

Teradata® DSA - DSE for IBM Spectrum Protect

Installation, Configuration, and Upgrade Guide

Release 17.20




November 2022

Copyright and Trademarks

Copyright © 2013 - 2023 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
 NOTICE	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.
 CAUTION	Indicates a hazardous situation which, if not avoided, could result in minor or moderate personal injury.
 WARNING	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 laws, all designs, specifications, statements, information, recommendations and content (collectively, "content") available from the Teradata Documentation website or contained in Teradata information products is presented "as is" and without any express or implied warranties, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or noninfringement, which are hereby disclaimed. In no event shall Teradata corporation, its suppliers or partners be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of content, even if advised of the possibility of such damage.

The Content 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 Content 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 the Content at any time without notice.

The Content is subject to change without notice. Users are solely responsible for their application of the Content. The Content does not constitute the technical or other professional advice of Teradata, its suppliers or partners. Users should consult their own technical advisors before implementing any Content. Results may vary depending on factors not tested by Teradata.

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.

Confidential Information

Confidential Information means any and all confidential knowledge, data or information of Teradata, including, but not limited to, copyrights, patent rights, trade secret rights, trademark rights and all other intellectual property rights of any sort.

The Content available from the Teradata Documentation website or contained in Teradata information products may include Confidential Information and as such, the use of such Content is subject to the non-use and confidentiality obligations and protections of a non-disclosure agreement or other such agreements to protect Confidential Information that you have executed with Teradata.

Contents

Chapter 1: Overview	6
Welcome to Teradata DSA - DSE for IBM Spectrum Protect Installation, Configuration, and Upgrade Guide	6
Introduction to Data Stream Architecture	6
Spectrum Protect Implementation	8
Dependencies	9
Chapter 2: Configuring the Environment Before Installing	12
Synchronizing Time on the Servers	12
Adding the TDPID to the /etc/hosts File on each TPA Node	12
Chapter 3: Configuring Spectrum Protect before Installing DSE	13
Spectrum Protect Policy Objects	13
Spectrum Protect Client Node	13
Spectrum Protect Server Options	14
Chapter 4: Migrate the DSC from Analytics Database to Postgres	16
Preparing to Migrate the DSC	16
Migrating Repository Data from Analytics Database to Postgres on a Single System	16
Migrating Repository Data from Analytics Database to Postgres on Another System	18
Migrating Repository Data from Analytics Database to Postgres in the Cloud	20
Migrating Repository Data from Postgres to Postgres	22
Properties.xml File	23
dsainputs File	26
Chapter 5: Repo Migration from Postgres to Postgres Using PG_DUMP Utility	30
Generate dsa_inputs.yml on Old DSC	30
Postgres to Postgres Migration on New DSC	30
Sample dsa_inputs.yml	31
Chapter 6: Installing Software	33
Dependencies	33
DSA Package Names	34
IBM Spectrum Protect Software Installation Workflow	36
Installing Software with Scripts	36
Verifying Installation	50
Verifying Teradata Connection to the ActiveMQ Server	51
Chapter 7: Configuring DSE after Installation	52

Setting Up SSL or TCP for JMS Workflow	52
Multiple DSA Network Client (ClientHandler) Instances	56
Restarting DSA Services	57
Verifying Teradata Connection to the ActiveMQ Server	58
Chapter 8: Configuring Spectrum Protect for Teradata DSE	59
Running configTool.sh	59
Managing the Configuration Set for the Selected Node	60
Chapter 9: Configuring Portlet Software	61
Configuring Viewpoint and BAR Setup	61
Enabling BAR Portlets	61
Adding Teradata System and Dictionary Collector to BAR Portlets	62
Enabling or Adding a DSC Server	63
Adding or Editing a Teradata System	64
Verifying the Media Server	66
Configuring Network Fabric: Portlets	67
Configuring a Backup Solution	68
Adding or Copying a Target Group	72
Chapter 10: Upgrading Software	74
Backing Up DSC Repository and Configuration Before Upgrading	74
Upgrading DSA Software Using Scripts or rpm	75
Upgrading the Database to 16.0 or Later	76
Resolving Failed Upgrades	76
Appendix A: DSA Properties	77
Appendix B: Administrative Tasks	84
Appendix C: Troubleshooting	87
Appendix D: Using PUT for Install and Upgrade	89
Appendix E: Additional Information	99

Overview

Welcome to Teradata DSA - DSE for IBM Spectrum Protect Installation, Configuration, and Upgrade Guide

Using the Teradata DSA - DSE for IBM Spectrum Protect Installation, Configuration, and Upgrade Guide

Teradata® Data Stream Extensions (DSE) is one of the components of Data Stream Architecture (DSA). DSE adds support for third-party backup applications.

Why Would Use this Content?

This content explains how to work with DSE to use advanced enterprise backup tools, such as scheduling, retention policies, archiving and allows customers to backup up directly to tape.

How Do I Use this Content?

Use this content to learn how to configure, initiate, and monitor backup and restore jobs across various Teradata systems. DSE offers these backup targets:

- Disk file systems
- Veritas NetBackup
- IBM Spectrum Protect
- Amazon S3
- Azure Blob

How Do I Get Started?

Start with [IBM Spectrum Protect Software Installation Workflow](#) to learn how to install the following components:

- IBM Spectrum Protect Server (supplied by customer)
- Standalone DSC Server
- IBM Spectrum Client Servers (BAR Media Server)

Reference to Other Relevant Content

Refer to [Related Documentation](#) for more information on various DSA components' systems and configurations.

Introduction to Data Stream Architecture

Teradata® Data Stream Architecture (DSA) enables you to back up and restore Teradata system data. DSA is optimized for Teradata MPP Architecture. It integrates with the Teradata® Viewpoint portlets: BAR Setup and BAR Operations. The portlets provide user interfaces to Teradata DSA that are similar to other Teradata ecosystem components. This integration uses Viewpoint account management features and enhances usability. Teradata DSA also provides a command-line utility that you can use to configure, initiate, and monitor backup and restore jobs.

Data Stream Extensions and Data Stream Utility

Beginning with DSA 15.10, the product has been bundled into two components: Data Stream Extensions (DSE) and Data Stream Utility (DSU). Both components offer BAR portlet and command line functionality.

- DSE adds support for third-party backup applications. DSE offers advanced enterprise backup tools, such as scheduling, retention policies, archiving and allows customers to backup up directly to tape. DSE offers these backup targets:
 - Disk file systems
 - Veritas NetBackup
 - IBM Spectrum Protect
- DSU does not offer third-party backup application support. DSU is a solution offered for sites without a need for the extended footprint offered by Teradata DSE. DSU is also used for public cloud solutions. DSU offers these backup targets:
 - Disk file systems
 - Dell EMC Data Domain
 - Amazon S3
 - Azure Blob
 - Google Cloud

In a typical DSU use case, the DSA Network Client (ClientHandler) is installed on the Teradata nodes, the DSC server is provided in a VM format, and a simple NFS environment is set up for use as a storage location for the backup files. A managed storage server can also act as a host server to the NFS environment if needed. When a Data Domain unit is used, EMC Data Domain Boost for DSU (DD Boost) allows a direct connection to the unit without using a third-party backup application.

Note that DSA consumes a certain amount of memory on the Teradata nodes. The amount of consumption depends on factors such as the following:

- Number of objects in the job plan
- Configuration, including how many nodes and many streams
- Throughput

For an estimate you can use the following:

Fixed consumption	$2\text{MiB} + (\text{Number of streams per node} \times 4\text{MiB})$
-------------------	--

	Number of AMPs per node x 15MiB
Variable consumption	With 80K objects, consumes around 1-2GiB per node (not constant consumption): $20\text{MiB} + (\text{Number of objects} \times 400) + ((\text{Total number of streams} \times 400) \times 3)$ For example, with 80K objects, 4000 total streams ~60MiB

Server Functionality

Server functionality includes the following servers:

- DSC server, which controls all BAR operations and is a part of all configurations. A DSC server must have the Data Stream Controller (DSC) installed.

Teradata DSC can be installed on a physical server, AWS, Azure, Google Cloud, or a VM (Teradata DSC on VMware) and back up and restore data from and to the database on-premises, in AWS, Azure, Google Cloud, or VMware.

- Media server (physical or logical), which writes to the target storage device. A media server must have the DSA Network Client (ClientHandler) installed.

A machine in a DSA configuration can include different types of server functionality. For example, the managed storage server in a DSU configuration functions as disk storage, the DSC server, and a media server. In another configuration, the DSC server could be a standalone server.

Backup Solutions

DSA backup solutions can include any of the following:

- Dell EMC Data Domain
- Quantum Tape
- Disk file system
- Third-party backup application software, such as NetBackup or IBM Spectrum Protect
- Amazon S3
- Azure Blob
- Google Cloud Platform

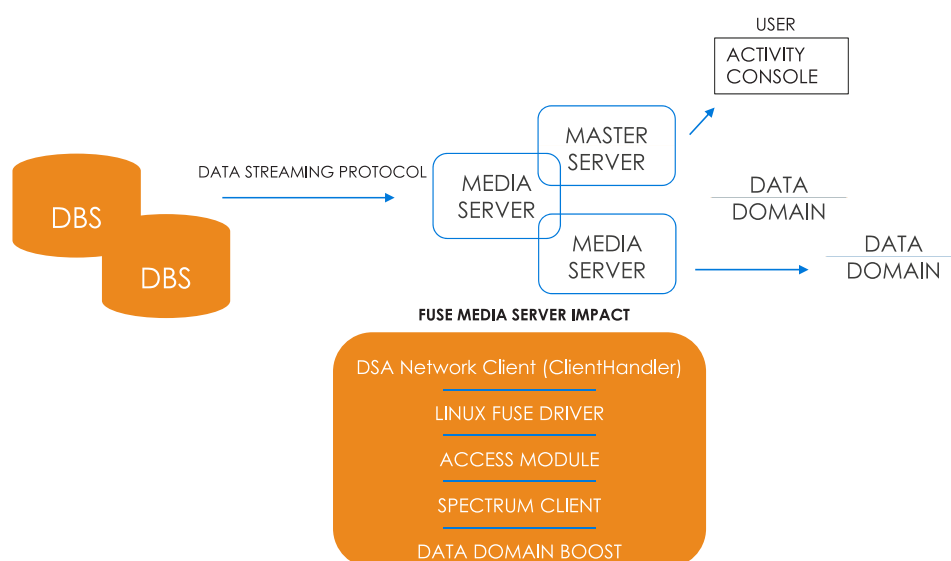
Spectrum Protect Implementation

In a DSE implementation for IBM Spectrum Protect, the following components are installed:

Server	Components Installed on Server
IBM Spectrum Protect Server (supplied by customer)	<ul style="list-style-type: none"> • SLES 12 SP3 • Spectrum Version 8.1.4
Standalone DSC Server	Teradata SLES 11 SP3

Server	Components Installed on Server
IBM Spectrum Client Servers (BAR Media Server)	<ul style="list-style-type: none"> • [BYNET support] Teradata supplied server (R720, R730, R740) with TDSTD Teradata Standard SLES 12 SP3 • [No BYNET] Generic SLES 12 SP3 on customer supplied hardware • DSA Network Client (ClientHandler) • Spectrum Protect backup-archive client 8.1.4 and Storage Agent 8.1.4 • DSE access module for Spectrum Protect (AXMSpectrum)

IBM Spectrum Protect – FUSE Approach



© 2018 Teradata

TERADATA

Dependencies

DSC Server Software Specifications

Software	Level
Operating system	<ul style="list-style-type: none"> • Teradata SUSE Linux Enterprise Server 12 SP3 • Teradata SUSE Linux Enterprise Server 11 SP3 <p>Note: This version is based on the original installation media and customized by Teradata OS Engineering for installation on Teradata Enterprise Data Warehouse systems.</p>

Software	Level
Postgres and Postgres Server rpm for the DSC repository (DSA 17.02.00.00 to <DSA 17.10.01)	SLES 11 SP3: 10.10-0.2.14 SLES 12 SP3: 10.10-1.15.1
Postgres and Postgres Server rpm for the DSC repository (DSA 17.10.01.00 to <DSA 17.20.00.00)	SLES 11 SP3: 10.15-4.9.1 SLES 12 SP3: 10.15-4.9.1
Postgres and Postgres Server rpm for the DSC repository (DSA 17.20.00.00 and later)	SLES 11 SP3 : 10.17-0.2.30 SLES 12 SP3 : 10.17-4.16.4
Postgres and Postgres Server rpm for the DSC repository (DSA 17.20.00.03 and later)	SLES 11 SP3 : 10.17-0.2.30 SLES 12 SP3 : 10.17-4.16.4 SLES 15 SP2 : 10.17-4.16.4
Postgres and Postgres Server rpm for the DSC repository (DSA 17.20.03.00 and later)	SLES 11 SP3 : 10.22-0.2.46 SLES 12 SP3 : 10.22-4.31.1 SLES 15 SP2 : 10.22-150100.8.50
Teradata JDK package	Install JDK on any server where BARCmdline is installed. Version11 (teradata-jdk11)
Teradata ActiveMQ	Version 5.17.2 (requires Teradata JDK Version 11)
DSAPostAMQ	Required to configure Teradata ActiveMQ

Note:

The Relay Services Gateway (RSG) virtual processor is required for DSA installation for both the TPA nodes and the DSC Server. Configure the RSG virtual processor for your installation, but do not install the RSG package.

Media Server Software Specifications

Software	Level
Operating system	<ul style="list-style-type: none"> SUSE Linux Enterprise Server 11 SP3 SUSE Linux Enterprise Server 12 SP3
Teradata JDK	Teradata JDK is required only if the DSA command line (BARCmdline) is installed on this server.

DSC Server Hardware Specifications

Option	Level
Dell 740xd	Conforms to current Teradata Managed Server for DSA with DSC specifications
Dell 730	Conforms to current Teradata Managed Server for DSA with DSC specifications

Option	Level
Dell 720	Conforms to current Teradata Managed Server for DSA with DSC specifications

Media Server Hardware Specifications

Option	Description
Dell 740xd	Conforms to current Teradata Managed Server for DSA Media Server specifications
Dell 730	Conforms to current Teradata Managed Server for DSA Media Server specifications
Dell 720	Conforms to current Teradata Managed Server for DSA Media Server specifications

Related Software Specifications

Software	Description
Teradata Viewpoint	Minimum version: <ul style="list-style-type: none"> • 16.50.01.00 • 16.20.23.05

Configuring the Environment Before Installing

Synchronizing Time on the Servers

The time must be synchronized between all servers in the DSA environment so that messages expired from the ActiveMQ server are not lost. The servers include:

- DSC server
- DSA media server
- Viewpoint server
- DBS node(s)

The servers should be set in the same time zone with `teradata-ntp` to achieve synchronization of timestamps.

Use this procedure for each server in the DSA environment.

1. Log on as root to the server.
2. Open and edit `/etc/ntp.conf`.
3. Add the following to the end of the file where *host* is the hostname of the time server:
`server host`
 For example:

```
server time00.teradata.com
```

4. To verify that the NTP service runs when the server starts up, type:
`chkconfig ntp on`
5. To restart the NTP service manually, type:
`/etc/init.d/ntp restart`

Adding the TDPID to the /etc/hosts File on each TPA Node

Add the Teradata system name to the `/etc/hosts` file on each TPA node. It must be added to the TPA node that hosts the master DSmain process (usually the highest numbered node, excluding hot standby nodes) plus all the other nodes to make sure that DSA still works when the highest numbered node is out of the configuration.

- On each TPA node, edit the `/etc/hosts` file:
`vi /etc/hosts`
 Change `127.0.0.1 localhost` to
`127.0.0.1 localhost TDPID`
 or
`127.0.0.1 localhost TDPIDcop1`

Configuring Spectrum Protect before Installing DSE

Important:

Configure Spectrum Protect before configuring Teradata DSE.

Log file text: The default size of the DSC server logfile is 2GB. When this limit is reached, the DSC server saves the existing log as logfile.prev, then creates a new logfile before writing more log entries. Do not set the value greater than 2GB. Doing so can cause the DSC server to become unresponsive.

Configure the Spectrum Protect components in the following order:

1. Spectrum Protect server
2. Spectrum Protect client
3. Spectrum Protect options

Spectrum Protect Policy Objects

Spectrum Protect policy objects manage how data is stored, where client data is stored, the number of maintained versions, and the length of time those versions are stored.

Spectrum Protect allows a variety of configurations using Spectrum Protect policy objects, but regardless of the configuration, Teradata DSE for Spectrum Protect requires a backup copy group policy object. The backup copy group policy object can be pre-existing or newly-created, but only Spectrum Protect backup object types are supported.

The following table lists Spectrum Protect policy object fields that control the removal of inactive objects from storage. Objects become inactive when a backup is performed with the same name as an object that is already stored on the server.

Field	Description	Default
Versions Data Deleted (VERDELETED)	Number of inactive versions, if active versions do not exist.	1
Versions Data Exist (VEREXISTS)	Number of inactive versions, if active versions exist.	1
Retain Extra Versions (RETEXTTRA)	Number of days to keep the last inactive versions, if active versions do not exist.	30
Retain Only Version (REONLY)	Number of days to keep the last inactive versions, if active versions do not exist.	

Spectrum Protect Client Node

In the Spectrum Protect software, by default, a client node can access only the backup storage objects that it creates. For instance, when a backup is performed on client node1, all DSE backups are registered in the Spectrum Protect server catalog as belonging to node1 and all other nodes are prevented from accessing the storage objects created by node1. However, it is possible to grant authorization for nodes to access other backups by creating a pseudo node that is used by all clients performing backups.

To create a pseudo node, use the Spectrum Protect register node command that provides the node name and password. Then set the BACKDELETE option to YES. If this option is not set to YES, backup objects cannot be deleted with the TDDSMC utility. For information about the Spectrum Protect register node command, refer to the *IBM Spectrum Protect for Windows: Administrator Reference*.

Spectrum Protect Server Options

If needed for your site, adjust the Spectrum Protect server option values for the Spectrum Protect server (`dsmserv.opt`) and the Spectrum Protect Storage Agent (`dsmsta.opt`). Use SETOPT on the Spectrum Protect server to set these global variables.

Spectrum Protect Server Option	Description
COMMTIMEOUT	<p>Specifies how long the server waits for an expected client message during an operation that causes a Spectrum Protect database update. If a message does not arrive before the specified wait period, the server ends the session with the client.</p> <p>To prevent clients from timing out while backing up large files or during a heavy network load, increase the time-out value.</p>
MAXNUMMP	<p>Setting in the DEFINE NODE and UPDATE NODE commands, determines the maximum number of mount points possible for this node.</p> <p>A mount point is a tape or a file device class volume. Parallel (concurrent) backup and restore operations that work with sequential file or tape storage pools require multiple mount points. The resource utilization client option governs the maximum number of concurrent backup or restore sessions that the client can use. The MAXNUMMP server parameter, on the UPDATE NODE or REGISTER NODE commands, and the MOUNTLIMIT setting in the DEFINE DEVCLASS and UPDATE DEVCLASS commands, determines how many mount points a client node can use, at one time.</p> <p>Configure these settings according to your requirements and available hardware. Take into account the number of mount points that all nodes might need, at any one time.</p> <p>For example, if you have four client nodes and only eight tape drives, if you configure all four nodes with MAXNUMMP 8, one node can seize all of the tape drives, leaving no tape drives for other nodes to use.</p>
MOUNTLIMIT	<p>Setting in the DEFINE DEVCLASS and UPDATE DEVCLASS commands, determines how many mount points a client can use at once.</p> <ul style="list-style-type: none"> Default: Set to DRIVES instead of a number. DRIVES specifies that when a mount point is allocated, the number of drives defined and online in the library is used to calculate the true value.

Spectrum Protect Server Option	Description
	<ul style="list-style-type: none"> EXTERNAL library types: Do not specify DRIVES. Specify the number of drives for the library as the MOUNTLIMIT value.
IDLETIMEOUT	<p>Specifies the amount of time, in minutes, that a client session can be idle before the server cancels the session.</p> <p>To prevent clients from timing out due to a heavy network load in the environment, increase the time-out value in the <code>dsmssta.opt</code> file for the storage server and SETOPT on the Spectrum server.</p> <p>Note:</p> <p>If the time-out value is increased, a large number of idle sessions could prevent other users from connecting to the server.</p>
RESOURCE TIMEOUT	<p>Specifies the maximum number of minutes that a storage agent waits for a resource on the server. Range is 1 to 60 minutes. SETOPT on the Spectrum server. Default: 60</p>
TXNGROUPMAX	<p>Indicates the maximum number of logical files (client files) that a client can send to the server in a single transaction. The server might create multiple aggregates for a single transaction, depending on the size of the transaction.</p> <p>The TXNGROUPMAX option controls the number of files allowed in a transaction. Although the maximum value allowed is 65000, Spectrum Protect limits the number of objects restored at the same time to 4080 objects. Set this option to 4080.</p>

Teradata Extension for Spectrum Protect maps DSE backup files to a series of smaller storage objects or files segments with an object size of 2 GB. Therefore, the maximum size of a single backup cannot exceed 4080 * 2 GB, or approximately 8.1 TB.

Migrate the DSC from Analytics Database to Postgres

Starting with DSA 17.02.00, the DSC repository runs on a Postgres database instead of Analytics Database.

- If you are doing a fresh install of DSA, see [Installing Software](#).
- If you are migrating an existing DSC, see [Preparing to Migrate the DSC](#).

Postgres is installed on the same machine as the DSC.

Preparing to Migrate the DSC

Before you migrate to DSA 17.02 or later (with Postgres) you must back up your current repository then upgrade your current DSA system to 16.20.54 or later. Back up the repository after each upgrade.

Back Up the Existing Repository

1. Run a repository backup on the current DSC. See [Backing Up DSC Repository and Configuration Before Upgrading](#).
2. If the DSC is not on 16.20.54 or later, upgrade the DSC. See [Installing Software with Scripts](#).
3. If you upgrade the DSC, run the repository backup again.

Locate this Information

4. See [Gather Information before You Begin](#) and collect this information.

Migrating Repository Data from Analytics Database to Postgres on a Single System

Follow these instructions to migrate the DSC to a Postgres repository on the same system.

Important:

- This process installs Teradata Parallel Transporter (TPT) and Postgres if they are not already installed.
If the TPT install fails, you must manually install it and if necessary, CLlV2.
 - If the DSC is currently on Teradata Database 15.10, both TPT and CLlV2 must be version 15.10.
 - If the DSC is currently on Analytics Database 16.20, both TPT and CLlV2 must be version 16.20.
- A folder, pgdata, is created during this process. Do not delete it or its content until the migration is successfully completed.

1. ssh to the DSC system and navigate to a folder where you have enough free space to export the BAR repository.
2. Download DSAMetaDataMigrator__sles11-12_x8664.17.xx.xx.xx-xxx.tar.gz from the Teradata Software server (<https://support.teradata.com>) and transfer to the DSC system.
3. Extract the content.
tar -xvzf DSAMetaDataMigrator__sles11-12_x8664.17.xx.xx.xx-xxx.tar.gz
4. Go to the extracted folder and run the following steps from there.
5. Install python3 and its dependency module.
installpython3.sh

6. Generate a property file using these commands:

- On SLES15 run python3 runAutoMigration.py - g
- On SLES12.3-TDC/STND run python3.6 runAutoMigration.py - g
- On SLES11.3 run ./runAutoMigration.py - g

This generates a properties.xml file prepopulated with values available from the DSC installation. Use this file as input for rest of the options.

7. Edit properties.xml to update it with credentials of DSC box, systems and media servers. More information about properties.xml (and a commented sample) can be found in [Properties.xml File](#).

8. Export the metadata:

- On SLES15 run python3 runAutoMigration.py - e
- On SLES12.3-TDC/STND run python3.6 runAutoMigration.py - e
- On SLES11.3 run ./runAutoMigration.py - e

The metadata from the Teradata repository is exported to a flat file in .csv format in a folder called pgdata.

9. Run ./dscinstall.sh -r DSC.17.xx.xx.xx-xxxxxx.rpm to upgrade the currently installed DSC version to new DSC version DSC 17.xx.00.00 having Postgres as the repository. Be sure to use the same credentials as are put in the properties file.

10. Verify DSC with REST API is running.
/etc/init.d/dsc status

Note:

If DSA >=17.20.04.00 then, run \$DSA_DSC_ROOT/postgres_access.sh -t disable

11. Import the metadata from the flat files to the new repository.

- On SLES15 run python3 runAutoMigration.py - i
- On SLES12.3-TDC/STND run python3.6 runAutoMigration.py - i
- On SLES11.3 run ./runAutoMigration.py - i

This imports the exported data from flat file to Postgres database. If not in silent mode, and any user data is present in the Postgres repo, user is asked if clean up can proceed.

12. [Optional] Validate the import process.

- On SLES15 run `python3 runAutomigration.py - v`
- On SLES12.3-TDC/STND run `python3.6 runAutomigration.py - v`
- On SLES11.3 run `./runAutoMigration.py - v`

This validates the export and import process by comparing the number of rows for each table in the Teradata repo and Postgres.

13. Reconfigure the new DSC.

- On SLES15 run `python3 runAutoMigration.py - r`
- On SLES12.3-TDC/STND run `python3.6 runAutoMigration.py - r`
- On SLES11.3 run `./runAutoMigration.py - r`

14. Download and upgrade the ClientHandler, Access Modules, and the BAR command line components (See [Installing Software with Scripts](#)). In case you have ClientHandler locally installed to new DSC, then make sure it's up and running.

Note:

If DSA >=17.20.04.00 then run, `$DSA_DSC_ROOT/postgres_access.sh -t disable`

Migrating Repository Data from Analytics Database to Postgres on Another System

In a multiple DSC environment, target groups must have different names on each DSC. For example, use `target_group_a` and `target_group_a1`.

Important:

- This process installs Teradata Parallel Transporter (TPT) and Postgres on the new system if they are not already installed.

If the TPT install fails, you must manually install it and if necessary, CLIV2.

- If the DSC is currently on Teradata Database 15.10, both TPT and CLIV2 must be version 15.10.
- If the DSC is currently on Teradata Database 16.20, both TPT and CLIV2 must be version 16.20.
- A folder, `pgdata`, is created during this process. Do not delete it or its content until the migration is successfully completed.

-
1. ssh to the new DSC system and navigate to a folder where you have enough free space to export the BAR repository.
 2. Download `DSAMetaDataMigrator__sles11-12_x8664.17.xx.xx.xx-xxx.tar.gz` from Teradata Software server and transfer to the DSC system.

3. Extract the content.

```
tar -xvzf DSAMetaDataMigrator__sles11-12_x8664.17.xx.xx.xx-xxx.tar.gz
```

4. Go to the extracted folder and run the subsequent steps from there.

5. Install python3 and its dependency module.

```
installpython3.sh
```

6. Generate a property file using these commands:

- On SLES15 run `python3 runAutoMigration.py - g`
- On SLES12.3-TDC/STND run `python3.6 runAutoMigration.py - g`
- On SLES11.3 run `./runAutoMigration.py - g`

This generates a `properties.xml` file prepopulated with values available from the DSC installation.

This step assumes it's being created on the source system so it can update the DSC server details. Use this file as input for rest of the options.

7. Edit `properties.xml` to update it with credentials of DSC boxes.

More information about `properties.xml` (and a commented sample) can be found in

[Properties.xml File](#).

8. Export the metadata:

- On SLES15 run `python3 runAutoMigration.py - e`
- On SLES12.3-TDC/STND run `python3.6 runAutoMigration.py - e`
- On SLES11.3 run `./runAutoMigration.py - e`

The metadata from the Teradata repository is exported to a flat file in `.csv` format in a folder called `pgdata`.

9. Run `./dscinstall.sh -r DSC.17.xx.xx.xx-xxxxxx.rpm` to install DSC 17.xx.00.00 on the new system with Postgres as the repository.

Be sure to use the same credentials as are put in the `properties` file.

Make sure DSC and REST service is up and running after installation. In case you have client handler locally installed to new DSC, then make sure it's up and running.

10. Verify DSC with REST API is running.

```
/etc/init.d/dsc status
```

Note:

If DSA >= 17.20.04.00 then, run `$DSA_DSC_ROOT/postgres_access.sh -t disable`

11. Import the metadata from the flat files to the new repository.

- On SLES15 run `python3 runAutoMigration.py - i`
- On SLES12.3-TDC/STND run `python3.6 runAutoMigration.py - i`
- On SLES11.3 run `./runAutoMigration.py - i`

This imports the exported data from flat file to Postgres database. If not in silent mode, and any user data is present in the Postgres repo, user is asked if clean up can proceed.

12. [Optional] Validate the import process.

- On SLES15 run `python3 runAutoMigration.py - v`
- On SLES12.3-TDC/STND run `python3.6 runAutoMigration.py - v`
- On SLES11.3 run `./runAutoMigration.py - v`

This validates the export and import process by comparing the number of rows for each table in the Teradata repo and Postgres.

13. [Optional] Reconfigure the new DSC.
 - a. Update the properties file with media servers and systems details.
 - On SLES15 run `python3 runAutoMigration.py - g`
 - On SLES12.3-TDC/STND run `python3.6 runAutoMigration.py - g`
 - On SLES11.3 run `./runAutoMigration.py - g`
 - b. Edit `properties.xml` with the credentials of the systems and media servers.
 - c. Run configuration.
 - On SLES15 run `python3 runAutoMigration.py - r`
 - On SLES12.3-TDC/STND run `python3.6 runAutoMigration.py - r`
 - On SLES11.3 run `./runAutoMigration.py - r`
14. Download and upgrade the ClientHandler, Access Modules, and the BAR command line components (See [Installing Software with Scripts](#)).

Note:

If DSA >=17.20.04.00 then, run `$DSA_DSC_ROOT/postgres_access.sh -t disable`

Migrating Repository Data from Analytics Database to Postgres in the Cloud

1. Using its public IP, ssh to the cloud VMs having DSC 17.xx. For example:
`ssh -i access_key.pem ec2-user@34.221.73.10`
2. Change to super user using command `sudo su -`.
3. Go to `/var/opt/teradata/dsu-migration/DSAMetaDataMigrator.17.xx.xx.xx/pkgs/`
4. Generate a property file using this command:
 - On SLES15 run `python3 runAutoMigration.py - g`
 - On SLES12.3-TDC/STND run `python3.6 runAutoMigration.py - g`
 - On SLES11.3 run `./runAutoMigration.py - g`

This generates a `properties.xml` file prepopulated with values available from the DSC installation. This step assumes it's being created on the source system so it can update the DSC server detail. This generated file can be used as input for rest of the other options.

5. Edit `properties.xml` to update it with credentials of DSC.

More information about `properties.xml` (and a commented sample) can be found in [Properties.xml File](#).

6. Export the metadata:

- On SLES15 run `python3 runAutoMigration.py - e`
- On SLES12.3-TDC/STND run `python3.6 runAutoMigration.py - e`
- On SLES11.3 run `./runAutoMigration.py - e`

The metadata from the Teradata repository is exported to a flat file in `.csv` format in a folder called `pgdata`.

7. Verify DSC with REST API is running.
`/etc/init.d/dsc status`

Note:

If DSA \geq 17.20.04.00 then, run `$DSA_DSC_ROOT/postgres_access.sh -t enable`

8. Import the metadata from the flat files to the new repository.

- On SLES15 run `python3 runAutoMigration.py - i`
- On SLES12.3-TDC/STND run `python3.6 runAutoMigration.py - i`
- On SLES11.3 run `./runAutoMigration.py - i`

This imports the exported data from flat file to Postgres database. If not in silent mode, and any user data is present in the Postgres repo, user is asked if clean up can proceed.

9. Validate the import process.

- On SLES15 run `python3 runAutoMigration.py - v`
- On SLES12.3-TDC/STND run `python3.6 runAutoMigration.py - v`
- On SLES11.3 run `./runAutoMigration.py - v`

This validates the export and import process by comparing the number of rows for each table in the Teradata repo and Postgres.

10. Reconfigure the new DSC.

a. Generate another property file using these commands:

- On SLES15 run `python3 runAutoMigration.py - g`
- On SLES12.3-TDC/STND run `python3.6 runAutoMigration.py - g`
- On SLES11.3 run `./runAutoMigration.py - g`

This generates a property file containing details for media servers and systems.

b. Edit `properties.xml` with credentials of media servers and systems.

c. Run the reconfiguration:

- On SLES15 run `python3 runAutoMigration.py - r`
- On SLES12.3-TDC/STND run `python3.6 runAutoMigration.py - r`
- On SLES11.3 run `./runAutoMigration.py - r`

Migrating Repository Data from Postgres to Postgres

1. Run a repository backup on DSC old source.
2. Restore repository on target or new DSC source.

Note:

When latest bootstrap file is available and can be copied to new DSC source, follow these steps.

- a. Create DFS/AWS/Azure/etc, Media Server and Replication target group on new DSC machine.
 - b. Copy the bootstrap_<backupID>.out in the landing zone from old DSC machine to the new DSC machine.
default is: /var/opt/teradata/dsa/postgres
 - c. Go to
/opt/teradata/client/17.20/dsa/dsc
 - d. User:
su dscuser
 - e. Restore the repository:
sh recover.sh -m recovery
 - f. Get <backupID> from replication target group.
h recover.sh -m replicate_from -v 1602081495349 -r file_replicating_tg
For example, h recover.sh -m replicate_from -v 1602081495349 -r file_replicating_tg
 - g. Check the replication status:
sh recover.sh -m save_sets_replication_status
 - h. Restore the backup:
sh recover.sh -m restore -v <backupID>
For example, sh recover.sh -m restore -v 1602081495349
 - i. Restart DSC after successful restore.
-

Note:

When latest bootstrap file is not available, follow these steps.

- a. Update Media Server on old DSC to communicate with New DSC as well.
Append new DSC ActiveMQ IP to broker.list in clienthandler.properties to point to new DSC.
- b. To configure with new DSC, restart media:
/etc/init.d/clienthandler restart-hwupgrade
- c. Configure backup solution (DFS/AWS/Azure/etc), Media and Target Group similar to old DSC for replication.
- d. Go to
/opt/teradata/client/17.20/dsa/dsc

- e. User:
 - `su dscuser`
 - f. To check the list of backup IDs available on replication target group:
 - `sh recover.sh -m list_backupids -r replicating_target_group`
 - g. Get <backupID> from replication target group.
 - `sh recover.sh -m replicate_from -v <backupID> -r <replicationTargetGroupName>`
 - For example, `sh recover.sh -m replicate_from -v 1603437512425 -r gcp_tg`
 - h. Restore the backup.
 - `sh recover.sh -m restore -v <backupID>`
 - For example, `sh recover.sh -m restore -v 1603437512425`
 - i. Restart DSC after successful restore.
3. Modify DSC name on new DSC.
 - a. Go to
 - `/opt/teradata/client/17.xx/dsa/dsc`
 - b. To modify the DSC name, run the command:
 - `./modify_dsc_name.sh`
 4. Reconfigure systems and media on new DSC.
 - a. Download
 - `DSAMetaDataMigrator__sles11-12-15_x8664.17.20.xx.xx-xxx.tar.gz`
 - b. To extract the content:
 - `tar -xvzf DSAMetaDataMigrator__sles11-12-15_x8664.17.20.xx.xx-xxx.tar.gz`
 - c. Go to the extracted folder.

Important:

Perform the following steps in this extracted folder.

- d. To install python3 and its dependency module:
 - `./installpython3.sh`
- e. To generate properties.xml run the command:
 - `./runPostgres2PostgresMigration.py -g`
- f. Modify properties.xml (generated in the previous step) with new DSC Systems and Media Server login credentials.
- g. Run the command to reconfigure DSC. This script re-configures the connected Systems and Media Servers with new DSC.
 - `./runPostgres2PostgresMigration.py -r`
- h. The properties.xml file will be removed on successful reconfigure.

Properties.xml File

The `properties.xml` file contains input parameters for the `DSAMetaDataMigrator` application. It includes credentials and associated information for DSC, systems and media servers in XML format. A template file is generated using the application.

- Generate the template `properties.xml` file using the following commands. The file is created in the current directory.
 - On SLES15 run `python3 runAutoMigration.py - g`
 - On SLES12.3-TDC/STND run `python3.6 runAutoMigration.py - g`
 - On SLES11.3 run `./runAutoMigration.py - g`
- The generated file includes all the information available in system as part of DSC installation.
- You must fill in the missing information before using the input file.
- If passwords are not in the file, the system prompts for the credentials while running the app.
- To avoid prompts during execution, you can set `<silentmode>` to yes and you must record passwords in the file.
- Media server and system detail can be updated for this file after export operation on the target or new DSC system.
- Cloud platform:
 - To ssh to the DSC VM using a `.pem` file, you must provide the path of the `.pem` file in the `<private_key_file>` tag and the user name in the `<private_username>` tag.
 - Without a `.pem` file, you can ssh and enter user name and password.
 - When using `.pem` file for cloud, do not enter values for `<systemusername>` and `<systemuserpass>` in the `properties.xml` file, they will override the values in the `.pem` file.

Sample properties.xml File

```
<data>
<!-- This properties.xml is the input file having parameters required
during migration
    Credential provided in this file is not encrypted
    Migrator application delete this file after successful migration
    In case of failure or partial migration, file remain present so user
should delete
    when not in use -->

<!-- provide path of the pem file along with user name for authentication on
cloud platform-->

<!--
<private_key_file>/var/opt/teradata/scripts/access_key.pem</private_key_file>
<private_username>ec2-user</private_username>
```



```

-->

<!-- set silent mode YES in case don't want to get prompt during migration
process -->
<silentmode></silentmode>

<!-- provide old DSC detail -->
<olddscserver>
  <systemname></systemname> <!-- system name -->
  <tdrepohost></tdrepohost> <!-- host of the Teradata repo, default is DSC
system -->
  <tdrepodbname></tdrepodbname> <!-- name of the Teradata repo DB, default is
bar (please do not edit) -->
  <tdrepodbpas></tdrepodbpas> <!-- Teradata repo (bar) DB password (should not
include space, single or double quotes) -->
  <brokerurl></brokerurl> <!-- broker URL of the old DSC -->
  <systemusername></systemusername> <!-- user name of the old DSC system -->
  <systemuserpass></systemuserpass> <!-- password of the old DSC system (should
not include space, single or double quotes) -->
</olddscserver>

<!-- provide new DSC detail -->
<dscserver>
  <dsaresthost></dsaresthost> <!-- system name hosting dsarest, default is DSC
server -->
  <dsarestport></dsarestport> <!-- port of the dsa rest server -->
  <dsarestwebservice></dsarestwebservice> <!-- dsa rest web service, it can be
https or http -->
  <brokerurl></brokerurl> <!-- broker URL of the new DSC -->
  <brokerport></brokerport> <!-- broker port of the new DSC -->
  <pgrepohost></pgrepohost> <!-- host of the Postgres repo, default is DSC
system -->
  <pgrepodbname></pgrepodbname> <!-- name of the Postgres repo DB, default is
bar (please do not edit) -->
  <pgrepodbpas></pgrepodbpas> <!-- Postgres repo (bar) DB password (should not
include space, single or double quotes) -->
</dscserver>

<!-- provide list of media servers to be reconfigured -->
<mediaservers>
  <mediaserver>
    <mediaservername></mediaservername> <!-- name of the media server -->
    <username></username> <!-- user name for the media server -->
    <password></password> <!-- password of the media server (should not include

```

```

space, single or double quotes) -->
  </mediaserver>
</mediaservers>

<!-- provide list of systems to be reconfigured -->
<systems>
  <system>
    <systemname></systemname> <!-- system name -->
    <db_username></db_username> <!-- database user name -->
    <db_password></db_password> <!-- database password (should not include
space, single or double quotes) -->
    <system_username></system_username> <!-- user name of the system (master
node) -->
    <system_password></system_password> <!-- password of the system (master
node) -->
  </system>
</systems>
</data>

```

dsainputs File

Use the existing dsainputs file in the /tmp location to edit the new dsainputs_template file that you just downloaded. Save the new file as dsainputs in the /tmp location.

Parameter	Component	Description
BROKERLIST	ClientHandler	List of broker:port pairs separated by a comma. For example: dsasrv1:61616
BURL	DSC, ClientHandler, BAR Command Line	Hostname or IP address of the machine running the JMS broker (ActiveMQ). Hostname or IP address of the machine running the ActiveMQ broker (where tdactivemq is installed), usually the DSC server.
BPORT	DSC, ClientHandler, BAR Command Line	Port number on the server where the ActiveMQ broker is listening (61616 for tcp, 61617 for ssl). Default: 61616
LANDINGZONE	DSC	/var/opt/teradata/dsa/postgres Default location for DSC repository backup files. Temporary location before replication to the target group.
CONNECTION	DSC, ClientHandler, BAR Command Line, BARPortlets	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
DSCNAME	DSC, BAR Command Line	Unique name for the DSC server. Maximum of 128 characters: alphanumeric, "-", and ".". The first character of the name can be alphanumeric (a-z, A-Z, and 0-9) only.

4: Migrate the DSC from Analytics Database to Postgres

Parameter	Component	Description
		Important: DSCNAME must be specified for an upgrade or the repository restore from the previous version will fail. Analyze_read jobs may also fail.
CBBFILEPATH	ClientHandler	The path needed for Change Block Backup temporary file storage: /var/opt/teradata/dsa/cbb
POSTGRESSPASSWORD	DSC	Password for Postgres user. No space, ', or " allowed.
BACKUPAPPCLIENTNAME	AXMNetbackup	The name of this media server. In NetBackup, this is the client name.
ISMASTER	ClientHandler	Specify yes or no on whether this server is the Web Service master server used in incremental job communication.
MASTERHOSTNAME	ClientHandler	Specify the host name of the Web Service master server used in incremental job communication.
VIEWPOINTURL	DSC	Hostname or IP address of the Viewpoint server.
VIEWPOINTPORT	DSC	Port number of the Viewpoint server.
CAMPRIMARYURL	DSC	Hostname or IP address of primary CAM system, which enables alert messaging
CAMPRIMARYPORT	DSC	CAM port number of primary CAM system. Default: 61616. [DSA 16.20.51 and later] CAM does not support SSL in this version. Port must be 61616.
CAMCLUSTERENABLED	DSC	Flag for enabling CAM clustering
CAMCLUSTERURL	DSC	Hostname or IP address of primary and failover CAM systems, which enable alert messaging
CAMCLUSTERPORT	DSC	CAM port number for clustered environment. This has the same value as CAMPRIMARYPORT. Default: 61616. [DSA 16.20.51 and later] CAM does not support SSL in this version. Port must be 61616.
DSARESTPORT	DSC	Port number for DSARest Web Service running on DSC server. Default: 9090.
DSARESTSHEME	DSC	DSARest Web Service scheme, http or https. Default: https.
KEYSTOREPASS	DSC	Required if DSARESTSHEME is https. Password for keystore. Minimum of 6 characters. No space, ', or " allowed. If JMS SSL is enabled, this password must match SSLKEYSTOREPASSWORD.
BARPASSWORD	DSC	Password for the BAR user. Used for Create, Read, Update and Delete (CRUD) operations on BAR. No space, ', or " allowed.

4: Migrate the DSC from Analytics Database to Postgres

Parameter	Component	Description
SERVERID	ClientHandler	The server ID is the name of a DSA media server, and is a unique logical name across a single DSA domain. It is defined using SQL 92 syntax and used as the selector for JMS message headers. If the ClientHandler package is installed on a TPA node, the server ID cannot be equal to the name of that system. It is not the ID for NetBackup or other third party servers. Note: When upgrading a media server for multiple DSA Network Client (ClientHandler) instances, specify the server IDs in a comma-separated list, for example, server1, server2.
SERVERPORT	ClientHandler	Port number for datapath traffic, corresponds to the server.port property in clienthandler.properties. Default: 15401.
SSLTRUSTSTOREFILE	ClientHandler	Full file path for truststore file.
SSLKEYSTOREFILE	ClientHandler	Full file path for keystore file.
SSLKEYSTOREPASSWORD	ClientHandler	The value for the JMS SSL keystore password, in clear text. If DSARESTSCHEME is set to https, this value must match KEYSTOREPASS.
SSELENCKEYSTOREPASSWORD	ClientHandler	The value for the JMS SSL keystore password, in clear text. If DSARESTSCHEME is set to https, this value must match KEYSTOREPASS.
WSPORT	ClientHandler	Port number for ClientHandler Web Service traffic, corresponds to the WebService.port property in clienthandler.properties. Default: 15402.

The following is an example of a DSC server dsainputs file:

Important:

DSCNAME must be specified for an upgrade or the repository restore from the previous version will fail. Analyze_read jobs may also fail.

```
# DSC, Clienthandler, and BARCmdline AMQ Broker connection type ssl or tcp
CONNECTION=tcp

# DSC and BARCmdline shared fields
DSCNAME=
BURL=
BPORT=61616

# DSC dsainputs fields
POSTGRESPASSWORD=
BARPASSWORD=
```

```

KEYSTOREPASS=
DSARESTPORT=9090
DSARESTSHEME=https
LANDINGZONE=/var/opt/teradata/dsa/postgres
VIEWPOINTURL=viewpointurl
VIEWPOINTPORT=80
VIEWPOINTTYPE=http
CAMCLUSTERENABLED=no
CAMPRIMARYURL=viewpointurl
CAMPRIMARYPORT=61616
CAMCLUSTERURL=camurl
CAMCLUSTERPORT=61616

#BARCmdline only dsainputs
BARCMDLINE_JAVA_HOME=

# Clienthandler dsainputs fields
BROKERLIST=
SERVERID=
SSLTRUSTSTOREFILE=/etc/opt/teradata/dsa/client.pem
SSLKEYSTOREFILE=/etc/opt/teradata/dsa/client-keystore.pem
SSLKEYSTOREPASSWORD=
SSLENCKEYSTOREPASSWORD=
ISMASTER=
MASTERHOSTNAME=
CBBFILEPATH=/var/opt/teradata/dsa/cbb
SERVERPORT=15401

# AXMNetbackup dsainputs fields
BACKUPAPPCLIENTNAME=

```

Repo Migration from Postgres to Postgres Using PG_DUMP Utility

DSA 17.20.01.00 supports DSC repository migration from postgres to postgres using PG_DUMP utility. You can perform the these tasks:

1. Generate `dsa_inputs.yml` on old DSC, see [Generate dsa_inputs.yml on Old DSC](#)
2. Run postgres repo migration on new DSC, see [Postgres to Postgres Migration on New DSC](#)

Generate dsa_inputs.yml on Old DSC

1. SSH logon to old DSC machine (if needed, switch to admin user using `sudo -su`).
2. Download and extract **DSAMetadataMigrator** 17.20.01.00 or later.
3. Run `./installPython3.sh` to install PyYAML.
4. If new DSC is 17.20.03.00 or later then set `$DSA_DSC_JSK_HOME` using `export $DSA_DSC_JDK_HOME in /etc/bash.bashrc`
5. If SLES15, use `python3 generateYml.py -all/-online`.
6. If SLES11 and SLES12, use `./generateYml.py -all/-online`.

Postgres to Postgres Migration on New DSC

1. Download and extract **DSAMetadataMigrator**-17.20.01.00 or later.
2. Prepare or use previous `dsa_inputs.yml` generated using `./generateYml.py`.
3. Only one Media_Server per Teradata MPP system is allowed when `isMPP : true`. It internally uses PCL tool to communicate with all other media_servers on Teradata MPP system.
4. Run the following:
 - On SLES15 run `python3 runAutoMigration.py - f`
 - On SLES12.3-TDC/STND run `python3.6 runAutoMigration.py - f`
 - On SLES11.3 run `./runAutoMigration.py - f`

This script performs the following tasks:

- SSH logon to old DSC and read the POSTGRES password from `jdbc.properties`.
- Use PG_DUMP to read old DSC repo data and store it in *LandingZone* at new DSC.
- Run restore with `recover.sh` utility into local new DSC Repo.
- Validate with ROW count between old and new DSC.
- Run upgrade scripts (change log) based on old DSC version.
- If needed, update or modify DSC name.
- Reconfigure only components given `dsa_inputs.yml`.
- Compare `list_consumers` and `list_components` on old and new DSC.

- Provide appropriate message or action or exit code.
 - **EXIT 0** (Migration completed successfully).
 - **EXIT 1** (Migration completed with warnings. Needs changes or executions).
 - **EXIT 2** (Migration failed).

Sample dsa_inputs.yml

```
olddsc:
  -name:
    system_username:
    system_password:
    private_key_file:

silent_mode : yes/no

tdsystems:
  - name: tdprod1
    db_user_name:
    db_password:
    system_username:
    system_password:
    private_key_file:

  - name: tdprod2
    db_user_name:
    db_password:
    system_username:
    system_password:
    private_key_file: /* password will be ignored if key is provided */

mediaservers:
  - name: database001_media
    public_ips : /* Optional only when configured IPs not reachable */
    isMPP : true /* true if media servers are on TD MPP nodes */
    system_username:
    system_password:
    private_key_file: /* password will be ignored if key is provided */

  - name: proddatabase001_media
    public_ip : /* Optional only when configured IPs not reachable */
    isMPP : false /* true if media servers are on TD MPP nodes */
    system_username:
    system_password:
```

```
private_key_file: /* password will be ignored if key is provided */  
  
- name: qadatabase001_media  
  system_username:  
  private_key_file: /* password will be ignored if key is provided */
```


Installing Software

Dependencies

DSC Server Software Specifications

Software	Level
Operating system	<ul style="list-style-type: none"> Teradata SUSE Linux Enterprise Server 12 SP3 Teradata SUSE Linux Enterprise Server 11 SP3 <p>Note: This version is based on the original installation media and customized by Teradata OS Engineering for installation on Teradata Enterprise Data Warehouse systems.</p>
Postgres and Postgres Server rpm for the DSC repository (DSA 17.02.00.00 to <DSA 17.10.01)	SLES 11 SP3: 10.10-0.2.14 SLES 12 SP3: 10.10-1.15.1
Postgres and Postgres Server rpm for the DSC repository (DSA 17.10.01.00 to <DSA 17.20.00.00)	SLES 11 SP3: 10.15-4.9.1 SLES 12 SP3: 10.15-4.9.1
Postgres and Postgres Server rpm for the DSC repository (DSA 17.20.00.00 and later)	SLES 11 SP3 : 10.17-0.2.30 SLES 12 SP3 : 10.17-4.16.4
Postgres and Postgres Server rpm for the DSC repository (DSA 17.20.00.03 and later)	SLES 11 SP3 : 10.17-0.2.30 SLES 12 SP3 : 10.17-4.16.4 SLES 15 SP2 : 10.17-4.16.4
Postgres and Postgres Server rpm for the DSC repository (DSA 17.20.03.00 and later)	SLES 11 SP3 : 10.22-0.2.46 SLES 12 SP3 : 10.22-4.31.1 SLES 15 SP2 : 10.22-150100.8.50
Teradata JDK package	Install JDK on any server where BARCmdline is installed. Version11 (teradata-jdk11)
Teradata ActiveMQ	Version 5.17.2 (requires Teradata JDK Version 11)
DSAPostAMQ	Required to configure Teradata ActiveMQ

Note:

The Relay Services Gateway (RSG) virtual processor is required for DSA installation for both the TPA nodes and the DSC Server. Configure the RSG virtual processor for your installation, but do not install the RSG package.

Media Server Software Specifications

Software	Level
Operating system	<ul style="list-style-type: none"> SUSE Linux Enterprise Server 11 SP3 SUSE Linux Enterprise Server 12 SP3
Teradata JDK	Teradata JDK is required only if the DSA command line (BARCmdline) is installed on this server.

DSC Server Hardware Specifications

Option	Level
Dell 740xd	Conforms to current Teradata Managed Server for DSA with DSC specifications
Dell 730	Conforms to current Teradata Managed Server for DSA with DSC specifications
Dell 720	Conforms to current Teradata Managed Server for DSA with DSC specifications

Media Server Hardware Specifications

Option	Description
Dell 740xd	Conforms to current Teradata Managed Server for DSA Media Server specifications
Dell 730	Conforms to current Teradata Managed Server for DSA Media Server specifications
Dell 720	Conforms to current Teradata Managed Server for DSA Media Server specifications

Related Software Specifications

Software	Description
Teradata Viewpoint	Minimum version: <ul style="list-style-type: none"> 16.50.01.00 16.20.23.05

DSA Package Names

The following table lists the software packages and dependencies for each DSA component, plus a summary of component functionality.



NOTICE

DSC, DSAPostAMQ, ClientHandler, BARCmdline, and BARPortlets must be on the same version.

Software Package Name	Dependencies	Description
DSC-version	[DSA 17.20.03.xx and later] Teradata-Jdk11 [DSA 17.20.02.xx and earlier till DSA 16.20.24.xx] Teradata-Jdk8 [DSA 16.20.23.xx and earlier] TeradataJdk7	The Data Stream Controller (DSC) controls BAR operations and allows communication between DSMain, the BAR portlets, and the DSA Network Client (ClientHandler). All installations require Version 7. From DSA 16.20.24 till DSA 17.20.02.XX versions require Version 8. DSA 17.20.03.00 and later versions require Version 11.
ClientHandler-version	None	ClientHandler is the base package for both DSU and DSE, and handles communication to the targets of backup and restore jobs that are remote from the Analytics Database / Teradata Database nodes. ClientHandler is also known as DSA Network Client or DSA NC.
BARCmdline-version	None	The DSA command-line interface provides an alternative to the BAR portlets, allowing job creation, launch, monitoring, and scheduling and providing commands to configure DSA.
BARPortlets-version	Viewpoint software	The BAR Setup portlet allows you to designate the hardware and software to use when backing up your Teradata system. The BAR Operations portlet allows you to create, manage, and submit jobs.
AXMNetbackup-version	ClientHandler	AXMNetbackup is an access module you can install for NetBackup targets.
AXMSpectrum-version	ClientHandler	AXMSpectrum is an access module you can install for Spectrum Protect targets.
AXMS3-version	ClientHandler	AXMS3 is an access module you can install for Amazon S3 targets.
AXMAzure-version	ClientHandler	AXMAzure is an access module you can install for Microsoft Azure targets.
AXMGCP-version	ClientHandler	AXMGCP is an access module you can install for Google Cloud Platform targets.
DSAPostDeployer-version	None	Contains a script, <code>modify_dsc_name.sh</code> , and a jar file, <code>dsa-post-deployer.jar</code> . These are used to update the DSC name in the repository.
DSAPostAMQ-version	tdactivemq 5.17.2.0-1	Contains one script, <code>tdactivemq_wrapper.py</code> . This required script configures <code>tdactivemq</code> for use. Important: DSC, DSAPostAMQ, ClientHandler, BARCmdline, and BARPortlets must be on the same version.

Version numbers for DSA software packages are displayed in a xx.xx.xx.xx-xxxxxx format, for example, DSC-17.00.00.00-431571.x8664.rpm.

IBM Spectrum Protect Software Installation Workflow

In a typical Spectrum Protect implementation, you have the following configuration:

- Spectrum server
- DSC server running SLES 11 SP3
- Media servers (client servers) running SLES 12 SP3, that must have Spectrum Protect Backup-Archive Client and Storage Agent installed

Before installing the software, do the following:

1. Verify the media servers have the Spectrum Protect Backup-Archive Client and Storage Agent installed.
2. Configure Spectrum Protect to prepare for installation. See [Configuring Spectrum Protect before Installing DSE](#).
3. Install the DSE software packages. See [Installing Software with Scripts](#).
4. Perform any necessary post-installation DSE configuration. See [Configuring DSE after Installation](#).
5. Configure Spectrum Protect for DSE. See [Configuring Spectrum Protect for Teradata DSE](#).
6. Configure the portlets. See [Configuring Portlet Software](#).

Installing Software with Scripts



NOTICE

DSC, DSAPostAMQ, ClientHandler, BARCmdline, and BARPortlets must be on the same version.

You must install the software packages in the following order:

1. Check if Data Mover is installed.
2. Teradata ActiveMQ
3. DSC
4. ClientHandler - this package includes DSE support, but also is required by AXMSpectrum
5. AXMSpectrum
6. AXMS3 - use when Amazon S3 is the backup target from an on-premises system
7. AXMAzure - use when Azure Blob is the backup target from an on-premises system
8. AXMGCP - use when Google Cloud is the backup target from an on-premises system
9. BARCmdline
10. barportlets

Check If Data Mover Is Installed

NOTICE

If Data Mover is installed you must be careful when installing or upgrading 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 or upgrade 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

Important:

Spectrum Protect must be completely set up and working before you install Teradata DSE.

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	

Type of Information	Description	Record the Value for Your Environment
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 Extension**.
6. Select the release information and click **Submit**.
Select SLES 11 for Spectrum Protect, it refers to the DSE software release, not the OS on your media servers.
7. Check the **Select All On This Page** box.
8. Deselect the AXMNetbackup 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 SLES15SP2 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-jdk11`.

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 11.
 - a. Check if Teradata JDK 11 is installed:
`rpm -q teradata-jdk11`
 - b. If necessary, install Teradata JDK 11 by extracting then running the script:
`tar -zxvf teradata-jdk11__slesxx_arch.xx.xx.xx.xx-#####.tar.gz`
`rpm -ivh teradata-jdk11__xx.xx.xx.xx-#####-arch.rpm`
2. Install Teradata ActiveMQ.
`rpm -ivh tdactivemqslesxx_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:
 - If SLES 15 run `python3 tdactivemq_wrapper.py`
 - For others run `./tdactivemq_wrapper.py`

Installing the DSC Package

Prerequisite:

- DSC, DSAPostAMQ, ClientHandler, BARCmdline, and BARPortlets must be on the same version.
- If this is an upgrade you must follow the procedure in [Backing Up DSC Repository and Configuration Before Upgrading](#) before preceding.

Install the DSC package on the server you want to be the DSC server. The DSC server must be running SLES 11 SP3.

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

/opt/teradata/client/version/dsa

1. If this is an upgrade, follow these steps first:
 - a. [Back up the DSC repository](#).
 - b. Verify the existing DSC server is accessible in the BAR Setup portlet. See [Enabling or Adding a DSC Server](#).
2. On the DSC server, extract the script rpm file:


```
tar zxvf DSC_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 *DSC.xx.xx.xx.xx* is extracted in the current working directory.
3. Change to the *DSC.xx.xx.xx.xx* directory.
4. Run the installation script.


```
./dscinstall.sh -r DSC-xx.xx.xx.xx-#####.arch.rpm
```
5. Enter values for the DSC component. If you are doing an upgrade, the previous settings are displayed and can be changed.

DSC Prompts	Description and Default Values
Landing Zone	Filepath to temporary location for DSC backup before replication to storage. Default: /var/opt/teradata/dsa/postgres
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
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	Applicable to an install only, not an upgrade. 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

DSC Prompts	Description and Default Values
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. Note: You cannot change the name of a DSC during an upgrade.
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 (jms ssl) password should match the DSA REST API https password. Default: tcp

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

Postrequisite:

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

Installing the ClientHandler Package

Prerequisite:

DSC, DSAPostAMQ, ClientHandler, BARCmdline, and BARPortlets must be on the same version.

Important:

Make sure the DSC is up and running before installing DSA Network Client (ClientHandler).

The BARNC [DSA Network Client (ClientHandler)] process queries the broker (ActiveMQ) for the existing DSC instances pointing to the broker. If the DSC is not running, autodiscovery fails.

Install the ClientHandler package on the hardware media 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.

1. If you are upgrading from DSA 16.20.00.02 or earlier to DSA 16.20.00.03 or later, you must remove the installed AXM packages before reinstalling ClientHandler.
 - a. Get a list of the installed packages: `rpm -qa | grep AXM`
 - b. Remove each package: `rpm -e nameofpackage`
2. On the DSC server, verify that the DSC is up and running.
`/etc/init.d/dsc status`
3. On the ClientHandler server, extract the script rpm file:
`tar zxvf ClientHandler_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 `ClientHandler.xx.xx.xx.xx` is extracted in the current working directory.
4. Change to the `ClientHandler.xx.xx.xx.xx` directory.
5. Run the installation script.
`./clienthandler_install.sh -r ClientHandler-xx.xx.xx.xx-#####.rpm`
6. Enter values for ClientHandler.
For an upgrade, the previous settings are displayed and can be changed.

ClientHandler Prompts	Description and Default Values
Enter the base directory	<code>base_dir/teradata/client/version/dsa</code>
ActiveMQ Broker Host Name and Port	<p>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</p> <p>Usually the DSC server, the format is: hostname:port, for example dsc1:61616</p> <p>You can enter multiple hostnames and ports. Press Enter when done to continue.</p>
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	<p>If you are using SSL, enter the value for the client's keystore password in clear text. Default: none</p> <p>If you set DSARest web services to https, the SSL Keystore password must match the DSARest keystore password.</p>
Server ID	Unique Server ID for this ClientHandler. The hostname of the server is recommended. Default: hostname
Is Master Server?	<p>Indicates whether this server is the CBB web service master server used in incremental job communication.</p> <p>Note:</p> <p>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.</p>
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: <code>/var/opt/teradata/dsa/cbb</code>
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.

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

```
clienthandlerConfigure.sh
```

Postrequisite:

Install the access module for the backup solutions or targets you plan to use:

Backup Solution	Go to
Spectrum Protect	Installing the AXMSpectrum Package
Amazon S3	Installing the AXMS3 Package
Azure Blob	Installing the AXMAzure Package
Google Cloud Platform	Installing the AXMGCP Package

Installing the AXMSpectrum Package

Prerequisite:

The DSC and ClientHandler packages must already be installed. The IBM Spectrum Protect Backup-Archive Client must already be installed.

- [Installing the DSC Package](#)
- [Installing the ClientHandler Package](#)

Install the AXMSpectrum access module, if you use Spectrum Protect.

1. On the media server, unzip and extract the script rpm file:

```
tar zxvf AXMSpectrum_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 *AXMSpectrum.xx.xx.xx.xx* is extracted in the current working directory.
2. Run the installation script from the extracted directory.

```
./axm_install.sh -r AXMSpectrum-xx.xx.xx.xx-#####.rpm
```
3. Accept the default options or provide the appropriate inputs.
4. Log off and log back in to the server to set the Linux environment variables.

Verify Installation

5. Verify that `/opt/teradata/client/xx.xx/dsa/AXMSpectrum` was created and contains executables, libraries, and scripts.
6. Verify that fusedriver service is running:

```
/etc/init.d/fusedriver status
```

```
Fuse Driver Service Status ----> Running
```

- From the media server, verify Spectrum mount point was created and mounted:
mount

```
Spectrum_FUSE on /Spectrum type  
fuse.Spectrum_FUSE (rw,nosuid,nodev,user=dscuser)
```

Postrequisite:

Install any other needed access module. If the access modules are all installed, go to [Installing the BARCmdline Package](#).

Installing the AXMS3 Package

Prerequisite:

The DSC and ClientHandler packages must already be installed.

- [Installing the DSC Package](#)
 - [Installing the ClientHandler Package](#)
-

This access module is not applicable when using a disk file system as a target device.

DSA Package	Installation Directory	Notes
AXMS3	<i>base_dir/teradata/client/version/dsa</i>	You can specify the directory as <i>base_dir</i> .

Note:

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

- On the server, unzip and extract the rpm file:

```
tar zxvf AXMS3_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 *AXMS3.xx* is extracted in the current working directory.
- Run the installation script from the extracted directory.

```
./axm_install.sh -r AXMS3-xx.xx.xx.xx-#####
```

- Log off and log back in to the server to set the Linux environment variables.

Postrequisite:

Install any other needed access module. If the access modules are all installed, go to [Installing the BARCmdline Package](#).

Installing the AXMAzure Package

Prerequisite:

The DSC and ClientHandler packages must already be installed.

- [Installing the DSC Package](#)
- [Installing the ClientHandler Package](#)

This access module is not applicable when using a disk file system as a target device.

DSA Package	Installation Directory	Notes
AXMAzure	<i>base_dir/teradata/client/version/dsa</i>	You can specify the directory as <i>base_dir</i> .

Note:

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

- On the server, unzip and extract the rpm file:

```
tar zxvf AXMAzure_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 *AXMAzure.xx* is extracted in the current working directory.
- Run the installation script from the extracted directory, where *arch* is the architecture, *xx* is the version number, and *#####* is a unique number.

```
./axm_install.sh -r AXMAzure-xx.xx.xx.xx-#####
```
- Log off and log back in to the server to set the Linux environment variables.

Postrequisite:

Install any other needed access module. If the access modules are all installed, go to [Installing the BARCmdline Package](#).

Installing the AXMGCP Package

Prerequisite:

The DSC and ClientHandler packages must already be installed.

- [Installing the DSC Package](#)
- [Installing the ClientHandler Package](#)

This access module is not applicable when using a disk file system as a target device.

DSA Package	Installation Directory	Notes
AXMGCP	<i>base_dir/teradata/client/version/dsa</i>	You can specify the directory as <i>base_dir</i> .

Note:

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

1. On the server, unzip and extract the rpm file:

```
tar zxvf AXMGCP_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 *AXMGCP.xx* is extracted in the current working directory.
2. Run the installation script from the extracted directory, where *arch* is the architecture, *xx* is the version number, and *#####* is a unique number.

```
./axm_install.sh -r AXMGCP-xx.xx.xx.xx-#####
```
3. Log off and log back in to the server to set the Linux environment variables.

Postrequisite:

Install any other needed access module. If the access modules are all installed, go to [Installing the BARCmdline Package](#).

Installing the BARCmdline Package

Prerequisite:

DSC, DSAPostAMQ, ClientHandler, BARCmdline, and BARPortlets must be on the same version.

The DSC, ClientHandler, and any required Access Modules must already be installed.

Teradata JDK must be installed on the command line server.

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 11 is installed:

```
rpm -q teradata-jdk11
```

2. If necessary, install Teradata JDK 11.

- a. Extract the script:

```
tar -zxvf teradata-jdk11__slesxx_arch.xx.xx.xx.xx-#####.tar.gz
```

- b. Run the script:

```
rpm -ivh teradata-jdk11__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.

If you are upgrading, the previous settings are displayed and can be changed.

BAR Command-Line Prompts	Description and Default Values
Enter the base directory	<i>base_dir/teradata/client/version/dsa</i>

BAR Command-Line Prompts	Description and Default Values
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
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:

DSC, DSAPostAMQ, ClientHandler, BARCmdline, and BARPortlets must be on the same version.

Install the DSC, ClientHandler, Access Modules, 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`
 where xx.xx.xx.xx is the version number

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
```

4. [Optional] Verify the BAR portlets:

```
rpm -qa |grep barportlets
```
5. Start Viewpoint.

```
/etc/init.d/viewpoint restart
```
6. If this is a fresh install, [Add the DSC Server](#) in the BAR Setup portlet.
7. If this is an upgrade and the DSC server is not available, go to [Enabling or Adding a DSC Server](#) and add the DSC manually.

Postrequisite:

If you want to use SSL, see [Setting Up SSL or TCP for JMS Workflow](#).

Verifying Installation

Prerequisite:

If you had any failures during installation, you must run the configuration scripts at the end of the procedure before continuing.

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

1. Verify that the ClientHandler web 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.
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
```

Verifying Teradata Connection to the ActiveMQ Server

All Teradata nodes require a network connection to the Teradata ActiveMQ (TDAMQ) server. The startup listener DSMAIN process runs on the node with the lowest online vproc number and does not start if the TDAMQ server cannot be reached.

If a Teradata system is not on the same network domain as the TDAMQ server, you must update the hosts file with the TDAMQ server IP address.

1. [Teradata Database 16.0 and later] If you have multiple DSCs, get the list of ActiveMQ servers:
 - a. Log on to the database system using bteq.
 - b. Issue this command to get a list of the DSCs and their associated ActiveMQ server:


```
select cast(activemqserver as char(30)), cast(dscname as char(30))
from sysbar.dsaconnectionstbl;
```
2. On every node, run `ping TDAMQservername` to check the connection to the TDAMQ server. Every node must be able to ping the TDAMQ server.
3. If DSMAIN did not start, go to the node with the lowest online RSG vproc number, and look at the startup listener log in `/var/opt/teradata/tdtemp/bar` for a message to troubleshoot the problem. The startup listener log uses the format `BARLog_rsgno_40.txt` where *rsgno* is the lowest RSG vproc number, such as `BARLog_26621_40.txt`.

Note:

As of Analytics Database 16.20 and Teradata Database 15.0.6.1, 15.10.04.04 and 16.0, the startup listener log has changed from `BARLog_rsgno_15.txt` to `BARLog_rsgno_40.txt`.

Configuring DSE after Installation

Setting Up SSL or TCP for JMS Workflow

Prerequisite:

Important:

To prevent a connection failure, install all DSA software including all the steps in [Installing Teradata ActiveMQ](#) before enabling SSL.

Important:

All DSA components must have JMS SSL enabled if using SSL, or disabled if not using SSL.

These tasks must be completed in this order to set up SSL for JMS on all client components.

1. [Configure ActiveMQ for SSL or TCP](#)
2. Manage the keys and certificates:
 - For SSL, [Set up self-signed keys and certificates](#)
 - For TCP, [Remove SSL keys and certificates](#)

Configuring ActiveMQ for SSL or TCP

The ActiveMQ script prepares your environment for SSL or TCP.

Note:

The SSL feature is optional and is turned off, by default.

1. Run the `activemq_ssl_setup.sh` script that is located on the DSC server in the `$DSA_DSC_ROOT` directory to configure ActiveMQ for SSL or TCP.
2. At the ActiveMQ directory prompt, enter the full path to the ActiveMQ directory, for example `/opt/teradata/tdactivemq/apache-activemq-5.xx.xx`.
3. At the ActiveMQ connection prompt, choose one of the following:
 - SSL
 - TCP
4. If SSL was selected, enter the password used to create the keystore at the Keystore password prompt. The password must be at least 6 characters in length.

If DSARest is set to https, the SSL keystore password must match the DSARest keystore password.

Enabling SSL - Setting Up Self-Signed Keys and Certificates

Prerequisite:

To prevent connection failure, you must follow the steps in [Installing Teradata ActiveMQ](#) and [Configuring ActiveMQ for SSL or TCP](#) before setting up the self-signed keys and certificates.

You must create self-signed keys and set up certificates for your SSL environment.

1. Use the `ssl_setup_cert_wrapper.sh` script to create self-signed keys and certificates in the ActiveMQ directory.

The script is located on the DSC server in the `$DSA_DSC_ROOT` directory.

Script usage is `ssl_setup_cert_wrapper.sh [-h] [-C] [-a activemq_dir]`, where:

Option	Description
-h	Displays help information.
-C	Cleans up the configuration files in the specified ActiveMQ directory.
-a	Specifies the directory where ActiveMQ is installed.

2. Copy files `client.pem` and `client-keystore.pem` and preserve file permissions as follows:

a. Go to: `/opt/teradata/tdactivemq/apache-activemq-5.xx.xx/conf`

b. For all Teradata systems and TPA nodes in the DSA environment, type:

```
#cp -p <file_name> /etc/opt/teradata/tdconfig
#chown teradata /etc/opt/teradata/tdconfig/<file_name>
#chmod 600 /etc/opt/teradata/tdconfig/<file_name>
```

c. For DSA media servers (anywhere ClientHandler is installed), type:


```
#cp -p <file_name> /etc/opt/teradata/dsa/
#chown dscuser /etc/opt/teradata/dsa/<file_name>
#chmod 600 /etc/opt/teradata/dsa/<file_name>
```

3. Copy `client.ts` to the systems where DSC or BARCmdline are installed and preserve file permissions by typing:

```
#cp -p <file_name> /etc/opt/teradata/dsa
```

Note:

Certificates are valid for 20 years.

4. Enable JMS SSL on the BAR portlets by installing the `client.pem` certificate on the **Viewpoint** portal:
 - a. From the Teradata **Viewpoint** portal, click .

- b. Open the **Certificates** portlet.
- c. From the **Setup** list, click **Certificate Authority**.
- d. Click **Install Certificate**.
- e. Enter an alias for the Certificate Authority, up to 30 characters.
- f. Click **Browse** and select the `client.pem` certificate.

Important:

Copy `client.pem` from `/etc/opt/teradata/dsa`.

- g. Click **Install**.
- h. Restart Viewpoint.
`/etc/init.d/viewpoint restart`
5. When you add the DSC using the **BAR Setup** portlet (see [Enabling or Adding a DSC Server](#)), select SSL as the Broker Connectivity and add the Broker Port.

Changing to TCP by Removing SSL Keys and Certificates

You must remove SSL keys and certificates to switch from an SSL to a TCP configuration. The manual steps taken in setting up self-signed keys and certificates for SSL must be reverted to TCP manually.

1. Use the `ssl_setup_cert_wrapper.sh` script with the `-C` option to clean up configuration files in the ActiveMQ directory. The script is located in the `$DSA_DSC_ROOT` directory. Script usage is `ssl_setup_cert_wrapper.sh [-h] [-C] [-a activemq_dir]`, where:

Option	Description
<code>-h</code>	Displays help information.
<code>-C</code>	Cleans up the configuration files in the specified ActiveMQ directory.
<code>-a</code>	Specifies the directory where ActiveMQ is installed.

2. At the Directory prompt, type the full path to the ActiveMQ directory: `/opt/teradata/tdactivemq/apache-activemq-5.xx.xx`.
 ActiveMQ restarts after certificates are removed.

Toggling SSL or TCP after Installation

If you have SSL set up and you want to switch to TCP, you can use these steps with the toggle script. You also must remove and re-add the DSC Server in the **BAR Setup** portlet.

If you want to switch from TCP to SSL, you need to follow the steps in *Enabling SSL - Setting Up Self-Signed Keys and Certificates* in your installation guide. See *Teradata® DSA - DSU Installation, Configuration, and Upgrade Guide*, *Teradata® DSA - DSE for Veritas NetBackup Installation*,

Configuration, and Upgrade Guide, or Teradata® DSA - DSE for IBM Spectrum Protect Installation, Configuration, and Upgrade Guide.

1. Remove the DSC Server using the **BAR Setup** portlet.
2. To toggle SSL for each client component (DSC, DSARest, BARCmdline, and ClientHandler), run the toggle script on each client.

`./ssl_jms_toggle.sh` is located in each client's installed directory:

- `$DSA_DSC_ROOT`
- `$BARCMDLINE_ROOT`
- `$CLIENTHANDLER_ROOT`

Syntax: `ssl_jms_toggle.sh [DSC | DSARest | BARCmdline | ClientHandler] [tcp | ssl] [61616 | 61617]`

For example: `ssl_jms_toggle.sh DSC ssl 61617`

For ClientHandler the following is true:

- The script prompts you for the SSL keystore password. This is the client's keystore password.

Important:

If DSARest web service is https, the SSL keystore password must match the DSARest web service keystore password.

If you want to switch from TCP to SSL, you need to follow the steps in *Enabling SSL - Setting Up Self-Signed Keys and Certificates* in your installation guide. See *Teradata® DSA - DSU Installation, Configuration, and Upgrade Guide*, *Teradata® DSA - DSE for Veritas NetBackup Installation, Configuration, and Upgrade Guide*, or *Teradata® DSA - DSE for IBM Spectrum Protect Installation, Configuration, and Upgrade Guide*.

-
- If `clienthandler.properties` contains multiple brokers, the script asks if you want to use the same port number for all brokers.
 - y - All port numbers are changed to the number listed in the command
 - n - Port numbers are left as is. To change any broker port numbers, you must change them in `broker.list` in `clienthandler.properties`.
3. Add the DSC server using the **BAR Setup** portlet (see [Enabling or Adding a DSC Server](#)), select SSL or TCP as the Broker Connectivity and Broker Port.
 4. From the **BAR Setup** portlet, select your DSC Server, and click **Systems and Nodes** under **Categories**.
 5. Select the system name under **Systems**, then **System Details** under **Setup**.
 6. To enable SSL, under **SSL Communication**:
 - a. Check the **Enable SSL over JMS Communication** box.
 - b. Enter the keystore password in the **Truststore Password** box.
 - c. Click **Apply**, then follow on-screen instructions.

7. To configure TCP, under **SSL Communication**:
 - a. Clear the **Enable SSL over JMS Communication** box.
 - b. Remove the keystore password from the **Truststore Password** box.
 - c. Click **Apply**, then follow on-screen instructions.
8. Restart the DSMain process on DSC server for the repository database cnsterm 6:
 - a. Stop bardsmain:


```
cnsterm 6
start bardsmain -s
```
 - b. Start bardsmain:


```
cnsterm 6
start bardsmain
```

Multiple DSA Network Client (ClientHandler) Instances

Configuring multiple DSA Network Client (ClientHandler) instances is required when there are two different networks at a site. Sometimes a site might have two private networks, or a public network and a private network.

For example, at a site where one media server is configured with a private network and a public network, in order to run a restore job using the public network, the private network IP addresses must not be used. In this situation, create two instances of DSA Network Client (ClientHandler) so that you can create two media servers in DSC. You can configure one of the media servers with addresses belonging to the public network, and one media server with addresses belonging to the private network. When a restore job must run on the public network, the media server configured with the public address is used instead of the media server with the private address.

You can also create a target group with the public media server and another target group with the private media server. If you create a Restore group between the private target group and the public target group, you can run a restore job using the Restore group over the public network.

Configuring Multiple DSA Network Client (ClientHandler) Instances

You can configure up to two instances of DSA Network Client (ClientHandler) on a single media server by running the `config_multiple_instances.sh` script. The `config_multiple_instances.sh` script configures the server's ClientHandler startup script to run multiple instances of ClientHandler.

NOTICE

Running `config_multiple_instances.sh` overwrites property files for the additional DSA Network Client (ClientHandler) instances but does not modify the original `clienthandler.properties` file.

1. At the command line, in the `CLIENTHANDLER_ROOT` directory, enter:


```
./config_multiple_instances.sh [-h] [-i] [-n Number_of_instances] [-s List_of_server_ids]
```

- -h displays parameter usage
- -i adds a date to the output messages but does not start or stop the ClientHandler service
- -n specifies the number of DSA Network Client instances to configure
- -s specifies the list of SERVER IDS to use for configuring the requested DSA Network Client instances

The list of SERVER IDS must be in double quotes, for example "server1 server2".

Restarting DSA Services

To have a fully functional Teradata DSA environment, you must have the Teradata ActiveMQ service, DSC, DSA Network Client (ClientHandler), and Viewpoint running. Follow these steps if you need to restart DSA Services.

Note:

The Teradata ActiveMQ service must be running before the DSC and DSA Network Client (ClientHandler) process are started, although, after installation, the DSC and ClientHandler should already be running.

1. If the Teradata ActiveMQ, DSC, and DSA Network Client (ClientHandler) are not running, at the command line, type the following and press **Enter** after each component string to start the service:

```
/etc/init.d/tdactivemq start
```

```
/etc/init.d/dsc start
```

```
/etc/init.d/clienthandler start client_handler_name (optional)
```

If the *client_handler_name* parameter is not provided, the command will start all instances if you have multiple DSA Network Client (ClientHandler) instances configured. To specify an instance of DSA Network Client, type `/etc/init.d/clienthandler start client_handler_name`, where *client_handler_name* specifies the DSA Network Client instance and refers to the Server ID parameter (usually the hostname).

Note:

Analytics Database must be active in order to start the DSC service.

2. Verify that the services are running:

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

```
/etc/init.d/dsc status
```

```
/etc/init.d/clienthandler status client_handler_name (optional)
```

If the *client_handler_name* parameter is not provided, the command will start all instances if you have multiple DSA Network Client (ClientHandler) instances configured. To specify an instance of DSA Network Client, type `/etc/init.d/clienthandler status client_handler_name`, where *client_handler_name* specifies the DSA Network Client instance and refers to the Server ID (usually the hostname).

Verifying Teradata Connection to the ActiveMQ Server

All Teradata nodes require a network connection to the Teradata ActiveMQ (TDAMQ) server. The startup listener DSMAIN process runs on the node with the lowest online vproc number and does not start if the TDAMQ server cannot be reached.

If a Teradata system is not on the same network domain as the TDAMQ server, you must update the hosts file with the TDAMQ server IP address.

1. [Teradata Database 16.0 and later] If you have multiple DSCs, get the list of ActiveMQ servers:
 - a. Log on to the database system using `bteq`.
 - b. Issue this command to get a list of the DSCs and their associated ActiveMQ server:


```
select cast(activemqserver as char(30)), cast(dscname as char(30))
from sysbar.dsaconnectionstbl;
```
2. On every node, run `ping TDAMQservername` to check the connection to the TDAMQ server. Every node must be able to ping the TDAMQ server.
3. If DSMAIN did not start, go to the node with the lowest online RSG vproc number, and look at the startup listener log in `/var/opt/teradata/tdtemp/bar` for a message to troubleshoot the problem. The startup listener log uses the format `BARLog_rsgno_40.txt` where *rsgno* is the lowest RSG vproc number, such as `BARLog_26621_40.txt`.

Note:

As of Analytics Database 16.20 and Teradata Database 15.0.6.1, 15.10.04.04 and 16.0, the startup listener log has changed from `BARLog_rsgno_15.txt` to `BARLog_rsgno_40.txt`.

Configuring Spectrum Protect for Teradata DSE

Running configTool.sh

Prerequisite:

Before running `configTool.sh`, make sure that the IBM Spectrum Server, Client and Storage Agent are properly configured and running.

Use `configTool.sh` to configure DSE and Spectrum Protect to work together.

1. Login as `dscuser`.
2. Go to `/opt/teradata/client/xx.xx/dsa/AXMSpectrum`.
3. Run `configTool.sh`.
4. Select **Create Config Set** to create the node on the Spectrum Protect Mount point, the node that is available on the IBM Spectrum Protect server and enter the following:

Item	Description
Owner Name	Any alphanumeric string
Node Name	Located in the IBM Spectrum Client <code>dsm.sys</code> file at <code>/opt/Tivoli/tsm/client/api/bin64/</code>
Password	Located in the IBM Spectrum Client <code>dsm.sys</code> file at <code>/opt/Tivoli/tsm/client/api/bin64/</code>

5. Select one of the following options:

Option	Description
Remove Config Set	Removes the created node from the Spectrum mount point. Does not delete the actual node from the IBM Spectrum Server.
Manage Config Set	Manage the configuration set for the selected node. Select the node you want to modify. See Managing the Configuration Set for the Selected Node for detailed information.
List NodeNames	List the node details. Displays the following: <ul style="list-style-type: none"> • Displays the files for this node that exist under the Spectrum Protect Mount point. • Displays the job details for each Management Class created/configured for this node. • For each Management Class it displays: <ul style="list-style-type: none"> ◦ Applicable device count ◦ All job details created or executed using this Management Class

Managing the Configuration Set for the Selected Node

If you selected **Manage Config Set** after running `configTool.sh`, use these instructions.

1. Select the node you want to manage.
2. Select one of the following options:

Option	Description
Edit Credentials	Enter the new Owner Name and Password. This changes the details stored on the Spectrum Mount point.
Add Management Class	Creates the new Management Class for this node and stores the details locally.
Remove Management Class	Removes the selected Management Class. This is visible locally and does not delete the node on the IBM Spectrum Server.
Set Device Count	Select a Management Class and change the device count when prompted. Default: 1 This sets the number of parallel streams allowed for this Management Class.
Rebuild Management Class	Gets the Management Classes for this node and rebuilds them. It does not delete the user created Management Classes.

Configuring Portlet Software


Configuring Viewpoint and BAR Setup



You must enable and add BAR portlets to Teradata Viewpoint before you can configure the BAR portlets for running jobs.

1. [Enable BAR portlets for the role and for Viewpoint access.](#)
You can set BAR administrator privileges for any Viewpoint role in **Roles Manager**. You can set access to the portlet in **Portlet Library**.
2. [Add a Teradata system to Viewpoint portlets.](#)
You must add and enable a Teradata system in **Monitored Systems** to make it available in the **BAR Setup**, **BAR Operations**, and **Viewpoint Monitoring** portlets.
3. [Set up the systems and nodes from the BAR Setup portlet.](#)
Nodes are configured through autodiscovery. You can view the information but not edit it.
4. Media servers are autopopulated with default BAR NC [DSA Network Client (ClientHandler)] port 15401 and IP address. Edit if needed.
5. Configure a backup solution:
 - [Disk File System](#)
 - [Amazon S3 Storage](#)
 - [Azure Blob Storage](#)
 For Spectrum Protect, choose Disk File System.
6. [Configure target groups for backup.](#)
The target groups must be mapped to the correct backup solutions.




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**.

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. Click **Apply**.

Enabling or Adding a DSC Server

Use these instructions to enable or add an additional DSC. If you have a DSC and are upgrading or adding another DSC, use this procedure before upgrading.

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. Enter the **Server Settings** and **BAR Logging** settings:

Option	Description
Security Management	Require Teradata Viewpoint authentication on the DSA command-line interface. If checked, a user submitting certain commands from the command-line interface must enter a valid Teradata Viewpoint user name and password.
BAR Logging	<p>Level of BAR log information to display for the Data Stream Controller and the BAR Network Client. Extensive logging information is typically only useful for support personnel when gathering information about a reported problem.</p> <p>Error Default. Enables minimal logging. Provides only error messages.</p> <p>Warning Adds warning messages to error message logging.</p> <p>Info Adds informational messages to warning and error message logging.</p> <p>Debug Full logging. All messages, including debug, are sent to the job log.</p> <div data-bbox="506 861 958 989">  NOTICE This setting can affect performance. </div>
Delete Retired Jobs	<p>Delete Retired Jobs determines the time period before retired jobs are deleted.</p> <p>After Number of days from the date a job is retired to wait before deleting the job.</p> <p>Never Prevents deletion of retired jobs.</p>

7. Click **Apply**.

Adding or Editing a 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 Analytics Database 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. Do one of the following:

Add a new target system	<ol style="list-style-type: none"> a. Click <input type="checkbox"/> next to Systems. b. Select Add Teradata System.
Edit an existing system	Select the name under Systems .

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>
System Selector	<p>[Optional] When editing a system, to change the system selector, click Update. The credentials to the system are verified before the update can occur.</p> <p>Note: You must stop and start DSMain in the database after changing the system selector.</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 Analytics Database 16.20 or later / Teradata Database 16.10 or later. The `-d` parameter only starts and stops the ActiveMQ connection. It will not affect any feature that requires DSMain to be completed restarted; for example GDO flag 553 (EnableBackupsforIncrementalRestore).

- c. Enter `start bardsmain` (this starts DSMain).
- d. [Analytics Database 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	<p>Verify that the number of the BAR network server matches the server port setting in the DSA client handler property file. Default port: 15401</p> <p>Note: If you change the port number in the <code>clienthandler.properties</code> file, you must restart the DSA Network Client using <code>/etc/init.d/clienthandler restart-hwupgrade</code>.</p>
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>

Option	Description
Network Mask	Refer to Network Masks for more information.

Network Masks

The subnet mask used by DSA is a logical mask, that is, it is treated as a mask to determine what connection paths are allowed between Teradata nodes and media servers. You can use a DSA network mask to create a data path between a Teradata node and a media server if the Teradata node and media server are physically connected. The DSA network mask setting does not override any physical subnet mask.

Use the default network mask, populated by DSA, that is based on the data path between Teradata nodes and media servers.

Note:

Remove network interfaces not used in the data path from the media server definition in the **BAR Setup** portlet.

Guidelines for DSA Network Masks


- Teradata nodes and media servers should be on the same logical subnet.
- If Teradata nodes and media servers are on different logical subnets, but can communicate with each other, open up the network mask as relevant.

Configuring Network Fabric: Portlets

Beginning with DSA 17.06, you can configure multiple fabrics.

Update `dsc.properties` for the number of fabrics allowed per Teradata system:




`maxlimit.fabric=number-fabrics`. Default is 64.

1. Restart ClientHandler to discover all changed IP addresses.
`/etc/init.d/clienthandler restart-hwupgrade`
2. Open the **BAR Setup** portlet.
3. Under **DSC Servers**, select your DSC server.
4. From the **Categories** list, click **Fabrics**.
5. Click  next to **Fabrics**.
6. Under **Fabric Details**, enter the following:

Option	Description
Fabric Name	Alphanumeric characters plus "-" and "_".

System Name	Choose the system from the drop-down list.
--------------------	--

7. Under **Nodes**, associate the media servers with the nodes:

Node	Choose the node from the drop-down list. Click  to add another.
Media server	Select a media server. Click  to add another.
IP Address	Select an IP address. Click  to add another.

Note:

For standby nodes, you can reduce maintenance by setting `dsc.properties` to `validate.fabric=off`. Restart the DSC after changing the properties file. The undefined paths use `bynet` to move the data. This solution degrades performance.

8. Select the **Enable fabric** checkbox.
9. Click **Apply**.

Configuring a Backup Solution

Configure the backup solution suited to your configuration.

Adding or Editing a Disk File System, Including Spectrum Protect

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.
6. To edit an existing system, change the number of **Max open files** next to its name.

Adding an Amazon S3 Account

When using Amazon S3 storage to back up and restore data, you must add and configure the S3 account using the **BAR Setup** portlet.

1. Under **DSC Servers**, select your DSC server.
2. Under **Categories**, select **Backup Solutions**.
3. From the **Solutions** list, click **Amazon S3**.
4. Click  next to **Accounts**.
5. Under **Amazon S3 Storage Details**, enter the **Account Name**.
Account name is alphanumeric, maximum of 32 characters.
6. Select an access type and enter its values:

Access Type	Values
Key authentication	<p>Enter these items as they are configured on AWS.</p> <p>Account Id AWS account ID</p> <p>Account Key IAM user access key</p> <p>Region Region associated with this bucket; for example: us-east-1 Regions are validated but you can override if a new region becomes available.</p> <p>Bucket S3 bucket name</p>

Access Type	Values
	<p>Prefix Alphanumeric, followed by / to be used as a folder</p> <p>Storage Units Maximum of 3 characters, numeric range between 1-999</p> <p>You can enter multiple regions and/or buckets by selecting .</p>
IAM Role	<p>Enter these items as they are configured on AWS.</p> <p>Role Name As established on AWS When roles are used, all components must be in the cloud and assigned to this role.</p> <p>Region Region associated with this bucket; for example: us-east-1 Regions are validated but you can override if a new region becomes available.</p> <p>Bucket S3 bucket name</p> <p>Prefix Alphanumeric, followed by / to be used as a folder</p> <p>Storage Units Maximum of 3 characters, numeric range between 1-999</p> <p>You can enter multiple regions and/or buckets by selecting .</p>
Snowball	<p>Enter these items as they are configured on AWS.</p> <p>Account Id AWS account ID</p> <p>Account Key IAM user access key</p> <p>Network IP Local IP address for the Snowball device</p> <p>Region Data target region, assigned with the Snowball</p> <p>Note: Snowball cannot be associated with multiple regions.</p> <p>Bucket S3 bucket name</p> <p>Prefix Alphanumeric, followed by / to be used as a folder</p>

Access Type	Values
	Storage Units Maximum of 3 characters, numeric range between 1-999 You can enter multiple buckets by selecting .

- Click **Apply**.

Adding Azure Blob Storage

When using Azure Blob storage to back up and restore data, you must add and configure the Azure Blob account using the **BAR Setup** portlet.

For optimal performance, configure 4 Blob containers per media server with 6 storage units each.

- Under **DSC Servers**, select your DSC server.
- Under **Categories**, select **Backup Solutions**.
- From the **Solutions** list, click **Azure Blob Storage**.
- Click next to **Accounts**.
- From the **Azure Blob Storage Details** screen, configure the following:

Option	Description								
Storage Account	Storage account name from Azure								
Account Key	Account Key from Azure								
Blob Type	Cool or Hot. Default: Cool								
Specialized Endpoint	<p>Leave blank. This field is only for National Clouds, which have sovereign endpoints. If you are in one of these national clouds, set the specialized endpoint entry as shown (the leading '.' is required).</p> <table> <tr> <th>Azure API Endpoint</th><th>Region Entry</th></tr> <tr> <td>Azure US Government</td><td>.blob.core.usgovcloudapi.net</td></tr> <tr> <td>Azure Germany</td><td>.blob.core.cloudapi.de</td></tr> <tr> <td>Azure China</td><td>.blob.core.chinacloudapi.cn</td></tr> </table> <p>For additional sovereign endpoints, check the Blob storage documentation for your national cloud.</p>	Azure API Endpoint	Region Entry	Azure US Government	.blob.core.usgovcloudapi.net	Azure Germany	.blob.core.cloudapi.de	Azure China	.blob.core.chinacloudapi.cn
Azure API Endpoint	Region Entry								
Azure US Government	.blob.core.usgovcloudapi.net								
Azure Germany	.blob.core.cloudapi.de								
Azure China	.blob.core.chinacloudapi.cn								
Blob Container	Container name from Azure. The first 3 characters must be unique for each container.								
Prefix	Alphanumeric, followed by / to be used as a folder								
Storage Units	Maximum number of files you can write. Maximum of 3 numbers, range between 1-999								



- Click **Apply**.

Adding or Copying 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 and copy.


When DSC is deployed in the Public Cloud, a default disk file system target group is created (`defaultDFTGsystem_name`). This target group scales out/in with the database.

- Open the **BAR Setup** portlet.
- Under **DSC Servers**, select your DSC server.
- From the **Categories** list, select **Target Groups**.
- From the **Target Groups** list, select **Remote Groups** or **Replication Groups**.
- 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

- Enter a **Target Group Name** for the new target group.
You can use alphanumeric characters, dashes, dots, and underscores, but no spaces.
- Select the **Enable target group** checkbox.
- Select a **Solution Type**.
- 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.
Use Disk File System for IBM Spectrum Protect.
 - Amazon S3: Select the **Account Name**, **Region**, **BAR Media Server**, **Bucket**, **Prefix**, and enter the number of **Storage Units**.
 - Azure Blob Storage: Select the **Storage Account**, **BAR Media Server**, **Prefix**, and set the number of **Storage Units**.
To use multiple storage accounts, select  next to **Targets** and enter the information for another account.
 - Google Cloud: Select the **Service Account**, **BAR Media Server**, **Bucket**, **Folder**, and set the number of **Devices**.

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

Option	Description
Remove	Click <input type="checkbox"/> 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. IBM Spectrum Protect cannot be used for replication.
- Amazon S3: Select the **Account Name**, **Region**, **BAR Media Server**, **Bucket**, **Prefix**, and enter the number of **Storage Units**.
- Azure Blob Storage: Select the **Storage Account**, **BAR Media Server**, **Prefix**, and set the number of **Storage Units**.

12. Click **Apply**.

Upgrading Software

Backing Up DSC Repository and Configuration Before Upgrading

The DSC repository stores all DSA data, including configuration definitions and settings, job definitions, job status, and job history. Protecting the data in the DSC repository is critical. Without the DSC repository, database backup data sets cannot be restored.

Important:

- If you are upgrading DSC to version 17.10.01.00 then make sure to upgrade Postgres to version 10.15 (SLES 11 SP3 : 10.15-0.2.24 and SLES 12 SP3 : 10.15-4.9.1) before upgrading the DSC.
- If you are upgrading DSC to version 17.20.00.00 then make sure to upgrade Postgres to version 10.17 (SLES 11 SP3 : 10.17-0.2.30 and SLES 12 SP3 : 10.17-4.16.4) before upgrading the DSC.
- If you are upgrading DSC to version 17.20.00.03 then make sure to upgrade Postgres to version 10.17 (SLES 11 SP3 : 10.17-0.2.30, SLES 12 SP3 : 10.17-4.16.4 and SLES 15 SP2: 10.17-4.16.4) before upgrading the DSC.
- If you are upgrading DSC to version 17.20.03.00 then make sure to upgrade Postgres to version 10.22 (SLES 11 SP3 : 10.22-0.2.46, SLES 12 SP3 : 10.22-4.31.1 and SLES 15 SP2: 10.22-150100.8.50) before upgrading the DSC.

It is critical to save copies of the following configuration information before you upgrade.

- The backup repository configuration
- The information required by the `/tmp/dsainputs` template if you are using PUT

Most of this information is in the properties files saved in `/etc/opt/teradata/dsa`.

Important:

If you change the DSC name during the upgrade you must repeat the repository backup when you are done.

Use the following procedure to back up the DSC repository.

1. Run the `config_repository_backup` command followed by the parameters to configure a target group for the DSC repository backup and schedule a DSC repository backup.

Parameter	Description
<code>f file filename</code>	The full path and name of the file containing the necessary configuration parameters.

Parameter	Description
<code>u user_authentication User</code>	Required when security management is enabled. Supplies the command with the Viewpoint user, and triggers a password prompt for authentication.

Sample XML file:

```
<dscRepositoryBackup dscVersion="dscVersion1" xmlns="http://
schemas.teradata.com/v2012/DSC">
  <!-- 'target_name' - Required, max 32 characters -->
  <target_name>SampleBackupRepoTargetGroup</target_name>

  <!-- 'frequency_value' - Required, Value between 1-4, Defaults to 1 -->
  <frequency_value>1</frequency_value>

  <!-- 'day_selection' - Required, accepted values: Su, Mo, Tu, We, Th, Fr,
  Sa -->
  <day_selection>Sa,Su</day_selection>

  <!-- 'start_time' - Required, Max characters 5, Values 1:00-12:00 -->
  <start_time>12:00</start_time>

  <!-- 'start_am_pm' - Required, accepted values: AM/PM -->
  <start_am_pm>AM</start_am_pm>

</dscRepositoryBackup>
```

2. Type `dsc export_repository_backup_config -f export_repository_backup_config.xml`.

Note:

You need to run `export_repository_backup_config` every time the configuration for repository backup is changed.

NOTICE

Keep `export_repository_backup_config.xml` in a safe, known location to be imported back into DSC in case of a disaster.

3. Type `dsc run_repository_job -t backup`, and press **Enter** to run a DSC repository backup.

Note:

The `run_repository_job` command can only be initiated if no operational jobs are running.

Upgrading DSA Software Using Scripts or rpm

The process for upgrading using scripts or rpm is the same as that for the initial installation. The values entered at the time of the initial installation are displayed and can be changed if necessary.

1. If you are upgrading from DSA 16.20.00.02 or earlier to DSA 16.20.00.03 or later, you must remove the installed AXM packages before reinstalling ClientHandler.
 - a. Get a list of the installed packages: `rpm -qa | grep AXM`
 - b. Remove each package: `rpm -e nameofpackage`
2. Follow the instructions at [Installing Software with Scripts](#).

Upgrading the Database to 16.0 or Later

If you upgrade to Teradata Database 16.0 or later, you must reconfigure the database in the **BAR Setup** portlet and restart DSmain on the database.

1. Run DIPBAR on the target system.
2. Follow the instructions in [Adding or Editing a Teradata System](#).

Resolving Failed Upgrades

To resolve a failed upgrade, you must determine whether the failure is of the DSC or some other component and the point where the failure occurred.

Note:

DSC, DSAPostAMQ, ClientHandler, BARCmdline, and BARPortlets must be on the same version.

Resolving Failed Upgrade of DSA Component other than the DSC

If the upgrade fails for DSA components other than the DSC, the environment may be corrupt.

1. Uninstall both the previous and the new version of the component.
2. After determining the cause of the failure, do a fresh install of either the new or the previous version using the information you exported before attempting the upgrade (see [Backing Up DSC Repository and Configuration Before Upgrading](#)).

DSA Properties

DSA Property Files

DSA property files are created during installation with environment-specific configurations. These files do not require modification after installation unless there are changes in your environment, such as the ActiveMQ server, SSL, or TVI settings. Other changes in your environment, such as the IP address of the host server running the ActiveMQ broker or the logging levels, can be updated using the **BAR Setup** portlet.

The Teradata DSA property files are located in `/etc/opt/teradata/dsa`:

- `barportlet.properties`
- `commandline.properties`
- `clienhandler.properties`
- `dsarest.properties`
- `dsc.properties`

Note:

These files should not be altered. However, if any of the settings in `barportlet.properties`, `commandline.properties`, `clienhandler.properties`, `dsarest.properties`, or `dsc.properties` are changed because of environment updates, the changes do not take effect until DSC and the ClientHandler are restarted.

Data Stream Controller (DSC) Properties

Note:

Do not edit any property setting after installation. If any change is made, the change does not take effect until DSC and the ClientHandler are restarted.

Property	Description	Default Setting
<code>broker.url</code>	Hostname or IP address of the machine running the ActiveMQ broker (where <code>tdactivemq</code> is installed), usually the DSC server.	
<code>broker.port</code>	Port number on the server where the ActiveMQ broker is listening (61616 for tcp, 61617 for ssl). Default: 61616	61616
<code>broker.type</code>	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	tcp

Property	Description	Default Setting
	should match the DSA REST API https password. Default: tcp	
dataset.retention.days	Number of days used for checkretention (previously listed) to determine if a save set (or data set) is at risk of being expired on the backup application. This value is used both for the checkretention task and the sync_save_sets user command to compile a list of save sets to send to DSA Network Client (ClientHandler).	30 days
dsarest.webservice.host	DSARest web service host, which is where the web service runs. The host is usually the DSC server.	
dsc.name	Name of the DSC.	
executormanager.maxConcurrentJobs	Maximum number of jobs allowed to run on DSC at the same time	100
executormanager.maxQueuedJobs	Maximum number of jobs placed on the queue and executed when slots become available	20
fullExport.landingZone	Directory on the DSC server where the job status log is output when you use the -E -full_export parameter with the job_status_log command.	/var/opt/teradata/dsa/export
log4j.rootLogger	Logging level of the DSC component	INFO Other values: ERROR WARN DEBUG
log4j.appender.logfile.file	Location of the log file	
log4j.appender.logfile	Internal setting for logging infrastructure	
log4j.appender.logfile.maxFileSize	Maximum size of the logging file before being rolled over to backup file	10 MB
log4j.appender.logfile.maxBackupIndex	Number of backup logging files that are created. The oldest file is erased if the maximum number of files has been created.	20
log4j.appender.logfile.layout	Internal setting for logging infrastructure	
log4j.appender.logfile.layout.ConversionPattern	Pattern of the log file layout	
logger.useTviLogger	TVI logger on or off setting. When set to true, fatal error messages can be sent to TVI.	true
maxlimit.fabric	The number of fabrics allowed per Teradata system.	64
startup.retry.interval	Time interval measured in seconds for retrying the connection to ActiveMQ during DSC startup	300

Property	Description	Default Setting
tviretry	Number of times DSC will retry to connect to ActiveMQ during DSC startup before error messages are reported to TVI	10
validate.fabric	DSC validates the fabric configuration when a job is executed	on
viewpoint.url	Hostname or IP address of the system running Viewpoint	
viewpoint.port	Port number of the machine where viewpoint is listening	80
cam.activemq.host	Hostname or IP address of primary CAM system, which enables alert messaging	
cam.activemq.port	CAM port number of primary CAM system [DSA 16.20.51 and later] CAM does not support SSL in this version. Port must be 61616.	61616
cam.cluster.enabled	Flag for enabling CAM clustering	false
cam.clustered.activemq.host	Hostname or IP address of primary and failover CAM systems, which enable alert messaging	
cam.clustered.activemq.port	CAM port number [DSA 16.20.51 and later] CAM does not support SSL in this version. Port must be 61616.	61616
autodeletejob.cronstring	Time when retired jobs scheduled for deletion are deleted. The string must be in the form of a valid cron expression. Cron expressions are comprised of 6 required fields and one optional field, each of which is separated by one white space. The fields are: <i>Seconds Minutes Hours Day-of-month Month Day-of-week Year</i> (optional)	autodeletejob.cronstring=0 0 0 * * ? The default runs the delete job every night at 0 seconds, 0 minutes, and 0 hour, which is equivalent to midnight.
message.timeToLive	JMS message time-to-live configuration	1200000

DSA REST Properties

The DSA REST property file is located at: `/etc/opt/Teradata/dsa/dsarest.properties`.

Property	Description	Default Setting
dsarest.certificate.keystorepass	Stores the keystore password used for the DSARest web service via https	
dsarest.webservice.port	Port for the DSARest web service running on DSC server	9090

Property	Description	Default Setting
dsarest. webservice.scheme	Scheme for the DSARest web service running on DSC server	https
dsc.name	Name of the DSC.	
broker.url	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	61616
transport	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	tcp
log.LandingZone	Location of the consolidated logs on the DSC server	/var/opt/ teradata/dsa/ landing_zone

ClientHandler Properties

Note:

Do not edit any property setting after installation.

Property	Description	Default Setting
broker.list	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	61616
broker.type	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	tcp
log4j.rootLogger	Logging level of the DSC component. Note: Changing the logging level requires a manual restart of the ClientHandler.	INFO Other values: ERROR WARN DEBUG
log4j.appender.logfile.file	Location of the log file	
log4j.appender.logfile	Internal setting for logging infrastructure	
log4j.appender. logfile.maxFileSize	Maximum size of the logging file before being rolled over to backup file	10 MB

Property	Description	Default Setting
log4j.appender. logfile.maxBackupIndex	Number of backup logging files that are created. The oldest file is erased if the maximum number of files have been created.	3
log4j.appender. logfile.layout	Internal setting for logging infrastructure	
log4j.appender.logfile. layout. ConversionPattern	Pattern of the log file layout	
memory.numbuffers	Number of buffers per stream that are allocated. This parameter is useful for limiting memory.	
memory.sizebuffers	The initial size of buffers. Even if the initial buffer size is low, a buffer may grow to approximately 1MB during a backup or restore job. This is the size of a single, full record from the database. If the default value causes a problem, such as when buffers are frequently reallocated and memory fragmentation occurs, you can use this parameter to allocate buffers of the appropriate size.	
perf.buffersperstream	The number of buffers that DSA Network Client allocates per network stream or socket. The minimum value is 1. The maximum value is 64.	16
perf.sizebuffers	The starting size of the buffers. The minimum value is 1. The maximum value is 2097152.	1572864
server.port	Socket number on which the BAR server is listening	15401
server.id	Name of the BAR server	Hostname of the BAR master server.
server.protocol	Protocol used for communication between the database and the BAR server. Values: SSL or TCP.	TCP
ssl.truststore.file	Used for setting up SSL truststore information. Only required if protocol is SSL.	
ssl.keystore.file	Used for setting up SSL keystore information. Only required if protocol is SSL.	
ssl.keystore. passwordencoded	Used by SSL communication and is the encrypted password for the keystore.	
CBBTempFile.path	Path to the temporary file repository for CBB. The path is found only on the Web Service master server, which is used for incremental job communication.	/var/opt/ teradata /dsa/cbb

Property	Description	Default Setting
Master.hostname	Host name of the Web Service master server, which is used for incremental job communication. The CBBTempFile.path is mounted on the Web Service master server.	
logger.useTviLogger	TVI logger on or off setting. When set to true, fatal error messages can be sent to TVI .	true
startup.retry.interval	Time interval measured in seconds for retrying the connection to ActiveMQ during ClientHandler startup.	300
tvi.retry	Number of times the ClientHandler tries to connect to ActiveMQ during DSC startup before error messages are reported to TVI	10
Webservice.port	Port number that the ClientHandler Web Service uses for incremental job media server communication.	15402

Command Line Properties

Note:

Do not edit any property setting after installation.

Property	Description	Default Setting
broker.url	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	61616
broker.type	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	tcp
dsc.name	DSC name the BAR command-line interface connects to.	none
log4j.rootLogger	Logging level of the DSC component. Values are: INFO ERROR WARN DEBUG	INFO
log4j.appender.logfile.file	Location of the log file	
log4j.appender.logfile	Internal setting for logging infrastructure	

Property	Description	Default Setting
log4j.appender. logfile.maxFileSize	Maximum size of the logging file before rolling over to backup file	10 MB
log4j.appender. logfile.maxBackupIndex	Number of backup logging files created. The oldest file is erased if the maximum number of files have been created.	3
log4j.appender.logfile.layout	Internal setting for logging infrastructure	
log4j.appender.logfile. layout.ConversionPattern	Pattern of the log file layout	
BARCMDLINE_ JAVA_HOME	Path where Java is installed. This is just for a generic SLES Linux environment; it is not used by Java.	

BAR Portlets Properties

Note:

Do not edit any property setting after installation.

Property	Description	Default Setting
file.uploadsizelimit	Maximum size of file that can be uploaded	1048576
file.uploaddirectory	Directory where files are uploaded.	/tmp/

Administrative Tasks

Creating an Incident

You must obtain an Incident number from Teradata customer portal prior to performing any software upgrades.

1. Go to <https://support.teradata.com>.
2. Log in.
3. Click **Incidents** and follow the instructions.

Creating a Diagnostic Bundle for Support

Teradata DSA provides a command-line, interactive script to collect:

- Current time on the server
- Component versions, for Analytics Database/Teradata Database, DSC, DSA Network Client, Spectrum Protect, Viewpoint, BAR Command Line, ActiveMQ
- General system configurations, such as the number of media servers, DSC server status
- Property files and logs for the DSC component and the DSA Network Client (ClientHandler)

This information is useful for troubleshooting by Teradata Services.

The `dsa_support_info.sh` script is installed in the root directory associated with a DSA installation package:

- `$DSA_DSC_ROOT` on the DSC server
 - `$CLIENTHANDLER_ROOT` on a media server
 - `$BARCMDLINE_ROOT` on the command line server
1. [Optional] To set up an SSH trust relationship between the DSC server and BAR servers or remote servers, run `dsatrust.sh` with the following syntax:
`dsatrust.sh [-a] [-l <hosts>] [-u user] [-v] [-h]`

Parameter	Description
<code>-a</code>	Sets trusted relations between the DSC server and other BAR servers.
<code>-l hosts</code>	Sets trusted relations to the listed hosts. Host names must be separated by commas.
<code>-u user</code>	Specify login user name. You must use this parameter with the <code>-a</code> or <code>-l</code> parameter.
<code>-v</code>	Displays the script version.

Parameter	Description
-h	Displays help.

2. Run `dsa_support_info.sh` on a server to collect local information, using the following syntax:
`dsa_support_info.sh [-c][-d <path>][g][-h][-i][-j <job>][-s <timestamp>][-t][-v][-x]`

Parameter	Description
-c	Collects core dumps for the DSA Network Client (ClientHandler).
-d <i>path</i>	Specifies the dump directory path. Default: <code>/var/opt/teradata/dsa/support/hostname_current timestamp</code>
-g	Collects general support information.
-h	Displays help.
-i	Collects installation logs.
-j <i>job</i>	Collect job information. Enter the job name as <i>job</i> .
-s <i>timestamp</i>	Collects logs for the date and time specified in the timestamp. Specify the timestamp in the following format, for example, 2015-05-15 09:50.
-t	Triggers a TVI event. If the -t parameter has been used to trigger a TVI event, the data is zipped. If the 50 MB limit per TVI event is exceeded, the support bundle is split into multiple zip files, and a separate TVI event is triggered for each zip file. The zip files are copied to <code>/var/opt/teradata/SupportBundle/</code> . You can access the unzipped files in the dump directory specified by the -d parameter.
-v	Displays the script version.
-x	Bypasses all user prompts.

After the script runs, files specific to the local server are output and can include:

- Component information in `.out` files
- Job output xml and `.out` files
- Log files
- Property files
- DSA Network Client (ClientHandler) core dumps

The output directory is `/var/opt/teradata/dsa/support/hostname_current timestamp` or a user-specified directory.

Updating Passwords

The `configureDBSPassword.sh` script allows system password information to update the `dbc`, `admin`, `BAR`, and `BARBACKUP` passwords that DSA uses so that they match the database passwords. The script does not change the passwords in the database. It is included in the DSC install directory at `$DSA_DSC_ROOT`.

Note:

If there is a password mismatch, DSC services cannot be started.

- Run `configureDBSPassword.sh` as shown:

```
configureDBSPassword.sh
-h Display help
-d Directory where DSC is installed. Defaults to current directory if
not specified.
```

Troubleshooting

Logs

Logs Created During DSA Installation

Logs in the following table contain messages produced during package installation.

Log File	Location
dscinstall.log	Resides on the DSC server in /tmp.
clienthandlerinstall.log	Resides on media servers in /tmp.
axms3install.log	On media servers that are configured for S3, resides in /tmp.
axmazureinstall.log	On media servers that are configured for Azure, resides in /tmp.
axmgcpinstall.log	On media servers that are configured for GCP, resides in /tmp.
barcmdlineinstall.log	Resides in one of the following servers in /tmp: <ul style="list-style-type: none"> • DSC server • Media server
barportletsinstall.log	Resides on the Viewpoint server in /tmp.
axmspectruminstall.log	On media servers that are configured for Spectrum Protect, resides in /tmp.

DSA REST Log

The DSA REST log is the log from the DSARest web service.

Log File	Location
dsarest.log	Resides at /var/opt/teradata/dsa/logs/. <ul style="list-style-type: none"> • To check status of DSARest /etc/init.d/dsc wsstatus • Start DSARest - /etc/init.d/dsc wstart • Stop DSARest - /etc/init.d/dsc wstop • Restart DSARest - /etc/init.d/dsc wsrestart

Spectrum Protect Key Log and Configuration Files

Location	Logs
/opt/teradata/client/16.20/dsa/AXMSpectrum	<ul style="list-style-type: none"> • dsmerror.log – key error log • dsminstr.log – key instrumentation log

Location	Logs
	<ul style="list-style-type: none"> • <code>devconfig.txt</code> – Storage Server connection information used to start the server
<code>/opt/tivoli/tsm/ StorageAgent/bin/</code>	<ul style="list-style-type: none"> • <code>dsmerror.log</code> – Key log file for Storage agent errors • <code>dsmsta.opt</code> – Key config file for Storage Agent. <ul style="list-style-type: none"> ◦ <code>TCPPort</code> (Shared Memory) – Found you may need this setting to force shared memory access for LANFree to the Node from the Storage Agent. Use a port other than the default 1500 that typically used between the Node and the IBM Server; for example, <code>TCPPort 3700</code> ◦ <code>IDLETIMEOUT</code> – Increase timeout if long restores are not getting resources allocated as expected. Recommended: <code>IDLETIMEOUT 600</code> • <code>dsmsta.rc</code> – Start and stop the storage agent on a client; for example, <code>./dsmsta.rc stop/start/restart</code> <p>Note: A <code>dsmserve.v6lock</code> file is found in this directory whenever the storage agent is running.</p> <ul style="list-style-type: none"> • <code>./dsmsta</code> – Start the storage agent in the foreground, gives a prompt. Use <code>HALT</code> to exit from storage agent and stop the service. This is a good way to watch and catch errors.
<code>/opt/tivoli/tsm/client /api/bin64/bin and /opt/tivoli/tsm/ client/ba/bin/</code>	<ul style="list-style-type: none"> • <code>dsmerror.log</code> – Key error log • <code>dsm.opt</code> – Client options file used at startup • <code>dsm.sys</code> – Client connection file used at startup • <code>dsmc</code> – Spectrum client (CLI) • <code>dsmj</code> – Spectrum client (GUI) • <code>dsmadm</code> – Spectrum Server (CLI)

Using PUT for Install and Upgrade

Before using PUT, you must have already installed Postgres and have the DSC installed and running.

Setting Up PUT

Before You Begin

Before installing, upgrading, migrating, or major system restores, make sure you have the latest version of PUT installed. PUTTools, which are also used by processes other than PUT are also available.

PUT Package	Description
TDput	TDput is the PUT application. If installed, it must be installed first.
PUTSRC [optional]	System Readiness Check (SRC). Must be separately installed after PUT is installed using PUT's Install/Upgrade Software operation.
PUTTools	A package of tools designed to assist with system changes. This package contains the Upgrade and Migration Scripts necessary to prepare a system for these activities. The files and scripts in the PUTTools package are installed in the following location: /opt/teradata/PUTTools/ This package must be installed using PUT's Install/Upgrade Software operation after PUT is installed.

Software Installation Preparation

Prior to downloading and installing software packages, you must make sure you have the following items completed:

- Find the version of PUT currently running on the system.
- Determine the latest available version of PUT and compare that version to the one running on the system.
- If the version on the system is not the latest:
 - Download the newest PUT version.
 - Install or upgrade the PUT version on the system.
- Check that there is enough space on the server for the new software.

Creating a Target Directory

- Set up a target directory on the server to hold the downloaded packages with the following command:

```
mkdir -p /var/opt/teradata/ccnumber/pkg
```

where the *ccnumber* is the Teradata Change Control Number, as shown in the following example:

```
/var/opt/teradata/VECD2RQ9B/pkg
```

Downloading Software Packages

1. Log in to <https://support.teradata.com>.
2. Select **Software Downloads**, then click **All Downloads**.
3. Under **Tools**, click **Software Downloads**.
4. Click **Backup Archive Restore**.
5. Select the product and release information and click **Submit**.
6. Select all packages.
7. Download the packages and follow the instructions.

Installing PUT

- To install PUT, follow the instructions in the *Parallel Upgrade Tool (PUT) Reference*.

Note:

Make sure the version of PUT is the same on all nodes, including managed servers. Always use the latest version of PUT.

Creating the DSC User

You must create the DSC User before installing ClientHandler and DSC with PUT. This applies only to new installations, not upgrades.

- At the command-line prompt, type `#/usr/sbin/useradd -m <DSCUSER> -u <USERID>`.
DSCUSER and *USERID* correspond to the values in the *dsainputs* file.

Installing DSA Using PUT

Customizing Values Used in PUT Installation

A *dsainputs* file, which includes the input values for all the DSA components being installed on that server, is required to install DSA components with PUT. Each DSA server needs its own *dsainputs* file, customized for that server. The values will vary from server to server.

1. Create a *dsainputs* file under the `/tmp` directory on the system where the DSA packages will be installed.
A *dsainputs* template is available in all DSA packages. The template for the DSC is a compilation of all inputs required for all the packages: `dsacomp_tdput_template`.

Note:

Keep the dsainputs file in a secure location. The dsainputs file that is placed in /tmp cannot be used by subsequent installation or upgrade processes.

2. Insert the parameters and values for the component you are installing. Values are specific for that server.

For example: BURL=dsasrv1

Important:

You must add DSARESTSCHEME to the dsainputs file.

Parameter	Component	Description
BROKERLIST	ClientHandler	List of broker:port pairs separated by a comma. For example: dsasrv1:61616
BURL	DSC, ClientHandler, BAR Command Line	Hostname or IP address of the machine running the JMS broker (ActiveMQ). Hostname or IP address of the machine running the ActiveMQ broker (where tdactivemq is installed), usually the DSC server.
BPORT	DSC, ClientHandler, BAR Command Line	Port number on the server where the ActiveMQ broker is listening (61616 for tcp, 61617 for ssl). Default: 61616
LANDINGZONE	DSC	/var/opt/teradata/dsa/postgres Default location for DSC repository backup files. Temporary location before replication to the target group.
CONNECTION	DSC, ClientHandler, BAR Command Line, BARPortlets	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
DSCNAME	DSC, BAR Command Line	Unique name for the DSC server. Maximum of 128 characters: alphanumeric, "-", and ".". The first character of the name can be alphanumeric (a-z, A-Z, and 0-9) only. Important: DSCNAME must be specified for an upgrade or the repository restore from the previous version will fail. Analyze_read jobs may also fail.
CBBFILEPATH	ClientHandler	The path needed for Change Block Backup temporary file storage: /var/opt/teradata/dsa/cbb
POSTGRESSPASSWORD	DSC	Password for Postgres user. No space, ', or " allowed.

Parameter	Component	Description
BACKUPAPPCLIENTNAME	AXMNetbackup	The name of this media server. In NetBackup, this is the client name.
ISMASTER	ClientHandler	Specify yes or no on whether this server is the Web Service master server used in incremental job communication.
MASTERHOSTNAME	ClientHandler	Specify the host name of the Web Service master server used in incremental job communication.
VIEWPOINTURL	DSC	Hostname or IP address of the Viewpoint server.
VIEWPOINTPORT	DSC	Port number of the Viewpoint server.
CAMPRIMARYURL	DSC	Hostname or IP address of primary CAM system, which enables alert messaging
CAMPRIMARYPORT	DSC	CAM port number of primary CAM system. Default: 61616. [DSA 16.20.51 and later] CAM does not support SSL in this version. Port must be 61616.
CAMCLUSTERENABLED	DSC	Flag for enabling CAM clustering
CAMCLUSTERURL	DSC	Hostname or IP address of primary and failover CAM systems, which enable alert messaging
CAMCLUSTERPORT	DSC	CAM port number for clustered environment. This has the same value as CAMPRIMARYPORT. Default: 61616. [DSA 16.20.51 and later] CAM does not support SSL in this version. Port must be 61616.
DSARESTPORT	DSC	Port number for DSARest Web Service running on DSC server. Default: 9090.
DSARESTSCHHEME	DSC	DSARest Web Service scheme, http or https. Default: https.
KEYSTOREPASS	DSC	Required if DSARESTSCHHEME is https. Password for keystore. Minimum of 6 characters. No space, ', or " allowed. If JMS SSL is enabled, this password must match SSLKEYSTOREPASSWORD.
BARPASSWORD	DSC	Password for the BAR user. Used for Create, Read, Update and Delete (CRUD) operations on BAR. No space, ', or " allowed.
SERVERID	ClientHandler	The server ID is the name of a DSA media server, and is a unique logical name across a single DSA domain. It is defined using SQL 92 syntax and used as the selector for JMS message headers. If the ClientHandler package is installed on a TPA node, the server ID cannot be equal to the name of that system. It is not the ID for NetBackup or other third party servers.

Parameter	Component	Description
		Note: When upgrading a media server for multiple DSA Network Client (ClientHandler) instances, specify the server IDs in a comma-separated list, for example, server1,server2.
SERVERPORT	ClientHandler	Port number for datapath traffic, corresponds to the server.port property in clienthandler.properties. Default: 15401.
SSLTRUSTSTOREFILE	ClientHandler	Full file path for truststore file.
SSLKEYSTOREFILE	ClientHandler	Full file path for keystore file.
SSLKEYSTOREPASSWORD	ClientHandler	The value for the JMS SSL keystore password, in clear text. If DSARESTSCHEME is set to https, this value must match KEYSTOREPASS.
SSENCKEYSTOREPASSWORD	ClientHandler	The value for the JMS SSL keystore password, in clear text. If DSARESTSCHEME is set to https, this value must match KEYSTOREPASS.
WSPORT	ClientHandler	Port number for ClientHandler Web Service traffic, corresponds to the WebService.port property in clienthandler.properties. Default: 15402.

The following is an example of a DSC server dsainputs file:

Important:

DSCNAME must be specified for an upgrade or the repository restore from the previous version will fail. Analyze_read jobs may also fail.

```
# DSC, Clienthandler, and BARCmdline AMQ Broker connection type ssl or tcp
CONNECTION=tcp

# DSC and BARCmdline shared fields
DSCNAME=
BURL=
BPORT=61616

# DSC dsainputs fields
POSTGRESPASSWORD=
BARPASSWORD=
KEYSTOREPASS=
DSARESTPORT=9090
DSARESTSCHEME=https
```

```

LANDINGZONE=/var/opt/teradata/dsa/postgres
VIEWPOINTURL=viewpointurl
VIEWPOINTPORT=80
VIEWPOINTTYPE=http
CAMCLUSTERENABLED=no
CAMPRIMARYURL=viewpointurl
CAMPRIMARYPORT=61616
CAMCLUSTERURL=camurl
CAMCLUSTERPORT=61616

#BARCmdline only dsainputs
BARCMDLINE_JAVA_HOME=

# Clienthandler dsainputs fields
BROKERLIST=
SERVERID=
SSLTRUSTSTOREFILE=/etc/opt/teradata/dsa/client.pem
SSLKEYSTOREFILE=/etc/opt/teradata/dsa/client-keystore.pem
SSLKEYSTOREPASSWORD=
SSLENCKEYSTOREPASSWORD=
ISMASTER=
MASTERHOSTNAME=
CBBFILEPATH=/var/opt/teradata/dsa/cbb
SERVERPORT=15401

# AXMNetbackup dsainputs fields
BACKUPAPPCLIENTNAME=

```

The following code is an example of a dsainputs file for a DSA media server:

```

BROKERLIST=tdactivemq_server:61616
CONNECTION=TDActiveMQ connection type, either tcp or ssl
SERVERPROTOCOL=tcp
SERVERID=dsams name: uname -n
BACKUPAPPCLIENTNAME=media server for third-party name, generally dsams name:
uname -n
DSCUSER=dscuser
USERID=600
SSLTRUSTSTOREFILE=/etc/opt/teradata/dsa/client.pem
SSLKEYSTOREFILE=/etc/opt/teradata/dsa/client-keystore.pem
SSLKEYSTOREPASSWORD=Client keystore password in clear text, used for ssl
on TDActiveMQ
ISMASTER=n

```

```
MASTERHOSTNAME=dsadsc server where the master server is running
CBBFILEPATH=/var/opt/teradata/dsa/cbb
```

Installing DSA Software on BAR Servers Using PUT

Prerequisite:

- Master server - Teradata ActiveMQ, Analytics Database, and PUT are installed and running on a SUSE LINUX server before installing any of the DSA component packages.
- Media server - PUT is installed and running on a SUSE LINUX server before installing any of the DSA component packages.
- For new installations, the dscuser must be created prior to installing DSC and ClientHandler. This does not apply to upgrades.

A Teradata Version Migration and Fallback (VM&F) upgrade is not required nor suggested for DSA package installation. However, if major OS changes are being applied when the DSA packages are being installed, you should use a VM&F upgrade.

1. Start PUT.
2. In the main screen, select **Install/Upgrade Software** and click **Next**.
3. In the **Configuration Mode** screen, select **Typical** and click **Next**.
4. In **Network Subnet Selection**, select **127.0.0.0 (LOOPBACK)** and click **Next**.
5. In **Select Nodes**, verify that the node name in the **Selected** list represents the BAR servers where DSA will be installed and click **Next**.
6. In the **System Information Warning** screen, click **Next**.
7. If the **System Check Found Problems** screen appears, verify that there are no issues that need attention (or correct any issues that need correcting), and click **Ignore**.
8. Accept the default selection in the **Select Spool Area for Linux Nodes** screen and click **Next**.
9. In the **Enter Source for New Packages** screen, enter or select the path `/var/opt/teradata/ccnumber/pkgs` and click **Next**.
10. In the **Media Source Confirmation** screen, enter or select the source for the new package and click **Next**.
11. In the **Group Nodes** screen, verify that the nodes displayed in the right panel have the following settings and click **Next**. If they do not have these settings, select **Modify Group** and make the necessary changes.

Server Type	Description
DSC	Node Type - DSADSC
Media	Node Type - DSAMS

12. In the **Select Packages** screen, select and add the software packages:

Server Type	Component Description
DSC	DSC
Media	<ul style="list-style-type: none"> • AXMNetbackup • ClientHandler • BARCmdline

If the machine on which you are installing packages has DSC and media server functionality, you would install the DSC, ClientHandler, AXMNetbackup, and BARCmdline packages.

13. Accept the default options for the remaining steps.

Note:

If failures are encountered during the Package Support step, review the `/tmp/put-dscschemaupgrade.log` file located on the system.

Installing BAR Portlet Software Using PUT

Prerequisite:

The DSA components must already be installed on the DSC server or DSA media server before you install BAR portlet software on the Viewpoint server.

Important:

You cannot upgrade the BAR portlet software using this procedure. Use [Installing the BARPortlets Package](#) for upgrades.

Install the BAR portlet software on the Viewpoint server. If you have two or more Viewpoint portals in a clustered environment, the BAR portlets must be deployed on all the portal instances in order for them to be part of the cluster environment. For more information, please see *Teradata® Viewpoint Installation, Configuration, and Upgrade Guide for Customers*, B035-2207.

1. Move `barportlet-xx.xx.xx.xx-1.noarch.tar.gz` into the `/var/opt/teradata/ccnumber/pkgs` directory on the Viewpoint server.
2. Start PUT.
3. In the main screen, select **Install/Upgrade Software** and click **Next**.
4. In the **Configuration Mode** screen, select **Typical** and click **Next**.
5. In **Network Subnet Selection**, select **127.0.0.0 (LOOPBACK)** and click **Next**.
6. In **Select Nodes**, verify that the node name in the **Selected** list is **localhost (LINUX)**, and click **Next**. If a warning message appears, click **Ignore**.

7. In the **System Information Warning** screen, click **Next**.
8. If the **System Check Found Problems** screen appears, verify that there are no issues that need attention (or correct any issues that need correcting), and click **Ignore**.
9. Accept the default selection in the **Select Spool Area for Linux Nodes** screen and click **Next**.
10. In the **Enter Source for New Packages** screen, enter or select the path `/var/opt/teradata/ccnumber/pkgs` and click **Next**.
11. In the **Media Source Confirmation** screen, enter or select the source for the new package and click **Next**.
12. In the **Group Nodes** screen, verify that the node displayed in the right panel has the following settings and click **Next**:
 - **System** - System0
 - **Group** - Group0
 - **Node Type** - Viewpoint
13. When the question "**If you do not designate TPA nodes, the Teradata Database software will not be installed on any nodes. Do you wish to continue?**" appears, select "**Yes, keep them as they are**" and click **Next**.
14. Select **BARPortlet** and click **Next**.
15. Accept the default options for the remaining steps.
16. To verify the BAR portlet installed, type `rpm -qa | grep 'barportlet*'`

Note:

The BAR portlet should be included in the output.

Upgrading DSA Software Using PUT

If you are making major OS changes when you are upgrading the DSA packages, use a VM&F upgrade.

Note:

A VM&F upgrade automatically reboots the server. For all other upgrades, a reboot of the server is not required.

1. Check whether the PUT version running on your system is the latest PUT release.
 - a. Find the PUT version running on your system.
 - b. Determine the latest PUT release.
2. If you do not have the latest version of PUT running on your system:
 - a. Download new PUT packages.
 - b. Upgrade PUT.
3. Create a target directory.
4. Download or copy the latest software packages. DSC, DSAPostAMQ, ClientHandler, BARCmdline, and BARPortlets must be on the same version.

Upgrade Type	Description
Base release to an eFix	Downloading Software Packages
One base release to another	<p>Copy the contents of the DSA CD to a directory on the BAR server.</p> <ol style="list-style-type: none"> Insert the Teradata staging media into the drive. Perform the mount by typing the following at the command line: <code>mount /dev /dvd /media 2.</code> Copy the files from the staging media to the server: <code>cp -r /media /var/opt /teradata/packages/DSA.</code>

5. [Ensure that the dsainputs file is available in the /tmp directory.](#)

Important:

DSCNAME must be specified for an upgrade or the repository restore from the previous version will fail. Analyze_read jobs may also fail.

6. If you are upgrading to DSA 15.11 or later, change the following parameters in the dsainputs file or the ClientHandler configuration will be corrupt:
 - Change ISNFSMASTER to ISMASTER.
 - Change NFSMASTERHOSTNAME to MASTERHOSTNAME.
7. If you are upgrading to DSA 16.20 or later, you must include the following new parameters:
 - DSARESTSCHEME
 - KEYSTOREPASS
8. Install the new release of DSA software on the BAR servers as you did initially. However, in the **Network Subnet Selection**, select the Ethernet interface where all of the BAR servers are configured.
 - [Install DSA Software on BAR master and media servers using PUT.](#)
 - [Install BAR portlet server using PUT.](#)

Additional Information

Changes and Additions

Date	Release	Description
March 2023	17.20.04.00	Added following updates: • Supported python paths
February 2022	17.20.00.03	Upgrade in TD ActiveMQ version
March 2021	17.10	Initial release

Supported Releases

This document supports the following versions of Teradata products.

- Teradata Vantage 2.2, which includes support for Analytics Database:
 - 17.05.xx
- Teradata Vantage 2.0 and Vantage 2.1, which include support for Analytics Database:
 - 17.00.xx
- Teradata Vantage 1.1, which includes support for Analytics Database:
 - 16.20 Feature Update 2
- Teradata Vantage 1.0, which includes support for Teradata Database:
 - 16.20 Feature Update 1
 - 16.20
- Teradata Database:
 - 16.10
 - 15.10
- Teradata DSA:
 - 17.10
- Teradata Viewpoint (minimum):
 - 16.50.01.00
 - 16.20.23.05
- IBM Spectrum Protect:
 - 8.1.6

Teradata Links

Link	Description
https://docs.teradata.com/	Search Teradata Documentation, customize content to your needs, and download PDFs. Customers: Log in to access Orange Books.
https://support.teradata.com	Helpful resources in one place: <ul style="list-style-type: none"> • Support requests • Account management and software downloads • Knowledge base, community, and support policies • Product documentation • Learning resources, including Teradata University
https://www.teradata.com/University/Overview	Teradata education network
https://support.teradata.com/community	Link to Teradata community

Related Documentation

Title	Publication ID
<i>Teradata® DSA Release Definition</i> Summarizes new features and fixed issues associated with the release.	B035-3154
<i>Teradata® DSA User Guide</i> Describes how to use the Teradata Data Stream Architecture (DSA) portlets and command-line interface.	B035-3150
<i>Teradata® DSA - DSE for Veritas NetBackup Installation, Configuration, and Upgrade Guide</i> Describes how to configure Data Stream Extensions software and devices.	B035-3151
<i>Teradata® DSA - DSU Installation, Configuration, and Upgrade Guide</i> Describes how to configure Data Stream Utility software and devices.	B035-3153
<i>Teradata® DSA - DSE for IBM Spectrum Protect Installation, Configuration, and Upgrade Guide</i> Describes how to configure Data Stream Extensions software and devices.	B035-3155
<i>Teradata® DSA Quick Start Guide</i> Guides you through a simple set up to verify connections.	B035-3156
<i>Teradata® Viewpoint User Guide</i> Describes the Teradata Viewpoint portal, portlets, and system administration features.	B035-2206
<i>Teradata® Viewpoint Installation, Configuration, and Upgrade Guide for Customers</i>	B035-2207

Title	Publication ID
Describes how to install Viewpoint software, configure settings, and upgrade a Teradata Viewpoint server.	
<i>Parallel Upgrade Tool (PUT) Reference</i> Describes how to install application software using PUT.	B035-5716
<i>Teradata Vantage™ - Database Administration</i> Describes how to administer the Analytics Database.	B035-1093
<i>Teradata® VantageCore VMware - Base, Advanced, Enterprise Tiers Getting Started Guide</i>	B035-5958
<i>Teradata® VantageCloud Enterprise on AWS (DIY) Installation and Administration Guide</i> Describes how to deploy and configure Teradata software components to run in the AWS public cloud.	B035-2800
<i>Teradata Vantage™ on Azure (DIY) Installation and Administration Guide</i> Describes how to deploy and configure Teradata software components to run in the Azure public cloud.	B035-2810