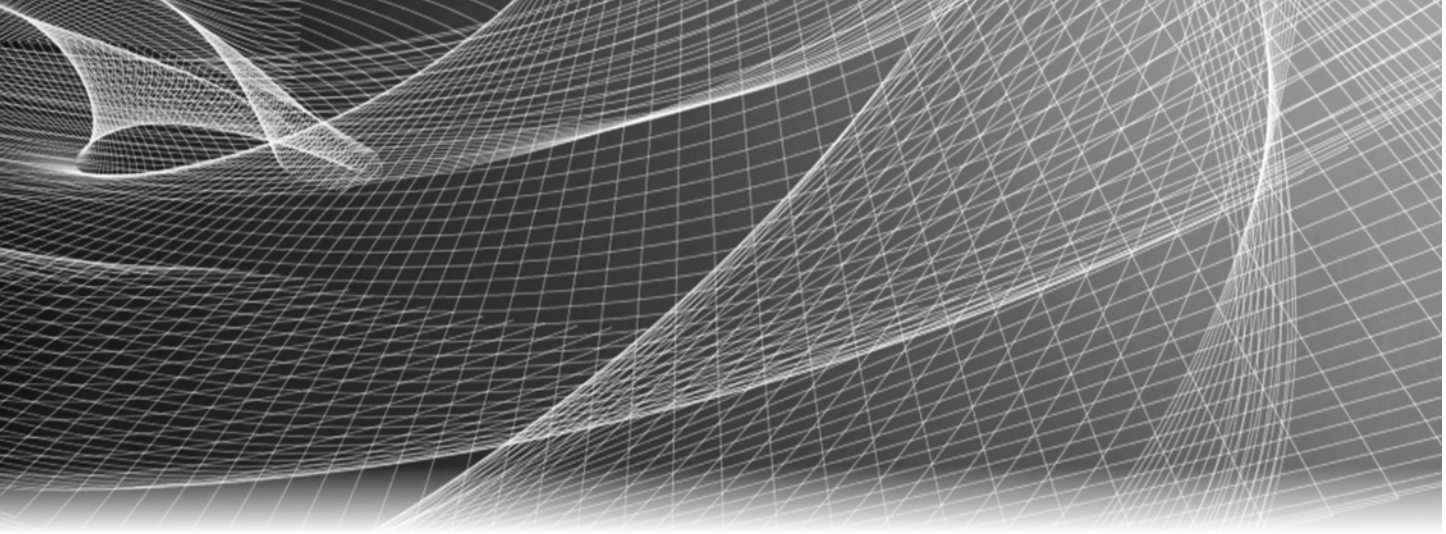

EMC Data Domain and VMware Data Recovery

Integration Guide

302-000-504

EMC²

Published November 2013

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date regulatory document for your product line, go to EMC Online Support (https://support.emc.com).

EMC Data Domain and VMware Data Recovery Integration Guide

This document explains how to configure EMC Data Domain® systems as a Backup destination for the VMware Data Recovery for CIFS Protocol. .

About This Document

Note: Prior to performing this integration, be sure to consult the *EMC Data Domain Backup Product Compatibility Matrix* on the EMC Support portal (https://support.emc.com) or the Data Domain support portal (https://support.datadomain.com) for the versions of VMware Data Recovery and DD OS certified for use with the respective products.

This document explains how to configure EMC Data Domain® systems as a Backup destination for the VMware Data Recovery for CIFS Protocol. Please confirm you have the most recent version of the Integration Guide specific to your environment before proceeding to ensure you have the latest best practices information.

This document is applicable for the following versions of the VMware Data Recovery:

- VMware Data Recovery v 2.0

Audience

This paper is intended for customers, technical field consultants, and customer engineers who have familiarity with either VMware Data Recovery and/or Data Domain operations.

Related Documents

The EMC Data Domain system and VMware Data Recovery documents referred to in this guide provide additional information for configuring and using Data Domain and VMware Data Recovery.

The VMware Data Recovery documents are available on the following links

http://www.vmware.com/support/vdr/doc/vdr_201_releasenotes.html

Documentation for the EMC Data Domain system is available at:

https://my.datadomain.com/documentation and on Powerlink.

Configuration Overview

Configuring an EMC Data Domain system to be a backup target for VMware Data Recovery involves completing the following steps:

1. Create CIFS shares on the EMC Data Domain system. These shares will become backup targets.
2. Configure the VMware Data Recovery on the vCenter Server, adding an EMC Data Domain system as a backup target.
3. Perform a test backup and verify that the test backup completed successfully.

These steps are covered in more detail in this integration guide, the VMware Data Recovery documentation, and the EMC Data Domain system user documentation.

Prerequisites

The following are the minimum requirements when integrating the VMware Data Recovery with an EMC Data Domain system:

- One EMC Data Domain system
- One VMware vCenter Server

Note: Since the VMware Data Recovery tool performs "block level deduplication" by default, the compression rates on the will be very low.

VMware recommends using Windows CIFS shares as the dedupe store. The maximum supported size is 500 GB, although the file system may show higher capacity. For more details, please refer to the *VMware Data Recovery 2.0 Administration Guide*.

EMC Data Domain Configuration

This section assumes that the EMC Data Domain system is named `ddhostname`. You may need to use the fully qualified domain name in your environment.

When using the CIFS protocol, it is recommended the EMC Data Domain system be joined to the same Microsoft Active Directory domain as the VMware Data Recovery plugin installed on the vCenter Server. Please refer to the CIFS section of the *EMC Data Domain 5.x Administrator's Guide* for detailed instructions on how to configure an EMC Data Domain system when using the CIFS protocol.

All Data Domain CLI commands are executed via an SSH session. For Windows clients, use a freeware tool like PUTTY.exe to establish an SSH session with the EMC Data Domain system.

MTree Setup and Configuration

DD OS uses MTrees (that is, managed trees). An MTree is an active file system that provides the ability to perform object/data management such as access policies, snapshots, replication, and data retention.

EMC recommends that you create at least one MTree to contain the target CIFS share or NFS export.

To create an MTree, complete the following steps:

1. Click the Data Management > MTree tab.
2. In the MTree overview area, click Create. The Create MTree dialog box appears.
3. Enter a name for the MTree in the MTree Name text box. For example, enter *Archive1* as the MTree name.
4. Click OK. The new MTree displays in the MTree table. (Figure 1)

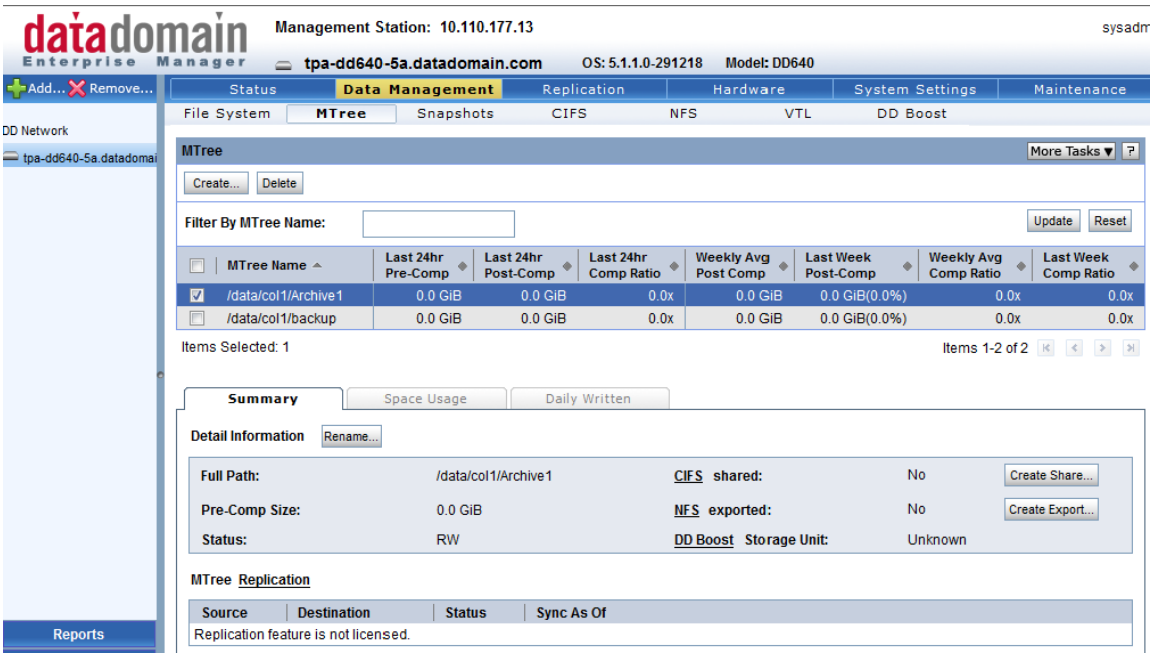

Figure 1: Creating an MTree

5. Repeat steps 2 through 4 to create additional MTrees, as needed.

Configuring a CIFS Share in an MTree on the EMC Data Domain System

Follow the steps in this section to create a CIFS share, *archivedata*, in the Archive1 MTree on the EMC Data Domain system and to give the archive (or authorized administrative) server access to the share using the Data Domain Enterprise Manager.

1. Click Data Management > MTree tab to navigate to the MTree view.
2. Select the MTree and click Create Share in the MTree Summary area. The Create Share dialog box appears. (Figure 2)
3. In the Create Share dialog box, enter the following information:
   a. Enter a name for the share (for example, `archivedata`).
   b. Add a client by clicking the plus sign (+) in the Client area. The Client dialog box appears.
   c. Enter the name of the client in the Client text box and click **OK**. Repeat step 3c for each client you want to configure.

Note: Using an asterisk (*) as a client name grants all servers who can access the specified path access to the share.

   d. Click **OK**.
4. Repeat steps 2 and 3 to create a share for another MTree, as needed.

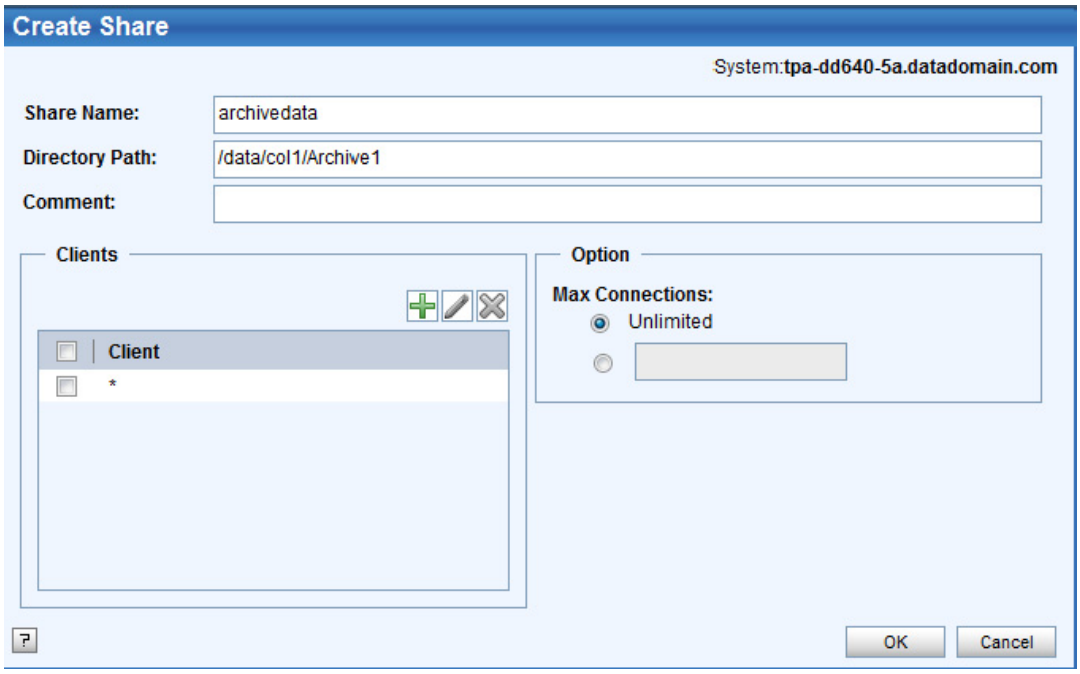

Figure 2: Creating a Share

You can also create shares for an MTree under **Data Management > CIFS** by completing the following steps:

1. Select the Shares tab.
2. Click **Create** and enter the following information:
   a. Enter a name for the share.
   b. Enter the directory path for the share. This directory path will be **/data/col1/<MTree name>.**
   c. Add a client by clicking the plus sign (+) in the Client area. The Client dialog box appears.

d. Enter the name of the client in the Client text box and click **OK**. Repeat step 2d for each client you want to configure.

e. Click **OK**.

3. Repeat step 2 for each additional share.

Note: Alternatively, you can use the Data Domain CLI to configure the appropriate shares.

You should now be able to map a drive on the archive server (or another authorized administrative server) to each Data Domain share (for example, \\<ddhostname>\<share name> or \\<Data Domain IP address>\<share name>).

VMware Data Recovery Configuration—CIFS

Follow the steps in this section to configure the VMware Data Recovery to use the EMC Data Domain system as a backup target, perform a test backup, and retrieve an archived file in a Windows environment.

Configuring the EMC Data Domain System as a Backup Target

After installing the VMware Data Recovery Appliance on the vCenter Server, log on to the vCenter Server using the vSphere client and complete the following steps:

1. Click **Home-> Solutions and Applications -> VMware Data Recovery**.
2. On the Configuration tab, select Destinations and click Add Network Share. (Figure 3)

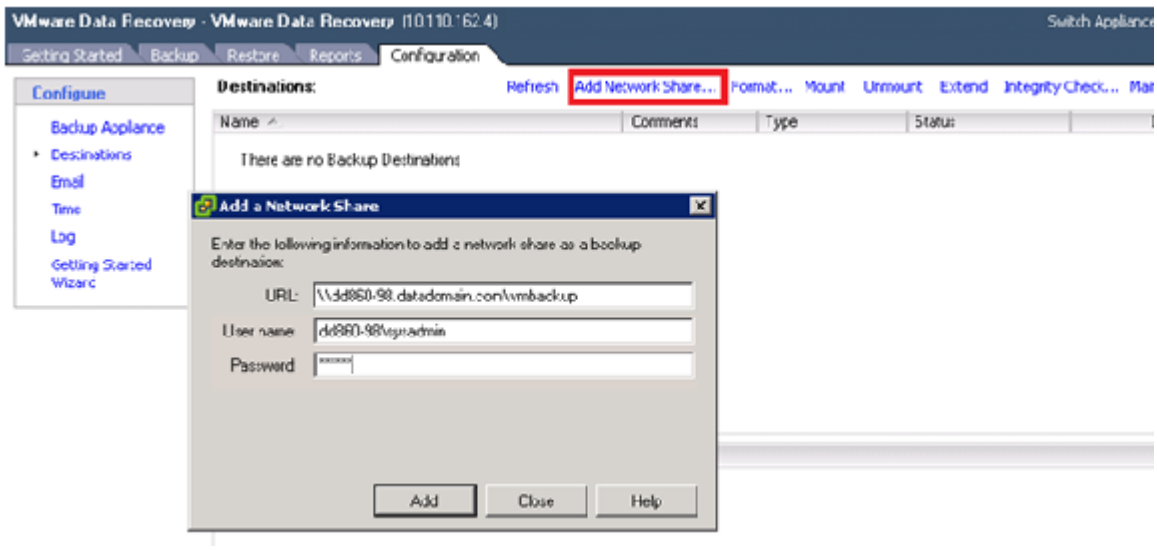

Figure 3: Configuring a Backup Destination during VMware Data Recovery

Performing a Backup

Before running the backup on the VMware Data Recovery Server, ensure that the existing backup jobs were created using the EMC Data Domain Recovery CIFS mount as a destination.

Log on to the vCenter Server using the vSphere client and complete the following steps:

1. Click **Home-> Solutions and Applications -> VMware Data Recovery**.
2. On the Backup tab, right-click one of the back up jobs and select **Backup Now-> All Sources**. (Figure 4)

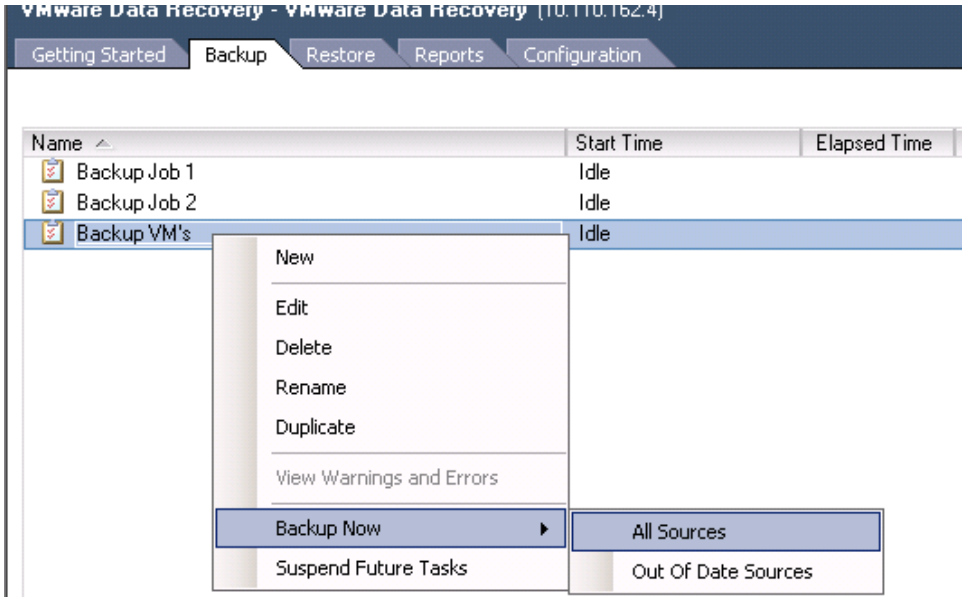

Figure 4: Performing a Backup on VMware Data Recovery

Restoring the Virtual Machines From VMware Data Recovery

To restore the virtual machines from VMware Data Recovery, log on to the vCenter Server using the vSphere client and complete the following steps:

1. Click **Home-> Solutions and Applications -> VMware Data Recovery**.
2. On the Restore tab, select the Virtual Machine and click Restore. (Figure 5)

Figure 5: Restoring Virtual Machines during VMware Data Recovery

Performing a Replication

For more information about performing a replication, see the *EMC Data Domain Operating System User Guide*.

If a backup is replicated to a secondary EMC Data Domain system, an administrator can browse the recovery points on the secondary EMC Data Domain system. The backup destination location can point to the secondary EMC Data Domain system.

Restoring the Virtual Machines From the Replication EMC Data Domain System

To restore data from the replicated EMC Data Domain system, change the backup destination settings on the Backup File Location.

Log on to the vCenter Server using the vSphere client and complete the following steps:

1. Click **Home-> Solutions and Applications -> VMware Data Recovery.**
2. On the Configuration tab, select Destinations and click Add Network Share.
3. Enter the EMC Data Domain system CIFS share in the URL field, along with the username and password in the appropriate fields, and then click Add. (Figure 6)

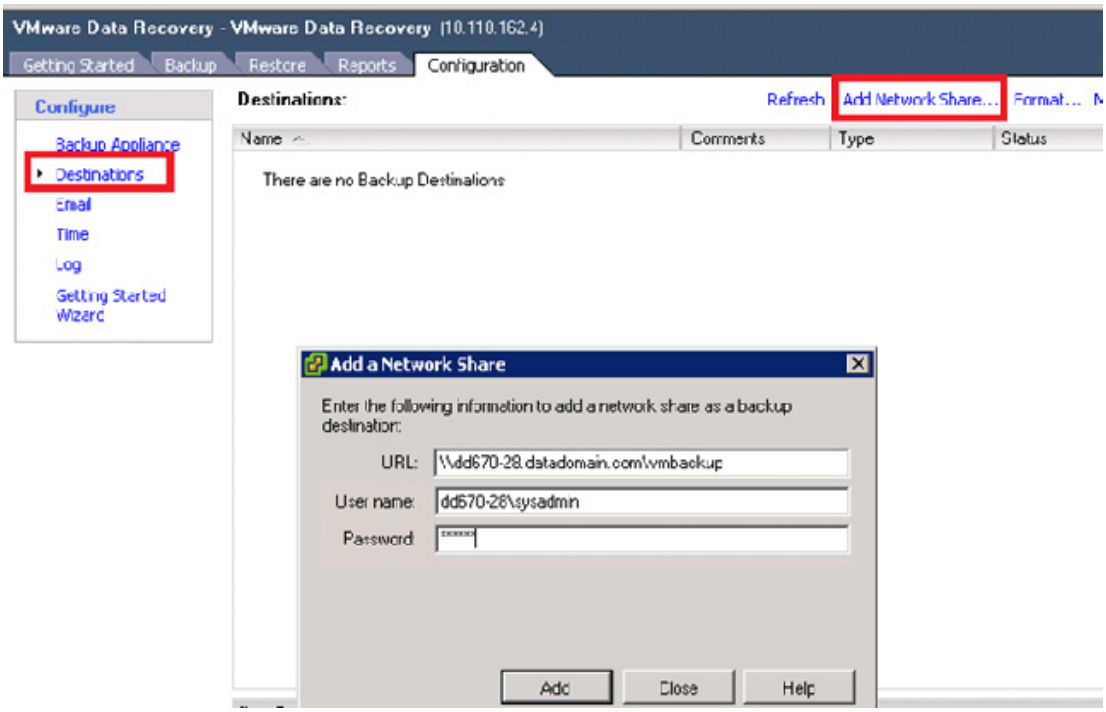

Figure 6: Changing the Backup Destination to the Replicated EMC Data Domain System

After adding the replicated EMC Data Domain system o the destination path, click the Restore tab and browse the list of virtual machines. Check the status of the replicated EMC Data Domain system destination.

If you do not see the virtual machines backup history on the Restore tab, restart the VMware Data Recovery Service. (Figure 7)

After restarting the VMware Data Recovery Service, the virtual machines backup history should be visible on the Restore tab.

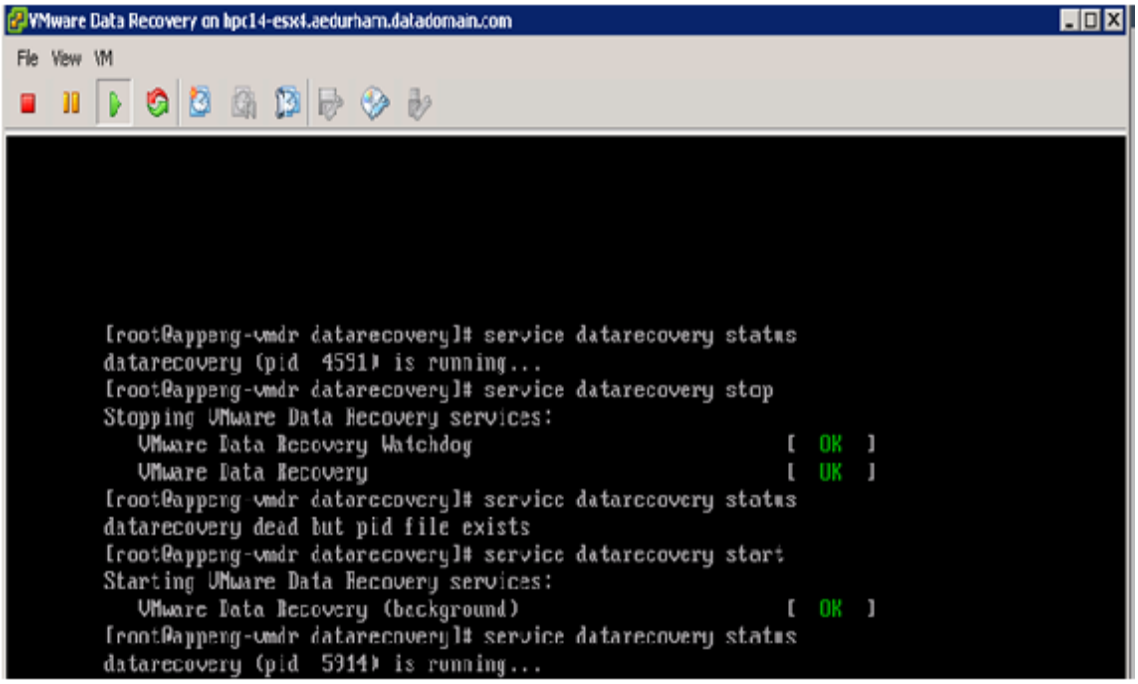

Figure 7: Restarting the VMware Data Recovery Service

If you see the "Integrity Check failed" status for a destination, click Integrity Check on the Configuration tab to run the Integrity Check manually. (Figure 8)

For more information about known issues related to integrity check failures, see the *VMware Data Recovery 2.0.1 Release Notes* at the following link:

http://www.vmware.com/support/vdr/doc/vdr_201_releasenotes.html

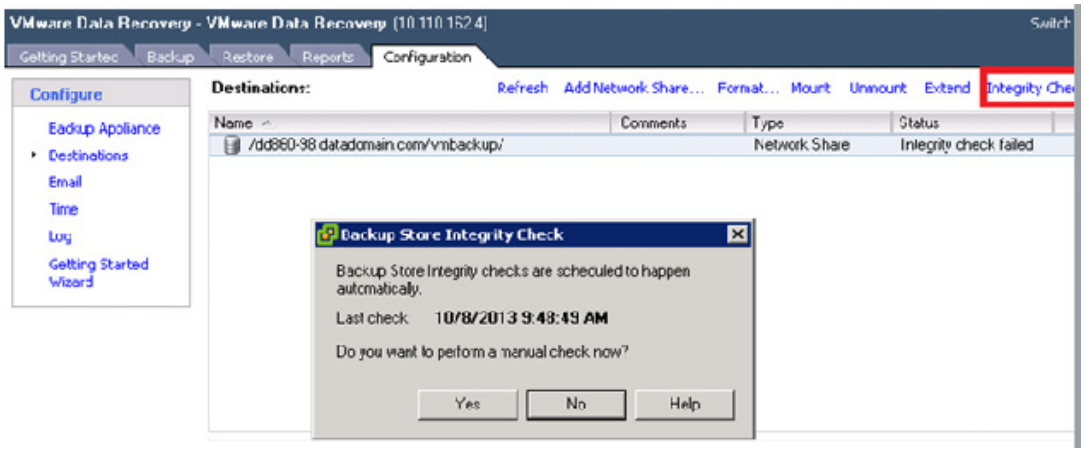

Figure 8: Running an Integrity Check

Documentation Feedback

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send your opinions of this document to BRSdocumentation@emc.com.