



Veritas InfoScale Operations Manager Patch 7.4.2.200

Last updated: 2020-10-26

VERITAS[™]

The truth in information.

Contents

Reports on Volume Replicator configurations	2
Generating a report for a VVR configuration	2
LDAP configurations using CLI	5
Configuring an LDAP domain.....	6
Assigning permissions to a user group.....	7
Unconfiguring an existing LDAP configuration.....	8
Changing the password for a bind user	8

Reports on Volume Replicator configurations

Veritas InfoScale Operations Manager lets you generate a variety of reports for your InfoScale configurations. Earlier InfoScale Operations Manager releases provide monitoring and management for Volume Replicator (VVR) configurations, but they do not provide comprehensive reports related to VVR operations.

InfoScale Operations Manager patch 7.4.2.200 provides the ability to generate VVR replication status reports. These reports provide the following point-in-time details over a specified week or a month:

- Replication status (repstatus)
- Activities like disconnects, data transfer, replication link (rlink) status, and so on
- Host status and details

These reports are available from the Server perspective. As an administrator, you can generate these reports either at the data center level or at the organization level. You can perform the following tasks from the Management Server console:

- Run a report
- Subscribe to a report
- Save a report as a comma-separated values (CSV) file
- Share the report via email in the CSV and the HTML formats
- Set schedules to generate reports

For details on using reports and performing the related tasks, see *Veritas InfoScale™ Operations Manager User's Guide*.

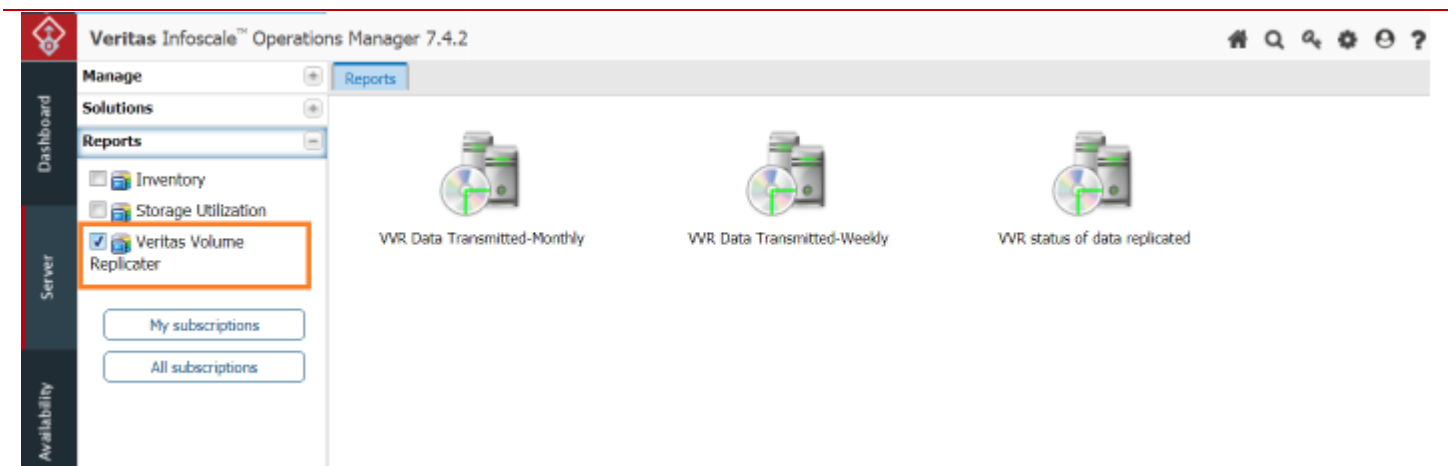
Generating a report for a VVR configuration

1. In the Management Server console, open a perspective, and select **Reports** in the left pane.
2. Expand **Reports** in the left pane and select **Veritas Volume Replicator**.
3. In the **Reports** view, click the report that you want to view.
4. In the **Select scope to run report** wizard panel, select the data range and the organization, and click **Run**.

You can generate the following reports:

Report	Description
VVR status of data replicated	Provides details on the replication status of a Replicated Volume Group (RVG) at the time of report generation.
VVR Data Transferred-Weekly	Provides details on the amount of the data that is transferred using the VVR configuration over a period of one week.
VVR Data Transferred-Monthly	Provide details on the amount of data that is transferred using a VVR configuration over a period of one month.

Figure 1: Reports view in a perspective



Report 1: VVR replication data status

Subscribe Save as CSV Email											
Veritas Volume Replicator (VVR) status This report lists the replication status of an RVG at the time of report generation. Generated on: Aug 25, 2020 11:29:41 AM											
RVG name	Source system	Target system	Replicated volumes	Current mode	Replication status	Replicated data status	Replication link status	Current logging	Time lag (in seconds)	Data lag (in bytes)	Log usage (in %)
vrldg_rvg	Linux, InfoScale 7.4.2	Linux, InfoScale 7.4.2	vrvol, vrvol	asynchronous	Replicating(Connected)	Consistent, up-to-date	Active	SRL	0	0	0
vrldg_rvg	Windows, InfoScale 7.4.2	-, InfoScale -	vrvol (X:)	asynchronous	Replicating(Connected)	Consistent, up-to-date	Active	SRL	0	0	0

This report displays the following details:

Column	Description
RVG name	Name of the RVG.
Source system	Name of the source system from which the data is replicated.
Target system	Name of the target system to which the data is replicated.
Replicated volumes	Name of the volume that is configured for replication or from which data replication is ongoing.
Current mode	Mode of replication: synchronous or asynchronous.
Replication status	Status of replication: completed, in progress, paused, and failed.
Replication data status	Replication status values: consistent, up-to-date, or consistent but stale.
Replication link status	Status of a target system: active or stale.
Current logging	Type of logging used for the replication: storage replicator log (SRL) or data change ,map (DCM).
Time lag (in seconds)	Time remaining, in seconds, for the replication to complete
Data lag (in bytes)	Data remaining, in bytes, for the replication to complete
Log usage (in %)	Percentage volume of the SRL that is used.

Report 2: Data Replication Status-Weekly

 Subscribe
  Save as CSV
  Email



Veritas Volume Replicator (VVR) weekly data transfer
This report lists the data transferred using a VVR configuration over a week.

Generated on: Aug 25, 2020 11:28:18 AM

Week ending on	RVG name	Source system	Target system	Replication link name	Data transferred (in bytes)	Time lag (in seconds)	Data lag (in bytes)
Aug 30, 2020 12:00 AM	vvr_dg_rvg	esx5-vm16	esx5-vm16	rik_vom-esx5-vm16_vvr_dg_rvg	6656		
Aug 23, 2020 12:00 AM	vvr_dg_rvg1	esx5-vm7	esx5-vm7	rik_vom-esx5-vm7_vvr_dg_rvg2	4096		
Aug 23, 2020 12:00 AM	vvr_dg_rvg1	esx5-vm7	esx5-vm7	rik_vom-esx5-vm7_vvr_dg_rvg1	1536		
Aug 30, 2020 12:00 AM	vvr_dg_rvg	esx5-vm05	esx5-vm05	rik_xeniavm05_vvr_dg_rvg	0		
Aug 23, 2020 12:00 AM	vvr_dg_rvg	esx5-vm05	esx5-vm05	rik_xeniavm05_vvr_dg_rvg	14114304		

Report 3: Data Replication Status-Monthly
[Subscribe](#) [Save as CSV](#) [Email](#)


Veritas Volume Replicator (VVR) monthly data transfer
This report lists the data transferred using a VVR configuration over a month.

Generated on: Aug 25, 2020 11:29:05 AM

Month ending on	RVG name	Source system	Target system	Replication link name	Data transferred (in bytes)	Time lag (in seconds)	Data lag (in bytes)
Aug 31, 2020 12:00 AM	vvr_dg_rvg			rlk_vom-esx5-vm16_vvr_dg_rvg	6656		
Aug 31, 2020 12:00 AM	vvr_dg_rvg1			rlk_vom-esx5-vm7_vvr_dg_rvg2	4096		
Aug 31, 2020 12:00 AM	vvr_dg_rvg1			rlk_vom-esx5-vm7_vvr_dg_rvg1	1536		
Aug 31, 2020 12:00 AM	vvr_dg_rvg			rlk_xeniavm05_vvr_dg_rvg	14114304		

These reports display the following details for a specified week or a specified month:

Column	Description
Week ending on	Date on which the week specified in the data range ends.
Month ending on	Date on which the month specified in the data range ends.
RVG name	Name of the RVG.
Source system	Name of the system from which the data is replicated.
Target System	Name of the system to which the data is replicated.
Replication link name	Name of the replication link (rlink).
Current mode	Mode of replication: synchronous or asynchronous.
Data transferred (in bytes)	Amount of data transferred, in bytes.
Time lag (in seconds)	Time remaining, in seconds, for the replication to complete.
Data lag (in bytes)	Data remaining, in bytes, for the replication to complete.

LDAP configurations using CLI

InfoScale Operations Manager leverages existing user groups that are present in the Lightweight Directory Access Protocol (LDAP) or the Active Directory (AD) configuration of your environment. Alternatively, it uses the native authentication mechanism of a

Windows or a UNIX system. You can use the Management Server console to configure LDAP and assign permissions to user groups. However, to perform this task, your user group must be assigned the Admin role from the perspective.

When you apply InfoScale Operations Manager patch 7.4.2.200, users other than administrators also can perform the following tasks using the command line interface (CLI):

- Configuring LDAP in InfoScale Operations Manager
- Unconfiguring an existing LDAP configuration
- Changing user permissions in InfoScale Operations Manager
- Changing the password for the bind user from the existing LDAP configuration in InfoScale Operations Manager

For details on the syntax and usage of the command-line options, log on to the CMS, and run the following command:

```
# /opt/VRTSsfmcs/webgui/jre/bin/java -cp
/opt/VRTSsfmcs/webgui/tomcat/lib/vom_shared.jar vrts.vom.shared.util.ConfigLdap help
```

Important: Follow these guidelines when you use the command-line options for this utility:

- The utility should be run from the master node only.
- File name and paths should not include spaces. Otherwise, you might encounter errors, especially on Windows systems.
- User input options that are specified in the CLI prompts are case sensitive. You must enter a string exactly as displayed in response to the prompt.

Configuring an LDAP domain

1. Log on to the CMS.
2. To configure a LDAP domain, run the following command:

```
# /opt/VRTSsfmcs/webgui/jre/bin/java -cp
/opt/VRTSsfmcs/webgui/tomcat/lib/vom_shared.jar vrts.vom.shared.util.ConfigLdap
configure
```

3. The utility prompts you to choose whether you want to only configure the LDAP domain or only assign permissions to the user groups.

Enter **Yes** to only configure the LDAP domain but not assign permissions.

Alternatively, you can enter **No** and later run the **vrts.vom.shared.util.ConfigLdap configure** utility only to assign permissions for a user group.

4. Enter the name of the LDAP server that you want to configure.
5. Enter the port for the LDAP server.

The default port for LDAP without SSL certificates is 389 and for LDAP with SSL certificates is 636.

6. Enter the name of the bind user or the DNS name.
7. Enter a password for the bind user account.
8. (Optional) Enter the path of the SSL certificate. Press Enter to skip this step.
9. Enter the username of the user on the LDAP or the AD server.

This name is used to determine the default search base.

10. Enter a numeric or an alphabetical LDAP domain configuration name.

Note: Alphanumeric characters are not supported.

11. Enter the search base.

The LDAP domain is discovered and enabled.

12. When prompted, enter **Yes** to add permission to a user group in the added LDAP domain. Enter **No** to skip this step.
13. Restart the Web service to reflect the configuration changes on the browser-based CMS interface.

Assigning permissions to a user group

You can assign administrator permissions to the user groups in an existing or a newly configured LDAP domain.

Note: To assign the Guest or the Operator role to a user group on a perspective, you must log in as an administrator using the browser-based CMS user interface.

1. Log in to the CMS as an administrator.
2. To assign permissions, run the following command:

```
# /opt/VRTSsfmcs/webgui/jre/bin/java -cp
/opt/VRTSsfmcs/webgui/tomcat/lib/vom_shared.jar vrts.vom.shared.util.ConfigLdap
configure
```

3. The system prompts you to choose whether you want to only configure the LDAP domain or only assign permissions to the user groups.

Enter **No** to only assign permissions for a user group.

4. At the prompt, enter **Yes** to add permissions to a user group in an existing LDAP domain.
5. Enter the name of the LDAP server that you want to configure.
6. Enter the LDAP or the AD domain that corresponds to the user group to which you want to assign permissions.
7. Enter the name of the user group to which you want to assign permissions.
8. Enter one or more perspectives on which you want to assign the permission to the user group: SERVER, AVAILABILITY, STORAGE, VIRTUALIZATION, and INFRA.

This input is case sensitive. Ensure that your input matches exactly with the input options specified at the prompt.

9. Enter **Admin** to assign the administrator permissions to the user group on the selected perspective.

This input is case sensitive. The system checks and removes any old permissions that are assigned to the specified user group.

10. When prompted, enter **Yes** to continue assigning permissions to other groups in the same LDAP domain, or enter **No** to exit.

On successful completion, the newly assigned permissions are visible on the browser-based CMS user interface.

Unconfiguring an existing LDAP configuration

Perform the following steps to unconfigure an existing LDAP configuration:

1. Log on to the CMS as an administrator.
2. Run the following command:

```
# /opt/VRTSsfmcs/webgui/jre/bin/java -cp
/opt/VRTSsfmcs/webgui/tomcat/lib/vom_shared.jar vrts.vom.shared.util.ConfigLdap
unconfigure
```

3. Enter the name of the existing LDAP or the AD configuration that you want to unconfigure.
4. Restart the Web service to reflect the configuration changes on the browser-based CMS interface.

Changing the password for a bind user

You can change the password for an existing bind user account using the **changepass** command. While using this command, ensure that except for the password, you provide the exact details of the existing configuration.

1. Log on to the CMS as an administrator.
2. Run the following command:

```
# /opt/VRTSsfmcs/webgui/jre/bin/java -cp
/opt/VRTSsfmcs/webgui/tomcat/lib/vom_shared.jar vrts.vom.shared.util.ConfigLdap
changepass
```

3. Enter the existing LDAP server name.
4. Enter the port for the LDAP server.

The default port for LDAP without SSL certificates is 389 and for LDAP with SSL certificates is 636.

5. Enter the name of the bind user or the DNS name.
6. Enter a new password for the bind user account.
7. (Optional) Enter the path of the SSL certificate. Press **Enter** to skip this step.
8. Enter the username of the user on the LDAP or the AD server.

This name is used to determine the default search base.

9. Enter a numeric or an alphabetical LDAP domain configuration name.

Note: Alphanumeric characters are not supported.

10. Enter the search base.

ABOUT VERITAS TECHNOLOGIES LLC

Veritas Technologies empowers businesses of all sizes to discover the truth in information—their most important digital asset. Using the Veritas platform, customers can accelerate their digital transformation and solve pressing IT and business challenges including multi-cloud data management, data protection, storage optimization, compliance readiness and workload portability—with no cloud vendor lock-in. Eighty-six percent of Fortune 500 companies rely on Veritas today to reveal data insights that drive competitive advantage. Learn more at veritas.com or follow us on Twitter at [@veritastechllc](https://twitter.com/veritastechllc).

Veritas World Headquarters
2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
www.veritas.com

For specific country offices
and contact numbers,
please visit our website.

VERITAS™
The truth in information.