Dell EMC Data Protection Advisor

Version 6.5

Product Guide

302-004-607

REV 01

DELL EMC

Published February 2018

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

TABLES

Preface

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC technical support professional if a product does not function properly or does not function as described in this document.

Note

This document was accurate at publication time. Go to EMC Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

Purpose

This document provides information on how to use the DPA web console to run and create reports, view alerts, and view the status of replication operations.

ISO 9001 certification

The management system governing the design and development of this product is ISO 9001:2015 certified.

Audience

This document is intended for system administrators. Readers of this document must be familiar with the following tasks:

- Identifying the different hardware and software components that make up the backup and replication environment.
- Following procedures to configure backup and replication operations.
- Following guidelines to locate problems and implement solutions.

Revision history

The following table presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
01	February 2, 2018	First release of this document for DPA 6.5

Related documentation

The DPA documentation set includes the following publications:

- *Data Protection Advisor Custom Reporting Guide*
- *Data Protection Advisor Data Collection Reference Guide*
- *Data Protection Advisor Installation and Administration Guide*
- *Data Protection Advisor Migrator Technical Notes*
- *Data Protection Advisor online help system*
- *Data Protection Advisor Product Guide*
- *Data Protection Advisor Release Notes*

- *Data Protection Advisor Report Reference Guide*
- *Programmers' Guide to Using DPA REST API*
- *Data Protection Advisor Security Configuration Guide*
- *Data Protection Advisor Software Compatibility Guide*
- *Other Technical Notes/White Papers*

Special notice conventions that are used in this document
EMC uses the following conventions for special notices:

NOTICE

Identifies content that warns of potential business or data loss.

Note

Contains information that is incidental, but not essential, to the topic.

Typographical conventions
EMC uses the following type style conventions in this document:

Table 2 Style conventions

Bold	Used for names of interface elements, such as names of buttons, fields, tab names, and menu paths (what the user specifically selects or clicks)
Italic	Used for full titles of publications that are referenced in text
`Monospace`	Used for: • System code • System output, such as an error message or script • Pathnames, file names, prompts, and syntax • Commands and options
Monospace italic	Used for variables
`Monospace bold`	Used for user input
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections - the bar means "or"
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate non-essential information that is omitted from the example

Where to get help
EMC support, product, and licensing information can be obtained as follows:

Product information
For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at https://support.emc.com.

Technical support
Go to EMC Online Support at https://support.emc.com, and click **Service Center**. Several options for contacting EMC Technical Support appear on the site. Note that

to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Online communities

Go to the EMC Community Network at https://community.emc.com for peer contacts, conversations, and content on product support and solutions. Interactively engage online with customers, partners, and certified professionals for all EMC products.

Your comments

Your suggestions help to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to DPAD.Doc.Feedback@emc.com.

CHAPTER 1

The DPA web console overview

This chapter includes the following section:

DPA web console

The DPA web console is a browser embedded Flash-based graphical user interface (GUI) that allows you to manage, monitor, analyze, configure and view alerts, and report on the backup and replication environments. The *DPA Installation and Administration Guide* provides information on installing and configuring the web console.

After you log in to DPA web console, DPA launches the dashboard by default and occupies the web console window.

The DPA web console consists of primary and secondary navigation options.

Primary navigation area bar

The primary navigation consists of an area bar that is arranged vertically on the left of the web console window. The primary areas consist of the following: **Dashboard**, **Advisor**, **Reports**, **Policies**, **Inventory**, and **Admin**. Throughout this document, *area* refers to the primary navigation.

Secondary navigation section bar

The secondary navigation consists of a section bar that is arranged horizontally on the top of the web console window. These sections appear in relation to the primary navigation area that you select. For example, if you click the **Reports** area, the section bar displays the various tasks related to the **Reports** area, such as **Run Reports**. Throughout this document, *section* or *tab* refer to the secondary navigation.

CHAPTER 2

Reports

This chapter includes the following sections:

Reports in DPA

DPA offers a very robust reporting functionality with dedicated sections for various features. Through the **Reports** area, you can create and run various types of out-of-the-box reports or customize the reports to meet enterprise requirements. *Reports* provide detailed information derived from various objects in the configuration tree.

The reports in DPA help you to retrieve information about the environment so that you can review and analyze the activities in the environment. Using these reports, you can identify outages in the environment, diagnose problems, plan to mitigate the risks, and forecast future trends.

The **Dashboard Templates** tab is used to create a dashboard template. A *Dashboard* is a collection of reports or viewlets grouped together into a single panel to provide you with multiple views of the application. Dashboards are viewed from the **Dashboard** area. Dashboard provides more information.

The **Reports** area is available on the left vertical navigation of the web console and offers a user interface that provides a centralized reporting functionality. The five sections that are available for the Reports area includes: Run Reports, Report Jobs, Report Templates, Dashboard Templates, Report Menus.

When you select **Reports**, by default the **New Report** page under the **Run Reports** area launches. Each of the sections have options that enable you to: **Run Reports**, **Manage running and scheduled reports**, **Create custom reports**, **Create custom dashboard templates**, **Manage report menus**.

On-demand or scheduled report templates and dashboard templates

You can run custom and system report and dashboard templates on demand or on a schedule at defined time intervals, per the enterprise requirements.

On-demand reports are reports and dashboard templates that can be run at any time per the requirement. They are ad hoc reports and dashboard templates that you can run with the currently available data and viewed immediately.

The on-demand reports are very useful in daily operations where you can run any report at any time, from the various types of reports that DPA offers. By running an on-demand report, you can:

- Generate point-in-time report.
- Run from several predefined or scheduled reports.

A scheduled report is a report that the DPA Server runs at a scheduled time and publishes the results in one or more formats. The **Scheduled Run Reports** is available only if `Manage scheduled reports` privilege is assigned to the user's user role. By scheduling a report, you can:

- Automate the generation of report.
- Schedule the report generation frequency.
- Configure the email addresses of users to whom the report must be sent.
- Publish to SharePoint server.

Running on-demand reports

You can run a report through **Reports** > **Run Reports**. The New Report is the default section of the Run Reports section. You can run a report by either browsing the menu, by searching the available reports, or by running the report from a list of reports from the Favorites menu.

The *EMC Data Protection Advisor online help system* provides more information.

Procedure

1. Select the object for which you want to run a report.
2. Select the report to run on the object. You can browse through the tree or search for a specific report in the **Find** field to list the reports containing the search string.
3. (Optional) Select the desired time period or choose from a predefined time period.

   The time period depends on the type of report you have selected. For example, the option **Last Day** is inappropriate for **Data Backed up Daily**; whereas **Last Week** or **Last Month** is more appropriate.
4. Click **Finish, Run in New Tab** or **Run in New Window**.

Re-running reports with updated information

To refresh the data in the original report, go to **Run Reports**, select the report, and click **Refresh Report**.

To change some information in a previously run report, for example, to change the scope or time period, make the information changes in the pertinent information, and click **Refresh Report**.

Testing system template reports

Use the following procedure to ensure that the format you've chosen is ideal or for any reason you want to test a report format.

Procedure

1. Open the system template.
2. Go to the **Preview** tab of the **Report Editor** and select the scope and time period for the report.

   DPA generates the report output in the right-hand side. If you wish to make changes to the report, go back to the **Design** tab, or make any changes you wish within the **Preview** tab, and then and click **Refresh**.

   Ensure that you do not save. As long as you do not save, DPA will not create a custom template.

Scheduling report templates and dashboard templates

You can schedule reports through **Report Jobs** > **Scheduled Reports** or after running a report through **Run Reports**.

The **Create Scheduled Run Reports** guides you to create a scheduled report. The *EMC Data Protection Advisor online help* system provides more information on scheduled reports.

Viewing, enabling, and disabling Dashboard Scheduled Content

You can quickly and easily view and control the dashboard components that display in your Dashboard. For example, if you know a certain backup server within your environment included in one of your scheduled dashboard templates is experiencing problems, you can disable the dashboard template from displaying in your Dashboard until the problem is fixed.

Procedure

1. Go to **Reports** > **Report Jobs** > **Dashboard Scheduled Content**.

   DPA displays the list of scheduled dashboards. The Dashboard template name is repeated in the **Dashboard** column for each element in the **Report** column that is included in the Dashboard template.
2. Click on the entry.
   - To disable the Dashboard, click **Disable**.
   - To enable the Dashboard, click **Enable**.

Results

Report summary details appear in the lower **Details - Summary** pane. Disabled content does not run on schedule but remains visible in the Dashboard showing the latest generated result

Publishing scheduled reports to file

Before you begin

- Ensure that you create a subdirectory for the reports. The subdirectory must exist before you can specify it in the relative path.
- When you create the filename, ensure that it does not contain any invalid characters. The file name cannot contain any invalid characters for the operating system or the save will fail.

Procedure

1. Go to **Reports** > **Report Jobs** and then click **Scheduled Reports**.
2. Specify the fields in the steps. Particularly in the **Publish Settings**, **File Name** field, type a unique file. Note the following:

   The DPA Server process allows date or time substitution using @ tags. The Java API documentation defines the tags. For example:

   - *report1 @ddMMMyyyy@* displays as *report1 20Sep2013*
   - *report2 @EEE@ @dd@ @MMM@ @yyyy@* displays as *report2 Mon 20 Sep 2013*

- *report@yyyyMMddHHmm@* displays as *report201309201556*
- *report @HH@_@mm@*displays as *report 10:34*

You can also specify a relative path. For example:
bdb/bdb_@ displays as the file located and named `$docroot/bdb/bdb_<date>.jpg`

3. Complete the fields and click **OK**.

Scheduled reports folder location

All scheduled report output files are located in the following folder, where *<DPA_HOME>* is the location of the DPA installation:

`<DPA_HOME>/services/shared/report-results/scheduled`

You can also use a web browser to view scheduled reports, at `https://<hostname>:9002/dpa-api/scheduledreport/results/<filename>`

System report templates and dashboard templates

DPA includes several predefined system templates, viewlets, and dashboards, which you can use to run reports on selected users in the backup and replication environment. Use these system templates to quickly and easily retrieve information and monitor the environment.

These are available when DPA is installed and are not editable. To modify a system template or dashboard, you must make a copy using **Save As**. Only users with the appropriate privileges can create customized versions of system templates and dashboards.

Custom report templates and dashboard templates

You can create custom report and dashboard templates by saving an existing report or dashboard template and by building a new custom template and dashboard specifying all of the parameters.

Creating a custom report template or dashboard template from a system template

Procedure

1. Go to **Reports** > **Report Templates** > **System Report Templates** or to **Reports** > **Dashboard Templates** > **System Dashboard Templates** as applicable.
2. Select the system report or dashboard from which you'd like to create a template.
3. Click **Save as Custom Template or Save as Custom Dashboard Template**.
4. Type a name in the **Name** field.
5. (optional) Type a description in the **Description** field.
6. Modify the parameters and other properties in the Report Editor or Dashboard Editor.

7. Click **Save** or **Save & Close**.

Building a new custom template and dashboard template

The *Data Protection Advisor online help system* provides more information on how to create a custom template and dashboard.

Note

After you add the report template or dashboard template to a report menu and add the menu to a user, you must click **Refresh** in **Run Reports** > **Select Scope** to ensure that the new report appears in the **Run Reports** area. Alternatively, close DPA completely and then log back in.

Procedure

1. Go to **Reports** > **Report Templates** > **Custom Report Templates** > **Create Custom Template**.

   or

   Reports > **Dashboard Templates** > **Custom Dashboard Templates** > **Create Custom Dashboard Template**.

2. Type a name in the **Name** field.
3. (optional) Type a description in the **Description** field.
4. Specify parameters and other properties in the Report Editor or Dashboard Editor.
5. Click **Save** or **Save & Close**.

   You can view viewlets that are added to the custom dashboard template in the **Dashboards** area of the DPA web console.

Using a command in drill down menu

Commands may be executable files or scripts, such as batch files or shell scripts. To run the command, you need to add it to a drill down menu.

- Create an executable or script and then store the command in `<install-dir>/services/shared/commands`.
- Create or edit a custom template and then add the command string in a drill down menu using the following syntax:

  <install-dir>/services/shared/commands/<command> <param1> <param2> @<variable1>@ @<variable2>@

  The command string contains the command and optional parameters and report variables appropriate to the command. Parameters and report variables get resolved at runtime. Parameters, without @@, are passed through unmodified and controls the way the command runs. For example, a command line switch that orders by name and does not show directory entries. Report variables are surrounded by @@ and pass data specific to the selected row to the command. For example, the report variable *@Server@* is replaced with the server name and *@Status@* is replaced with the current status.

  For tree menus, you can include system and user-defined attribute values from the object for which the menu item is run. Input the attributes values using the *@<attributename>@* format (for example, *@Cost Centre@* passes the value of

the Cost Centre attribute of the object to the command). *$name* passes the name of the object from which the report was run.

The actual names of the *@@variable@@* available for use as a parameter in the script is taken directly from the table column names that the script is attached to. For example, if the table has a column name called 'Server Name' then a script can be written with a parameter called `@Server Name@` that will be substituted from the row on the table selected when activating the script.

- Ensure that the template with the command is used in a Report Menu.
- Run the report that includes the command and then run the command from the drill down menu. By default, any output files are stored in `<install-dir>/services/shared/commands`.

The *EMC Data Protection Advisor online help* system provides more information on how to add a command to a drill down menu.

For example:

To run a command and include the server name, client name, backup set, and size, type:

```
C:\Program Files\EMC\DPA\services\shared\commands\analyseEntry.bat
@Server@ @Client@ @Backup Set@ @Size@
```

To send a page message, type:

```
C:\Program Files\EMC\DPA\services\shared\commands\pager.exe @host@
@job@ @status@ at @endtime@
```

Script command folder location

All command scripts and executables you create for drill-down menus are located in the following folder, where <DPA_HOME> is the location of the DPA installation:

`<DPA_HOME>/services/shared/commands`

About Federating Reporting

Federated Reporting is designed for summary-level reporting. Federated Reporting provides aggregated reporting across multiple DPA servers.

Federated Reporting is a useful feature if you have a large environment with multiple DPA servers. If these multiple DPA servers, in turn, are categorized into different geographies or different customer groups, you may want to run one report across all the DPA servers. Instead of running the same report separately and repeatedly across each of the DPA server groups and merging the reports, Federated Reporting merges all of the DPA servers into one supertree structure on a DPA server that you have designated as the Federated DPA server from which to run the Federated report. Federated Reporting allows you to run a report on the Federated DPA server and utilize the new Federated data source across the supertree structure. DPA sends the run report request to the individual Regional DPA servers. The results from each of the Regional DPA servers are sent back to the Federated DPA server as an output of the Federated data source. You can then choose to return those results or apply additional DPA operators to the result to manipulate the data further. For example, you can calculate a true success rate based on the total counts across all regional DPA servers.

The following terms are useful to note:

- Federated DPA server is a DPA Application server that has Federated Groups configured on it.

- Federated Group is a group on a Federated DPA server that contains groups pulled from regional DPA server by schedule.
- Regional DPA server is a DPA Application server from which the Federated DPA group collects data.
- Federated report is an aggregated report from Regional DPA server.

Configuring Federated Reporting

Federated Reporting provides aggregated reporting across multiple DPA servers.

Before you begin

- Ensure that you install a DPA server as the Federated DPA server with the latest version of DPA. The *Data Protection Advisor Installation and Administration Guide* provides system requirements and installation procedures. Alternatively, allocate an existing DPA server as the Federated DPA server.
- Ensure that you upgrade all of the DPA server instances that you intend to set as a Regional DPA server to the latest version of DPA. If you are using an existing DPA server as a Federated DPA server, ensure that you upgrade that server instance to the latest version of DPA. The *Data Protection Advisor Installation and Administration Guide* provides upgrade procedures.
- Ensure that the grouping structure you wish to have on the Federated DPA server exists on each of the Regional DPA servers. This will allow the groups to be merged into a single tree structure on the Federated DPA server. The object grouping structure must match exactly on each of the Regional DPA servers.

Procedure

1. Create the attribute you will use to mark the federated or regional group:

   You may have multiple groups in a DPA server and not all of them are required in the global Federated Reporting structure. An attribute allows you to specify which groups to pull in to the Federated DPA server superstructure tree.

   a. On the Federated DPA server, go to **Admin** > **Systems** > **Manage Custom Attributes** and click **Create Attribute**.

      The **Attribute Properties** dialog appears.

   b. Populate the fields accordingly:

      In the **Name** field, type the name you would like to give to your federated or regional group. For example, **Regional Group Flag**.

      In the **Type** field, select the **Flag**. The attribute type for Federated Reporting is restricted to Flag only.

      In the **Default Value** field, select the box and choose the value of attribute you would like to mark your federated or regional group.

   c. Click **OK** and **Close**.

   d. Repeat steps a-c on each Regional DPA server from which you plan to pull data to the Federated DPA server.

2. On each regional DPA server, go to **Inventory** > **Group Management** and select **Groups**.
3. On the Regional DPA servers, assign the attribute:

   a. Go to **Inventory** > **Group Management** .

b. Select the group that you want to report on, right-click, and select **Properties of** the group you have selected.

c. Click the **Custom Attributes** tab.

d. Select the attribute that you created in step 1, and click **Apply** and **OK**.

Note that you must repeat step 3 for each Regional DPA server.

4. On the Federated DPA server, select **Create Group**, and then select **Create Federated Group**.

   The **Create Federated Group** dialog appears.

   The Federated Group is a group on a Federated DPA server that contains groups pulled from regional DPA server by schedule.

5. In the **Create Federated Group** dialog on the Federated DPA server, on the **Federated Group Name** field, type a name for the Federated Group.
6. In the **Create Federated Group** dialog on the Federated DPA server, click **Add** to add a Regional DPA server.

   A Regional DPA server is a DPA application server from which the Federated DPA group collects data.

   The **Create DPA Node** dialog appears.
7. In the **Create Federated Group** dialog on the Federated DPA server, populate the required fields in the **Add DPA Server** dialog:

   a. In the **DPA Server Name/IP Address** field, type the host address or DNS of the server you would like to assign as the regional DPA server.

   b. Under the **Credentials** field, click **Select Credential**.

   c. Click **Create Credential**.

      The **Create Credential** dialog appears.

   d. Enter the credentials for the Regional DPA server to communicate with, and select **OK** to close the **Create Credential** dialog and then click OK to close the **Select Credential** dialog.

   e. Click **OK** in the **Add DPA Server** dialog to save the newly created Regional DPA server.
8. Repeat steps 6 and 7 for any additional Regional DPA servers from which you plan to pull data to the Federated DPA server.
9. In the **Create Federated Group** dialog on the Federated DPA server, set the attribute and schedule that you would like to pull groups from the newly created Regional DPA server:

   a. In the **Attribute Name** field, select the attribute you created in step 1.

   b. In the **Attribute Value** field, select the attribute default value you set in step 1.

   c. Click **Select Frequency**.

      The **Generation Frequency** dialog appears.

   d. Set the Generation Frequency as desired and click OK.
10. On the Federated DPA server, on the **Create Federated Group** dialog, click **OK**.

A message appears that indicates that the process of content generation for Federated Groups has started. Environmental factors such as connection speed can affect the time of content generation.

11. Test the newly created Regional DPA server: Select the newly created Regional DPA server from the Regional DPAs list and select **Test**.

    DPA supports pulling only regular groups and Smart Groups from Regional DPA servers.

After you finish

- Verify that the regional group data is collected on the Federated DPA server.
  1. Go to **Inventory** > **Group Management** > **Custom Groups**.
  2. Look for the group marked with custom attribute you assigned for the Federated or Regional group.
- Configure a custom menu on the Federated DPA server.
- Use the Federated Remote Report data source to create a custom report to run on each Regional DPA server. Creating a custom Federated Report on page 22 provides more information.
- Add the newly created custom report to a newly created custom menu. *Data Protection Advisor Custom Reporting Guide* provides information creating new custom reports and adding new reports to custom menus.

Creating a custom Federated Report

Create a custom Federated Report Aggregated report from Regional DPA machine report data.

Before you begin

Carry out the procedure outlined in Configuring Federated Reporting on page 20

The Federated DPA machine merges the output from the Regional DPA machines and displays it in DPA web console or in any of the other supported DPA report formats. You must use the Federate Remote Report data source for Federated Reports. The Federate Remote Report data source communicates with Regional DPA machines, handles the execution of the report template on each Regional DPA machine, and merges the report results from each Regional DPA machine into a single consolidated report. After running the custom Federated report, you can do post-processing on the data to calculate consolidated statistics using standard report operators. DPA does not support drill-downs on custom Federated Reports.

Procedure

1. Go to **Report Templates** > **Custom Report Templates**.
2. Click **Create Custom Template**.

   The **Create Custom Template - New Report** dialog appears.
3. Click **Add Data Source** > **Federated Reports** > **Federated Remote Report**, and then click **Select Source**.
4. In the **Federated Remote Report Properties** window, edit the Fields according to your wishes.
5. If you would like to use a report system template for your custom Federated Report, select the report template you would like to use. In the **Federated Remote Report Properties** window, click **Parameters**, and then click **Edit**.

   The **Edit Parameters** dialog appears.

6. In the **Edit Parameters** dialog, click **Select Report** > **System Report Templates**.

   The System Report Templates list appears.
7. Sort through the System Reports Templates list and select the report system template you would like to use for your custom Federated Report. Alternatively, use the filter to find the report system template you would like.
8. If applicable, add an Operator; for example, Group By: and Close.
   a. Click **Add Operator**.
   b. Select the desired operator from the list and click **Select Operator**.
   c. In the Parameters section of the **Group By Properties** window, click **Edit** and configure the parameter by which you would like to group the report.
9. Go to the **Preview** tab and review the custom Federated Report results.
10. Type a name in the **Name** field.
11. (Optional) Type a description in the **Description** field.
12. Modify the parameters and other properties in the Report Editor or Dashboard Editor.
13. Click **Save** or **Save & Close**.

Report writing tips and best practices

The following section describes best practices and tips for report writing.

Data sources and operators

We recommend efficiency with data sources and operators. The fewer operators you use, the better.

If you have no idea where to start with a data source, the DPA web console itself includes a wealth of information about source categories and the data sources included therein. Go to **Reports** > **Report Templates** > **Custom Report Templates** > **Create Custom Template** and click **Add Data Source**. By reviewing the source categories and data sources, you gain an understanding of the way DPA categorizes data for reporting.

A distinction to consider when choosing a data source is whether you would like aggregated and summary information, or if you would like detailed information in your report. Data sources that include words like *summary*, *aggregation*, *num*, *total*, and *statistics* are ones that provide aggregated or summary information. Data sources that include words like *details*, *config*, or *status* provide detailed information.

For example, as a custom report writing best practice, if you want a report that shows the top 10 longest running jobs over the last week, use only one data source, the Backup Statistics data source, and no operators. If you choose an optimal data source at the start of building the custom report, you save yourself the step later of setting conditions to eliminate unwanted data. It also saves computing time and power, so you retrieve the data sooner.

An example of this would be Backup Statistics data source versus the Backup Job Details data source. This is the equivalent of the performance impact of running a report that returns all the data within the reporting window—for example by using a Backup Job Details data source—versus one that just returns the information required to get the desired output—using Backup Statistics data source instead. Using the Backup Statistics data source creates a report that is easier to understand for anyone

using or modifying it because it simplifies the report design. It is also quicker to run when either the data set or the time period over which the report is run becomes large.

Useful operators and data sources

This section contains frequently used data sources and operators and the categories in which they can be found. The *Data Protection Advisor online help system* provides detailed explanations of all the operators and data sources in DPA.

To view a data source and description, click **Add Data Source**. Select a data source and click**View Data Source Description**. The following are frequently used and very useful data sources:

- Database Query—Returns the output of a SELECT statement against a database (External Category).
- Read CSV—Reads data from a comma separated values file, and turns it into a data set (External Category).

To view an operator description, click **Add Operator**. Select an operator and click **View Operator Description**. The following are frequently used operators:

- Merge—Merges data from two different data sources based on the same key fields (Misc Category).
- Count—Counts the number of elements in a data set (Math Category).
- Group By—Applies a grouping operation to fields in a data set (Aggregate Category).
- Extended Job Rollup—Rolls up backup jobs to a summary based on the specified fields (Backup Category).
- Search and Replace—Uses regular expressions to look at values in a field and alter their contents as per the replacement string (Misc Category). This concept is probably familiar to UNIX users. This is not a DPA invention; DPA merely use it as a Java function. DPA uses Java's implementation of regular expressions.
- Translation—Uses a flat file containing key pair values to map the value of one field in a data set to a different value (Misc Category).
- Concatenate—Concatenates two fields with string values to a single output (Misc Category).
- Set Value—Gives you the ability to set a value of a field based upon a condition (Misc Category).

Data Protection Advisor Custom Reporting Guide provides examples of how to use these operators and data sources.

Examples of Search Replace regular expressions

- $1 up to 1st underscore $2 is between 1st & 2nd underscore
  - Replace String :$1$2 ,
  - Search String :^(.*?_.*?)_.*|^(.*?)_.*
- For first three alphanumeric characters:
  - Replace String : $1
  - Search String : (^\w{0,3})(.*)
- Append domain name static suffix:

    - Replace String : $0.fully.qualified.name
    - Search String: (.*)[^\\1]
- $1 is to first full stop
    - Replace String : $1
    - Search String : ([^\.]*).*
- change Tue3 to Tu3 :
    - Replace String: $1$3
    - Search String: (.{2})(.)(.)
- take string until end of a 12 digit date:
    - Replace String: $1
    - Search String : (.*[0-9]{12})(.*)
    - Based upon one set of 12 numbers in a row (the date format)

Smart Groups

If you find yourself reporting repeatedly on the same groups, create Smart Groups to enable reporting by desired groups. Ideal groups are business-centric and applicable. For example, if you create Smart Groups by business unit, cost centre, or geographic distribution with other server and client information, you can then optimize the groups and other DPA system template or custom reports to gather more data. You do not have to re-create the same custom reports repeatedly.

The *Data Protection Advisor online help system* and *DPA Installation and Administration Guide* provide information on creating Smart Groups.

Date and timestamps in DPA

All dates and timestamps are stored in UNIX format (that is, epoch format) within the DPA database. Because date and time stamps are in UNIX time, they are just integers and you can use mathematical operators on them. However, you should be aware of the 'cast' of the resultant field.

There are free downloads available to convert from UNIX time.

Results after running report template and dashboard template

After you run a report template and dashboard template, the results open in a new tab. The tab displays the name of the report. On the left pane of results page, the details such as the scope of and the time period for which the report was generated is displayed. The report appears on the right pane.

If you have multiple reports, the reports appear in a tabbed view.

From the results, you can:

- Publish the report or dashboard to Microsoft SharePoint as a CSV, Image (png), PDF, HTML, or XML file. The format type options vary based on whether you are publishing a report or dashboard.

  Ensure that the Shared Documents folder and path, for example exist before publication.

  By default, the file is uploaded to the SharePoint site shared documents folder.

- Save the report or dashboard as a CSV, Image (PNG), PDF, HTML, or XML file. The format type options vary based on whether you are saving a report or dashboard. Dashboards may save only as one page in PDF format.
- Email the report or dashboard as a CSV, Image (PNG), PDF, HTML, or XML file. The format type options vary based on whether you are emailing a report or dashboard. If the report is too large to be delivered through email, an alert is sent indicating that the report was not sent.
- Schedule a report template or dashboard template to run on a reoccurring basis, for example daily or weekly. The Schedule report option on this page allows you to schedule the report you just generated.
- Add the report template or dashboard template to Favorites. Then you can run the report template or dashboard template by clicking on the Favorites drop-down at the top right of the **Run Reports** area and select the report template or dashboard template to run. You can also run the report template or dashboard template directly from Custom Reports and Custom Dashboard by clicking **Run Report** and **Run Dashboard**, respectively.
- Customize the appearance of reports templates and dashboards templates. From **Dashboard Templates** > **Custom Dashboard Templates and Report Templates** > **Custom Report Templates**, select the report template or dashboard template of which you'd like to change appearance, then click **Edit**. The Design tab opens, where you can edit the custom report or dashboard layout. Click the **Preview** tab to run a custom report or dashboard as a test. By specifying a scope and time period in the left-hand pane with which to run the report, it will automatically run in the main pane. If changes are subsequently made in the **Design** tab, clicking on the refresh icon in the Preview tab refreshes the report with the changes, using the already selected scope and time period. Report appearance customization provides additional information.

  Note that reports inside dashboards can have a default scope and time period set which are saved as part of the dashboard. Otherwise, scope and time period are part of the runtime and not saved as part of the layout.
- Compare up to four reports. If you compare the performance of one object to another object, the resulting report displays a comparison of these two objects for the report specified. The reports can be split horizontally, vertically, or tiled. The maximum number of reports a user can run is set in **Admin** > **Manage Users** > **Edit User Properties** > **Preferences** .

Report output file locations

All required files for the web console to show a report and report output files are located in the following folders, where <DPA_HOME> is the location of the DPA installation:

- `<DPA_HOME>/services/shared/report-results/rds`—Report Data Set files produced by the reporter.
- `<DPA_HOME>/services/shared/report-results/temp`—Report XML output files required by the web console for showing a report.
- `<DPA_HOME>/services/shared/report-results/exports`—Report exports.
- `DPA_HOME>/services/shared/webroot`—CSV files. Note that ReadCSVFile source should point to `https://dpaserver:9002/webserver/file.csv`
- `<DPA_HOME>/services/shared/report-results/viewlets`—Viewlet XML output files required by the web console for showing a viewlet.

Files older than 24 hours are removed by default trigger at 6 am daily from the following folders:

- <DPA_HOME>/services/shared/report-results/exports
- <DPA_HOME>/services/shared/report-results/temp
- <DPA_HOME>/services/shared/report-results/rds

Report appearance customization

You can change the appearance of the report to suit your needs, such as changing the report format and modifying the colors and fonts to use, the X and Y axes on charts, and other table and chart data.

- DPA supports the following report formats:
  - Table
  - Report Card
  - Health Status
  - Line
  - Column
  - Area
  - Pie
  - Stacked Column
  - Stacked Area
  - Timeline
  - Bullet Chart
  - Topology

    Table reports with more than 250 records cannot be converted to pivot tables. If you are not pleased with the updated report format, select **Report Format** > **Revert Format**.
- Modify the custom template.
- Modify the report after running a report. Preferences are stored on a per-user basis. If a different user runs the same report it will display without the update changes. The modifications you make through Run Reports do not permanently change the templates. To modify the appearance of reports for all users, update the template through Custom Templates.

The *EMC Data Protection Advisor online help* system provides more information on how to customize the appearance of reports.

Dashboard template appearance customization

You can change the appearance of the dashboard templates by modifying the custom dashboard. You can add a report, viewlet template, label, button, or an image. You can also configure the scope, time period, and custom options for the viewlet and report template chosen to build the dashboard.

Supported image formats are GIF, PNG, and JPG. Images must be stored in the `<install-dir>/services/shared/webroot` folder. Type **`https://localhost:9002/webserver/<imageName>.<imageFormat>`** to the image stored in

the webroot directory, where *imageName* is the name of the image and *imageFormat* is gif, png, or jpg. The URL to the image must use https.

The *EMC Data Protection Advisor online help* system provides more information on how to customize the appearance of dashboard templates.

Creating report menus

Through the **Report** area, you can manage report menus. The report menus are available to the users and the options available, if any, depend on the report type.

By default, a newly created report is not available through the **Navigation** Menu. The **Navigator** Menu is a read-only menu that ships with DPA and includes all system reports and dashboards. This is the menu found in Run Reports where you select the report that you want to run.

The *EMC Data Protection Advisor online help* system provides more information on how to add a report to a report menu.

Procedure

1. Create a copy of the **Navigation** Menu or add the report to another custom report menu.
2. Go to **Admin** > **Manage Users**.
3. Add the menu to the user roles.

CHAPTER 3

Dashboard

This chapter includes the following sections:

Dashboard overview

The Dashboard area presents a visual representation of the enterprise-wide summary of the backup and replication environment. It provides information at-a-glance enabling you to make quick decisions.

The primary workflow of the Dashboard leads you to other areas such as Reports or Alerts. When accessing other areas from the Dashboard, the destination is automatically filtered to display only the relevant and applicable content.

The Dashboard area provides a tabbed interface for defining multiple dashboards. These cater to different roles in an organization. By default, the dashboards detailed below are available. The following table lists the system dashboards, user roles, user function, and the default contents available for these roles.

Table 3 User roles and default viewlets or reports

System dashboard	User role	Function	Default viewlets/ reports
Summary	IT Manager	Provides an overall picture of the entire IT setup	• Alert status by Group • Backup Key Performance Indicators (KPIs) • Data Collection Agent Health • Replication Key Performance Indicators (KPIs)
Backup	Backup Administrator	Monitor the backup processes in the environment	• Client Backup Success Rate by Group • Clients Not Backed Up by Group • Failed Backups and Restores by Group
Replication	Replication Administrator	Monitor replication in the environment	• Replication Alerts by Group • Replication Exposure Age by Group • Objects with Replication Exposures • RecoverPoint Performance

Table 3 User roles and default viewlets or reports (continued)

System dashboard	User role	Function	Default viewlets/ reports
RecoverPoint Protected Capacity	RecoverPoint Administrator	Monitor the RecoverPoint protected capacity in the environment	• RecoverPoint Protected Capacity by CG (Consistency Group) • RecoverPoint Protected Capacity by System
Data Domain Overview	Backup Administrator	Monitor Compression Ratio and utilization status overview information for Data Domain	• Data Domain Compression Ratio Count • Data Domain Low System Compression Ratio Trend • Data Domain Filesystem Utilization Status Count • Data Domain Filesystem Utilization for Warning/Critical Systems

Dashboard area and viewlets customization

You must have the required Manage Dashboards privilege to alter or modify the system dashboards. Without the required privileges, when you attempt to modify an existing dashboard, you can create only a copy of the current dashboard.

From the **Dashboard** area, you can view and edit existing dashboards. You can also create a dashboard. You can use the following components to build dashboards:

- System or custom report templates
- System or custom dashboard templates
- Viewlets
- Buttons, labels, and images

Creating new dashboards

Procedure

1. Click the plus icon near the system dashboards **Create New Dashboard**.

   When a new dashboard is created, it is named *Page<n>* where *n* is the count of the new dashboard added.

2. Type a name for the new dashboard.

   This new dashboard is saved by default in the DPA server.

3. Select the new dashboard options:

   a. Click **Select Dashboard Template**, choose a custom dashboard template or a system dashboard template, and click **Select**.

   b. Click **Select Scope**, choose the scope for the new dashboard, and click **OK**.

   c. Click **Select Time Period**, make the desired changes within the **Manage Time Periods, Window Properties, Manage Times,** > **Time Properties** windows, and click **Select**.

   d. Click **Select Schedule**, make the desired selections in the **Manage Schedules** window, and click **OK**.

   e. Click **OK**.

Customizing existing dashboards

You can customize dashboards with buttons, labels, images, reports, and viewlets.

Procedure

1. Click the plus icon near the system dashboards **Open Existing Dashboard** to open an existing dashboard.
2. Select the dashboard that you would like to customize. The last five recently opened pages are listed.

   You can also find the dashboard by going to the default location on the DPA server. Report output file locations provides information on default folder locations.

   - To set a refresh rate for each report in the dashboard, go to **Edit Dashboard** > **Refresh Settings**. In the **Refresh Rate** field, enter the number of minutes you'd like to set for the dashboards refresh rate. Note that the dashboards default auto-refresh rate is 15 minutes.
   - To configure additional viewlet configuration options and control the content, click **Edit Dashboard**. The configuration options vary by viewlet. Some viewlets do not have additional configuration options. Configuration options include scope, time period, and options. When configuring viewlets to reflect scope changes that show content by group, selected groups appear in the viewlet.
   - To set generation frequency for Dashboard scheduled content, go to **Edit Dashboard** > **Generate Frequency**. You can specify a particular time or schedule the content generation. The date and time that content is generated appears at the bottom left of the content.

Hiding dashboards

Place the cursor in the dashboard tab and click **Close Tab**.

Deleting dashboards

Procedure

1. Click the plus icon near the system dashboards **Open Existing Dashboard** to open an existing dashboard.
2. Select the dashboard to delete and click **Delete**. You cannot delete System dashboards.

Dashboards considerations

Bear the following considerations in mind for dashboards:

- Since viewlets are miniature windows in the dashboard, they do not display all content within them. Use the Show All link at the bottom of the viewlet to see additional information on the viewlet.

  For example, to view all the groups in the Replication Alerts by Group viewlet, click **Show All Group** at the bottom of **Replication Dashboard** window. This redirects you to the Reports area and opens the Replication Alerts by Group report.
- When you hover over a chart component or a number in the viewlet, more details about it are displayed as a tool tip. For example, when you hover over success rate value in the Backup KPI viewlet, it indicates the period for which the success rate is calculated and also provides links to the **Reports** section.

CHAPTER 4

Alerts

This chapter includes the following sections:

Alerts in DPA

The Advisor area tightly integrates with DPA's sophisticated policy-driven analysis engine. Alerts show problems and possible causes. Alerts identify the problems within the environment and recommends appropriate solutions, enabling you to resolve problems faster, thereby reducing the impact on business.

A new alert is raised when the threshold defined in the policy is exceeded. Alerts show the problems and how to solve them. The alerts are the outcome of the Analysis Engine, which is driven by Policies. The alerts are not dependent on a particular group. The system shows all alerts together, regardless of which groups they affect.

The Advisor area consists of the Alerts and Replication Analysis sections. The Replication Analysis section lists the replication gaps related to recoverability and provides the graphical representation of how the object selected in the Service Tree (which mirrors the DPA navigation tree) is replicated throughout the environment.

By default you will receive all the Replication gaps, but only the ones you configure in your policies will appear in the **Advisor** > **Alerts** tab. You manage Replication Alerts the same way you manage other alert types. To configure alerting on Replication Monitoring, you must assign Recoverabilty rules to the Analysis Policy and assign the policy to the desired object. Go to **Policies** > **Analysis Policies**. The same alerting capabilities that exist for other alerts are available for Recoverability Alerts: email, SNMP, scripting, and writing to a Windows alert log.

All alerts can be viewed within the DPA web console and in the Windows log event, emailed, or sent into an external operations system. A common requirement for integration into large environments is to be able to send alerts into an operations system. The standard format for transmitting such information is the Simple Network Management Protocol, or SNMP. All results from the Predictive Analysis Engine (PAE) can be sent in the format of SNMP traps. If you have an agent installed on the host, then DPA collects the data directly. DPA does not receive SNMP traps, however.

Another common method of notification is email. The PAE allows for information regarding alerts to be sent to one or more email addresses, and provides custom email headers to allow for programmatic sorting and assignment of alerts by the receiving processes. Email transfer is through the industry standard SMTP mechanism and only requires an active mail hub to operate.

Finally, the PAE also has the ability to run an arbitrary script in an alert condition. The script can carry out any customized action required by the user, such as sending the alert to a trouble ticketing service or paging support personnel with the details of the problem.

The *EMC Data Protection Advisor Installation and Administration Guide* and the *EMC Data Protection Advisor online help system* provides more information.

Alert management

Through the Alerts section, you can:

- Acknowledge new alerts.
- Close alerts that you have acknowledged or resolved.
- Add notes to an alert for future reference.
- Edit or change the policy associated with an alert to suit the requirement. It opens the policy with the rule that generated the alert selected automatically.

- Freeze auto refresh to ensure that the alert that you are currently addressing is not moved down the list of alerts and out of view. You might need to do this since alerts refresh and new alerts may appear at any time.

In DPA 6.x you create an alert for events by defining rule templates. In the rule template you define the alert's message, description, category, severity, and the conditions to fulfill in order to raise an alert.

When you raise an alert, be sure to check if you already have the same alert in the DPA Datastore. This is so that you do not to create a new alert instead of increasing the incremental count.

You define and identify uniqueness of an alert is by using the following fields:

- Same rule ID
- On the same node ID
- On the same child node ID
- On the same component

If you have the same alert already in the DPA Datastore, and the alert has not been closed, update the existing alert with the current message and description, increase the count and mark the last time it was updated.

If you make a change to the original rule template - for example, change the severity value that the alert is being raised for, you continue to adhere to the uniqueness criteria you originally specified determining if DPA should send an alert or increase the increment count.

You must close or acknowledge any alert produced, and hence stored in the Datastore, as a result of a rule template before changing the rule template.

Thus, DPA treats subsequent alerts raised by the updated template as a new alert. This includes a new severity level. Additionally, the first alert raised by the updated template is transmitted and subsequent alerts has the increment count increased.

The DPA 6.x behavior described above is the same for all alert communication protocols: SNMP, SMTP, Windows Event Log.

Alert details

When you select an alert in the Alerts or Replication Analysis sections, the bottom pane displays the alert properties, details on the associated policy and groups, and related reports.

Bear in mind the following information about alert properties and details about policies, groups, and reports:

- Properties includes a description of what caused the alert, a possible resolution, and any notes associated with the alert. The description and resolution is part of the rule that generated the alert.
- Policy displays the policy details that includes the rule which generated the alert.
- Groups displays the groups in the inventory that are affected by the alert.
- Root Cause displays the root cause control panel associated with the respective backup or replication failure. To open directly to the root cause control panel for the respective backup or replication failure, click **Run Selected**.
- Related Reports includes reports pertaining to the identified problem, thus getting more insight into the problem itself. You can run the reports directly from the Alerts section. Reports are displayed in the Reports area.

- Storage Mapping displays the host physical devices for the backup object. It allows you to determine the local or remote storage system for the object, and whether it has been replicated.
- Visualization displays where the problem occurred in a visual mode along with the alert timestamp.

Alert examples

DPA includes many options tied to policy rules that determine when to send an alert. Some examples of alerts include:

- Backup job failed
- Backup job did not occur for 5 days or larger than X GB
- Configuration Change occurred on a Node
- Discarded Frames on a Fibre Channel port increase x 5 than last sample
- Backup job size is 50% larger than the average size of the jobs on a certain backup server computed over the last 5 days
- Four weeks before a File System reaches 1 GB in size

Best practices for using filters

Since the Alerts section displays all alerts irrespective of the view, filters enable you to control what displays.

Bear in mind the following when using filters:

- Use inline table filters to filter based on a column value.
- Use the Scope link to narrow alerts displayed to a particular Group from inventory.
- Use the Filters button to set up Advanced Filters. You can choose to make them persistent so that DPA remembers the filters from a previous session.

DPA retains the last filter used for you to reuse at the next login, if desired.

CHAPTER 5

Replication Analysis

This chapter includes the following sections:

Replication Analysis overview

NOTICE

The Replication Analysis section in the DPA 6.0 and later web console replaces the SLM workspace menu available in DPA versions prior to 6.0.

Through the Advisor area > Replication Analysis section, you can analyze and view the status of recoverability, replication operations, and the storage mapping for objects and individual arrays, file systems, and applications. The options available through the Replication Analysis section also show a graphical representation of recovery points and gaps in the data protection environment.

The reports available from the configuration tree provide an overall view of the replication environment, summarizing the exposures, exclusions, unprotected objects and obsolete recovery points. Through the Replication Analysis section, you can analyze and view the status of replication operations and the storage mapping for objects and individual arrays, file systems, and applications.

The Replication Analysis section allows you to view high level status according to business units or groups. It provides details, status, and mapping of all of the primary storage objects and replicas in the environment. Unlike the reports that you can run in the report display window, the **Replication Analysis** section cannot be scheduled, exported, or saved in any format. There are overlapping reports to the data that appear in the **Replication Analysis** section that can be scheduled, exported, or saved.

The **Replication Analysis** section consists of three primary views: The **Service tree**, **Process view**, and **Details view**.

Recoverability analysis

You can perform recoverability analysis on the data protection environment in the following ways:

- The reports available from the Run Reports section provide an overall view of the replication environment, summarizing the exposures, exclusions, unprotected objects, and obsolete recovery points.
- The options available from the Replication Analysis section show a graphical representation of recovery points and gaps in the data protection environment. Through the Replication Analysis section, you can analyze and view the status of replication operations and the storage mapping for objects and individual arrays, file systems, and applications. The **Replication Gaps** section displays the information required to resolve the issue.
- Some data protection mechanisms such as RecoverPoint Point In Time copies or VMAX3 SnapVX and Data Domain Static images can produce many recovery points per each device or protected object. This can overload the display and make the Visualization graph unreadable. The supported replication technologies for aggregation are SnapVX, Linked, StaticImage, RecoverPoint/S, and RecoverPoint/A.
  If you set the **Aggregate recovery point** setting, each time a group of replications contains more than the chosen number of recovery points, the group is aggregated to a single aggregation box. The aggregation is done per storage array:

file system, application, application component. An aggregation box represents the most updated replication for a single protected object.

For example, if for a single file system there are 10 replications using RecoverPoint (as an example), and the last one is valid, the aggregation box with a valid icon is displayed indicating that it was the last replication and the time. The node includes a folder icon on it, and it's clickable. When you click on such a node, a list with all replications that were aggregated is displayed. Recovery Point details in Process View on page 43 provides RecoverPoint Process view icons and descriptions.

The Replication analysis table of the "Configuring users, security, and system settings" chapter in the *Data Protection Advisor Installation and Administration Guide* provides information on Aggregate recovery point settings.

Service tree

The Service tree mirrors the DPA navigation tree and displays all the discovered replication objects. The Service tree lists all of the servers, applications, and storage devices configured in DPA and are monitored for replication. Select objects in the Service Tree to see the storage topology in the Process view and details in the Details view. You can limit the information to specific scope. Icons in the service tree indicate at a glance whether an object has any Replication gaps or not.

Object recoverability status

The service tree displays a status indicator to the right of every client, application, or storage object, showing the recoverability status for the object and objects residing under the objects.

Node initiators in the Service Tree

Node Initiators and sub-objects are found in the Replication Analysis section under **Storage** > **Disk Storage**. The Node Initiator contains all the application hosts connected to the storage array.

EMC VNX Block/CLARiiON in the Service Tree

VNX Block/CLARiiON storage arrays and sub-objects are found in the Replication Analysis section under **Storage** > **Disk Storage**. Under VNX Block/CLARiiON, you can see each discovered storage array and the following objects:

- MirrorView Session
- Storage Group
- MirrorView Consistency Group

EMC Symmetrix in the Service Tree

Symmetrix storage arrays and sub-objects are found in the Replication Analysis section under **Storage** > **Disk Storage**. Under EMC Symmetrix, you can see each discovered storage array and the following objects:

- Consistency Groups
- Device Groups
- RDF Groups

- All the objects (initiators) that have masking information. The object is displayed as the user-defined object (from the display name field) or as the object WWN retrieved from the Symmetrix.
- A Masking View entry includes all the masking views with its information (Storage groups, objects).

The RDF Groups object includes the RDF groups.

The Device Groups (DG) includes all the DGs that are configured with devices on the defined Symmetrix. The DG includes also the name of the connector that retrieved the DG or the GNS Symmetrix name (because two different DGs with the same name can exist).

The Consistency Groups (CG) includes all the CGs that are configured with some of the Symmetrix devices. The same CG may exist on different arrays and should be the same one displayed to the user in the reports and any editor. The CG includes also the name of the connector that retrieved the CG or the GNS Symmetrix name.

EMC VPLEX in the Service Tree

NOTICE

DPA 6.x does not support applications or file system that are using VPLEX and replicated by the other backed storage-array replication technologies other than EMC RecoverPoint.

VPLEX storage arrays and sub-objects are found in the Replication Analysis section under Storage > Disk Storage.

In a VPLEX storage environment, DPA retrieves the information from VPLEX and maps between the host disks and VPLEX virtual-volumes. It also maps between VPLEX virtual volumes and RecoverPoint volumes and calculates the recoverability status for the applications and file systems.

Process view

The Process view shows the primary storage and all existing recovery points for a file system or logical storage unit selected from the Service tree. Only one file system or logical unit can be viewed at a time in the view.

Example
A file system, E:\ is replicated from primary storage to three local RecoverPoint groups by Clone job, SNAP, and BCV, and also replicated to a fourth remote RecoverPoint group by SRDF/S. Each RecoverPoint group contains only a single recovery point instance.

If the object is replicated and has Recovery Points, arrows will lead from the primary storage to icons that represent Recovery Point groups. A Recovery Point group is a group of all the Recovery Points created using the same Replication Method, for example, a Clone or remote SRDF/S replication.

Each primary storage and Recovery Point group is contained inside the storage array (for example, an EMC CLARiiON or Symmetrix) in which it is physically located. A timestamp accompanies each Recovery Point group showing the date and time that the initial replica was created (or derived from another replica).

At the top left of each storage array container is Storage Array: Type of Storage Array: the identifier for the storage array (usually the serial number)]. In the example,

all three local Recovery Point groups are stored inside the storage array 00190300519, so the container label will be Storage Array: SYMMETRIX: 00190300519.

Process view navigation

You can zoom in and out of the Process view, use the overview map to shift the structure in the view. Right-click anywhere in the view to see the following options:

- Zoom In to zoom in closer to the recovery point mapping.
- Zoom Out to zoom out of the recovery point mapping.
- Actual Size to zoom the viewer to a default setting.
- Fit Content to zoom in or out to fit all of the mapping into the viewing space.
- Hide Overview or Show Overview to hide or reveal the overview in the left corner.

Recovery Point details in Process View

The following table presents the icons displayed in the **Process View** and their associated status.

Table 4 Process View icon display description

Icon	Description
	Invalid Continuous recovery point This item has at least one critical gap. The underlying object is continuous replication as opposed to the Point In Time replication.
	Warning Continuous recovery point Continuous replication has at least one warning gap.
	Valid Continuous recovery point Continuous replication has no gap.
	Deleted recovery point
	Dirty recovery point
	Invalid Diskless recovery point
	Valid Diskless recovery point
	File System
	ILU
	In Progress recovery point
	VNX/CLARiiON Storage group
	Critical gap

Table 4 Process View icon display description (continued)

Icon	Description
	Invalid Point In Time recovery point
	Invalid range replica. Has at least one critical gap. In a range of replica, RecoverPoint keeps a journal. This contain the change history. This allows you to recover from a range of times.
	LUN
	Missing recovery point
	Node initiator
	Primary storage
	Primary storage with gap
	Single sided replication
	Warning
	Point In Time recovery point has at least one warning
	Range recovery point has at least one warning
	Generic array
	Validation continuous replication Indicates that it is a continuous replication and everything is okay
	Valid Point In Time replication Indicates a Point In Time replication and that everything is okay. It also indicates a paused replication where everything is okay.
	Valid Point In Time recovery point
	Valid range recovery point

Process View for VPLEX

When you select to view the process view of a file-system or an application, the replication process view displays the VPLEX system as a storage array.

VPLEX is not displayed as a storage array in the tree of the replication analysis tab, so it is seen only if you select to see a file system, an application, or a host.

Details view

The Details view provides more detailed information on the object selected in the Process view.

Replication Gaps details

The **Replication Gaps** tab contains a sortable list of all the replication gaps and exposures found for a particular recovery point, including Administrative issues related to system functions such as discovery and security. The details displayed depends on the object selected, but may include:

- Severity
- Category
- Message
- Object Name (example Host, Storage Array)
- Child objects (file system or logical object)
- Component - The path to the object like tablespace
- Last Update - Time of discovery
- Storage Array - The storage array on which the Recovery Point resides
- Replication - The replication technology used to create the Recovery Point

Storage Mapping

The Storage Mapping tab displays the host physical devices for the object, which allows you to determine the local or remote storage system for the object and whether it has been replicated.

The mapping view provides the following additional information for each file system and application:

- Gap
- Node initiator
- Primary Storage Array
- Primary device name
- Source RDF group
- Source MV session
- Replication Method
- Target Storage Array
- Target device

This information can help identify issues with missing recovery. For example:

- You want to protect an unprotected application or file system, and you need the physical details of host and storage volumes to configure the replication.
- You want to know the details of host physical devices, logical volumes, volume groups, and storage volumes. This information is needed, for example, when you are planning migrations, or when you need to validate data from other sources.

Obtaining detailed gap information

Procedure

1. Select the gap.
2. Click **Details**.

   Details describes the cause for the gap and suggests a resolution, if one is entered.

Excluding a gap

You might have to exclude gaps in scenarios where a policy for the host that requires an SRDF replication and the condition is that one file system of the host should not be replicated.

Procedure

1. Select the gap.
2. Click **Exclude** or **Manage Excludes**.
3. Specify the exclusion criteria.

   NOTICE

   When excluding a gap from the Datastore Replication Point the exclude will not have any impact on gaps on the objects that have files on the Datastore.

List of recoverability gaps

The following sections describe all of the types of recoverability gaps reported by DPA and their possible causes.

Administrative

The following table lists the administrative type recoverability gaps detected by DPA.

Table 5 Administrative gaps

Gap name	Description in DPA	Explanation	Possible causes
Application discovery last run failed	Application last run failed.	The last run of the application discovery process failed.	• The application or host authentication was change • The application is not available or not running

Table 5 Administrative gaps (continued)

Gap name	Description in DPA	Explanation	Possible causes
Client last run failed	An error occurred in the last discovery process.	The last run of the client discovery process failed.	• The client is down • Authentication was changed or incorrectly supplied
Engine discovery last run failed	Storage Array {Storage Array} last run failed, Missing information.	The last run of the Storage Array discovery process failed.	• The Storage Managed Host (Solution Enabler Client) client is down • authentication was changed or incorrectly supplied • the gatekeeper device has an error
Volume groups discovery process failed	Failed to retrieve information for volume group {VG Name}.	An error occurred in the last discovery process during the volume group discovery phase for volume group.	Failure in the Solution Enabler API
Logical groups discovery process failed	Failed to retrieve information for LV {LV Name} on VG {VG Name}.	An error occurred in the last discovery process during the logical volume discovery phase for a volume group.	Failure in the Solution Enabler API
Additional required objects retrieval process last time failed	Extra SO failed	An error occurred in the last application discovery process during the retrieval of the additional required files discovery phase.	A failure occurred during the extra SO retrieval process.
Retrieve Application information last run failed	Retrieve Application information last run failed, Missing information.	During the analysis process, additional information such as, Activation Times or Archive Logs could not be retrieved.	• The application or host authentication was change • The application is not available or not running
Missing Previous Replication Info	Missing information to determine Recovery point time for Replication Method {Replication Method} and hop {Hop}.	DPA is unable to locate a previous image for replication on source device.	Consider the following scenario: An Oracle file system resides on storage 0001 and is replicated to storage 0011 at 10:00 a.m.; and then replicated to 0021 at 11:00 a.m. Then, 0001 is replicated again to 0011 at 1:00 p.m. DPA scans at 2 p.m. and cannot determine the time of the 'base' image for 0021,

Table 5 Administrative gaps (continued)

Gap name	Description in DPA	Explanation	Possible causes
			since 0011 was already overwritten by a new replication. An attempt was made to complete this information from the audit log, but this information was not available.
Missing information	Missing information on {SO} due to monitoring error.	{Application} cannot be monitored due to an error.	• Storage object was removed or no longer on disk • Missing information on {SO} due to SRDF link failure

Replication configuration

The following table lists the replication configuration type recoverability gaps detected by DPA.

Table 6 Replication configuration gaps

Gap Name	Description in DPA	Explanation	Possible causes
Application Not In Backup mode	Application was not in backup mode during replication creation	Application was not in backup mode during replication creation	{BaseImageEndTime}";"{SO} was not in backup mode during image creation. {SO} was replicated using consistency technology at {Engine}:{Facility} on {BaseImageEndTime}".
Partially Replicated	{Object} is partially replicated by {Storage Array}/ {Replication Method}	At least one of the logical volume or volume group storage devices were not replicated, while others were replicated.	One or more of the Object's devices: • Was not replicated. • Was not replicated by using the same Replication Method as the other devices (for example BCV/Clone/ Snap). • Was not replicated with the same state as the other devices (for example Split/Sync). • Was not replicated in the same time (60 seconds grace by default in the

Table 6 Replication configuration gaps (continued)

Gap Name	Description in DPA	Explanation	Possible causes
			Grace Time Images system setting).
Partially Replicated	{Object} protection configuration is invalid at {Storage Array}/{Replication Method}	One or more of the physical devices of the Object, file system/volume group were not replicated.	
Invalid Replica	{Object} has invalid image at {Storage Array}/{Replication Method}	One or more of the application's file systems have no suitable image, or one of the Object's devices has an invalid image.	One or more of the application's file systems: • Was not replicated. • Was not replicated by using the same Replication Method as the other file systems. • Was not replicated with the same state as the other file systems. • Was not replicated in the same time (15 minutes grace by default in the recovery point span system setting). • One or more of the Objects devices has an image in an invalid state.
Image Exception	{Object} not protected by {Storage Array}/{Replication Method}	Object not protected.	The entire application component is not protected. Extend {Storage Array}/{Replication Method} protection to cover the Object.
Not Protected Logs	{Object} is not protected	One or more of an Oracle archive log's storage devices needed to recover the application by using this Recovery Point has no image.	One or more of the archive log's devices: • Was not replicated. • Was replicated by using a different Replication Method type than the application devices.
Logs not on Disk	{Object} is not found on disk, may not be protected by {Storage Array}/{Replication Method}.	One or more of an Oracle archive log's storage devices needed to recover the application by using this Recovery Point were missing (or suspected as missing) from replication.	One or more of the archive log's devices: • Was replicated before all the necessary archive logs were created.

Table 6 Replication configuration gaps (continued)

Gap Name	Description in DPA	Explanation	Possible causes
			• Was replicated after the required archive logs were deleted from disk. • Was replicated successfully, as needed, but is suspected as missing because during the time that DPA was sampling the required archive logs, the logs had been already deleted from disk.
Different Consistency Violation	The application's files were not replicated in the same consistency action.	While the database was up, an application's logical volumes or volume groups were not replicated in the same consistency action. Consistency action means that the replication actions included the consistency option, and each action has a different consistency ID as described in the gap details. For example, replication was executed by two different SYMCLI commands.	The application's logical volumes or volume groups were not replicated in the same consistency action. For example: e:\oradata \orcl10\example01.dbf was replicated by action {ConsistencyId1} from audit log. However, the g:\oradata \orcl10\datafile_on_g.dbf was replicated by action {ConsistencyId2} from audit log.
Different Consistency Violation	The Object devices were not replicated in the same consistency action.	At least one of the Object devices was not replicated in the same consistency action as the other devices. Consistency action means that the replication actions included the consistency option, and each action has a different consistency ID as described in the gap details. For example, replication was executed by two different SYMCLI commands.	At least one of the Object devices was not replicated in the same consistency action as the other devices. For example (assuming /data resides in devices 000A, 000B): Device 000A was replicated by action {ConsistencyId1} from {Storage Array}. However, device 000B was replicated by action {ConsistencyId2} from {Storage Array}.
Consistency Violation	{EL} Not part of an enabled Consistency group.	At least one of the Target Devices replicated using SRDF were part of an enabled consistency group.	Assign all the devices to an enabled consistency group.

Application recovery

The following table lists the application recovery type recoverability gaps detected by DPA.

Table 7 Application recovery gaps

Gap name	Description in DPA	Explanation	Possible causes
Application Consistency Violations Backup mode scenarios on page 64 provides more information on the possible recovery point scenarios for Consistency Violations.	Inconsistent Recovery Point: application not in backup mode during recovery point creation {BaseImageEndTime}	The backup mode gap is issued whenever the application was not in the correct state while the copy was taken. The state depends also on the copy type, meaning that in case the copy was taken for a synchronous replication, there is no requirement that the application will be in a specific state and therefore for synchronous replication no backup mode gap will be generated.	The application's devices were replicated by using inconsistent Point In Time replication while: • None or part of the application's components were in backup mode. • The application was running without using consistency technology. Specifically, per application type: • For Oracle - database was up and was not put in backup mode. • For SQL Server - database was up and VDI, VSS were not used. • For Exchange Server - server was running and VSS was not used.
Mixed Facilities	Application files were not replicated by using the same method.	Not all of the application's components were in the same state while they were replicated. Part of the application was replicated by using one method, and the other was replicated by using a different method.	The application's devices were replicated with two different methods: • Some of the application's components were replicated by using Point In Time replication while the application state was in backup mode, and the other part was replicated by using Point In Time consistent replication when the application state was up. or • Some of the application's components were replicated by using Point In Time replication while the application state was Down and the other part

Table 7 Application recovery gaps (continued)

Gap name	Description in DPA	Explanation	Possible causes
			was replicated by using continuous replication when the application state was Down. or • Some of the application's components were replicated by using Point In Time replication while the application state was in backup mode and the other part was replicated by using continuous replication when the application state was in backup Mode. For example: `/oradata1/orcl10/example01.dbf` was in a state up, replicated as a Point In Time consistent image, for a Restartable Recovery Point. `/oradata2/orcl10/example02.dbf` was in state Backup Mode, replicated as a Point In Time image, for a Recoverable Recovery Point.
Different Activation Window	The application's files were not replicated in the same activity window.	The application has changed its state during the backup process. The state change means that during the device's replication process, the application was started up, shut down, or switched to backup mode.	The application's devices were replicated in two different activation windows. Part of the application's components were replicated while the application was down. Then, after starting up and shutting down the application, the other part of the application's components were replicated. or Part of the application's components were replicated while the application was in Backup Mode.

Table 7 Application recovery gaps (continued)

Gap name	Description in DPA	Explanation	Possible causes
			Then, after ending Backup Mode and shutting down the application, the other part of the application's components were replicated. For example: The following list includes one file from each activity window: • Tablespace1 was replicated in activity window: 10:00-10:02 • Tablespace2 was replicated in activity window: 10:03-10:04

Protection configuration

The following table lists the protection configuration type recoverability gaps detected by DPA.

Table 8 Protection configuration gaps

Gap name	Description in DPA	Explanation	Possible causes
Missing RP	Recovery Point was not created on {Storage Array}/ {Replication Method} per protection rule {Rule}.	{SO} has missing recovery point at {Storage Array}/ {Replication Method}, Schedule: {Schedule}	The replication was not taken in the configured time (as configured in the protection rule).
Consistency Violation	The storage object devices were not replicated by using a consistency technology.	At least one of the storage object devices was not replicated by using a consistency technology. The following devices were not replicated by using consistency technology: {Devices}	The storage object's devices (file systems) were not replicated by using a consistency option (for example, a split command without the -consistent option). Refer to support matrix regarding limitations caused by using older versions of SE.
Consistency Group Violation	Not all Target Devices are in the same enabled Consistency group	Not all Target Devices are in the same enabled consistency group.	Part or all of the application's or SO's devices were replicated by using an SRDF Replication Method without using consistency group. or

Table 8 Protection configuration gaps (continued)

Gap name	Description in DPA	Explanation	Possible causes
			The consistency group is not enabled. Notes: • The Storage Array should be imported from the host where the consistency group is defined. If the Storage Array is discovered by another host, this gap will be created even though there is a consistency group. • Refer to support matrix regarding limitations caused by using older versions of SE.

Disaster recovery host configuration

The following table lists the Disaster Recovery host type recoverability gaps detected by DPA.

Table 9 Disaster Recovery host configuration gaps

Gap name	Description in DPA	Explanation	Possible causes
Not Mapped	Device not mapped to Fibre Adaptor (FA) port.	One or more of the destination devices within the recovery point at {Storage Array}/{Replication Method} are not mapped to the FA port.	The application or SO devices were replicated successfully, but part or all of their destination devices are not mapped to any FA port. For example: An Oracle file system resides on object 0011 and is replicated to object 1122. However, object 1122 is not mapped to any FA port.
Not Masked	Device not masked to HBA.	One or more of the destination devices within the recovery point at {Storage Array}/{Replication Method} are not masked to an HBA.	The application or SO devices were replicated successfully but part or all of their destination devices are not masked to any HBA. They may be mapped to an FA port. For example:

Table 9 Disaster Recovery host configuration gaps (continued)

Gap name	Description in DPA	Explanation	Possible causes
			• `/oracle` file system resides on object 0011 and is replicated to object 1122. • Object 1122 is mapped to FA 1B:0. • Object 1122 is not masked to any HBA WWN.
Map/Mask information does not match	FA port in device mapping does not match the FA port in device masking.	One or more of the destination devices within the recovery point at {Storage Array}/{Replication Method} have a mismatch in mapping or masking configuration.	The application / SO devices were replicated successfully and part or all of their destination devices are mapped to an FA port and masked to the HBA through a different FA port. For example: • /oracle file system resides on object 0011 and is replicated to object 1122. • Object 1122 is mapped to FA 1B:0. • Object 1122 is masked to the HBA WWN through port 16B:1.
Recovery Point-to-Host connection error	Parts of Recovery Point connected to different hosts.	The destination devices within the recovery point at {Storage Array}/{Replication Method} are split between hosts, or not all of the destination devices are mapped to a single host.	The application / SO devices were replicated successfully but part or all of their destination devices are visible to one host while other devices are not visible to the host or are visible to a different host. Visible to host means that the devices exist as physical disks in the host. For example: • `/oracle` resides on 0011 and 0012 and is replicated to 1122 and 1123 • 1122 and 1123 are mapped to FA 1B:0. • 1122 is masked to host01 HBAs and visible to that host.

Table 9 Disaster Recovery host configuration gaps (continued)

Gap name	Description in DPA	Explanation	Possible causes
			• 1123 is masked to host02 HBAs and visible to that host.
RP is not connected to Host	Host mapped and masked to Recovery Point, but Recovery Point is not accessible.	Host is mapped or masked to Recovery Point destination devices, but end-to-end path cannot be verified.	The application / SO devices were replicated successfully. Part or all of their destination devices are mapped and masked correctly but are not visible to the host. Visible to host means that the devices exist as physical disks in the host. HBA details of the DR host client were discovered by Illuminator. For example: • `/oracle` resides on 0011 and 0012 and is replicated to 1122 and 1123. • 1122 and 1123 are mapped to FA 1B:0 • 1122 is masked to host01 HBA and visible to the host (exist as /dev/sdg in the host). • 1123 is masked to host01 HBAs but not visible to the host (does not exist as a physical disk).
RP could not be associated to a host	Recovery Point masking does not match any managed host scanned by Illuminator.	Recovery Point masking of the destination devices does not match any managed host scanned by Illuminator	The application / SO devices were replicated successfully. The destination devices are mapped and masked correctly. However, the DR host, which those devices are masked to, was not discovered by Illuminator or its HBA information could not be retrieved. For example: • `/oracle` resides on 0011 & 0012 and is replicated to 1122 & 1123.

Table 9 Disaster Recovery host configuration gaps (continued)

Gap name	Description in DPA	Explanation	Possible causes
			• 1122 and 1123 are mapped to FA 1B:0 • 1122 and 1123 are masked to host01 through FA 1B: 0. Client discovery was not performed on host01. or Client discovery on host01 finished with warnings regarding HBA discovery.

Execution gaps

The following table lists the execution type recoverability gaps detected by DPA.

Table 10 Execution gaps

Gap name	Description in DPA	Explanation	Possible causes
Application Consistency Violation	Application has changed state during the replication on the application files.	The application state changed during the replication of the application files. All application files should be replicated while the application is in the same Down/Backup-Mode state throughout the process. This means that all application files should be replicated within the same application Down/ Backup-Mode operation.	When checking the dependency type within activation times, this applies to only the case where all storage objects were backup up in the Cold state but not in the same activation time.
Not Protected Logs	Inconsistent Recovery Point: {Storage Object} is not protected.	The `file: {Storage Object)` is not protected. The file is required for recovery.	One or more of the archive log's devices was not protected and is not part of the recovery point.
Logs not on Disk	{SO} is not found on disk, may not be protected by {Storage Array}/{Replication Method}.	Storage object is not found on disk, may not be protected by `{Storage Array}/ {Replication Method}`. One or more of an Oracle archive log's storage devices needed to recover the application by using this Recovery Point were missing	One or more of the archive log's devices: • Was replicated before all the necessary archive logs were created. • Was replicated after the required archive logs were deleted from disk.

Table 10 Execution gaps (continued)

Gap name	Description in DPA	Explanation	Possible causes
		(or suspected as missing) from replication.	• Was replicated successfully, as needed, but is suspected as missing because during the time that DPA was sampling the required archive logs, the logs had been already deleted from disk.
Logs on derived RP do not exist in source RP	{Storage Object} not found in source image for this recovery point.	One or more of an Oracle archive log's storage devices needed to recover the application by using this Recovery Point were missing in the source recovery point.	One or more of the archive log's devices may have been deleted by an earlier data protection process.
Consistency Violation	The application's files were not replicated in the same consistency action.	While the database was up, an application's logical volumes or volume groups were not replicated in the same consistency action. Consistency action means that the replication actions included the consistency option, and each action has a different consistency ID as described in the gap details. For example, replication was executed by two different SYMCLI commands.	The application's logical volumes or volume groups were not replicated in the same consistency action. For example: `e:\oradata \orcl10\example01.dbf` was replicated by action {ConsistencyId1} from audit log. However, the `g:\oradata \orcl10\datafile_on_g. dbf` was replicated by action {ConsistencyId2} from audit log.
Consistency Violation	The storage object devices were not replicated by using a consistency technology.	At least one of the storage object devices was not replicated by using a consistency technology. The following devices were not replicated by using consistency technology: {Devices}	The storage object's devices (file systems) were not replicated by using a consistency option (for example, a split command without the -consistent option). Refer to support matrix regarding limitations caused by using older versions of SE.
Consistency Violation	Application's files were not replicated in the same consistency action.	While the database was up, an application's logical volumes or volume groups were not replicated in the same consistency action.	The application's logical volumes or volume groups were not replicated in the same consistency action. For example:

Table 10 Execution gaps (continued)

Gap name	Description in DPA	Explanation	Possible causes
		Consistency action means that the replication actions included the consistency option, and each action has a different consistency ID as described in the gap details. For example, replication was executed by two different SYMCLI commands.	`e:\oradata \orcl10\example01.dbf` was replicated by action {ConsistencyId1} from audit log. However, the `g:\oradata \orcl10\datafile_on_g. dbf` was replicated by action {ConsistencyId2} from audit log.
Mixed Facilities	Application files were not replicated by using the same method.	Not all of the application's components were in the same state while they were replicated. Part of the application was replicated by using one method, and the other was replicated by using a different method.	The application's devices were replicated with two different methods: • Some of the application's components were replicated by using Point In Time replication while the application state was in backup mode, and the other part was replicated by using Point In Time consistent replication when the application state was up. or • Some of the application's components were replicated by using Point In Time replication while the application state was Down and the other part was replicated by using continuous replication when the application state was Down. or • Some of the application's components were replicated by using Point In Time replication while the application state was in backup mode and the other part was replicated by using continuous replication when the application state was in backup Mode. For example:

Table 10 Execution gaps (continued)

Gap name	Description in DPA	Explanation	Possible causes
			`/oradata1/orcl10/example01.dbf` was in a state up, replicated as a Point In Time consistent image, for a Restartable Recovery Point. `/oradata2/orcl10/example02.dbf` was in state Backup Mode, replicated as a Point In Time image, for a Recoverable Recovery Point.

Service Level Agreements

The following table lists the Service Level Agreement (SLA) type recoverability gaps detected by DPA.

Table 11 SLA gaps

Gap name	Description in DPA	Explanation	Possible causes
Missing RP	Recovery Point was not created on {Storage Array}/{Replication Method} per protection rule {Rule}.	{SO} has missing recovery point at {Storage Array}/{Replication Method}, Schedule: {Schedule}	The replication was not taken in the configured time (as configured in the protection rule).
RPO Violation	SLA Rule {Rule} RPO of {RPO} is not met by implemented data protection for Object. Actual RPO is {Actual RPO}.	SLA rule for RPO was not met for the latest Recovery Point or all Recovery Points.	The actual RPO is greater than the SLA rule RPO of the latest Recovery Point or all Recovery Points according to the rule definition.
Retention Violation	SLA Rule {Rule} Retention of {Retention} does not match implemented data protection for Object. SLA copies = X, Actual valid copies =Y.	SLA rule for Retention does not match the implemented data protection for the object.	The actual valid copies is less than the SLA rule copies.
Not Mapped	Device not mapped to Fibre Adaptor (FA) port.	One or more of the destination devices within the recovery point at {Storage Array}/{Replication Method} are not mapped to the FA port.	The application or SO devices were replicated successfully, but part or all of their destination devices are not mapped to any FA port. For example: An Oracle file system resides on object 0011 and is replicated to object 1122.

Table 11 SLA gaps (continued)

Gap name	Description in DPA	Explanation	Possible causes
			However, object 1122 is not mapped to any FA port.
Not Masked	Device not masked to HBA.	One or more of the destination devices within the recovery point at {Storage Array}/{Replication Method} are not masked to an HBA.	The application or SO devices were replicated successfully but part or all of their destination devices are not masked to any HBA. They may be mapped to an FA port. For example: • `/oracle` file system resides on object 0011 and is replicated to object 1122. • Object 1122 is mapped to FA 1B:0. • Object 1122 is not masked to any HBA WWN.
Map/Mask information does not match	FA port in device mapping does not match the FA port in device masking.	One or more of the destination devices within the recovery point at `{Storage Array}/{Replication Method}` have a mismatch in mapping or masking configuration.	The application / SO devices were replicated successfully and part or all of their destination devices are mapped to an FA port and masked to the HBA through a different FA port. For example: • /oracle file system resides on object 0011 and is replicated to object 1122. • Object 1122 is mapped to FA 1B:0. • Object 1122 is masked to the HBA WWN through port 16B:1.
Recovery Point-to-Host connection error	Parts of Recovery Point connected to different hosts.	The destination devices within the recovery point at `{Storage Array}/{Replication Method}` are split between hosts, or not all of the destination devices are mapped to a single host.	The application / SO devices were replicated successfully but part or all of their destination devices are visible to one host while other devices are not visible to the host or are visible to a different host. Visible to host means that the devices exist as physical disks in the host.

Table 11 SLA gaps (continued)

Gap name	Description in DPA	Explanation	Possible causes
			For example: • `/oracle` resides on 0011 and 0012 and is replicated to 1122 and 1123 • 1122 and 1123 are mapped to FA 1B:0. • 1122 is masked to host01 HBAs and visible to that host. • 1123 is masked to host02 HBAs and visible to that host.
RP is not connected to Host	Host mapped and masked to Recovery Point, but Recovery Point is not accessible.	Host is mapped or masked to Recovery Point destination devices, but end-to-end path cannot be verified.	The application / SO devices were replicated successfully. Part or all of their destination devices are mapped and masked correctly but are not visible to the host. Visible to host means that the devices exist as physical disks in the host. HBA details of the DR host client were discovered by Illuminator. For example: • `/oracle` resides on 0011 and 0012 and is replicated to 1122 and 1123. • 1122 and 1123 are mapped to FA 1B:0 • 1122 is masked to host01 HBA and visible to the host (exist as /dev/sdg in the host). • 1123 is masked to host01 HBAs but not visible to the host (does not exist as a physical disk).
RP could not be associated to a host	Recovery Point masking does not match any managed host scanned by Illuminator.	Recovery Point masking of the destination devices does not match any managed host scanned by Illuminator	The application / SO devices were replicated successfully. The destination devices are mapped and masked correctly. However, the DR host, which those devices are masked to, was not

Table 11 SLA gaps (continued)

Gap name	Description in DPA	Explanation	Possible causes
			discovered by Illuminator or its HBA information could not be retrieved. For example: • `/oracle` resides on 0011 & 0012 and is replicated to 1122 & 1123. • 1122 and 1123 are mapped to FA 1B:0 • 1122 and 1123 are masked to host01 through FA 1B: 0. Client discovery was not performed on host01. or Client discovery on host01 finished with warnings regarding HBA discovery.
Link Down	The link is down.	Link for at least one of the target devices is down causing the continuous replication not to be up-to-date.	The link status for a continuous application is down.
Incomplete Star Configuration	A problem was found in the star configuration. Not all devices are configured for replication.	Target devices on Storage Array {Storage Array name} are not configured as star. All the devices in the current replica are configured for replication, but there is a configuration problem in one of the previous replicas in the chain. Different Replication Methods are defined for the disabled link in the star environment.	The alternative link or a previous link in the chain is not complete or with different Replication Methods.
Consistency Violation	A problem was found in the star configuration. {EL} Not part of an enabled Consistency group.	At least one of the Storage Object devices was not replicated using a consistency technology.	The alternative link or a previous link are not part of an enabled consistency group. Assign all the devices to an enabled consistency group.
Replication Refresh Extension	Replication refresh time has been exceeded.	The replication refresh time has exceeded twice the defined refresh time.	The network bandwidth or the storage array performance is not sufficient to create the

Table 11 SLA gaps (continued)

Gap name	Description in DPA	Explanation	Possible causes
		The refresh time is defined in DPA under File > System Settings and is either: • Maximum RPO for MirrorView/A • Maximum RPO for SRDF/A	replication point within the defined window.

Backup mode scenarios

The following table lists the possible recovery states by storage array and replication method for backup modes.

Table 12 Backup mode scenarios

Array	Replication Method	Replication state	Recovery Point Type	Backup mode scenario
Symmetrix	BCV Clone Snap	Split / Activate	Recoverable	When the application was in backup mode during replication.
	BCV Clone Snap	Split / Activate	Restartable	When the -consistent option was used during replication.
	SRDF / S SRDF / A	Synchronized, Consistent	Continuous Restartable	
	SRDF / S SRDF / A	Split	Recoverable	When the application was in backup mode during replication.
CLARiiON	Clone	Consistent, Synchronized	Continuous Restartable	
	Clone	Fractured	Restartable	When the application was not in backup mode, and the replication was done by using the -consistentfracturclones option.

Table 12 Backup mode scenarios (continued)

Array	Replication Method	Replication state	Recovery Point Type	Backup mode scenario
	Clone	Fractured	Recoverable	When the application was in backup mode during replication.
	Snap	Consistent	Recoverable	When the application was in backup mode during replication.
	Snap	Consistent	Restartable	When the application was not in backup mode during replication.
	MirrorView/ S MirrorView/ A			
	SAN Copy	Complete	Recoverable	When the application was in backup mode during replication.
RecoverPoint	RecoverPoint	Bookmark	Recoverable	When the application was in backup mode during replication.
	RecoverPoint	Bookmark CDP CRR	Restartable	