Technical Report

Backup and Recovery of Siemens PLM Teamcenter on NetApp Clustered Storage Solutions

NetApp and Siemens PLM
April 2013 | TR-4167

Abstract

This technical report describes in detail the way to back up and recover Siemens PLM Teamcenter® data on NetApp® clustered storage solutions. It provides information on the critical Teamcenter data that is important to protect and some basic procedures for performing backup and recovery. It also discusses NetApp's solution for disaster recovery.

TABLE OF CONTENTS

LIST OF TABLES

1 Introduction

Siemens PLM Teamcenter is a product lifecycle management application that provides product development teams with the ability to help manage product information throughout the process of designing, developing, and building products. Siemens PLM Teamcenter provides engineering and manufacturing teams with the global sharing and workgroup management capabilities required to capture, manage, and leverage engineering data created by numerous CAD, CAM, CAE and other systems.

Data protection of Teamcenter's main repositories that hold a company's intellectual property is imperative to the success of product development companies. It can be very costly when critical data that has been developed for months or years is lost due to user error, hardware malfunction, or catastrophic failure.

NetApp clustered Data ONTAP® software provides data protection solutions that eliminate or minimize data loss and keep Teamcenter's main repositories safe. NetApp Snapshot™ technology enables backups to be performed in minutes, reducing backup windows. With NetApp SnapManager®, SnapDrive®, and Snap Creator™ products, backup and recovery of Teamcenter database and file vaults can be automated to reduce the complexity associated with this process. NetApp SnapMirror® solutions simplify disaster recovery using an easy-to-implement and robust mirroring solution. Implementing NetApp SnapMirror significantly reduces risks for an organization and protects Teamcenter data in the event of a catastrophic event.

1.1 Scope

Teamcenter repositories can be deployed on any NetApp supported storage protocol, including FC, iSCSI, NFS, CIFS, and even a split configuration in which the database is on SAN and file vaults are on NAS. This document provides methods and procedures for protecting Teamcenter database and file vaults on NetApp clustered storage.

1.2 Audience

This document is intended for use by individuals responsible for the backup and recovery of Teamcenter data on NetApp clustered Data ONTAP storage. It assumes that readers have experience with administration of NetApp clustered Data ONTAP solutions and Siemens PLM Teamcenter. It also assumes that the reader has read TR-4098: Deployment and Implementation Guide: Siemens PLM Teamcenter on NetApp Data ONTAP Operating in Cluster-Mode for an understanding of Teamcenter architecture and deployment options on NetApp clustered Data ONTAP storage.

2 Teamcenter Critical Data

The most critical data to protect and preserve in a Teamcenter environment is in the Teamcenter database and file vaults. This data contains all the files, directories, and metadata associated with the product development projects. Teamcenter can be deployed as a two-tier or four-tier configuration. In either configuration, there is a resource tier in which the Teamcenter application interact with and manage the database and file vaults.

2.1 Database

The database stores the metadata associated with the designs and files being managed by the Teamcenter File Management System. Databases that are supported include Oracle®, Microsoft® SQL Server®, and IBM DB2.

2.2 File Vaults

The File Vault stores all engineering documents and data files associated with the project or products in the product lifecycle. This can include engineering drawings (CAD, NX, and AutoCAD files), specifications, requirement documents, engineering calculations and analysis, safety documents, QC reports, vendor data, binary data, images, or any other document related to the product being developed.

2.3 Optional Files/Directories

There are other files and directories, although optional, that the "Teamcenter Administration Guide" recommends be backed up; however, these files do not necessarily reside on NetApp storage. The files include:

- *TC_DATA* directory - stores Teamcenter configuration and other data
- *TC_ROOT* directory - contains Teamcenter binaries
- Local Business Modeler IDE project folders - include project folders within source control management systems. These are typically located in the workspace directory defined by the USERPROFILE environment variable.

The TC_ROOT is the installation location of Teamcenter. These folders or directories can be placed on NetApp storage to ease the backup and recovery process.

3 NetApp Data Protection Solutions

NetApp's data protection solutions provide Teamcenter customers with a simplified and quick approach to backing up and recovering critical Teamcenter data. These solutions were designed to improve the overall operational efficiency of backup and recovery.

Integrated into NetApp's storage platform are capabilities that provide high availability and resiliency in case of storage hardware failures. These include:

- Raid-DP® - High-performance RAID 6 (dual parity) implementation that protects against simultaneous failure of two drives in the same RAID group
- Active-Active - HA pair controller configuration that provides high-availability solutions during planned and unplanned downtime events

Below are highlights of other integrated data protection solutions that NetApp provides to protect against many different types of disaster scenarios ranging from the most common failures, such as power, hardware, network, or application failures within the data center, to the most catastrophic events, such as floods, hurricanes, or natural disasters. These solutions include:

- Backup and Recovery
  - Snapshot - Creates disk-to-disk point-in-time backup copies in native format
  - SnapRestore® data recovery software - Uses stored Data ONTAP Snapshot copies to recover anything from a single file to multiterabyte volumes in seconds
- Disk-to-Disk Backup
  - SnapVault® software - Speeds up and simplifies backup and data recovery, protecting data at the block level; also a disk-to-disk backup for NetApp FAS systems
  - Open Systems SnapVault® (OSSV) software - Leverages block-level incremental backup technology to protect Windows®, Linux®, UNIX®, SQL Server, and VMware® systems running on mixed storage; replication-based disk-to-disk backup for open system storage servers
- Application-Aware Backup and Recovery Solutions for Applications
  - Snap Creator - Provides a central framework that integrates NetApp Snapshot technology with applications such as Oracle, IBM DB2, and Microsoft SQL Server

  - SnapManager - Simplifies configuration, backup, and restore operations for leading enterprise applications such as Oracle, Microsoft SQL Server, and Exchange
  - SnapDrive - Assists in storage provisioning for UNIX or Windows platforms and automates OS-consistent backup and restore of application data
- Tools for Backup Administrators to Simplify Processes
  - OnCommand® Unified Manager - Automates the management of physical and virtual storage for NetApp storage systems and clusters
  - SnapProtect® management software - Accelerates and simplifies backup and data recovery for shared IT infrastructures; provides a single management console that allows you to create, catalog (for indexing and fast search of Snapshot copies), and manage application-aware Snapshot copies across disk-to-disk to-tape processes
- Tools for Compliance
  - SnapLock® compliance software - A flexible data permanence solution for meeting strict data retention regulations or internal IT governance policies; allows creation of nonrewritable, nonerasable volumes to prevent files from being altered or deleted until a predetermined retention date
- High Availability and Business Continuity
  - SnapMirror data replication technology - Provides disaster recovery protection and simplifies the management of data replication; provides three modes of mirroring: sync, semi-sync, and asynchronous
  - MetroCluster™ high-availability and disaster recovery software - Delivers continuous availability, transparent failover protection, and zero data loss
- Archival
  - Tape - NetApp's tape backup and restore solution that uses Network Data Management Protocol (NDMP) version 3 and 4, which efficiently maximizes network bandwidth; NDMP-enabled commercial backup applications can be used to perform a dump backup or restore

NetApp also provides global support and services that assist in fixing problems and/or assist in backup and recovery planning. Services that are offered include:

- AutoSupport and Storage Availability Audits - Monitoring and reporting technology that checks the health of NetApp storage systems on a continual basis; provides a call-home feature that, if the storage has any failure, it will automatically contact NetApp Support to handle or replace the part
- Personalized Support Services - Availability of a NetApp Support Account Manager, NetApp Support Advisor, or NetApp Resident Support Engineer to provide 24/7 incident management, education, and on-site reactive and proactive support

In addition, NetApp's data protection services leverage NetApp storage efficiency technology to reduce both storage and management costs. Core to NetApp data protection is its Snapshot technology. When a snapshot is created, only new or changed blocks are transferred to disk to reduce backup windows, minimize network traffic, and reduce disk capacity.

Note: Some of the abovementioned features are not yet supported on NetApp clustered Data ONTAP. Refer to the Limitations section of this document for more information.

4 Backup and Recovery of Teamcenter Data

Regular backups of Teamcenter data are important for product development environments to recover from potential disasters and loss-of-data scenarios. Planning and implementing for backup and recovery are important to achieve optimal availability and IT efficiency. When developing a strategy for backup and recovery there are two objectives to consider:

- Recovery Point Objective (RPO) - The amount of acceptable data loss

- Recovery Time Object (RTO) - The amount of time it takes to perform the recovery

Your criteria for the above objectives would determine the backup and recovery strategy to select. As mentioned in the previous sections, NetApp provides a wide range of data protection solutions that would assist in improving your RPO and RTO. The following sections discuss the generic steps and procedures for doing regular backup and recovery of Teamcenter data kept on NetApp storage.

With the use of NetApp Snapshot technology together with NetApp SnapManager or Snap Creator and SnapDrive solutions, backup and recovery are fast and simple to administer. This section discusses the basic steps for backup and recovery of Teamcenter repositories and the tools that NetApp provides to assist in this process.

4.1 Backup

The resource tier of Teamcenter includes both the database and file vaults. Since the Teamcenter database contains references to content in the file vaults, NetApp recommends backing them up simultaneously for maximum consistency between the database and the file vaults.

There are two approaches to back up the database and file vaults:

- **Cold backups** - A complete shutdown of Teamcenter application services and database services in order to do the backup.
- **Hot backups** - Teamcenter application services are placed in temporary suspend mode, the database is set to quiesced mode, and the file vaults are in read-only mode in order to perform the backup.

Whether you have a two-tier or a four-tier Teamcenter configuration will determine which services would need to be shut down in order to do a cold backup. Since there is no web tier in a two-tier configuration, shutting down the web tier is not required. In general, the Teamcenter application services will need to be shut down prior to the shutdown of the database for cold backups. Once all Teamcenter and database services are shut down, a Snapshot copy of the volume(s) containing the database and file vaults can be made, followed by a restart of the database and Teamcenter application services. Table 1 describes the basic procedure for conducting a cold and a hot backup of Teamcenter.

In order to do hot backups, Teamcenter provides a **backup_modes** utility. This utility places the Teamcenter file vaults in certain operational modes that include:

- Read-Only Mode—Places Teamcenter file vaults into a read-only state
- Blobby Volume Mode—Places Teamcenter in blobby (temporary) volume mode, allowing continuous availability
- Normal Mode—Places Teamcenter back in normal mode from read-only or blobby volume mode

During hot backups, the Teamcenter backup_modes utility places Teamcenter in read-only mode and, when the Snapshot copy is complete, the backup_modes utility is used to place Teamcenter back in normal mode. Since the backups on NetApp are quick, placing Teamcenter in Blobby Volume mode is optional, but recommended to maintain database and volume consistency. The use of the backup_modes utility requires setting *TC_enable_backup_modes* to TRUE. If Blobby Volume mode is desired, the alternate location to store files during the hot backup needs to be specified using *blobbyVolume_UNIX* or *blobbyVolume_NT*. These values are set using the Teamcenter **preferences_manager** utility or the Teamcenter rich client administration application.

Table 1) Cold and hot backup procedures for Teamcenter data.

COLD BACKUP	HOT BACKUP
1. Shut down Teamcenter Application Services (FMS, TC_Server Pool Manager, any other Application services (eg. IDSM). 2. Shut down database. 3. Create a Snapshot copy of the volumes containing the database and file vaults. 4. Restart the database. 5. Restart Teamcenter application services.	1. Run the backup_modes utility to set Teamcenter in read-only mode. 2. Quiesce the database. 3. Create a Snapshot copy of the volumes containing the database and file vaults. 4. Unquiesce the database. 5. Run the backup_modes utility to set Teamcenter in normal mode. **Note:** NOTE: Snap Creator or SnapManager can be used to automate this process. If the database and/or file vaults reside on NetApp LUNs, use SnapDrive to create a consistent backup.

4.2 Restore

Although hot restores are possible, NetApp recommends doing a cold restore of the entire database and/or file vaults so that the Teamcenter database is synchronized with the file vaults. The basic procedure to do a restore is:

1. Shut down Teamcenter Application Services (FMS, TCServer, Application Server).
2. Shut down the database.
3. Restore the desired Snapshot copy of the database and file vaults.
4. Restart the database.
5. Restart Teamcenter Application Services.

Again, Snap Creator, SnapManager, or SnapDrive can be used to restore the desired Snapshot copy of the database and file vaults.

4.3 Snap Creator, SnapManager, and SnapDrive

As mentioned in Section 3, NetApp provides Snap Creator, SnapManager, and SnapDrive, which are application-aware backup and recovery solutions for applications such as Oracle, Microsoft SQL, and/or IBM DB2. The purpose of these products is to assist in automating the backup and recovery process of Teamcenter data. For instance, Snap Creator provides the framework that can quiesce Teamcenter Application Services and the database, take a Snapshot copy of the Teamcenter repositories residing on NetApp storage, and place the application and database services back online to resume normal operation.

Similarly, SnapManager for Oracle can also quiesce the database, take a Snapshot copy of the volumes containing the Teamcenter data, and then return the database to normal operation. The difference between SnapManager and Snap Creator is that SnapManager provides more features and integration with the database. For instance SnapManager for Oracle provides RMAN support, full or granular backups of tablespaces and data files, and automated archive log management. Although Snap Creator is designed to be more simplistic, it does provide the capability to add PRE and POST commands to quiesce and unquiesce other applications (such as Teamcenter) as well as allow customizations.

SnapDrive integrates with both Snap Creator and SnapManager. It also assists in provisioning clustered storage and provides consistent Snapshot copies when backing up the file system. SnapDrive is important when backing up LUNs on NetApp storage because it flushes the operating system buffers prior to creation of the Snapshot copy.

Refer to the Appendix for an example of how to set up Snap Creator to do a hot backup of a Teamcenter database on Oracle and file vaults. Refer also to the References section for links to technical reports and administration guides on SnapManager and SnapDrive.

4.4 Snapshot Schedules

When volumes are created, Snapshot copy schedules are set up by default to automatically take hourly, weekly, and monthly Snapshot copies. Since Teamcenter applications and the database needs to be quiesced prior to taking a Snapshot copy, the default scheduled Snapshot policy should be disabled in one of the following ways.

- When the volume is created, set the `snapshot-policy` option to none. For example:

  vol create –vserver test –volume test_vol –aggregate aggr_test –size 20MB –state online –type RW –snapshot-policy none

- Modify the volume Snapshot policy to none. For example:

  vol modify –vserver test –volume test_vol –snapshot-policy none

After the Snapshot policy has been disabled on the storage, Snap Creator can be configured to set up the schedule and Snapshot policies.

5 Disaster Recovery

Having a disaster recovery site to protect Teamcenter data minimizes data loss in the event of a catastrophic event at a main site. The NetApp SnapMirror solution creates an identical second set of data capable of replacing the primary set of Teamcenter data if something happens to the primary. In addition, the solution is built on a replication engine that provides a more robust, scalable, and higher-performing data copy infrastructure. SnapMirror utilizes Snapshot technology by replicating the image copy **asynchronously** from the source volume to the destination volume. To minimize the storage and network bandwidth impact, SnapMirror replicates only the changed blocks from the primary storage controller after the initial synchronization. There are two types of data protection mirrors:

- **Intracluster**—Mirrors within a cluster
- **Intercluster**—Mirrors to a different cluster in a different location

Intercluster SnapMirror should be used for disaster recovery of Teamcenter data for greater protection. It provides a failover and giveback solution for volumes residing on different clusters. This type of solution protects against hardware failures, data center or floor failures, and site failures.

As for mirror disk backups and restores using SnapMirror, see "TR-3999: SnapMirror Startup Guide for Data ONTAP 8.1 Operating in Cluster-Mode." It provides instructions for setting up SnapMirror relationships in clustered Data ONTAP, and thus this document does not cover these procedures. For detailed information on SnapMirror, refer to the "Data ONTAP Cluster-Mode Data Protection Guide" on the NetApp Support (formerly NOW) site for your particular release.

6 Limitations

At the time this technical report was written, NetApp clustered Data ONTAP 8.1 did not yet have support for the following features:

- Qtree SnapMirror
- Synchronous SnapMirror
- SnapVault
- MetroCluster

There are also limitations for the SnapManager and SnapDrive products. SnapManager and SnapDrive solutions currently are available only for Windows and Linux.

Future releases of NetApp clustered Data ONTAP will eventually provide support for the features mentioned above. Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to get the latest updates and information on supported features.

7 Conclusions

NetApp storage is an ideal choice to complement the flexibility and scalability as well as the ease of administration and backup and recovery of Siemens PLM Teamcenter. Protecting Teamcenter data is important for safeguarding a company's investment in product development efforts. NetApp provides an array of data protection solutions that reduce risk for an organization and simplify the protection of Teamcenter data.

References

- Data Protection Online Backup and Recovery Guides on NOW for the appropriate Data ONTAP version
  http://support.netapp.com/documentation/productlibrary/index.html?productID=30092
- Teamcenter System Administration Guides (requires a Siemens PLM WebKey)
  http://support.industrysoftware.automation.siemens.com/docs/teamcenter/
- SnapManager 3.2 for Oracle Best Practices
  http://www.netapp.com/us/media/tr-3761.pdf
- SnapDrive 6.5 for Windows for Clustered Data ONTAP
- http://www.netapp.com/us/media/tr-4000.pdf
- SnapManager for SQL Server on Data ONTAP 8.1 Operating in Cluster-Mode
  http://www.netapp.com/us/media/tr-4002.pdf
- SnapDrive 5.0 for UNIX Best Practices
  http://www.netapp.com/us/media/tr-3735.pdf

Version History

Version	Date	Document Version History
Version 1.0	March 2013	Agnes Jacob, NetApp and Siemens PLM

Appendix

Table 2, below, describes the basic steps to set up Snap Creator to take a hot backup of a Teamcenter database deployed on Oracle and file vaults in a UNIX (Solaris 10) environment.

Each configuration and setup is different and, thus, the following steps are only an example of how to use Snap Creator and they should be used only as a reference. For this example, the configuration is as follows.

- The database, file vaults, and Teamcenter installation files reside on NFS volumes (apa_clone, plmdb2_clone, plmtc) on NetApp clustered Data ONTAP 8.1.1.
- Oracle version 11*g*™ R2 database is on one server (sun880-svl03: 172.17.44.39) running Solaris 10.
- Teamcenter version 8.2, File Management system, is on another host (sun880-svl04: 172.17.44.40) running Solaris 10.
- Snap Creator version 3.6 will be installed and run on the same machine as the database server.

If the database, file vaults, and/or installation directory reside on LUNs, SnapDrive should be used in order to create a consistent backup.

The latest version of Snap Creator can be downloaded from the NOW site. Refer to the Snap Creator Installation and Administration Guide for more detailed explanations.

Table 2) Basic instructions to set up Snap Creator to back up Teamcenter data.

Steps	Commands
1. On the File Management System server (sun880svl-04), set TC_enable_backup_modes to TRUE in order to be able to use the backup_modes utility to place the Teamcenter database in hot backup mode. Run preferences_manager as the administrator of the Teamcenter application. For this example, the administrator username is "infodba."	a) Log in as Teamcenter administrator "infodba." b) Export the preferences by creating a pref.xml file. *preferences_manager –u=infodba –p=infodba –g=dba -mode=export –scope=SITE –out_file=/var/tmp/pref.xml* c) Edit the TC_enable_backup_modes value in pref.xml file generated from the previous step: *<preference name="TC_enable_backup_modes" type="Logical" array="true" disabled="false">* *<preference_description>Enables setting and checking for backup modes in a 24x7 scenario. Valid values are true or false (default value). </preference_description>* *<context name="Teamcenter">* *<value>TRUE</value>* *</context>* *</preference>* d) Import the preferences. *preferences_manager –u=infodba –p=infodba –g=dba –mode=import –scope=SITE –file=/var/tmp/pref.xml –action=override* Optionally, you can edit the blobbyVolume_UNIX string to set up a temporary location for files in the pref.xml file. For this example, blobbyVolume_UNIX was not set and used.

Steps	Commands
2. Set up ssh keys so no password is required to ssh onto the File Management System server to run the backup_modes utility from the Snap Creator running on the DB server.	a) Generate an ssh key on the DB server. *ssh-keygen –t rsa* b) A public key file of form “id_rsa.pub” is placed in ~/.ssh directory. Cut and paste the public key generated in the file and place as the value on the appliance. *$ cd .ssh* *$ ls* *id_rsa id_rsa.pub known_hosts* *$ cat id_rsa.pub* *ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAx76XzuCTrmo9y9v3M/k5WGBZCEzS1qsxpWzuw0QDYNW3* *hMAl+9ZoYoWnW65rL3IrhldHf70/yJeV8zcPIc75Yl96mLA8gIvq1JQrJ6ZGVtX1CCg42atzEej7RL8g* *ECUhz1uMw1f6dboY93hRc4+uxjQwwQB/tQfVWR9xx3xvhJU= sadmin@sun880-svl03* c) As Teamcenter administrator “infodba” on the File Management System server, paste or append the contents of id_rsa.pub to ~/.ssh/authorized_keys file.
3. On the DB server (sun880-svl03), extract the Snap Creator package into the /usr/local directory	*cd /usr/local* *unzip NetApp_Snap_Creator_Framework3.6.0-SolarisSparc.tar.gz* *tar xvf NetApp_Snap_Creator_Framework3.6.0-SolarisSparc.tar*
4. Run snapcreator setup from the /usr/local/scServer* directory.	*cd /usr/local/scServer3.6.0* *./snapcreator --profile setup*
5. On the NetApp storage create a management LIF such that Snap Creator can access the NetApp storage.	*network interface create -vserver plmtc -lif test_mgmt -role data -data-protocol none -home-node fas3170c-svl11 -home-port e4b -address 172.31.8.247 -netmask 255.255.255.0 -status-admin up -firewall-policy mgmt*

Steps	Commands
6. On the NetApp storage system create user roles and set admin privileges for the Vserver that holds the volumes containing the database, file vaults, and installation. Privileges being modified are for http, ontapi, and ssh.	*security login create -username scuser -application http -role vsadmin -vserver plmtc -authmethod password* *Please enter a password for user 'scuser':* *Please enter it again:* *security login create -username scuser -application ontapi -role vsadmin -vserver plmtc -authmethod password* *security login create -username scuser -application ssh -role vsadmin -vserver plmtc -authmethod password* Note: When you create a user for scuser, it will ask for a password; make note of the password to put in the config profile *.conf file in scServer*.
7. On the DB server, create a directory in /usr/local/scServer* to store the profile file. Use the default.conf directory as a base configuration.	*mkdir –p /usr/local/scServer3.6.0/configs/TC2* *cp /usr/local/scServer_v3.2/configs/default/default.conf /usr/local/scServer_v3.2/configs/TC2/TC2.conf* Note: The directory name should be the same as the name of the profile configuration file. This configuration file can also be created via the Snap Creator GUI.
8. Edit the TC2.conf file and set the following parameters. These values can also be set using the Snap Creator GUI.	*SNAME=TC2* *VOLUMES=172.31.8.247:apa,plmdb2,plmtc_data* *NTAP_SNAPSHOT_RETENTIONS=daily:7* *NTAP_USERS=172.31.8.247:scuser/53616c7465645f5f85da307c97bd6024825d3ed3080a9df5dd3c6fdb2ca52fd2* *NTAP_PWD_PROTECTION=Y* *CMODE_CLUSTER_USERS=172.31.8.200:admin/53616c7465645f5ffda4e6c221807e2dd6d3dbd598931675eced47e4994b19fa* *CMODE_CLUSTER_NAME=172.31.8.200* *NTAP_SNAPSHOT_RETENTION_AGE=7* *NTAP_SNAPSHOT_NODELETE=N* *NTAP_SNAPSHOT_RESTORE_AUTO_DETECT=N* *NTAP_SNAPVAULT_NODELETE=N* *NTAP_NUM_VOL_CLONES=1* *NTAP_NFS_EXPORT_PERSISTENT=false* *PRE_APP_QUIESCE_CMD01=ssh infodba@172.17.44.40 ".*

Steps	Commands
	~/.kshrc;backup_modes -u=infodba -p=infodba -g=dba -m=rdonly" *POST_APP_UNQUIESCE_CMD01= ssh infodba@172.17.44.40 ". ~/.kshrc;backup_modes -u=infodba -p=infodba -g=dba -m=normal"* *APP_NAME=oracle* *ARCHIVE_LOG_RETENTION=* *ARCHIVE_LOG_DIR=* *ARCHIVE_LOG_EXT=* *ORACLE_DATABASES=s11tcur:oracle* *SQLPLUS_CMD=/plmtc/plmdb/oracle/product/11gr2/bin/sqlplus* *CNTL_FILE_BACKUP_DIR=/tmp/oracle* *ORA_TEMP=/tmp* *ORACLE_HOME=/plmtc/plmdb/oracle/product/11gr2* **Note:** Note: The IP address of CMODE_CLUSTER_USERS is the cluster admin logical interface (LIF), and the IP address of the NTAP_USERS is the logical interface of the management LIF created in Step 6. The username and password for NTAP_USERS is also the user and password created in Step 6. If you are not using the GUI use "./snapcreator --cryptpasswd <usernamer>" to encrypt the password for both "scuser" and "admin" user. If using the GUI, enter NTAP_USERS when asked for the controller login credentials; enter CMODE_CLUSTER_USERS when asked for the cluster credentials. The PRE_APP_QUIESCE_CMD01 and POST_APP_UNQUIESCE_CMD01 would ssh onto the FMS server to quiesce and unquiesce the Teamcenter FMS. The ".kshrc" file set up the environment variables and library paths such that the backup_modes utility can be executed. This .kshrc file contains exports for the Teamcenter installation directory: *export TC_ROOT=/plmtc/data/tc830* *export TC_DATA=/plmtc/data/s11tcur_tcdata* *. $TC_DATA/tc_profilevars*
9. Run snapcreator (this can be added to a cron job or done manually). From the /usr/local/scServer3.6.0 directory run:	`./snapcreator --profile TC2 --action snap --policy daily --verbose`

Sample Output of the `SnapCreator` Command in Step 8

```
# ./snapcreator --profile TC2 --action snap --policy daily --verbose

[Thu Mar  7 16:43:30 2013] INFO: Logfile timestamp: 20130307164330
[Thu Mar  7 16:43:30 2013] INFO: Plugin validation skipped for oracle, no
plugin parameters file found or no parameters set

########## Parsing Environment Parameters ##########

########## PRE APPLICATION QUIESCE COMMANDS ##########

########## Detecting Data OnTap mode for 172.31.8.200 ##########
[Thu Mar  7 16:43:30 2013] INFO: Data OnTap Cluster mode detected
[Thu Mar  7 16:43:30 2013] INFO: Running pre application quiesce command
PRE_APP_QUIESCE_CMD01 [ssh infodba@172.17.44.40 ". ~/.kshrc;backup_modes -
u=infodba -p=infodba -g=dba -m=rdonly"]
[Thu Mar  7 16:44:01 2013] INFO: Running pre application quiesce command [ssh
infodba@172.17.44.40 ". ~/.kshrc;backup_modes -u=infodba -p=infodba -g=dba -
m=rdonly"] finished successfully

########## PRE APPLICATION QUIESCE COMMANDS FINISHED SUCCESSFULLY ##########

########## Application quiesce ##########
[Thu Mar  7 16:44:01 2013] INFO: Quiescing databases
[Thu Mar  7 16:44:01 2013] INFO: Quiescing database s11tcur
[Thu Mar  7 16:44:09 2013] INFO: Quiescing database s11tcur finished
successfully
[Thu Mar  7 16:44:09 2013] INFO: Quiescing databases finished successfully

########## POST APPLICATION QUIESCE COMMANDS ##########
[Thu Mar  7 16:44:09 2013] INFO: No commands defined

########## POST APPLICATION QUIESCE COMMANDS FINISHED SUCCESSFULLY ##########

########## PRE COMMANDS ##########
[Thu Mar  7 16:44:09 2013] INFO: No commands defined

########## PRE COMMANDS FINISHED SUCCESSFULLY ##########

########## Detecting Data OnTap mode for 172.31.8.247 ##########
[Thu Mar  7 16:44:09 2013] INFO: Data OnTap Cluster mode detected

########## Detecting Data OnTap mode for 172.31.8.200 ##########
[Thu Mar  7 16:44:09 2013] INFO: Data OnTap Cluster mode detected
[Thu Mar  7 16:44:09 2013] INFO: Discover cmode cluster nodes on 172.31.8.200
[Thu Mar  7 16:44:09 2013] INFO: Discover cmode cluster nodes on 172.31.8.200
completed successfully

########## Generating Info ASUP on 172.31.8.247 ##########
[Thu Mar  7 16:44:10 2013] INFO: ASUP create on 172.31.8.200:fas3170c-svl09
finished successfully

########## Gathering Information for 172.31.8.247:apa ##########
[Thu Mar  7 16:44:10 2013] INFO: Performing Snapshot Inventory for apa on
172.31.8.247
```

```
[Thu Mar  7 16:44:10 2013] INFO: Snapshot Inventory of apa on 172.31.8.247
completed Successfully

########## Gathering Information for 172.31.8.247:plmdb2 ##########
[Thu Mar  7 16:44:10 2013] INFO: Performing Snapshot Inventory for plmdb2 on
172.31.8.247
[Thu Mar  7 16:44:10 2013] INFO: Snapshot Inventory of plmdb2 on 172.31.8.247
completed Successfully

########## Gathering Information for 172.31.8.247:plmtc_data ##########
[Thu Mar  7 16:44:10 2013] INFO: Performing Snapshot Inventory for plmtc_data
on 172.31.8.247
[Thu Mar  7 16:44:11 2013] INFO: Snapshot Inventory of plmtc_data on
172.31.8.247 completed Successfully

########## Running Snapshot Rename on Primary 172.31.8.247 ##########

########## Creating snapshot(s) ##########
[Thu Mar  7 16:44:11 2013] INFO: NetApp Snap Creator Framework 3.6.0 detected
that SnapDrive is not being used. File system consistency cannot be
guaranteed for SAN/iSAN environments

########## Taking Snapshot on Primary 172.31.8.247:apa ##########
[Thu Mar  7 16:44:11 2013] INFO: Creating Snapshot for apa on 172.31.8.247
[Thu Mar  7 16:44:13 2013] INFO: Snapshot Create of TC2-daily_20130307164330
on 172.31.8.247:apa Completed Successfully

########## Taking Snapshot on Primary 172.31.8.247:plmdb2 ##########
[Thu Mar  7 16:44:13 2013] INFO: Creating Snapshot for plmdb2 on 172.31.8.247
[Thu Mar  7 16:44:13 2013] INFO: Snapshot Create of TC2-daily_20130307164330
on 172.31.8.247:plmdb2 Completed Successfully

########## Taking Snapshot on Primary 172.31.8.247:plmtc_data ##########
[Thu Mar  7 16:44:13 2013] INFO: Creating Snapshot for plmtc_data on
172.31.8.247
[Thu Mar  7 16:44:14 2013] INFO: Snapshot Create of TC2-daily_20130307164330
on 172.31.8.247:plmtc_data Completed Successfully

########## PRE APPLICATION UNQUIESCE COMMANDS ##########
[Thu Mar  7 16:44:14 2013] INFO: No commands defined

########## PRE APPLICATION UNQUIESCE COMMANDS FINISHED SUCCESSFULLY
##########

########## Application unquiesce ##########
[Thu Mar  7 16:44:14 2013] INFO: Unquiescing databases
[Thu Mar  7 16:44:14 2013] INFO: Unquiescing database s11tcur
[Thu Mar  7 16:44:17 2013] INFO: Unquiescing database s11tcur finished
successfully
[Thu Mar  7 16:44:17 2013] INFO: Unquiescing databases finished successfully

########## POST APPLICATION UNQUIESCE COMMANDS ##########

########## Detecting Data OnTap mode for 172.31.8.200 ##########
[Thu Mar  7 16:44:17 2013] INFO: Data OnTap Cluster mode detected
```

```
[Thu Mar  7 16:44:17 2013] INFO: Running post application unquiesce command
POST_APP_UNQUIESCE_CMD01 [ssh infodba@172.17.44.40 ". ~/.kshrc;backup_modes -
u=infodba -p=infodba -g=dba -m=normal"]
[Thu Mar  7 16:44:46 2013] INFO: Running post application unquiesce command
[ssh infodba@172.17.44.40 ". ~/.kshrc;backup_modes -u=infodba -p=infodba -
g=dba -m=normal"] finished successfully

########## POST APPLICATION UNQUIESCE COMMANDS FINISHED SUCCESSFULLY
##########

########## Generating Info ASUP on 172.31.8.247 ##########
[Thu Mar  7 16:44:47 2013] INFO: ASUP create on 172.31.8.200:fas3170c-svl09
finished successfully

########## POST DATA TRANSFER COMMANDS ##########
[Thu Mar  7 16:44:47 2013] INFO: No commands defined

########## POST DATA TRANSFER COMMANDS FINISHED SUCCESSFULLY ##########

########## Running Snapshot Delete on Primary 172.31.8.247 ##########
[Thu Mar  7 16:45:02 2013] WARN: More than 7 snapshots exist (3) but they
could not be deleted because they are not older than the retention age (7
days) for 172.31.8.247:apa
[Thu Mar  7 16:45:02 2013] WARN: More than 7 snapshots exist (3) but they
could not be deleted because they are not older than the retention age (7
days) for 172.31.8.247:plmdb2
[Thu Mar  7 16:45:02 2013] WARN: More than 7 snapshots exist (3) but they
could not be deleted because they are not older than the retention age (7
days) for 172.31.8.247:plmtc_data

########## POST COMMANDS ##########
[Thu Mar  7 16:45:02 2013] INFO: No commands defined

########## POST COMMANDS FINISHED SUCCESSFULLY ##########

########## ARCHIVE COMMANDS ##########
[Thu Mar  7 16:45:02 2013] INFO: No commands defined

########## ARCHIVE COMMANDS FINISHED SUCCESSFULLY ##########

########## NetApp Snap Creator Framework 3.6.0 finished successfully
##########
[Thu Mar  7 16:45:02 2013] INFO: INFO: Snap Creator finished successfully (
Action: snap )
```

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

Go further, faster®

www.netapp.com