Technical Note

Restoring Dell EMC Avamar Checkpoint Backups from a Dell EMC Data Domain System After a Single Node Avamar Failure

300-015-218
REV 03
February 2018

- Revision history 2
- Purpose 2
- Related documentation 2
- Performing a checkpoint restore 2

DELL EMC

Revision history

Review the revision history of this document.

Revision	Date	Description
01	July 10, 2013	First release of this document.
02	September 23, 2013	Added additional checkpoint after restore operation is completed.
03	February 23, 2018	Various edits throughout.

Purpose

This technical note provides the steps to restore an Avamar checkpoint from a Data Domain system in the event the single node Avamar server fails.

Avamar checkpoint backup support allows Avamar checkpoints to be stored on a Data Domain system (using DD OS 5.3 or later). These checkpoints are then used if disaster recovery is required.

This option is only available on a single node Avamar server or an Avamar Virtual Edition server. The backup option for Avamar checkpoint support is configured through the Avamar Administrator, but the restore option is only available through Dell EMC Professional Services.

Related documentation

The publications in this section provide additional information.

- *The Avamar Administration Guide* provides details on system migration and replacement, as well as other Avamar backup, restore, and administration tasks.
- *The Avamar and Data Domain Integration Guide* provides details on configuring a Data Domain system for use with an Avamar server.
- *The Avamar Technical Addendum* provides reference details on server scripts and commands.

Performing a checkpoint restore

If you have created Avamar checkpoint backups on a Data Domain system, you can restore a checkpoint (GSAN) to a new single node Avamar server in the event the original single node Avamar server fails.

Before you begin

Use this procedure for the following scenario:

- You have a valid checkpoint for a single node Avamar server on a Data Domain system target.
- The single node Avamar server that failed has been replaced.
- The replacement Avamar server is a new server with no backup data or metadata.

- Avamar 7.0 or later is installed on the replacement Avamar server.
- The replacement Avamar server is the same size as or larger than the original Avamar server.
- The replacement Avamar server must have the same data partition count as the original Avamar server.

Note

The `cprestore` script is used in step 2 for the restore operation. The `cprestore` command completes the following tasks:

- Creates NFS export on DD system.
- Mounts DD NFS export on Avamar server.
- copies GSAN backup files from backup on DD system to the corresponding Avamar server checkpoint directory in each data partition.
- Undoes NFS mount and export.

Procedure

1. Log in to the Avamar server as root and from a CLI prompt, query available GSAN backups by typing: **ddrmaint cp-backup-list --full --ddr-server=*Data_Domain_system* --ddr-user=*DD_Boost_user_name* --ddr-password=*DD_Boost_user_password***

   Where:

   - *Data_Domain_system* is the Data Domain system with the single node Avamar server checkpoint backup.
   - *DD_Boost_user_name* is the DD Boost user account used for Avamar and Data Domain system integration.
   - *DD_Boost_user_password* is the DD Boost user account password used for Avamar and Data Domain system integration.

   The output will be similar to the following example:

   ```
   ================== Checkpoint ==================
   Avamar Server Name    : a4dpe223d
   Avamar Server MTree/LSU    : avamar-1346892530
   Data Domain System Name    : griffin-dd10.asl.lab.emc.com
   Avamar Client Path    : /MC_SYSTEM/avamar-1346892530
   Avamar Client ID    : 8b75468f70dc8ff0fa2e5118cec8ecdddf7fccee
   Checkpoint Name : cp.20120919184604
   Checkpoint Backup Date : 2012-09-19 11:51:12
   Data Partitions : 6
   Attached Data Domain systems : griffin-dd10.asl.lab.emc.com
   ```

2. Restore the GSAN backups on the Data Domain system (requires the Data Domain server name and credentials of the default GSAN backups target Data Domain system) by typing the following command on the Avamar server: **/usr/local/avamar/bin/cprestore --hfscreatetime=*Avamar_ID* --ddr-server=*Data_Domain_system* --ddr-user=*DD_Boost_user_name* --cptag=*Checkpoint_name***

   Where:

   - *Avamar_ID* is determined from Avamar Server, for example, `MTree/LSU:avamar-1346892530`. The value is `1346892530`.

- *Data_Domain_system* is the Data Domain system with the single node Avamar server checkpoint backup. In the previous checkpoint output example, the value is `griffin-dd10.asl.lab.emc.com`.
- *DD_Boost_user_name* is the DD Boost user account used for Avamar and Data Domain system integration. In the previous checkpoint output example, the value is `avamar`.
- *Checkpoint_name* is the checkpoint name. In the previous checkpoint output example, the value is `cp.20120919184604`.

3. Stop the Avamar server by typing the following command: **`dpnctl stop`**
4. Type **`y`** to the confirmation message, `Do you wish to shut down the local instance of EMS?`
5. To initiate a rollback, type the following command: **`dpnctl start --force_rollback`**

   A message appears that the GSAN was shutdown.
6. In the list of choices that appears, select option 3, **Select a specific checkpoint to which to roll back**.
7. Wait for the rollback to complete.

   The rollback might take up to one hour, depending on the amount of data present in the Avamar server. When the rollback is complete, the command prompt returns.
8. Open the user-defined temporary file created during the rollback and verify that the rollback successfully completed without errors.

   The Avamar server automatically restarts after a successful rollback.
9. Create a checkpoint on the Avamar server:
   a. In Avamar Administrator, click **Server**.

      The **Server** window appears.
   b. Select **Checkpoint Management** > **Actions** > **Create Checkpoint**

      The **Create Checkpoint** dialog box shows the progress of the operation.
   c. When the *Create Checkpoint* dialog box shows that the checkpoint is complete, click **Close**.
10. Validate the checkpoint:
    a. On the **Checkpoint Management** tab of the **Server** window, select the new checkpoint.
    b. Select **Actions** > **Validate Checkpoint**.
    c. In the **Validation Type** dialog box, select **Full** from the list and click **OK**.

Published February 2018