# Symantec™ Disaster Recovery Orchestrator Release Notes

## Amazon Web Services

6.1.1

November 2014

# Symantec™ Disaster Recovery Orchestrator Release Notes



Product version: 6.1.1

Document version: 6.1.1 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_apj@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 6.1.1

This document includes the following topics:



## About this document

This document provides important information about Symantec Disaster Recovery Orchestrator 6.1.1. 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 in the Amazon cloud 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 in the cloud. An application that is configured with Disaster Recovery Orchestrator can also be migrated to the cloud.

# Product 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/TECH225292
- 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/TECH225292

# 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 supports the backup and restore operations only on files, folders, and applications.

---

**Note:** Disaster Recovery Orchestrator does not support the restore operation on volumes and virtual machines.

---

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 you perform a restore operation, the most recent configuration data is replaced with the old configuration data, which causes the replication to fail. Therefore, do not restore the files and folders that are associated with the replication configuration, for example, the `VfrDatabase` folder.

# Software limitations

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

## The session timeout duration of the Console UI does not apply to modal windows

The default timeout duration of the Disaster Recovery Orchestrator Console UI session is 30 minutes. However, this timeout does not apply to any modal windows that you may open from the browser. Consider the following example:

Launch the Disaster Recovery Configuration wizard and select an on-premises system that does not have an application monitoring configuration on it. Open the Application Monitoring Configuration wizard, and leave it idle for longer than the session timeout duration. After 30 minutes, navigate to the next panel; you can proceed to configure an application for monitoring and close the wizard when the operation is complete. When you return to the Disaster Recovery Configuration wizard and click **Next**, the Console displays a session timeout error and does not let you perform any further actions. To complete the disaster recovery configuration, you need to relaunch the Disaster Recovery Configuration wizard. If you select the

same system again, the wizard identifies the application monitoring configuration that you completed, and lets you proceed further.

# Known issues

This section lists the known issues that exist in Disaster Recovery Orchestrator 6.1.1.

## 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 SSO 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 (SSO) 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: Re-establish the SSO connections between the Console host and all the systems that are associated with the application recovery configurations.

Perform the following tasks for each Client host:

1. Sign in to the Disaster Recovery Orchestrator Console UI.

   The browser authenticates the SSO request based on this sign-in information.

2. Enter the following URL in the same tab or a different tab of the same browser instance:

   `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<br>**Note:** Make sure that the Client host is switched on and accessible. For example, if the cloud application host is not on at this time, you can perform this task at a later time when it is started. |

| | |
|---|---|
| *Domain\UserName* | Name of the domain and a user who has administrative privileges on the Console host |
| *Password* | Password of the user that was previously mentioned |

If the Console session has not been established in the previous step, the browser does not prompt for authentication and rejects the SSO request.

In any case, the browser displays the status of the SSO request.

3. Optionally, to double-check whether SSO has been re-established, open the Applications view and check whether the heartbeats of all the application recovery configurations are in sync.

## Uninstalling the Disaster Recovery Orchestrator Client fails if you take snapshots of the replicated volumes

Consider a scenario where an application is configured for monitoring on an on-premises system. You use Symantec Storage Foundation (SFW) to create snapshots of the volumes that are attached to the system. If you try to uninstall Disaster Recovery Orchestrator Client from such a system, the operation fails. (3627018)

Workaround: Perform the following procedure and then retry the uninstallation.

**To delete the replication database folder from the snapshot**

1. If the replication service is not already stopped, run the following command to stop it:

   ```
   net stop vxrepservice
   ```

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

   ```
   fltmc unload vxrep
   ```

3. (Optional) Use the Windows `mountvol` command to identify the SFW volume on which the folder for the replication configuration database exists.

   Identify the GUID of the volume whose snapshot was created. You can find this information in the uninstallation log.

4. By default, snapshot volumes are read-only; make the volume read-writeable.

5. Delete the `VfrDatabase` folder on the volume.

6. (Optional) Make the snapshot volume read-only again.

# 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.

## Launching multiple instances of the Disaster Recovery 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.

## Console UI displays the stale replication state of an application recovery configuration if it is not online

If an application recovery configuration is not online, its replication state is not refreshed on the Console UI. The Dashboard view and the Applications view display the stale replication state. (3620301)

You may ignore the replication state of such an application recovery configuration. When it is brought online at either the on-premises site or the cloud site, its replication status is refreshed automatically.

## 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.

### Incorrect link to Online Help on the Symantec Product Installer screen

The Online Help button that appears on the Symantec Product Installer screen points to the SymHelp topics of the previous release of Disaster Recovery Orchestrator. (3655737)

Workaround: Use the following URL to access the correct SymHelp topics.

http://help.symantec.com/CS?ProdId=SDRO_GSG&context=sdro6.1.1

## 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

If a task fails while configuring an application for recovery, the **Retry** link appears next to the task in the wizard. 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: For example, if you encountered this issue on the Disaster Recovery 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 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.

## 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.

## The volumes are not attached back to the cloud application host if it is already started during an Unconfigure operation

While an application that is configured for recovery is online at the on-premises site, the cloud application host is expected to be in the Stopped state. If you start the cloud application host outside of Disaster Recovery Orchestrator control, make sure to stop it before you run the Unconfigure operation. Otherwise, Disaster Recovery Orchestrator fails to detach the appropriate volumes from the Console host and attach them to the cloud application host. However, it completes the other tasks successfully, and does not display any error messages. (3654470)

---

**Note:** This issue does not occur if the application is online on the cloud application host when you trigger the Unconfigure operation

---

Workaround: Manually attach the volumes back to the cloud application host.

Perform the following tasks:

1. Sign in to the AWS Management Console.
2. Identify the volumes that were associated with the application recovery configuration.
3. Detach the volumes from the Amazon EC2 instance that acts as the Console host.
4. Attach the volumes to the instance on which the application was hosted.

# 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 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.

## The Failback operation fails if the replication configuration data is inconsistent

The last task of the Failback operation is to bring the application recovery configuration online, and it might fail if the associated replication configuration data is inconsistent. If this happens, the replication is stopped. (3622060)

Workaround: Manually start the replication from the Console host, wait for the replication state to become consistent, and then retry the task. If the task does not complete successfully even after the replication is in the consistent state, contact Symantec support.

**To start the replication and check the replication state**

1. Run the following command on the Console host to list all the replicated file group (RFG) names:

   ```
   vxfradmin -viewconfig
   ```

2. Identify the RFG that is associated with the application recovery configuration that you are trying to fail back to the on-premises site.

3. Run the following command to start the file replication:

   ```
   vxfradmin -startrep RFGName
   ```

   Replace the *RFGName* variable with the name of appropriate RFG.

4. Run the following command to check the replication status:

   ```
   vxfradmin -repinfo RFGName
   ```

   If the replication status is consistent, you see the following output:

   ```
   Replication Status :257
   ```

   If you see a different output, wait for a few moments and repeat the command until you see the output mentioned earlier.

# 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.

## Some issues may occur if Disaster Recovery Orchestrator 6.1.1 Client is installed on the same system as SFW 6.0.1 or SFW 6.0.2

Disaster Recovery Orchestrator 6.1.1 Client can coexist on a system with Symantec Storage Foundation (SFW) 6.1. However, you might encounter the following issues if older versions of SFW are installed on the same system:

- 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.