



Teradata® DSA

Quick Start Guide

Release 17.20

October 2021

Copyright and Trademarks

Copyright © 2018 - 2021 by Teradata. All Rights Reserved.

All copyrights and trademarks used in Teradata documentation are the property of their respective owners. For more information, see [Trademark Information](#).

Product Safety

Safety type	Description
	Indicates a situation which, if not avoided, could result in damage to property, such as to equipment or data, but not related to personal injury.
	Indicates a hazardous situation which, if not avoided, could result in minor or moderate personal injury.
	Indicates a hazardous situation which, if not avoided, could result in death or serious personal injury.

Third-Party Materials

Non-Teradata (i.e., third-party) sites, documents or communications ("Third-party Materials") may be accessed or accessible (e.g., linked or posted) in or in connection with a Teradata site, document or communication. Such Third-party Materials are provided for your convenience only and do not imply any endorsement of any third party by Teradata or any endorsement of Teradata by such third party. Teradata is not responsible for the accuracy of any content contained within such Third-party Materials, which are provided on an "AS IS" basis by Teradata. Such third party is solely and directly responsible for its sites, documents and communications and any harm they may cause you or others.

Warranty Disclaimer

Except as may be provided in a separate written agreement with Teradata or required by applicable law, the information available from the Teradata Documentation website or contained in Teradata information products is provided on an "as-is" basis, without warranty of any kind, either express or implied, including the implied warranties of merchantability, fitness for a particular purpose, or noninfringement.

The information available from the Teradata Documentation website or contained in Teradata information products may contain references or cross-references to features, functions, products, or services that are not announced or available in your country. Such references do not imply that Teradata Corporation intends to announce such features, functions, products, or services in your country. Please consult your local Teradata Corporation representative for those features, functions, products, or services available in your country.

The information available from the Teradata Documentation website or contained in Teradata information products may be changed or updated by Teradata at any time without notice. Teradata may also make changes in the products or services described in this information at any time without notice.

Machine-Assisted Translation

Certain materials on this website have been translated using machine-assisted translation software/tools. Machine-assisted translations of any materials into languages other than English are intended solely as a convenience to the non-English-reading users and are not legally binding. Anybody relying on such information does so at his or her own risk. No automated translation is perfect nor is it intended to replace human translators. Teradata does not make any promises, assurances, or guarantees as to the accuracy of the machine-assisted translations provided. Teradata accepts no responsibility and shall not be liable for any damage or issues that may result from using such translations. Users are reminded to use the English contents.

Feedback

To maintain the quality of our products and services, e-mail your comments on the accuracy, clarity, organization, and value of this document to: docs@teradata.com.

Any comments or materials (collectively referred to as "Feedback") sent to Teradata Corporation will be deemed nonconfidential. Without any payment or other obligation of any kind and without any restriction of any kind, Teradata and its affiliates are hereby free to (1) reproduce, distribute, provide access to, publish, transmit, publicly display, publicly perform, and create derivative works of, the Feedback, (2) use any ideas, concepts, know-how, and techniques contained in such Feedback for any purpose whatsoever, including developing, manufacturing, and marketing products and services incorporating the Feedback, and (3) authorize others to do any or all of the above.

Contents

Chapter 1: DSA Quick Start (Minimal Configuration)	4
Welcome to Teradata Vantage	4
Check If Data Mover Is Installed	4
Gather Information before You Begin	5
Downloading Software	6
Installing Teradata ActiveMQ	6
Installing the DSC Package	7
Installing the ClientHandler Package	9
Installing the BARCmdline Package	11
Installing the BARPortlets Package	12
Verifying Quick Start Installation	12
Adding Teradata System and Dictionary Collector to BAR Portlets	13
Enabling BAR Portlets	14
Enabling the DSC Server	14
Adding the Teradata System	15
Verifying the Media Server	17
Adding a Disk File System	17
Adding a Target Group	18
Creating and Running a Teradata Backup Job	19
Creating and Running a Teradata Restore Job	20

DSA Quick Start (Minimal Configuration)

Use this quick start to set up a simple disk file system configuration, do a full backup, and do a full restore. This gives you a quick way to evaluate basic product function and test simple backup and restore procedures.

Presumptions:

- Hardware is configured
- Teradata® NewSQL Engine / Teradata Database is installed and running
- Viewpoint is installed and running

If you are ready to install for other configurations, use these documents:

Use *Teradata® DSA - DSE for Veritas NetBackup Installation, Configuration, and Upgrade Guide*, B035-3151 or *Teradata® DSA - DSE for IBM Spectrum Protect Installation, Configuration, and Upgrade Guide*, B035-3155 to install the following:

- Veritas NetBackup
- Spectrum Protect
- AWS S3
- Azure Blob

Use *Teradata® DSA - DSU Installation, Configuration, and Upgrade Guide*, B035-3153 to install the following:

- Dell EMC Data Domain
- AWS S3
- Azure Blob

Welcome to Teradata Vantage

Teradata Vantage™ is our flagship analytic platform offering, which evolved from our industry-leading Teradata® Database. Until references in content are updated to reflect this change, the term Teradata Database is synonymous with Teradata Vantage.

Advanced SQL Engine is a core capability of Teradata Vantage, based on our best-in-class Teradata Database. Advanced SQL refers to the ability to run advanced analytic functions beyond that of standard SQL.

Check If Data Mover Is Installed

NOTICE

If Data Mover is installed you must be careful when installing DSA or you can break the Data Mover installation.

Data Mover 16.20 and higher comes with DSA pre-installed and only supports the version of DSA that is bundled with that specific release of Data Mover. You must understand if the DSA configuration will be sharing any components with Data Mover (for example, the DSC or DSA Network Client (ClientHandler)).

If you install a version of DSA different than the current Data Mover installation, you must arrange to upgrade Data Mover to match.

Logical netmask: If DSA Network Client (ClientHandler) is shared with Data Mover, the logical netmask must be configured to allow communication between the Data Mover source and target systems.

See *Teradata® Data Mover Installation, Configuration, and Upgrade Guide for Customers* for more information.

Gather Information before You Begin

Locate and record this information before beginning the installation.

Type of Information	Description	Record the Value for Your Environment
DSC server	Nickname for server. If you use the hostname, it must follow these guidelines: Maximum of 128 characters: alphanumeric, "-" and "." First character must be alphanumeric (a-z, A-Z, and 0-9) only.	
Using SSL or TCP? This is the type of ActiveMQ connection.	SSL connections encrypt passwords. TCP connections are open. Default: tcp.	
Is DSA REST https or http?	Default: https	
DSC repository DBS Superuser to create the DSC repository	Username: postgres Password	
BAR database	Username: bar Password	
Landing Zone	Filepath to temporary location for DSC backup before replication to storage. Default: /var/opt/teradata/dsa/postgres	

Downloading Software

Use these steps to download the latest versions of the packages, access modules, and the deployment scripts.

1. Go to <https://support.teradata.com>.
2. Log in.
3. Under **Downloads** select **Update Your Software**.
4. Select **Backup Archive Restore**.

Important:

If you do not see Backup Archive Restore, you need to log in.

5. Select **Data Stream Utility**.
6. Select the release information and click **Submit**.
7. Check the **Select All On This Page** box.
8. Deselect the TDVM package.
9. Select **Download All**.
10. Close the window about the download.
11. Select **Database and Applications**.
12. Select **Certification List**.
13. Select the following:

Option	Description
List Type	Current Certification
Node Type	TMS DSA DSC
Target OS	SLES11SP3 64bit SLES12SP3 64bit
Application Version	17.00
Teradata Release	As shown
Bus Type	As shown
Certification Date	As shown

14. Select **Submit**.
15. Locate and download `tdactivemq` and `teradata-jdk8`.

Installing Teradata ActiveMQ

Install Teradata ActiveMQ on the DSC server. If Teradata JDK is not installed on the DSC server, install it first.

1. Verify Teradata JDK 8.
 - a. Check if Teradata JDK 8 is installed:
`rpm -q teradata-jdk8`
 - b. If necessary, install Teradata JDK 8 by extracting then running the script:
`tar -zxvf teradata-jdk8__slesxx_arch.xx.xx.xx.xx-#####.tar.gz`
`rpm -ivh teradata-jdk8__xx.xx.xx.xx-#####-arch.rpm`
2. Install Teradata ActiveMQ.
`rpm -ivh tdactivemq__slesxx_arch.xx.xx.xx.xx.rpm`
3. [Required] Configure Teradata ActiveMQ with the DSAPostAMQ script to optimize memory utilization:
 - a. Extract the script:
`tar zxvf DSAPostAMQ_slesxx_arch.xx.xx.xx.xx-#####.tar.gz`
 - b. Run the script:
`./tdactivemq_wrapper.py`

Installing the DSC Package

Install the DSC package on the server you want to be the DSC server.

You cannot change the installation directory. The software is installed here:

`/opt/teradata/client/version/dsa`

1. On the DSC server, extract the script rpm file:
`tar zxvf DSC_slesxx_arch.xx.xx.xx.xx-#####.tar.gz`
 A directory with the format `DSC.xx.xx.xx.xx` is extracted in the current working directory.
2. Change to the `DSC.xx.xx.xx.xx` directory.
3. Run the installation script.
`./dscinstall.sh -r DSC-xx.xx.xx.xx-#####.arch.rpm`
4. Enter values for the DSC component.

DSC Prompts	Description and Default Values
Landing Zone	Filepath to temporary location for DSC backup before replication to storage. Default: <code>/var/opt/teradata/dsa/postgres</code>
Port for the DSARest web service	Port number for the DSAREST web service. Default: 9090
Scheme for the DSARest web service	Scheme for the DSAREST web service, http or https. Default: https

DSC Prompts	Description and Default Values
Keystore password for the DSARest web service	Prompt appears if REST is set to https. Keystore password for DSARest web service. Must be at least 6 characters. If using SSL for ActiveMQ Connection, this password must match the JMS SSL keystore password.
Username for account to run DSC	Username to set up a Linux account for running the DSC services. Default: dscuser
Userid (dscuser)	Userid of the dscuser. The userid must be the same across all DSA components and servers in the environment. For DSU when using NFS mounted storage targets, this ID must match the anonuid configured in the NFS server. Default: 600
Viewpoint URL	Hostname of the Viewpoint server. Used only for Viewpoint authentication.
Viewpoint port	Port number on the Viewpoint server. Default: 80 Used only for Viewpoint authentication.
Is CAM environment clustered	Specifies whether the CAM environment is clustered (two Viewpoint servers, primary or failover). Default: no
Primary URL CAM communication	Primary hostname or IP address for CAM communication, which enables alert messaging.
Failover CAM URL	If CAM environment is clustered, failover hostname or IP address for CAM communication.
CAM Communication port	Port number for CAM communication, which enables alert messaging. (61616 for tcp, 61617 for ssl). Default: 61616 [DSA 16.20.51 and later] CAM currently does not support SSL so the port must be 61616.
Password for DSC repository DBS Superuser	Password for the repository DBS superuser.
Password for BAR DBS User	Password for the BAR database user. Used for create, read, update, and delete operations on the BAR database, which contains information for operational jobs. Default: bar
Unique DSC Name	Nickname for this DSC. Used to differentiate this DSC from other DSCs in the portlets. Maximum of 128 characters: alphanumeric, "-" and "." First character must be alphanumeric (a-z, A-Z, and 0-9) only.
ActiveMQ Broker URL	Hostname or IP address of the machine running the ActiveMQ broker (where tdactivemq is installed), usually the DSC server.
ActiveMQ Broker Port	Port number on the server where the ActiveMQ broker is listening (61616 for tcp, 61617 for ssl). Default: 61616
Type of ActiveMQ Connection	Type of ActiveMQ connection (tcp or ssl). If tcp is chosen, the ActiveMQ connection is validated during install. If ssl is chosen, the ActiveMQ

DSC Prompts	Description and Default Values
	(jms ssl) password should match the DSA REST API https password. Default: tcp

- Log off and log back in to the DSC to set the Linux environment variables.
- If you have problems, run the configure script:
`dscConfigure.sh`

Postrequisite:

Go to [Installing the ClientHandler Package](#).

Installing the ClientHandler Package

Install the ClientHandler package on the DSC server.

You can specify the base directory (*base_dir*) for the ClientHandler installation. It is installed here:

base_dir/teradata/client/version/dsa

Note:

Do not use / or /usr as the installation directory. The permissions for the specified directory are modified so that the service user can access the directory.

- On the DSC server, verify that the DSC is up and running.
`/etc/init.d/dsc status`
- On the ClientHandler server, extract the script rpm file:
`tar zxvf ClientHandler_slesxx_arch.xx.xx.xx.xx-#####.tar.gz`
A directory with the format `ClientHandler.xx.xx.xx.xx` is extracted in the current working directory.
- Change to the `ClientHandler.xx.xx.xx.xx` directory.
- Run the installation script.
`./clienthandler_install.sh -r ClientHandler-xx.xx.xx.xx-#####.rpm`
- Enter values for ClientHandler.

ClientHandler Prompts	Description and Default Values
Enter the base directory	<i>base_dir/teradata/client/version/dsa</i>
ActiveMQ Broker Host Name and Port	Hostname or IP address of the machine running the ActiveMQ broker and port number on the server where the ActiveMQ broker is listening (61616 for tcp, 61617 for ssl). Default: 61616 Usually the DSC server, the format is: hostname:port, for example <code>dsc1:61616</code>

ClientHandler Prompts	Description and Default Values
	You can enter multiple hostnames and ports. Press Enter when done to continue.
ActiveMQ Connection	Type of ActiveMQ connection (tcp or ssl). If tcp is chosen, the ActiveMQ connection is validated during install. If ssl is chosen, the ActiveMQ (jms ssl) password should match the DSA REST API https password. Default: tcp
Filepath of SSL truststore	If you are using SSL, enter filepath of the SSL truststore file. Default: none
Filepath of SSL keystore	If you are using SSL, enter filepath of the SSL keystore file. Default: none
SSL Keystore Password	If you are using SSL, enter the value for the client's keystore password in clear text. Default: none If you set DSARest web services to https, the SSL Keystore password must match the DSARest keystore password.
Server ID	Unique Server ID for this ClientHandler. The hostname of the server is recommended. Default: hostname
Is Master Server?	Indicates whether this server is the CBB web service master server used in incremental job communication. Note: All media servers defined in the target group for a Changed Block Backup (CBB) restore job must have the same web service master server, or the restore job will fail.
CBB File Path	The web service master uses this path, which is a shared directory required for Change Block Backup (CBB) temporary file storage during restore operations. Default: /var/opt/teradata/dsa/cbb
Master Server's Hostname	The hostname of the CBB web service master server used in incremental job communication. This prompt appears only if you respond No to the "Is Master Server?" prompt.

6. Log off and log back in to the DSC to set the Linux environment variables.
7. Verify ClientHandler is running:
`/etc/init.d/clienthandler status`
8. If necessary, repeat these steps for each ClientHandler server.
9. If you have problems, run the configure script:
`clienthandlerConfigure.sh`

Postrequisite:

Go to [Installing the BARCmdline Package](#).

Installing the BARCmdline Package

Install the BARCmdline package (DSA command line interface) onto any server where you want to enter dsc commands.

You can specify the base directory (*base_dir*) for the BAR command line installation. It is installed here:

base_dir/teradata/client/version/dsa

Note:

Do not use / or /usr as the installation directory. The permissions for the specified directory are modified so that the service user can access the directory.

1. Check if Teradata JDK 8 is installed:

```
rpm -q teradata-jdk8
```
2. If necessary, install Teradata JDK 8.
 - a. Extract the script:

```
tar -zxvf teradata-jdk8__slesxx_arch.xx.xx.xx.xx-#####.tar.gz
```
 - b. Run the script:

```
rpm -ivh teradata-jdk8__xx.xx.xx.xx-#####-arch.rpm
```
3. On the DSC server, extract the script rpm file:

```
tar zxvf BARCmdline_slesxx_arch.xx.xx.xx.xx-#####.tar.gz
```

where *slesxx* is the OS, *arch* is the architecture, *xx.xx.xx.xx* is the version number, and *#####* is a unique number

A directory with the format *BARCmdline.xx.xx.xx.xx* is extracted in the current working directory.
4. Run the installation script from the extracted directory.

```
./barcmdline_install.sh -r BARCmdline-xx.xx.xx.xx-#####.arch.rpm
```
5. Enter values for the BAR command-line interface.

BAR Command-Line Prompts	Description and Default Values
Enter the base directory	<i>base_dir/teradata/client/version/dsa</i>
ActiveMQ Broker URL	Hostname or IP address of the machine running the ActiveMQ broker (where tdactivemq is installed), usually the DSC server.
ActiveMQ Broker Port	Port number on the server where the ActiveMQ broker is listening (61616 for tcp, 61617 for ssl). Default: 61616
ActiveMQ Connection	Type of ActiveMQ connection (tcp or ssl). If tcp is chosen, the ActiveMQ connection is validated during install. If ssl is chosen, the ActiveMQ (jms ssl) password should match the DSA REST API https password. Default: tcp
Java path	If this is a generic SLES installation, enter the path to Java. Default: none

BAR Command-Line Prompts	Description and Default Values
DSC Name	The DSC name that the BAR command-line interface connects to.

- Log off and log back in to the DSC to set the Linux environment variables.
- If you have problems, run the configure script:
`commandlineConfigure.sh`

Postrequisite:

Go to [Installing the BARPortlets Package](#).

Installing the BARPortlets Package

Prerequisite:

Install the DSC, ClientHandler, and BAR Command Line packages before installing this package.

You must install the BAR portlets (barportlets) on the Viewpoint server.

The package is installed here:

`/opt/teradata/viewpoint/portlets/barportlets`

- Extract the script rpm file:
`tar -xvf barportlets_xx.xx.xx.xx-1.noarch.tar.gz`
A directory with the format `barportlets.xx.xx.xx.xx` is extracted in the current working directory.
- Change to the `barportlets.xx.xx.xx.xx` directory.
- Run the installation script.
`rpm -i barportlets.xx.xx.xx.xx-1.noarch.rpm`
- [Optional] Verify the BAR portlets:
`rpm -qa |grep barportlets`
- Start Viewpoint.
`/etc/init.d/viewpoint restart`

Verifying Quick Start Installation

During DSA component installation, user accounts, initialization scripts, and environmental variables are created. You can verify proper installation by checking for these items.

- Verify that the ClientHandler service is running on all media servers:
`/etc/init.d/clienthandler status`

2. Verify installation:
rpm -q DSC ClientHandler BARCmdline
This command returns a list of installed packages.
3. Verify that the DSCUSER was created with the proper uid.
id -u dscuser



The response is positive and returns the uid configured during install time.
4. Log off and log back in to the DSC to set the Linux environment variables.
5. Run list_jobs to verify components.
dsc list_jobs
This command returns the following on a new installation:

```
no job is found
```
6. On the Viewpoint server, verify the BAR portlets:
rpm -qa |grep barportlets

Adding Teradata System and Dictionary Collector to BAR Portlets

You must add and enable a Teradata system in the **Monitored Systems** portlet to make it available in the **BAR Setup** portlet.

You must configure the systems, backup solutions, and target groups in the **BAR Setup** portlet to make them available in the **BAR Operations** portlet.

1. From the Teradata Viewpoint portal page, click .
2. Open the **Monitored Systems** portlet.
3. Click  next to **Systems**, and select **Add Teradata System**.
 - a. Enter the **System Nickname** of the Teradata system.
 - b. Enter the **TDPID**, formal name of the Teradata system.
 - c. Set the **Time Zone**.
 - d. Select the **Enable system** checkbox.
 - e. Enter **Login** credentials for a user that will log in from Viewpoint into the Teradata system to collect data.
Teradata recommends that you do not use dbcuser. During a full system restore, the system must be quiescent and dbcuser will automatically log in.
 - f. Click **Apply**.
4. Under **Systems**, select the newly enabled system.
5. Under **Setup**, select **Data Collectors**.
6. Under **Data Collectors**, select **Dictionary**.
7. Select the **Enable Dictionary Collector** checkbox.
8. [Optional] Set the **Sample Rate** to 300.




9. Click **Apply**.

Enabling BAR Portlets




If the BAR administrator does not have Viewpoint administrative privileges, the BAR portlets must be enabled from the **Roles Manager** and **Portlet Library** administrative portlets before accessing **BAR Setup** or adding **BAR Operations** to the Viewpoint portal page.

1. Enable **BAR Setup** and **BAR Operations** portlet access for the BAR Administrator role from **Roles Manager**.

The BAR administrator role can edit, run, or abort any BAR job, even if they do not own the job or are specifically granted permission in the job permissions. It is easier to grant permissions to roles than to each user separately.


- a. From the Teradata Viewpoint portal page, click .
- b. Select **Roles Manager**.
- c. Next to **Role** select **Administrator**.
- d. Select the **Portlets** tab.
- e. Under **Applications**, select  for the **BAR Operations** portlet to access the **Permissions** view. The  is on the right side of the screen. Widen your browser window if it does not appear.
- f. Select the permissions you want for this role.

Option	Description
Enable portlet settings	Allows role members to select default object types to display in the object browser of the BAR Operations portlet.
Share portlet	Allows users to share customized versions of the portlet with other users.
BAR Admin	Enables the BAR Setup portlet.

- g. Click **Apply**.
- h. Click **Close**.
2. Enable role access to the portlets from **Portlet Library**.
 - a. From the Teradata Viewpoint portal page, click .
 - b. Select **Portlet Library**.
 - c. Select the **Portlets** tab.
 - d. Under **Applications** select the **BAR Operations** checkbox.
 - e. Click **Apply**.
 - f. Click **Close**.
3. Add the **BAR Operations** portlet in Viewpoint portal page.
 - a. From your **Teradata Viewpoint** page, click  next to **Add Content**.
If  **Add Content** does not appear, make sure you are on your page and not the Dashboard.
 - b. Under **Applications** select **BAR Operations**, and then click **Add**.

Enabling the DSC Server

Use these instructions to enable the DSC server.

1. Open the **BAR Setup** portlet.
2. Click  next to **DSC Servers**.
3. Under **General System Details**, enter the broker information:

Option	Description
Broker IP/Host	Hostname or IP address of the machine running the ActiveMQ broker (where tdactivemq is installed), usually the DSC server.
Broker Port	Port number on the server where the ActiveMQ broker is listening (61616 for tcp, 61617 for ssl). Default: 61616
Broker Connectivity	Type of ActiveMQ connection (tcp or ssl). If tcp is chosen, the ActiveMQ connection is validated during install. If ssl is chosen, the ActiveMQ (jms ssl) password should match the DSA REST API https password. Default: tcp

4. Select **Enable DSC server**.
5. Select the DSC Server.
 - a. Click **Discover Servers**.
 - b. Select the **DSC Server Name** from the drop-down.

Troubleshooting:

If the DSC names are not populated in the menu, check the following:

- Verify that the Broker IP/Host is correct.
- Make sure ActiveMQ is running:

```
/etc/init.d/tdactivemq status
```

6. Click **Apply**.

Adding the Teradata System

Prerequisite:


Before you can work with the DSC in the BAR Setup portlet, you must add and enable the Teradata System and the Dictionary collector in the **Monitored Systems** portlet. Under **Setup** select **Data Collectors** and enable the **Dictionary** collector.

If you are upgrading to SQL Engine 16.20 or later or Teradata Database 16.0 or later, run DIPBAR on the Teradata system before this procedure.

Follow these steps to configure and enable the target database system.

Note:

- Nodes are configured through autodiscovery. You can view but not edit them.
- [DSA 17.02 and later] There is no longer a preconfigured backup system, you just need to enable the Teradata system.

1. Open the **BAR Setup** portlet.
2. Under **DSC Servers**, select your DSC server.
3. From the **Categories** list, select **Systems and Nodes**.
4. Add the target system:
 - a. Click  next to **Systems**.
 - b. Select **Add Teradata System**.
5. Under **Setup**, select **System Details** and enter the following:

Option	Description
System Name	<p>[Adding a new system] Choose the system from the drop-down list.</p> <p>Note: Make a system available from the Monitored Systems portlet.</p>
SSL Communication	<p>[Optional] Select the Enable SSL over JMS Communication checkbox to enable SSL communication.</p> <p>Note: You must add the TrustStore password created during SSL setup. You must stop and start DSMain in the database after enabling SSL communication.</p>
Default Stream Limits For Nodes	<p>Set the default limits for each node configured with the system.</p> <ul style="list-style-type: none"> • For each node: maximum number of concurrent streams allowed per node. For example, 5 times the number of AMPs on the node. • For each job on a node: maximum number of concurrent streams allowed for each job on the node. Cannot exceed the number of AMPs on the node. If you enter a higher number, it is reduced to the number of AMPs on the node.

6. Click **Apply** and enter the database credentials.
7. Under **Setup** select **Nodes** to view the details for the nodes on this system.
8. Restart DSMain on the destination system:
 - a. From the primary distribution node (usually Node 1), run `cnstern 6`.
 - b. Enter `start bardsmain -s -d dsc_name` (this stops DSMain on the destination system).

Note:

The `-d dsc_name` parameter applies to SQL Engine 16.20 or later / Teradata Database 16.10 or later.

- c. Enter `start bardsmain` (this starts DSMain).
- d. [SQL Engine 16.20 or later / Teradata Database 16.10 or later] Enter `start bardsmain -j` (this shows the status of the connections).

Note:

The system is automatically enabled.

Verifying the Media Server

Media server data is autopopulated. You can view and edit if necessary using the **BAR Setup** portlet.

1. Open the **BAR Setup** portlet.
2. Under **DSC Servers**, select your DSC server.
3. From the **Categories** list, select **Media Servers**.
4. For each media server, verify the following:


Option	Description
BAR NC Port	Verify that the number of the BAR network server matches the server port setting in the DSA client handler property file. Default port: 15401
IP Address	<p>This is the address of the media server. Do not use a link-local IPv6 address (begins with <code>fe80</code>).</p> <p>Additional addresses can be entered for network cards that are attached to the server. If there are multiple instances of DSA Network Client (ClientHandler), specify separate IP addresses. For example, configure the first media server configuration with the first IP address and the second media server configuration with the second IP address.</p> <p>Note: IP addresses are not validated. Teradata recommends verifying that you can ping from the media server to the database and from the database to the media server.</p>
Network Mask	Use the default network mask, populated by DSA, that is based on the data path between Teradata nodes and media servers.

Adding a Disk File System

When using a disk file system to back up and restore data, you must add and configure the disk file system using the **BAR Setup** portlet.

Note:

System names and open file limits are tied to media servers during the target group configuration.

1. Open the **BAR Setup** portlet.
2. Under **DSC Servers**, select your DSC server.
3. Under **Categories**, select **Backup Solutions**.
4. Under **Solutions**, select **Disk File System**.
5. Verify or add a disk file system:
 - a. [Optional] To add a disk file system, from the **Disk File System Details** screen, click .
 - b. Enter a **File system name** and path that meets the following criteria:
 - Entire file system path has necessary data write permissions by the DSCuser
 - Unique, fully qualified path name that begin with a forward slash, for example, /storage/mnt1/
 - Does not differ by case alone. For example, both /storage/mnt1/ and /storage/Mnt1/ cannot be configured.
 - Contains no spaces.
 - [Spectrum Protect] **File system name** must start with /Spectrum followed by the node name and management class for the node name; for example, /Spectrum/NodeName/ManagementClass

Note:



The disk file system filepath used by the replication target group cannot be used by the operational target group, and vice versa.

- c. Enter the maximum number of open files allowed.

Adding a Target Group



The data from Teradata systems is sent through media servers for backup by backup solutions. These relationships are defined in target groups, which you can create.

1. Open the **BAR Setup** portlet.
2. Under **DSC Servers**, select your DSC server.
3. From the **Categories** list, select **Target Groups**.
4. From the **Target Groups** list, select **Remote Groups** or **Replication Groups**.
5. Do one of the following:

Option	Description
Add	Click  next to Remote Groups/Replication Groups to add a remote group.
Copy	Click  next to the name of the group you want to copy. If you copy the target group, some items cannot be changed.

Remote Target Group

6. Enter a **Target Group Name** for the new target group.
You can use alphanumeric characters, dashes, dots, and underscores, but no spaces.
7. Select the **Enable target group** checkbox.
8. Select a **Solution Type**.
9. In the **Targets** and the **Remote Group Details** section, make selections for the Solution Type:
 - Disk File System: Select the **Bar Media Server**, the **Disk File System** and the **Open Files** limit.

Option	Description
Add	Click  to add; policies and devices, storage units and open files limit, or disk file systems and open files limit.
Remove	Click  to remove; policies and devices, storage units and open files limit, or disk file systems and open files limit.

10. Click **Apply**.

Replication Target Group

11. In the **Targets** and the **Replication Target Group Details** section, make selections for the Solution Type:
 - Disk File System: Select the **BAR Media Server**, the **Disk File System** and the **Open Files** limit.
12. Click **Apply**.

Creating and Running a Teradata Backup Job

Use these steps to create a standard CBB backup job.

Create the Job

1. Open the **BAR Operations** portlet.
2. Select **New Job**.
If the **New Job** window does not appear, select the **Saved Jobs** tab.
3. On the **New Job** screen:
 - a. Select **Backup** as the job type.
 - b. Click **OK**.
4. Under **New Backup Job**:
 - a. Enter a unique **Job Name**.
 - b. Select a **Source System**.
 - c. In **Enter System Credentials**, enter a user name and password for the system.
Account String information is not required.

Note:

The password is applied to all jobs associated with this system and user account.

- d. Select a **Target Group**.
- e. [Optional] Enter a job description.
5. Select the **Objects** tab.
6. Select the objects from the source system to backup.
7. Click **Save**.
The newly created backup job is listed in the **Saved Jobs** view.

Run the Job

8. Click ☐ next to a job.
9. Select **Run**.
10. Select **OK**.
11. Select the **Job Scope: Full**.
A newly created job only has Full as the available Job Scope. When you rerun an existing job, Delta and Cumulative are available.
12. Select **Run**.

Creating and Running a Teradata Restore Job

Use these steps to create a standard CBB restore job.

1. Open the **BAR Operations** portlet.
2. From the **Saved Jobs** view, do one of the following:

Option	Description
Create a new job	<ol style="list-style-type: none"> a. Click New Job. b. Select Restore as the job type and click OK.
Create a job from an existing job	<ol style="list-style-type: none"> a. Click <input type="checkbox"/> next to a backup job that has completed. b. Select Create Restore Job to create a restore job from the selected save set.

3. Under **New Restore Job** enter a unique **Job Name**.
4. Select the **Destination System** and enter the **Credentials** for it.

Note:

The password is applied to all jobs associated with this system and user account.

5. Select the **Target Group**.
6. [Optional] Add a job description.
7. Click **Save**.
8. To run the newly created restore job, in the **Saved Jobs** view:
 - a. Click ☐ next to a job.

- b. Select **Run**.