status column to proceed. You can attempt to address the related issues later.

3. On the Firedrill view, select the other applications on which the operation was completed successfully.

   On the command bar, click **Cleanup**.

Recovery administrators or guest users can be deleted even though an application is configured for recovery

A security administrator can add, edit, or delete any recovery administrator or guest user on the Privilege Settings page of the Console UI at any time. Any such user, who is configured for an on-premises application host, can be deleted even when the application is configured for recovery. (3446647)

Workaround: If you accidentally delete such a user, make sure to again add the user with the same privileges on the same application host.

Removing the recovery configuration of a custom application does not remove the replication data from all the associated volumes

Even though the Unconfigure operation on a custom application recovery configuration completes successfully, the replication data on the volumes might not be deleted. This issue occurs if the dependency of the volume mounts is not set when configuring the custom application for recovery. The option to set this dependency is provided on the Define Start-Stop Order panel of the Application Monitoring configuration wizard. (3496914)

Workaround: Perform the following tasks on the on-premises application host and the cloud application host to work around this issue.

Remove the replication data for an unconfigured application as follows:

1. Run the following command to stop the replication service:

   ```
   net stop vxrepservice
   ```

2. Run the following command to unload the replication drivers:

   ```
   fltmc unload vxrep
   ```

3. Access the appropriate volumes and delete the `vfrdatabase` folder.

4. Run the following command to load the replication drivers:

   ```
   fltmc load vxrep
   ```

5. Run the following command to start the replication service:

```
net start vxrepservice
```

Data synchronization issues

This section lists the known issues that you might encounter with the file replication component of Disaster Recovery Orchestrator. This component is used to synchronize the application data between the on-premises site and the cloud site.

Replication stops unexpectedly while the initial synchronization is in progress

This issue might occur due to various reasons. One of the possible reasons is that the folders configured for replication might be renamed or deleted at the primary while initial synchronization is in progress. (3390546)

Workaround: If a folder that is configured for replication is renamed or deleted during the initial synchronization, the application recovery configuration is corrupted. Remove the application recovery configuration, and create it again using the Disaster Recovery Orchestrator Configuration Wizard.

Unable to stop the replication even though the replication is in the Started state

This issue might occur due to various reasons. One of the possible reasons is that the application data disk is offline or is inaccessible. In this case, you would encounter other issues with the application itself. (3394660)

Workaround: Attach the application data disk if it has been detached, or bring the disk online if it is offline. Unless any changes are made to the configuration, the replication continues as expected.

Replication status appears as 'Error' for an application

You might encounter errors with application data replication due to various reasons.

Some of the possible reasons are:

- A file from an outside location, but one that exists on the same volume, is cut and pasted into a folder that is configured for replication.
- A file being replicated is deleted and then restored from the recycle bin.

If you paste or restore files in such a manner, they are not replicated, and an error is reported at the secondary system (replication target). Ideally, only the application that writes the data in the folders that are configured for replication should manage the data. (3336407)

Workaround: If files are incorrectly added or removed, the replication status appears as 'Error' in the Applications view of the Console UI. To resolve this issue, you must stop and start the replication again. Select the application, and click **Stop Replication**. After the operation is completed successfully, click **Start Replication**.

Some application data is lost if the replication volume is unresponsive or is detached for a few moments

If the disk on which the journal file is located is unresponsive or is detached for a few moments, the replication status is not updated. If the replication status was Consistent before the disk got detached, it remains unchanged if the disk is attached back in a few moments. However, if any application data was updated during that time, it is not replicated. (3425930)

Workaround: If you identify that such an event has occurred and that the application data is not consistently replicated, stop the replication and start it again. When you start the replication, initial synchronization is performed, which appropriately replicates all the application data at the source.

Internationalization issues

This section lists the known issues that you might encounter when running Disaster Recovery Orchestrator in locales other than U.S. English.

Only US-ASCII characters are supported

Disaster Recovery Orchestrator does not support file paths and the names of servers, application configurations, volumes, databases, directories, and files that include non-ASCII characters. You may not be able to map application data folders for replication if their names contain non-ASCII characters. (3380457)

Workaround: Only use US-ASCII characters in file paths and when naming servers, application configurations, volumes, databases, directories, and files.

Interoperability issues

This section lists the known issues that you might encounter when Disaster Recovery Orchestrator coexists or interacts with other software.

Multiple issues occur if Disaster Recovery Orchestrator 6.1 Client is installed on the same system as SFW 6.0.1 or SFW 6.0.2

Disaster Recovery Orchestrator Client can coexist on a system with Symantec Storage Foundation (SFW). No issues occur if the 6.1 versions of both the products

are installed. However, you might encounter the following issues if older versions of SFW are installed:

- Issue 1
  An application that is configured for monitoring with Disaster Recovery Orchestrator Client fails to start if SFW 6.0.1 or SFW 6.0.2 is installed on the same system.
- Issue 2
  Even though SFW 6.0.1 or SFW 6.0.2 is installed with a valid license key, the Veritas Enterprise Administrator (VEA) service fails to start.

The following message may be logged in the Event Viewer:

`The product on the computer` *`SystemName`* `contains no valid license.`

Here, *SystemName* is the name of the physical computer or the virtual machine. (3339065)

Workaround

Perform the following tasks to resolve this issue:

1. Navigate to the following folder:

   `C:\Program Files (x86)\Common Files\Veritas Shared\vrtslic\lic`

2. Copy the SFW license files. These files have the `.vxlic` extension.
3. Navigate to the following folder:

   `C:\Program Files\Common Files\Veritas Shared\vrtslic\lic`

4. Paste the copied SFW license files.

You may perform the following tasks to check whether the issue has been resolved:

- For issue 1
  From the Health View, click **Start Application**. Then, check whether the application comes online.
- For issue 2
  Manually start the VEA service. Then, open the VEA GUI and check whether you can configure disk groups and volumes.

A system crash occurs if you use SFW to create snapshots of the application data volumes or the replication volumes

You can use Symantec Storage Foundation (SFW) to create snapshots of the application data volumes. However, if you create the snapshots after configuring the application for recovery, the system crashes. (3504056)

Workaround: If you need to create snapshots, do so before you configure the application for recovery. If the application is already configured for recovery, unconfigure it, and then create the snapshots.

Recommendation: Do not use SFW to create snapshots on the systems that participate in the DR solution for an application.