The product or products described in this book are licensed products of Teradata Corporation or its affiliates.

Teradata, BYNET, DBC/1012, DecisionCast, DecisionFlow, DecisionPoint, Eye logo design, InfoWise, Meta Warehouse, MyCommerce, SeeChain, SeeCommerce, SeeRisk, Teradata Decision Experts, Teradata Source Experts, WebAnalyst, and You’ve Never Seen Your Business Like This Before are trademarks or registered trademarks of Teradata Corporation or its affiliates.

Adaptec and SCSISelect are trademarks or registered trademarks of Adaptec, Inc.

AMD, Opteron and Opteron are trademarks of Advanced Micro Devices, Inc.

BakBone and NetVault are trademarks or registered trademarks of BakBone Software, Inc.

EMC, PowerPath, SRDF, and Symmetrix are registered trademarks of EMC Corporation.

GoldenGate is a trademark of GoldenGate Software, Inc.

Hewlett-Packard and HP are registered trademarks of Hewlett-Packard Company.

Intel, Pentium, and XEON are registered trademarks of Intel Corporation.

IBM, CICS, RACF, Tivoli, and z/OS are registered trademarks of International Business Machines Corporation.

Linux is a registered trademark of Linus Torvalds.

LSI and Engenio are registered trademarks of LSI Corporation.

Microsoft, Active Directory, Windows, Windows NT, and Windows Server are registered trademarks of Microsoft Corporation in the United States and other countries.

Novell and SUSE are registered trademarks of Novell, Inc., in the United States and other countries.

QLogic and SANbox are trademarks or registered trademarks of QLogic Corporation.

SAS and SAS/C are trademarks or registered trademarks of SAS Institute Inc.

SPARC is a registered trademark of SPARC International, Inc.

Sun Microsystems, Solaris, Sun, and Sun Java are trademarks or registered trademarks of Sun Microsystems, Inc., in the United States and other countries.

Symantec, NetBackup, and VERITAS are trademarks or registered trademarks of Symantec Corporation or its affiliates in the United States and other countries.

Unicode is a collective membership mark and a service mark of Unicode, Inc.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

The information contained in this document is provided on an “AS-IS” basis, without warranty of any kind, either express or implied, including the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you. In no event will Teradata Corporation be liable for any indirect, direct, special, incidental, or consequential damages, including lost profits or lost savings, even if expressly advised of the possibility of such damages.

The information contained in this document 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.

Information contained in this document may contain technical inaccuracies or typographical errors. Information may be changed or updated without notice. Teradata Corporation may also make improvements or changes in the products or services described in this information at any time without notice.

To maintain the quality of our products and services, we would like your comments on the accuracy, clarity, organization, and value of this document. Please e-mail: teradata-books@lists.teradata.com

Any comments or materials (collectively referred to as “Feedback”) sent to Teradata Corporation will be deemed non-confidential. Teradata Corporation will have no obligation of any kind with respect to Feedback and will be free to use, reproduce, disclose, exhibit, display, transform, create derivative works of, and distribute the Feedback and derivative works thereof without limitation on a royalty-free basis. Further, Teradata Corporation will be free to use any ideas, concepts, knowledge, or techniques contained in such Feedback for any purpose whatsoever, including developing, manufacturing, or marketing products or services incorporating Feedback.

Copyright © 2008-2010 by Teradata Corporation. All Rights Reserved.
Table of Contents

Start and Stop Teradata Viewpoint Services ................................................. 7
Teradata System Preparation ........................................................................... 8
  Create a Teradata User for Data Collection ............................................... 8
  Set Up Access to Console Utilities ............................................................. 8
  Grant Permissions to the Teradata User for Data Collection ................. 9
Set Up TASM and Alerting Tables ................................................................. 11
  Set Up the PC .......................................................................................... 11
  Run the Application .................................................................................... 13
Configure Viewpoint to Monitor a Teradata Database System .............. 14
  Log on to the Teradata Viewpoint Server ............................................... 14
  Add Teradata Database Systems ............................................................... 15
  Enable the Data Collectors ........................................................................ 16
  Collector Information ................................................................................ 17
  Changing a Teradata System Nickname .................................................... 22
Configure Alerts ............................................................................................ 23
  Configure Alert Delivery Settings ............................................................ 23
  Configure Alert Time Frames ................................................................... 27
  Configure Alert Action Sets ...................................................................... 27
  Configure Alert Groups ............................................................................. 28
  Migrate Existing Alerts ............................................................................ 28
  Define New Alerts .................................................................................... 29
  View Alerts ............................................................................................... 29
  Use the AlertRequest Table ..................................................................... 30
  Use the MonitorRequest Table ................................................................ 31
Install Teradata Notification Service for Windows .................................. 32
  Software Dependencies ............................................................................ 33
  Prerequisites ............................................................................................. 33
  Install Teradata Notification Service ....................................................... 33
  Configure Teradata Notification Service .................................................... 33
  Configure TVI Logging ............................................................................. 34
  Service Control .......................................................................................... 34
Teradata Manager Feature Equivalence ..................................................... 35
Uninstall Teradata Manager .......................................................................... 35
Configure Managed Servers ......................................................................... 38
Configure Viewpoint LDAP ......................................................................... 39
  Prerequisites ............................................................................................. 40
  Definitions ................................................................................................. 40
  Before You Begin ....................................................................................... 41
  Determine LDAP Configuration Mode ...................................................... 42
  LDAP Configuration ................................................................................. 44
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Over SSL (LDAPS)</td>
<td>48</td>
</tr>
<tr>
<td>Enable Debug Logging</td>
<td>48</td>
</tr>
<tr>
<td><strong>Add Teradata Viewpoint Roles</strong></td>
<td>49</td>
</tr>
<tr>
<td><strong>Add Teradata Viewpoint Users</strong></td>
<td>50</td>
</tr>
<tr>
<td><strong>Configure Teradata Viewpoint Security</strong></td>
<td>50</td>
</tr>
<tr>
<td>- Control Access to Portlets</td>
<td>50</td>
</tr>
<tr>
<td>- Control Access within Portlets</td>
<td>50</td>
</tr>
<tr>
<td><strong>Configure Viewpoint to Log to TVI</strong></td>
<td>50</td>
</tr>
<tr>
<td><strong>Back Up Teradata Viewpoint Databases</strong></td>
<td>51</td>
</tr>
<tr>
<td>- Restore a Teradata Viewpoint Database</td>
<td>51</td>
</tr>
<tr>
<td><strong>Change the Session Timeout</strong></td>
<td>52</td>
</tr>
<tr>
<td><strong>Set the Default Locale</strong></td>
<td>52</td>
</tr>
<tr>
<td><strong>Reset the Admin User Password</strong></td>
<td>53</td>
</tr>
<tr>
<td><strong>Ports Used by Teradata Viewpoint</strong></td>
<td>53</td>
</tr>
<tr>
<td><strong>Set Teradata Viewpoint Server Time</strong></td>
<td>53</td>
</tr>
<tr>
<td><strong>Configure NTP Time Synchronization</strong></td>
<td>54</td>
</tr>
<tr>
<td><strong>Teradata Viewpoint Clustering</strong></td>
<td>55</td>
</tr>
<tr>
<td>- Cluster Configurations</td>
<td>55</td>
</tr>
<tr>
<td>- Failure Scenarios</td>
<td>59</td>
</tr>
<tr>
<td>- Create a Teradata Viewpoint Cluster</td>
<td>62</td>
</tr>
<tr>
<td>- Add Additional Teradata Viewpoint Servers to the Cluster</td>
<td>68</td>
</tr>
<tr>
<td>- Promote the Standby Cache Database</td>
<td>69</td>
</tr>
<tr>
<td>- Upgrade PostgreSQL to Enable Clustering</td>
<td>70</td>
</tr>
<tr>
<td>- Additional Considerations</td>
<td>72</td>
</tr>
<tr>
<td><strong>Configure Teradata Viewpoint SSL Support</strong></td>
<td>76</td>
</tr>
<tr>
<td>- Configure Viewpoint for SSL support</td>
<td>76</td>
</tr>
<tr>
<td>[Optional] Configure All Viewpoint Access to be Over SSL</td>
<td>77</td>
</tr>
<tr>
<td>- Create a Self-Signed Certificate</td>
<td>77</td>
</tr>
<tr>
<td>- Create a Certificate Signing Request</td>
<td>78</td>
</tr>
<tr>
<td>- Import a Certificate</td>
<td>78</td>
</tr>
<tr>
<td>- Install a CA Certificate in Cacerts Keystore</td>
<td>78</td>
</tr>
<tr>
<td><strong>Teradata Viewpoint Properties</strong></td>
<td>80</td>
</tr>
<tr>
<td>- Available Properties</td>
<td>80</td>
</tr>
<tr>
<td>- Accessing Properties</td>
<td>81</td>
</tr>
<tr>
<td><strong>Client-PC Recommendations</strong></td>
<td>84</td>
</tr>
<tr>
<td>- Browser Requirements</td>
<td>84</td>
</tr>
<tr>
<td>- Recommendations by PC Class</td>
<td>84</td>
</tr>
<tr>
<td><strong>Portlet Load Times</strong></td>
<td>84</td>
</tr>
<tr>
<td>- Low impact</td>
<td>85</td>
</tr>
<tr>
<td>- Medium impact</td>
<td>85</td>
</tr>
<tr>
<td>- High impact</td>
<td>85</td>
</tr>
<tr>
<td><strong>Install Teradata Viewpoint for Electronic Software Distribution</strong></td>
<td>86</td>
</tr>
<tr>
<td><strong>Upgrade to Teradata Viewpoint 13.10.xx.xx</strong></td>
<td>86</td>
</tr>
</tbody>
</table>
Upgrade Teradata Viewpoint ............................................................. 86
Download the Teradata Viewpoint 13.10 Software............................ 86
Run the Install Script ..................................................................... 87
Install and Uninstall Teradata Viewpoint Packages Manually .......... 88
Apply Customizations .................................................................. 90
Set Up New Collectors ................................................................. 90
Apply LDAP Customizations ...................................................... 90
Audience
This document is intended for Teradata Customer Services, Teradata Professional Services, and customers for configuring Teradata Viewpoint software.

Teradata Viewpoint Server
When the Teradata Viewpoint server arrives at the customer site, it has the necessary software installed and is ready to add Teradata Database systems to monitor and for users to access the portal. The Teradata Viewpoint server is ready if the login screen appears in the browser.
Start and Stop Teradata Viewpoint Services

Teradata Viewpoint 13.10 and later includes the following separate services:

- **viewpoint**
  The Teradata Viewpoint portal that provides web browser access.

- **dcs**
  The Data Collection Service that monitors and collects data from Teradata systems.

- **tmsmonitor**
  The Teradata Managed Server Monitor that monitors performance of the Teradata Viewpoint server.

- **camactivemq**
  The Teradata Alerting Message Service that allows for message exchange between the Teradata Alerting components.

- **camalert**
  The Teradata Alerting Alert Service that processes events and alerts.

- **camnotification**
  The Teradata Alerting Notification Service that provides SNMP and SMTP notifications.

Each service has an init script on the Teradata Viewpoint server located in the /etc/init.d directory. The init scripts support the following command arguments:

- **start** - Starts the service. If the service is already running, a new instance is not started.

- **stop** - Stops the service. The script succeeds even when the service is not running.

- **restart** - Stops and starts the service.

- **status** - Checks if the service is currently running.

For example, to start the Teradata Viewpoint portal, type:

/etc/init.d/viewpoint start
To stop the **Teradata Viewpoint** portal:

```
/etc/init.d/viewpoint stop
```

To restart the Data Collection Service:

```
/etc/init.d/dcs restart
```

To check if the Teradata Managed Server Monitor is running:

```
/etc/init.d/tmsmonitor status
```

**Teradata System Preparation**

To monitor a Teradata Database system, **Teradata Viewpoint** requires a Teradata system login with a set of specific permissions. SQL commands can be used to create a user and grant permissions.

The Teradata user, used by **Teradata Viewpoint**, must have sufficient spool space to allow **Teradata Viewpoint** to issue monitoring queries. Also, perm space is required by the Lock Information collector that is used by the Lock Viewer portlet starting with **Teradata Viewpoint** 13.0.1.

The user can be an existing user. The username and the password is called `viewpoint` in the following procedures as an example.

**Create a Teradata User for Data Collection**

Create a Teradata user for **Teradata Viewpoint** Data Collection.

1. Type the following command, where `<perm space>` and `<spool space>` are the respective perm space and spool space to allocate the user:

```
create user viewpoint as perm=<perm space>, spool=<spool space> password=viewpoint;
```

**Set Up Access to Console Utilities**

1. Do one of the following:

   o If Teradata Manager is not monitoring the target Teradata Database system, type:

```
create user console as perm=50000, spool=50000, account='$H-remote-console-use', password=console, fallback;
replace macro console.dbscontrol as ();
replace macro console.aborthost as ();
replace macro console.ampload as ();
replace macro console.config as ();
replace macro console.checktableb as ();
replace macro console.dumplocklog as ();
replace macro console.ferret as ();
replace macro console.xgtwglobal as ();
replace macro console.lokdisp as ();
```
If Teradata Manager is not monitoring the target Teradata Database system, or if Teradata Manager DBSSetup 7.x or earlier is the latest version run against the target Teradata System, run the following commands to create the default macros used to clean up the DBQL and TASM log tables:

```sql
REPLACE MACRO dbcmngr.dcDBQLDeleteOld (AgeDays INTEGER) AS ( DELETE dbc.DBQLSummaryTbl WHERE CAST(CollectTimeStamp AS DATE) <= (DATE - :AgeDays); DELETE dbc.DBQLStepTbl WHERE CAST(CollectTimeStamp AS DATE) <= (DATE - :AgeDays); DELETE dbc.DBQLogTbl WHERE CAST(CollectTimeStamp AS DATE) <= (DATE - :AgeDays); DELETE dbc.DBQLObjTbl WHERE CAST(CollectTimeStamp AS DATE) <= (DATE - :AgeDays); DELETE dbc.DBQLExplainTbl WHERE CAST(CollectTimeStamp AS DATE) <= (DATE - :AgeDays); DELETE dbc.DBQLSqlTbl WHERE CAST(CollectTimeStamp AS DATE) <= (DATE - :AgeDays); );
REPLACE MACRO dbcmngr.dcTDWMDeleteOld (AgeDays INTEGER) AS ( DELETE dbc.TDWMSummaryLog WHERE CAST(BufferTS AS DATE) <= (DATE - :AgeDays); DELETE dbc.TDWMEventLog WHERE CAST(BufferTS AS DATE) <= (DATE - :AgeDays); DELETE dbc.TDWMExceptionLog WHERE CAST(BufferTS AS DATE) <= (DATE - :AgeDays); );
```

If Teradata Manager is monitoring the target Teradata Database system, go to Grant Permissions to the Teradata User for Data Collection on page 9.

**Grant Permissions to the Teradata User for Data Collection**

Grant permissions to the Teradata user for Teradata Viewpoint Data Collection.

1. Do one of the following:
   - If the tdwm database exists on the target Teradata Database system, type the following command, then go to step 2:
     ```sql
     grant select on TDWM to viewpoint;
     ```
   - If the tdwm database does not exist, go to step 2.

2. Type the following commands:
   ```sql
   grant monitor to viewpoint;
   grant select on DBC to viewpoint;
   grant select, delete on dbcmngr to viewpoint;
   grant exec on console.ampload to viewpoint;
   ```
grant exec on console.dbscontrol to viewpoint;
grant exec on console.aborthost to viewpoint;
grant exec on console.config to viewpoint;
grant exec on console.checktableb to viewpoint;
grant exec on console.dumplocklog to viewpoint;
grant exec on console.ferret to viewpoint;
grant exec on console.xgtwglobal to viewpoint;
grant exec on console.lokdisp to viewpoint;
grant exec on console.cnsscons to viewpoint;
grant exec on console.schmon to viewpoint;
grant exec on console.qryconfig to viewpoint;
grant exec on console.qrysessn to viewpoint;
grant exec on console.rcvmanager to viewpoint;
grant exec on console.showlocks to viewpoint;
grant exec on console.vprocmngmner to viewpoint;
grant exec on console.tdwmdmp to viewpoint;

3. If the automatic rights granted to the viewpoint user were revoked, run the following commands:

   grant create table, drop table on viewpoint to viewpoint;
   grant select, insert on viewpoint to viewpoint;

4. To use the Log Table Clean Up functionality, run the following commands:

   a. For all databases, type:

      grant exec on dcmngr to viewpoint;
      grant delete on DBC.ResUsageSpma to viewpoint;
      grant delete on DBC.ResUsageSvpr to viewpoint;
      grant delete on DBC.ResUsageShst to viewpoint;
      grant delete on DBC.ResUsageIpma to viewpoint;
      grant delete on DBC.ResUsageIvpr to viewpoint;
      grant delete on DBC.ResUsageScpu to viewpoint;
      grant delete on DBC.ResUsageSldv to viewpoint;
      grant delete on DBC.AccLogTbl to viewpoint;
      grant delete on DBC.EventLog to viewpoint;
      grant delete on DBC.SW_Event_Log to viewpoint;
      grant select, delete on dbc.DBQLLogTbl TO dcmngr with grant option;
      grant select, delete on dbc.DBQLSummaryTbl TO dcmngr with grant option;
      grant select, delete on dbc.DBQLStepTbl TO dcmngr with grant option;
      grant select, delete on dbc.DBQLObjTbl TO dcmngr with grant option;
      grant select, delete on dbc.DBQLExplainTbl TO dcmngr with grant option;
      grant select, delete on dbc.DBQLSqlTbl TO dcmngr with grant option;
      grant select, delete on dbc.TDWMSummaryLog TO dcmngr with grant option;
      grant select, delete on dbc.TDWMExceptionLog TO dcmngr with grant option;
      grant select, delete on dbc.TDWMEventLog TO dcmngr with grant option;

   b. For Teradata V2R6, type:

      grant delete on DBC.ResUsageSobj to viewpoint;
c. For Teradata databases 12 or later, type:

```sql
grant delete on DBC.ResUsageSawt to viewpoint;
grant delete on DBC.ResUsageSps to viewpoint;
grant delete on DBC.ResUsageSpdsk to viewpoint;
grant delete on DBC.ResUsageSvdsk to viewpoint;
```

## Set Up TASM and Alerting Tables

To monitor a Teradata 12 or Teradata 13 database with **Teradata Viewpoint** 13.10, you must set up TASM and Alerting tables, using one of the following:

- The Teradata Manager setup application
- A Windows setup application, either downloaded from Teradata Software Server or copied from the Teradata Notification Service for Windows media.

If you have the Teradata Manager application available, perform the setup using the Database setup application. To setup tables on Teradata 12, use Teradata Manager 12.0. For Teradata 13, use Teradata Manager 13.0.

Download the Windows setup application in the following cases:

- When implementing TASM on an existing Teradata 12.0 or 13.0
- When running V2R6.2 with TASM, and migrating to Teradata 12.0
- When running Teradata 12.0 with TASM, and migrating to Teradata 13.0
- When installing a new Teradata 12.0 or 13.0 with TASM

From the Teradata Software server, download the Windows setup application that matches your version of the Teradata Database. The zip files including the application and the supporting files are named:

- `dbsetup12vp__Windows_i386.12.03.00.00.zip` for **Teradata 12**
- `dbsetup13vp__Windows_i386.13.03.00.00.zip` for **Teradata 13**

## Set Up the PC

1. Install the 32 bit client communication Windows packages to connect to the database. The following are the required packages:

   - Teradata Call-Level Interface version 2 (CLIV2) for Network Attached Systems
   - Shared ICU Libraries (TDICU) for Teradata
o Teradata GSS Client (TeraGSS)

The package version must match the version of the DBSSetup application: TTU 12 for dbsetup12vp, and TTU13 for dbsetup13vp.

2. Verify that the PC can communicate with the Teradata Database system by entering the PING command from a Windows DOS window.

For example: PING sscop1, where sss is the Teradata Database name. The system returns the message: Reply from xxx.xxx.xxx.xxx, where xxx.xxx.xxx.xxx is the IP address of the database.

Do one of the following:

o If the PING command does not receive a response from the database, contact your Network Administrator.

Note: An incorrect or missing IP address and system name in the HOSTS file on the PC can cause a failure to communicate with the Teradata Database. The HOSTS file is located in the directory where Windows is installed, under system32\drivers\etc.

o If Domain Name Services (DNS) is not used, check that the HOSTS file contains entries similar to the following: xxx.xxx.xxx.xxx sscop1 where xxx.xxx.xxx.xxx is the functional IP address and sss is the Teradata Database name.

o If DNS is used, contact your Network Administrator for help with system identification.

3. Move the DBSSetup .zip file to an empty folder on the PC.

4. Extract the content of the .zip file to the same folder.
Run the Application

1. In the folder where you extracted the .zip file, double-click dbsetup12vp.exe or dbsetup13vp.exe.

   The Database Setup window appears.

2. In the **System Name** field, enter the TDPID of the database where you want to set up the tables.

3. In the **Super User** and **Super User Password** fields, enter the name and password of a user who has permissions to create tables and grant access to existing DBC tables.

   DBC is the recommended user.

4. In the **Perm Space** field, enter appropriate values. The default values of 50 MB and 100 MB are likely sufficient.

5. [Optional] If you are migrating from a prior version of TASM (6.2 to 12.0 or 13.0, or 12.0 to 13.0), select the **Migrate TDWM Database** check box.

6. Click **OK** and let the application run to completion.
Depending on the load on the database, the setup application typically takes between 2 and 10 minutes. On a heavily loaded system, the setup can take longer.

**Note:** If the setup application has already been run, a confirmation message appears. Rerunning the setup program does not cause any data to be lost.

7. If an error message appears, review the output and inspect any reported errors.

   Typical errors are results of trying to delete items that do not exist, in preparation for the setup. You can find any errors by searching for `failed`.

8. Close the application.

9. Delete the application and .zip file from your system.


**Configure Viewpoint to Monitor a Teradata Database System**

**Log on to the Teradata Viewpoint Server**

1. Open a browser.

   **Teradata Viewpoint** 13.10 is compatible with the following browsers:
   - Mozilla Firefox version 3.5
   - Internet Explorer version 7 and 6

2. Enter the host name or IP address of the **Teradata Viewpoint** server.

   For example: `http://viewpoint`

3. Log on to **Teradata Viewpoint** with the username of `admin` and the password of `teradata` (default).

   The password can be changed at any time.
Add Teradata Database Systems

Add a Teradata Database system using the Teradata Systems admin portlet. Teradata Database systems must be added to the Teradata Systems admin portlet before you can configure the data collectors to monitor the database.

The following procedure is more fully described in Teradata Viewpoint Help.

1. Click **Admin > Teradata Systems**.
   The **TERADATA SYSTEMS** view appears.

2. Click **Add a System**.

3. Enter a **SYSTEM NICKNAME** (8 characters or less) for the Teradata Database system.

4. [Optional] Select **System Enabled** to activate the Teradata Database system for monitoring.

5. In the **TDPID** field, enter the TDPID of your Teradata Database system.

   Using the TDPID name allows **Teradata Viewpoint** to connect to multiple gateways. IP addresses are not recommended unless the system is an SMP. Do not use the Teradata Query Directory host name or IP address.

   If the TDPID cop addresses are not in DNS, define them in the HOSTS file located in the `/etc/hosts` directory on the Viewpoint server.

6. In the **LOGIN** section, create the user logins.

   a. Enter a user **Name**.

   b. Enter a **Password**.

   c. [Optional] Enter an **Account string** to differentiate the user account.

   d. Click + to add additional login accounts.

   There is no limit to the number of login accounts associated with a Teradata Database system. Multiple logins are useful for running canary queries using a specific user and account string.

   The user login must have specific permissions. See *Grant Permissions to the Teradata User for Data Collection* on page 9.

   e. [Optional] Enter a **Password** for the tdwm user.
This user login is used by the Workload Designer portlet to edit rule sets and to issue activate requests. It cannot be used by any data collectors.

7. [Optional] In the **COLLECTORS** section, select the **Turn on all collectors with default settings** checkbox to enable the default collectors for the new system.

8. In the **CHARACTER SET** section, set the session and monitor default character sets.

   The session character set defaults to UTF8; the monitor character set defaults to ASCII.

9. Click **Apply**.


    Viewpoint uses the System Heartbeat canary query to determine if the Teradata system is operational. You can also enable this query by selecting **Turn on all collectors with default settings** when creating a new system.

**Enable the Data Collectors**

Data collection must be enabled for each Teradata Database system you want to monitor.

To enable or disable a **Teradata Viewpoint** Data Collector, use the Viewpoint Teradata Systems portlet. For more information, see **Teradata Viewpoint** Help.

The **Teradata Viewpoint** Data Collection Service (DCS) connects to the Teradata Database system through the customer LAN and accesses the appropriate data sources through the Teradata JDBC driver. Generally, the default values can be used. In fact, using the default values initially and then fine tuning them at a later time is recommended. The setup must still be completed to enable the collectors if the **Turn on all collectors with default settings** checkbox was not selected when configuring the new system.

Set data collection parameters or save defaults for:

- Account Info
- Alert Request
- AWT Info
Configure Viewpoint to Monitor a Teradata Database System

- Database Space
- Disk Space
- Lock Info
- Query Count
- Resource Usage
- Sessions
- System Stats
- Table Space
- TASM Config
- TASM Distribution
- TASM Exception
- TASM State
- TASM Summary

Collector Information

Following is a description of each collector, its impact on a Teradata Database system, and how **Teradata Viewpoint** uses the data collected.

**Account Info**

The Account Info collector queries the AccountInfo table in the DBC database and collects a list of account strings. The Queries portlets use this data to list the available account strings for the Change Priority function. The Workload Designer portlet uses this data to provide a list of available account strings when creating classification criteria.

**Alert Request**

The Alert Request data collector monitors the dbcmngr.AlertRequest table for incoming alert requests. If the table row contains valid data, the contents are forwarded to the Alert Service to process the alert action.

The Alert Request data collector also monitors the dbcmngr.MonitorRequest table. Any Teradata Database utility or user program can request **Teradata Viewpoint** to monitor its progress, by inserting rows into the dbcmngr.MonitorRequest table. Each row includes fields that indicate the date and time by which the next row is inserted. If a new row is not inserted...
before the specified date and time, the Alert Request collector forwards the contents to the Alert Service to process the alert action.

**AWT Info**

AMP Worker Task (AWT) information is collected by running `ampload -a` through the Teradata CONSOLE partition.

The System Health, Node Resources, Metric Analysis, Capacity Heatmap, Metrics Graph, and Today’s Statistics portlets use the AWT Info collector. If this collector is not enabled, these portlets do not display AWT information.

The AWT Info collector is also required for alerts that depend on AWT information.

**Database Space**

The Database Space collector queries the DiskSpace and Databases views in the DBC database to collect database space usage metrics.

The Space Usage, Capacity Heatmap, and Metrics Graph portlets use the data collected by the Database Space collector. If this collector is not enabled, these portlets do not display up-to-date database space data. The Workload Designer portlet uses this data to provide a list of databases when creating classification criteria.

The Database Space collector is required for Database Space alerting.

**Disk Space**

The Disk Space collector queries the DiskSpace view in the DBC database to collect disk space usage data.

The System Health, Metrics Analysis, Capacity Heatmap, and Metrics Graph portlets use the data collected by the Disk Space collector. If this collector is not enabled, these portlets do not display up-to-date disk space data.

**Lock Info**

The Lock Info collector uses Locking Logger (a database utility) to capture a snapshot of lock information and stores this data in the PostgreSQL database. The Lock Viewer portlet uses the data collected by the Lock Info collector. Therefore, the portlet only displays updated lock data for the period of time when the collector is enabled.

For the Lock Info collector to run, the LockLogger flag in DBSCControl on the Teradata system must be set to TRUE.
Query Count

Query count and query log data are collected by querying the DBQLogTbl and DBQLSummaryTbl tables in the Teradata DBC database. For a query to be counted, it must be logged to the DBQLogTbl or DBQLSummaryTbl table by enabling query logging in the Teradata Database. When enabling query logging, it is important to manage the size of the DBQL tables. Clearing the DBQL tables nightly is recommended. The queries performed by Teradata Viewpoint against DBQL require an all-row scan. If the size of the DBQL tables is not managed, queries against them can cause unnecessary use of Teradata Database resources. Teradata Professional Services has a Data Collection and Capacity Planning offering that includes the movement and cleanup of DBQL data on a nightly basis. If DBQL is not cleaned up nightly, using the Query Count collector is not recommended.

The Productivity portlet uses query count data to show total query counts and query counts by application on an hourly basis. The Today's Statistics portlet also uses the data to show query counts and query log data for the last hour of collected data, grouped by duration. The Capacity Heatmap and the Metrics Graph portlets show query count and query log data collected over the hour. The Workload Designer portlet uses this data to populate several select lists when creating classification criteria. The default collection rate for querying DBQL is 1 hour. To get the portlets to show more up-to-date query counts, the collection frequency can be increased, at the cost of using up more Teradata Database resources to query DBQL more frequently.

Resource Usage

The Resource Usage collector queries the ResUsageSPMA and ResUsageIPMA tables in the DBC database to collect node resource usage data. The collector also queries the ResUsageSVPR table in the DBC database to collect vproc resource usage data.

The recommended collection is the rate that this information is logged to these tables in Teradata. You can set this rate in the Monitor Rates section of the Teradata Systems admin portlet.

This resource usage data is used by the Metrics Analysis, Capacity Heatmap, Metrics Graph, and Node Resources portlets.
**Sessions**

Session data is collected by querying the Teradata MONITOR partition using the PM/API. Session-level statistics are collected in memory by Teradata Database at a configurable sample rate. The default option in *Teradata Viewpoint* collects session data at the same rate as sampled by Teradata Database. Collecting session data more frequently than the session sample rate in Teradata Database results in duplicate data being collected and wasted CPU. You can change the Teradata Database session sample rate in the Monitor Rates section of the Teradata Systems admin portlet.

My Queries, Query Monitor, and Workload Monitor display session data. The data is also used for the Active Sessions metric in the System Health, Metrics Analysis, Capacity Heatmap, and Metrics Graph portlets. If this collector is not enabled, the Queries portlets always display zero sessions. If this collector is enabled and then disabled, the Queries portlets display stale session data. The Session collector and the System Statistics collector must be enabled for the Active Sessions metric to display data in the System Health, Capacity Heatmap, and Metrics Graph portlets.

The Sessions collector is required for Session alerting.

**System Stats**

System statistics data is collected by querying the Teradata MONITOR partition using the PM/API. Physical and virtual resource statistics are collected in memory by Teradata Database at a configurable sample rate. The default option in *Teradata Viewpoint* collects system statistics data at the same rate as sampled by the Teradata Database. Collecting system statistics data more frequently than the resource sample rate in Teradata Database, results in duplicate data being collected and wasted CPU. You can change the Teradata Database resource sample rate in the Monitor Rates section of the Teradata Systems admin portlet.

The System Health, Node Resources, Metrics Analysis, Capacity Heatmap, Metrics Graph, Today's Statistics, Workload Health, and Workload Monitor portlets use the System Stats collector. If this collector is not enabled, these portlets do not display system statistics data. The Workload Designer portlet uses node and vproc counts from this collector to assist with the creation of rule sets.

The System Stats collector is required for System, Node, Vproc, and System Health alerting.
Table Space
The Table Space collector queries the TableSize view in the DBC database to collect table space usage metrics.

The Space Usage, Capacity Heatmap, and Metrics Graph portlets use the data collected by the Table Space collector. If this collector is not enabled, these portlets do not display up-to-date table space data. The Workload Designer portlet uses this data to provide a list of tables when creating classification criteria.

TASM Config
The TASM Config collector collects configuration information about the TDWM version and the active rule set in Teradata from the TDWM database in Teradata. This collector replaces the Workload collector that was available in 13.0.1. This data is used by My Queries, Query Monitor, Workload Health, Workload Monitor, and Workload Designer.

The TASM Config collector needs to be enabled to use Workload Designer for a new Teradata System. If the collector is not enabled, the TDWM version information is not collected, and the Teradata System does not appear in the list of available Teradata Systems in Workload Designer.

TASM Distribution
The TASM Distribution collector collects CPU distribution by workload, by running the schmon –M –p utility through the Teradata CONSOLE partition.

The collected data is used by the Workload Monitor portlet.

TASM Exception
The TASM Exception collector collects TASM Exception data from the DBC.TDWMExceptionLog table. The collected data is used by the Workload Monitor portlet.
**TASM State**

The TASM State collector collects system regulation data for Teradata Database version 12.00 and later. For Teradata Database systems earlier than version 12.00, the TASM State collector collects period information from DBC.TDWMSummaryLog. This collector also uses PM/API to determine the active rule set. The data collected is used by the My Queries, Query Monitor, Workload Designer, Workload Health, and Workload Monitor portlets.

You must enable both the TASM Config and TASM State collectors to be able to associate the active workload name with the session information displayed in these portlets.

**TASM Summary**

The TASM Summary collector collects data for each active workload in the Teradata Database. It sends queries to the Teradata MONITOR partition using PM/API. The summary data is used by the Workload Health and Workload Monitor portlets.

**Changing a Teradata System Nickname**

To change the nickname associated with a Teradata Database system in **Teradata Viewpoint**:

1. Stop the Viewpoint Portal and the Data Collection Service (DCS).
2. Run the dcsadmin command:
   
   `/opt/teradata/dcs/bin/dcsadmin.sh`
3. Type `renamesystem` and press **Enter**.
4. Type the number of the system to rename and press **Enter**.
5. Type the new name and press **Enter**.
6. Verify that the new name is correct. If the name is correct, type **Y** and press **Enter** to confirm. If the name is incorrect, type **N** to cancel and return to step 3.
   
   The system is renamed.
7. Type `quit` and press **Enter** to exit the dcsadmin shell.
8. Restart the Viewpoint Portal and the DCS.
Configure Alerts

To configure alerts in Teradata Viewpoint, perform the following steps:

1. Configure the wanted alert delivery mechanisms using the Alert Setup portlet.
2. [Optional] Migrate alerts from previous Teradata Manager alerts, using the Teradata Systems portlet.
3. Define alert action sets and alert groups using the Alert Setup portlet.
5. View alerts in the Alert Viewer portlet.

Configure Alert Delivery Settings

Configure Email Alerts

You can configure the Alert Service to send alert notifications by email.

The following procedure is more fully described in Teradata Viewpoint Help.

1. From the Admin menu, click Alert Setup.
   
   The ALERT SETUP portlet appears.
2. From the SETUP OPTIONS list, click Delivery Settings.
3. From the DELIVERY TYPES list, click Email.
4. Under SMTP Host, type the host address of the outgoing (SMTP) email server.
5. In the Reply-to box, type the email address to use as the Reply-to address in delivered alert email messages.
6. To test your email delivery settings, type a valid recipient email address in the Test Recipient box and click Test.

Configure SNMP Alerts

You can configure the Alert Service to deliver alert notifications to third-party management applications using SNMP.

The following procedure is more fully described in Teradata Viewpoint Help.
Configure Alerts

1. From the **Admin** menu, click **Alert Setup**.
   The **ALERT SETUP** portlet appears.

2. From the **SETUP OPTIONS** list, click **Delivery Settings**.

3. From the **DELIVERY TYPES** list, click **SNMP**.

4. To add an SNMP configuration, click **+**.

5. In the **Configuration Name** box, type a name for the SNMP configuration.

6. In the **Destination** box, type the IP address or host name of the destination for SNMP alert notifications.

7. In the **Community** box, type a name for the SNMP community.
   The default is **public**.

8. To test the SNMP configuration on the specified destination host or hosts, click **Test**.

**Teradata SNMP MIB**

The Teradata Alerting SNMP MIB (Management Information Base) is available in:

/opt/teradata/cam/notification/config/teradataCamMib.txt

SNMP Object Identifiers (OIDs) for Teradata Alerting are defined under:

iso.org.dod.internet.private.enterprises.teradata.td-products.tdcam

The Teradata Alerting SNMP MIB defines a single trap, **tdCamAlertTrap**, identified as **trap 303** under the tdcam OID.

**Configure BTEQ Alerts**

You can configure the Alert Service to run BTEQ alert actions.

**Prerequisites**

The Teradata Notification Service must be installed and running on a Windows server.

**BTEQ Configuration**

The following procedure is more fully described in **Teradata Viewpoint Help**.
Configure Alerts

1. From the **Admin** menu, click **Alert Setup**.
   The **ALERT SETUP** portlet appears.

2. From the **SETUP OPTIONS** list, click **Delivery Settings**.

3. From the **DELIVERY TYPES** list, click **BTEQ**.

4. To add a BTEQ configuration, click `+`.

5. In the **TDPID** box, type the TDPID of the Teradata Database you want to log on to.
   
   **Note**: The TDPID must match the configuration in the Teradata Systems portlet.

6. In the boxes, type a valid **Username** and **Password** to use to log on to the specified TDPID.

7. To test the BTEQ configuration on the specified TDPID, click **Test**.
   Teradata Notification Service performs a test log on to the specified TDPID.

**Installing BTEQ Scripts**

The Teradata Alerting software runs BTEQ scripts on the server where the Teradata Notification Service software is installed. Place the BTEQ scripts in the following folder:

\[Install Folder\]\Teradata\Client\13.0\Teradata Notification Service\sql

When the Teradata Notification Service is running, it monitors the sql folder every 15 seconds. The Alert Setup portlet reflects any changes to the directory contents.

**About Running BTEQ Scripts**

When migrating from Teradata Manager alerts to Teradata Alerting, be aware of the following differences:

<table>
<thead>
<tr>
<th></th>
<th>Teradata Alerting</th>
<th>Teradata Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Program</strong></td>
<td>BTEQ</td>
<td>DMTEQ</td>
</tr>
<tr>
<td><strong>Supports</strong> .logon syntax</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Where to configure logon credentials</strong></td>
<td>Alert Setup portlet, in the BTEQ Delivery Settings view</td>
<td>Teradata Manager Administration, in the Systems window</td>
</tr>
<tr>
<td><strong>Script file location</strong></td>
<td>[Install folder]\Teradata\Client\13.0\Teradata Notification Service\sql</td>
<td>[Install folder]\Teradata\Teradata Manager 13.0\secure</td>
</tr>
</tbody>
</table>
Note: Ensure that any SQL scripts you want to use with Teradata Alerting do not contain the `.logon` command, as BTEQ does not support it. Logon credentials must be defined in the Alert Setup portlet.

Teradata Alerting submits the following BTEQ commands to create a Teradata session and to run a script file when performing a BTEQ alert action:

- `.LOGON`. The TDPID, username, password, and account credentials defined in the Alert Setup portlet.
- `.LOGMECH`. If you defined a Logmech Name in the Alert Setup portlet.
- `.LOGDATA`. If you defined Logmech Name and Logmech Data in the Alert Setup portlet.
- `.RUN FILE`. The name of the script file selected in the Alert Setup portlet.
- `.QUIT`
Configure Alert Time Frames

You can schedule alert actions to run during one or more of the following time frames:

- Core hours
- Evening hours
- Weekend hours

The following procedure is more fully described in Teradata Viewpoint Help.

1. From the Admin menu, click Alert Setup.
   - The ALERT SETUP portlet appears.
2. From the SETUP OPTIONS list, click Alert Presets.
3. From the PRESET OPTIONS list, click Core Hours.
4. Define time frames for core, evening, and weekend hours.

Configure Alert Action Sets

When you have configured the alert delivery settings, configure the alert actions you want to use when an alert occurs.

Alert actions can be combined into action sets. An action set allows you to run multiple alert actions in a single operation.

The following procedure is more fully described in Teradata Viewpoint Help.

1. From the Admin menu, click Alert Setup.
   - The ALERT SETUP portlet appears.
2. From the SETUP OPTIONS list, click Alert Presets.
3. From the PRESET OPTIONS list, click Action Sets.
4. To add an action set, click +.
5. Under Times, select check boxes for the hours of operation during which you want the action set to run.
Configure Alerts

6. Under **Actions**, select any of the following actions by selecting the appropriate check box:
   - Include in alert log
   - Send to person
   - SNMP
   - BTEQ
   - Run a program

   **Note**: You must configure the delivery settings for an alert delivery mechanism before that option is available.

Configure Alert Groups

When you have configured the alert delivery settings and the action sets, you can configure the alert groups you want to use when an alert occurs. A group allows you to run multiple action sets in a single operation.

The following procedure is more fully described in *Teradata Viewpoint* Help.

1. From the **Admin** menu, click **Alert Setup**.
   - The **ALERT SETUP** portlet appears.

2. From the **SETUP OPTIONS** list, click **Alert Presets**.

3. From the **PRESET OPTIONS** list, click **Groups**.

4. To add an action set, click +.

5. In the **Group Name** box, type a name for the group.

6. Select the action sets you want to include in the group.

Migrate Existing Alerts

When you have configured a Teradata System in *Teradata Viewpoint*, you can migrate all of the alerts from Teradata Manager to *Teradata Viewpoint*. The currently applied alert policy is migrated.

**Note**: Migrate existing alerts before you create any new alerts. The migration feature is disabled if any alerts are defined for a Teradata System.

The following procedure is more fully described in *Teradata Viewpoint* Help.
Configure Alerts

1. From the **Admin** menu, click **Teradata Systems**.
   
The **TERADATA SYSTEMS** portlet appears.

2. Select system, alerts, and alert type.

3. Under **ALERTS**, click **Migrate Alerts**.

4. Enter a **username** and **password** that has permission to read data from the AlertAction, AlertEvent, and AlertLevel tables in the dbcmngr database on the Teradata System.

**Define New Alerts**

You can configure alerts for seven types of data; system, node, vproc, database space, session, canary queries, and system health. Each alert contains rules that define when the alert is triggered and what actions occur when the rules are true.

The following procedure is more fully described in *Teradata Viewpoint* Help.

1. From the **Admin** menu, click **Teradata Systems**.
   
The **TERADATA SYSTEMS** portlet appears.

2. Select system, alerts, and alert type.

3. Enter the number of minutes in the **Only trigger if above is met for** box.
   
The alert triggers if the rule is true for the amount of minutes you entered.

4. Enter the number of minutes in the **Do not run twice in** box.
   
The alert action does not run twice in the minutes you entered.

**View Alerts**

The Alert Viewer portlet allows you to view logs of the alerts that have occurred. For the alert logs to show, you must enable the Include in alert log option for the action sets. This is done in the Alert Setup portlet.

The Alert Viewer portlet is more fully described in *Teradata Viewpoint* Help.

1. From the **Add Content** menu, go to **Monitoring > Alert Viewer**.
The **ALERT VIEWER** portlet appears and displays the alerts that have been triggered.

**Use the AlertRequest Table**

Any Teradata Database utility or user program can request an alert by inserting a row into the AlertRequest table in the Teradata dbcmngr database. The Alert Request Data Collector monitors the AlertRequest table for incoming alert requests. If the row contains valid data, the contents are forwarded to the Alert Service to process the alert action. You can view the details of the alert request in the Alert Viewer portlet.

The AlertRequest table is defined as follows:

<table>
<thead>
<tr>
<th>Column</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReqDate</td>
<td>Date</td>
<td>Request date generated on the Teradata Database</td>
</tr>
<tr>
<td>ReqTime</td>
<td>Integer</td>
<td>Request time generated on the Teradata Database</td>
</tr>
<tr>
<td>JobName</td>
<td>Char(60)</td>
<td>Name of the requesting job</td>
</tr>
<tr>
<td>Description</td>
<td>Char(120)</td>
<td>Text description of the event (the reason for the alert)</td>
</tr>
<tr>
<td>Event Value</td>
<td>Integer</td>
<td>Event value (if appropriate)</td>
</tr>
<tr>
<td>ActionCode</td>
<td>Char(1)</td>
<td>Type of action being requested. The action codes are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>'E' - send an email</td>
</tr>
<tr>
<td></td>
<td></td>
<td>'L' - write a log entry</td>
</tr>
</tbody>
</table>
| RepeatPeriod | Smallint | Minimum time (in minutes) between alerts for this event. Zero means 'always run the alert'. This value is ignored if the ActionCode is `+'.
| Destination  | Char(120)| Indicates the destination based on the ActionCode:                         |
|              |          | 'E' – the email address                                                    |
|              |          | 'R' – the program name to run                                              |
|              |          | 'T' – the BTEQ script to run                                               |
|              |          | 'S' – ignored – uses the default SNMP configuration for Alert Request Collector |
|              |          | '+' – the Action Set or Group action to run                                |
| Message      | Varchar(600)| Message to be sent for this alert (for example, email message, or numeric page and callback number.) |

**Request an Email Alert**

The following is an example of an insert statement. It causes an email message to be sent to the user named *dba* at mysite.com. The action does not repeat within 20 minutes.

```sql
insert dbcmngr.alertrequest values
(date, time, 'Job1', 'Load job completed', 0, 'e', 20, 'dba@mysite.com', 'This message indicates that the load job completed!');
```
Use the MonitorRequest Table

Any Teradata Database utility or user program can request that Teradata Viewpoint monitor its progress, by inserting rows into the MonitorRequest table in the dbcmngr database. Each row includes fields that indicate the date and time by which the next row is inserted.

The Alert Request Data Collector monitors the MonitorRequest table. If a new row is not inserted before the specified date and time, the Alert Request Collector forwards the contents to the Alert Service to process the alert action. You can view the details of the alert request in the Alert Viewer portlet.

When the job finishes, it inserts a final row containing a 0 (zero) in the ActionCode column. This ends the monitor request. No further alert actions are run.

The MonitorRequest table is defined as follows:

<table>
<thead>
<tr>
<th>Column</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MonitorId</td>
<td>Char(60)</td>
<td>A unique ID for the job: Date, StartTime, Host ID, and session id is recommended</td>
</tr>
<tr>
<td>ActionDate</td>
<td>Date</td>
<td>Date before which the next row for this job is inserted</td>
</tr>
<tr>
<td>ActionTime</td>
<td>Integer</td>
<td>Time before which the next row for this job is inserted</td>
</tr>
<tr>
<td>JobName</td>
<td>Char(60)</td>
<td>Name of the requesting job</td>
</tr>
<tr>
<td>EventValue</td>
<td>Integer</td>
<td>Any value to be displayed in the Alert Viewer, or included in the alert action. For example, if monitoring a load job, this could be the number of rows inserted so far.</td>
</tr>
<tr>
<td>ActionCode</td>
<td>Char(1)</td>
<td>Type of action being requested. The action codes are: 'E' - send an email 'L' - write a log entry 'R' - run a program 'S' - send an SNMP trap 'T' - run a BTEQ script 'S' - ignored - uses the default SNMP configuration for Alert Request Collector '0' - the job is completed (no alert is run)</td>
</tr>
<tr>
<td>Destination</td>
<td>Char(120)</td>
<td>Indicates the destination based on the ActionCode: 'E' - the email address 'R' - the program name to run 'T' - the BTEQ script to run 'S' - ignored - uses the default SNMP configuration for Alert Request Collector 'S' - the Action Set or Group action to run</td>
</tr>
<tr>
<td>Message</td>
<td>Varchar(600)</td>
<td>Message to be sent for this alert</td>
</tr>
</tbody>
</table>
Monitor a Five-Minute Job

If a job takes five minutes to complete, but sometimes hangs due to lock conflicts, two additional steps can be added as follows:

1. Before the job, run the following:

   ```sql
   insert dbcmngr.monitorrequest
   select '20010523100142011234', date, monTime, 'My Job', 0, '+', 'Email Admin', ''
   from (select extract(hour from xt)*10000+extract(minute from xt)*100+extract(second from xt), (current_time+interval '10' minute) as xt)
   tl(monTime, xt);
   ```

2. After the job, run the following:

   ```sql
   insert dbcmngr.monitorrequest values
   (`20010523100142011234', date, time, `My Job', 0, `0', `', `');
   ```

   This tells the Alert Request Collector to request the alert action Email Admin if the job does not finish within 10 minutes.

Monitor a Long-Running Job

The MonitorRequest feature can also be used to send updated status information on long-running jobs. In this context, the job uses date and time when inserting into the MonitorRequest table, forcing the designated alert action to run. The EventValue or Message fields can be used to indicate current status.

For example, a big load job can notify an administrator of its progress by running the following at regular intervals:

```sql
insert dbcmngr.monitorrequest values
(`20010523100142011234', date, time, `Load Job', 150000, `e',`BigAdmin@mysite.com', `');
```

The value 150000 represents the number of rows loaded so far. Each time the job inserts a row, it inserts the latest row count in the EventValue column.

Install Teradata Notification Service for Windows

To be able to use BTEQ and Run a program alert actions, you must first install the Teradata Notification Service. Install the service on a Windows server, and configure it with information about your Viewpoint server.
Software Dependencies
Teradata Notification Service has the following software dependencies:

1. Java JRE SE 5.0
   a. Set the JAVA_HOME environment variable at the System level. This is important because the Teradata Notification Service runs as a service.

2. Teradata BTEQ and all its dependencies

Prerequisites
Before installing Teradata Notification Service, ensure the following:

- The Viewpoint server is set up.
- The Viewpoint server is running.
- You know the hostname of the Viewpoint server.

Install Teradata Notification Service

1. Extract the Teradata Notification Service software to your server. The name of the zip file is: teradatacam_win32_x86.13.03.xx.xx.zip.

2. Navigate to the DISK1 folder, click setup.exe.

3. Select setup language, and click OK.

4. Follow the InstallShield Wizard, making the following settings:
   a. Accept the license agreement.
   b. [Optional] Change the destination folder.
   c. Specify the system name of your Teradata Viewpoint server.
   d. Click Install.
   e. Select Start the Teradata Notification Service now, and click Finish.

Configure Teradata Notification Service
The installation procedure asks to you enter the name of the Teradata Viewpoint Server. If you did not complete this step, you must manually
configure the Teradata Notification Service to know the location of the alert processes and the PostgreSQL database.

1. **Edit the** `config\cam-db.properties` **file as follows:**
   
   ```
   #cam.db.host=%{activeDatabaseHost}
   ```

2. **Remove the comment and assign** `cam.db.host` **to the server where PostgreSQL is running (the server, on which you installed Teradata Viewpoint and PostgreSQL).**
   
   ```
   cam.db.host=servername
   ```

3. **Edit the** `config\cam-jms.properties` **file as follows:**
   
   ```
   #cam.activemq.host=localhost
   ```

4. **Remove the comment and assign** `cam.activemq.host` **to the server where you have installed the camactivemq-13.03.xx.xx rpm.**
   
   ```
   cam.activemq.host=servername
   ```

### Configure TVI Logging

To enable TVI logging for the Teradata Notification Service, do the following:

1. **Copy** `config/tvilogger.properties` **to the following root folder.**
   
   ```
   [c:]\opt\teradata\tvilogger\tvilogger.properties
   ```

2. **Edit the properties as follows:**
   
   ```
   tvilogger.method=queuetable
   tvilogger.host=<Teradata TDPID containing the queue table>
   tvilogger.username=<Teradata username as appropriate for the site>
   tvilogger.password=<password as appropriate for the site>
   ```

### Service Control

The Teradata Notification Service is installed as a Windows Service using the name Teradata Notification Service. The default installation sets the service to automatically start on reboot. You can start and stop the service using the Services Administration tool in Windows.

To ensure the Teradata Notification Service is running, follow these steps:

1. **Go to** Start > Settings > Control Panel > Administrative Services.

2. **Locate the** Teradata Notification Service.

3. **Ensure the** Status **column for the service displays Started.

4. **In the** Name **column, double-click** Teradata Notification Service.

5. **The** Teradata Notification Service Properties **dialog box appears.

6. **Click** OK.
7. If the **Service status** is not **Started**, change it as follows:
   
a. Ensure the **Startup type** is Automatic, and click **Apply**

   b. Click **Start** to start the service.

---

**Teradata Manager Feature Equivalence**

**Teradata Viewpoint** 13.03 or later can be used as a replacement for Teradata Manager. Teradata Manager is not supported for Teradata Databases 13.10 and later. With the added support for Alerting, and viewing Node and vproc information, **Teradata Viewpoint** supports close to all features of Teradata Manager.

The following Teradata Manager features are not available in **Teradata Viewpoint**:

- **Scheduling**. Most operating systems provide scheduling features. In Microsoft Windows, use the Microsoft Task Scheduler. In Linux, use cron.

- **Priority Scheduler Administrator**. You can use TASM instead. If TASM is not available, use schmon.

If there are other features missing that are important to you, report them using the **Suggestion Box** link, located at the bottom of the **Teradata Viewpoint** portal.

**Uninstall Teradata Manager**

Follow this procedure to uninstall Teradata Manager, and to clean up directories, tables, and other files you no longer need.

1. Go to **Start > Control Panel > Add and Remove Programs**
2. **Remove** Teradata Manager.

![Add or Remove Programs](image)

3. **[Optional]** Delete the following directories:

**TTU 12.0**

- C:\Documents and Settings\<user login>\My Documents\Teradata\Teradata Manager
- C:\Documents and Settings\<user login>\My Documents\Teradata\PMON
- C:\Documents and Settings\All Users\Application Data\Teradata\Teradata Manager
- C:\Program Files\Teradata\Teradata Manager 13.0

**TTU 13.0**

- C:\Documents and Settings\<user login>\My Documents\NCR\Teradata Manager
Uninstall Teradata Manager

- C:\Documents and Settings\<user login>\My Documents\NCR\PMON
- C:\Documents and Settings\All Users\Application Data\NCR\Teradata Manager
- C:\Program Files\NCR\Teradata Manager 12.0

4. [Optional] Teradata Manager leaves behind registry keys that you no longer need. They do not do any harm, but you can remove them using the Windows Registry Editor. Remove the following registry keys:

**TTU 12.0**
- HKEY_LOCAL_MACHINE\SOFTWARE\Teradata\TeradataManager
- HKEY_CURRENT_USER\Software\Teradata\PSA
- HKEY_CURRENT_USER\Software\Teradata\TeradataManager

**TTU 13.0**
- HKEY_LOCAL_MACHINE\SOFTWARE\NCR\TeradataManager
- HKEY_CURRENT_USER\Software\NCR\PSA
- HKEY_CURRENT_USER\Software\NCR\TeradataManager

5. [Optional] Teradata Manager also leaves behind tables that you no longer need. You can delete the following tables from the dbcmngr database:

**Note**: Only delete the listed tables.
- dbcmngr.ampusageSnapshot1
- dbcmngr.ampusageSnapshot2
- dbcmngr.DbsType
- dbcmngr.Log* (any table in the dbcmngr that starts with Log)
- dbcmngr.tm* (any table in the dbcmngr that starts with tm)
Configure Managed Servers

**Teradata Viewpoint** can be configured to monitor certain system-level metrics for managed servers, including **Teradata Viewpoint** itself. These metrics include data on CPU usage, memory usage, system load, swap space usage, and I/O activity. Data that is collected from different managed servers can be viewed using the Viewpoint Monitoring portlet.

To set up monitoring of a managed server, install the tmsmonitor RPM on the server you want to monitor. This package is already installed on **Teradata Viewpoint** 13.0.1 or later staged systems. To install this package, see *Upgrade to Teradata Viewpoint 13.10.xx.xx* on page 86.

After the RPM has been installed and the service started, open the Viewpoint Managed Servers portlet and follow the steps in this topic to enable **Teradata Viewpoint** to start collecting data on the managed server.

The following procedure is more fully described in **Teradata Viewpoint** Help.

1. From the **Admin** menu, click **Managed Servers**.
2. Click **Add a System**.
3. Enter a nickname in the **MANAGED SYSTEM NAME** field.
   
   This nickname is used by the Viewpoint Managed Servers portlet to refer to this managed server.
4. [Optional] Select **System Enabled** to activate the managed system for monitoring.
5. In the **HOSTNAME** field, enter either an IP address for the managed system or a host name that resolves by DNS to the managed system.
   
   If the tmsmonitor service is running on a port other than the default of 8888, also specify the port number in the **HOSTNAME** field. For example, viewpoint.acme.com:8088.
6. In the **LOGIN Name** and **Password** fields, leave the default values unless the login and password for this managed system have been changed to different values.
7. [Optional] Test if the tmsmonitor service is accessible and the login and password are correct:
   a. Click Test, located at the bottom of the screen.
   b. If the test fails, check the Teradata Viewpoint log file located at:
      /opt/teradata/viewpoint/logs/viewpoint.log

8. Click Apply to save the new managed system.

9. [Optional] Select the System Enabled checkbox to immediately begin monitoring of the system.

### Configure Viewpoint LDAP

When using LDAP with Teradata Viewpoint, the following methods are used to add user accounts:

- Manually entered without LDAP authentication
- Manually entered with LDAP authentication
- Auto-provisioned with LDAP authentication

When users are auto-provisioned, the administrator does not have to enter their account into Teradata Viewpoint. The first time these users log on to Teradata Viewpoint, they are validated against the LDAP directory. If their credentials are valid, a Teradata Viewpoint account is created for them.

LDAP validation works in conjunction with the Externally Authenticated? flag on the Add User and Modify User dialog boxes in the User Manager portlet. If the Externally Authenticated? check box is selected, the user is authenticated through LDAP when logging in. The Externally Authenticated? check box is automatically selected when a user is created using auto-provisioning.

Use the LDAP Servers portlet to:

- Add and delete an LDAP configuration in Teradata Viewpoint.
- Enable and disable the LDAP after it has been added.
- Use the auto-provisioning feature to automatically add users to Teradata Viewpoint on first login.
- Use the role mapping feature to position the new user in Teradata Viewpoint.
Configure Viewpoint LDAP

As of Viewpoint 13.0.1, any changes made to the LDAP configuration using the Viewpoint Configuration portlet are automatically applied to Viewpoint. You no longer need to configure LDAP using the server.xml file or restart Viewpoint to apply LDAP configuration changes.

Prerequisites

- Have a **basic understanding** of LDAP.
- The URL of the LDAP server. For example:
- The username and password of a customer user or availability of that user to test the configuration.

Definitions

<table>
<thead>
<tr>
<th><strong>Term</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lightweight Directory Access Protocol (LDAP)</td>
<td>Technically an application-protocol, LDAP is frequently used to refer to a directory server such as Microsoft Active Directory or OpenLDAP.</td>
</tr>
<tr>
<td>LDAP Data Interchange Format (LDIF)</td>
<td>A standard, plain text data interchange format for representing LDAP directory content and update requests.</td>
</tr>
</tbody>
</table>
| Distinguished Name (DN) | The full "path" to a user-entry in LDAP. Every user's DN is, by definition, unique. The DN consists of its Relative Distinguished Name (RDN) constructed from some attribute(s) in the entry, followed by the parent entry's DN. Think of the DN as a full file name and the RDN as a relative filename in a folder.  

In the following example, the DN is the entire string:  
\- `cn=joec,OU=NorthAmerica,OU=User Accounts,DC=td,DC=acme,DC=com`

| Relatively Distinguished Name (RDN) | The part of a DN that distinguishes an entry from others at the same level in the tree. |
| Common Name (CN) | The CN is an attribute of a user-entry that is typically part of the user's DN and very often, but not always, the same value as the user's corporate username.  

In the following example, the CN is `joec`.  
\- `cn=joec,OU=NorthAmerica,OU=User Accounts,DC=td,DC=acme,DC=com`

| Bind | Used for LDAP authentication, binding is an LDAP operation that authenticates a username and a password. |
| Service Account | An LDAP service account is an account (username and password) not associated with a customer user, but existing for the purposes of binding to LDAP to perform a search of the directory. Typically, a service account is required when the DN of an authenticating-user is unknown, and an LDAP search (based on some other attribute of the user-entry such as sAMAccountName) must first be performed to determine the user's DN. After the user's DN has been determined, a normal bind using the user's |
## Configure Viewpoint LDAP

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DN and password is run.</td>
<td></td>
</tr>
<tr>
<td>Viewpoint Authenticator</td>
<td>Also referred to simply as the Authenticator, this is the component of Viewpoint that runs the authentication process against LDAP, among other actions.</td>
</tr>
<tr>
<td>log4j.xml</td>
<td>The XML file used to configure Viewpoint’s log output detail. The full path is: VIEWPOINT_DIR/common/classes/log4j.xml.</td>
</tr>
<tr>
<td>viewpoint.log</td>
<td>The file where Viewpoint logs messages by default. The full path is: VIEWPOINT_DIR/logs/viewpoint.log.</td>
</tr>
</tbody>
</table>

### Before You Begin

#### LDAP Data Interchange Format (LDIF)

1. Ask the LDAP administrator of the customer for:
   
   a. The user-entry details for the customer user in LDIF form.

   The following LDIF snippet is an example:

   ```ldif
   dn: cn=joec,dc=User Accounts,dc=acme,dc=com
   cn: joec
   givenName: Joe
   sn: Customer
   telephoneNumber: +1 888 555 6789
   telephoneNumber: +1 888 555 1232
   mail: [joe.customer@acme|mailto:joe.customer@acme].com
   sAMAccountName: customerjoe
   objectClass: inetOrgPerson
   memberOf: cn=Sales,ou=Groups,dc=acme,dc=com
   memberOf: cn=DBA,ou=Groups,dc=acme,dc=com
   ...
   
   b. At least one other future Viewpoint customer user, preferably in a different region or country.
Determine LDAP Configuration Mode

1. Read the following flowchart to determine which Viewpoint Authenticator configuration mode to use:
   - DN pattern bind
   - User search w/bind
Configure Viewpoint LDAP

Is Username in DN?

To bind to LDAP, the Viewpoint Authenticator must know the DN of Joe Customer. When logging in, Joe presents a corporate username, which is usually, but not always, part of the DN. Using the following DN as an example:

\[
\text{cn=joec,dc=User Accounts,dc=acme,dc=com}
\]

1. If the corporate username for Joe is \textit{joec} and the username is in the DN, perform a \textit{DN pattern bind}.

2. If the corporate username for Joe is \textit{customerjoe}, that is the \textit{sAMAccountName} attribute from the LDIF snippet, the username is \textit{not} in DN. Search the LDAP tree for a user entry where the attribute matches the username value presented by Joe Customer.

3. Proceed to \textit{Number of Bind Patterns} on page 43.

Number of Bind Patterns

After establishing Joe's DN and verifying the username for Joe is part of the DN string, bind to LDAP using the DN and password for Joe. As a reminder, following is the DN for Joe:

\[
\text{cn=joec,dc=User Accounts,dc=acme,dc=com}
\]

1. Are all users in Joe's company located at the same Base DN in LDAP? That is, do all user DNs have the following pattern?

\[
\text{cn=<USERNAME>,dc=User Accounts,dc=acme,dc=com}
\]

If yes, the \textit{number of bind patterns} is 1. Proceed to step 3. However, if users are located at multiple Base DNs, proceed to step 2.

2. If users are located at multiple Base DNs, you need to get this information from the LDAP administrator for the customer.

For example, at Joe's company, there might be the following users:

\[
\begin{align*}
\text{cn=joec,dc=User Accounts,dc=acme,dc=com} \\
\text{cn=janedoe,dc=Contractors,dc=User Accounts,dc=acme,dc=com} \\
\text{cn=kaizers,dc=Europe,dc=User Accounts,dc=acme,dc=com}
\end{align*}
\]

If there are multiple DN patterns, the Viewpoint Authenticator iterates over each of the patterns until it finds one that matches the username presented. If it does not match, it fails to authenticate. Therefore, if the number of patterns grows to seven or more, it might be faster to perform a \textit{user search}.

3. Select one of the following in the LDAP Servers portlet:

\begin{itemize}
\item If there are less than 7 DN patterns, select the \textbf{DN Pattern Bind} option.
\item If there are 7 or more DN patterns, select the \textbf{User Search} option.
\end{itemize}
Configure Viewpoint LDAP

**LDAP Configuration**

As of Viewpoint 13.0.1, the Viewpoint Authenticator is configured in the LDAP panel of the Viewpoint Configuration portlet.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Nickname</td>
<td>The short name by which this LDAP configuration is referred to in the LDAP Servers portlet. This name must be 8 characters or less.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Checked to enable this LDAP configuration as part of the Viewpoint authentication process. Unchecked to disable this LDAP configuration as part of the Viewpoint authentication process.</td>
</tr>
<tr>
<td>URL</td>
<td>One or more URLs for this LDAP configuration. The URL must include the appropriate protocol (ldap:// or ldaps://) as well as the port. For example, “ldap://ldap.acme.com:389”. Only enter more than one URL if all of the URLs point to a similarly-configured LDAP server. This might be the case if you have replicated LDAP servers or a failover LDAP server that should be used if the primary one is unreachable.</td>
</tr>
<tr>
<td><strong>DN Pattern Bind</strong></td>
<td></td>
</tr>
<tr>
<td>Pattern</td>
<td>The DN pattern(s) to perform the LDAP user bind attempt with. The patterns are invoked in the order specified, so it is recommended to put the patterns that match the most users before those that match fewer users. For example: “cn={0},OU=User Accounts,DC=acme,DC=com”</td>
</tr>
<tr>
<td><strong>User Search</strong></td>
<td></td>
</tr>
<tr>
<td>Service account DN</td>
<td>The DN of the LDAP service account. The DN must not be surrounded by parenthesis.</td>
</tr>
<tr>
<td>Service account password</td>
<td>The password of the LDAP service account specified in the Service account DN field above.</td>
</tr>
<tr>
<td>Search pattern</td>
<td>The LDAP attribute to match against the presented username when searching for a user-entry. If the cn attribute is the username, then set to (cn={0}). If the sAMAccountName attribute is the username, then set to (sAMAccountName={0}).</td>
</tr>
<tr>
<td>Search base</td>
<td>The entry that is the base of the subtree containing users. If not specified, the search base is the top-level context. For example: OU=User Accounts,DC=acme,DC=com</td>
</tr>
<tr>
<td>Search extent</td>
<td>Checked to search the entire subtree rooted at the Search base entry. Unchecked to request a single-level search including only the top level.</td>
</tr>
<tr>
<td><strong>Key User Information</strong></td>
<td></td>
</tr>
<tr>
<td>LDAP first name attribute</td>
<td>The name of the attribute on the LDAP user entry that specifies the first name of the user (given name).</td>
</tr>
<tr>
<td>LDAP last name attribute</td>
<td>The name of the attribute on the LDAP user entry that specifies the last name of the user (surname).</td>
</tr>
<tr>
<td>LDAP email attribute</td>
<td>The name of the attribute on the user object that specifies the email address of the user.</td>
</tr>
</tbody>
</table>
### Configure Viewpoint LDAP

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| Auto-Provisioning               | **Turn on auto-provisioning**  
  Set to true to enable auto-provisioning.  
  Set to false to disable auto-provisioning.  
  **Automatically assign these roles**  
  When auto-provisioning is enabled, the newly provisioned user is automatically added to these roles. This attribute is often set to User.  
  **Default email domain**  
  If auto-provisioning is enabled and the email address of the user cannot be determined from LDAP, the new user's initial email address is created in this domain. Set this to the domain of the customer. For example, acme.com. Usually this attribute does not have to be specified. |

### Role Mapping Global Settings

| Group search base                | The entry that is the base of the subtree containing groups. This field only needs to be specified if role mappings of type GROUP are used. |
| Group search subtree             | Checked to search the entire subtree rooted at the Group search base entry. Unchecked to request a single-level search including only the top level. This field only needs to be specified if role mappings of type GROUP are used. |
| Group attribute name             | The name of the attribute on the LDAP group entry that contains the DN s of the users in the group. |

### Role Mapping Individual Settings

| Type                             | Set to ATTRIBUTE to perform a mapping from a LDAP user's entry value to a Viewpoint role. Set to GROUP to perform a mapping from an LDAP group to a Viewpoint role. |
| Attribute name                   | The name of a LDAP attribute in the user's entry that specifies LDAP group and role membership for the purpose of mapping to Viewpoint roles. This setting is only applicable to mappings of type ATTRIBUTE. |
| LDAP value                       | The value of the attribute specified in the Attribute name field that should be mapped to the role specified in the Viewpoint role field. For more details, see Role-mapping on page 46. |
| Viewpoint role                   | The role in Viewpoint to which users are mapped. |

### Standard Configuration and Testing

The nickname, URLs, name matching (either DN Pattern Bind or User Search), and key user information sections are all part of the standard configuration for Viewpoint LDAP authentication.

After these sections are completed in the LDAP Servers portlet, you can test these settings before saving the changes. Any changes made to the LDAP configuration are instantly applied to the Viewpoint authentication process, therefore it is highly recommended you test the functionality before saving any changes.

To test the current LDAP configuration, perform the following steps in the LDAP Servers portlet.

The following procedure is more fully described in Teradata Viewpoint Help.

1. Click **Test** in the SETTING S TEST section.
2. Enter a username and password exactly as you would if you were logging into Viewpoint.
3. Click **Run**.
Configure Viewpoint LDAP

After the test is complete, an icon appears indicating if the authentication against LDAP was successful. If the authentication is successful, details of the test user are displayed in the **SETTINGS TEST** section. If the authentication was not successful, an error message displays.

Role-mapping

The examples below detail the two different types of role mapping available in **Teradata Viewpoint**. For both types of role mapping, the following characteristics apply:

- The Viewpoint role being mapped must be created beforehand by the Viewpoint Administrator.

- If a user is mapped into a role and logs out, each role-mapping is re-examined the next time they log on. If they are no longer a member of that LDAP group and role, they are removed from the mapped Viewpoint role. However, in the time between logging out and logging back in again, they are listed in Viewpoint as a member of that role.

Example 1

1. Configure the Viewpoint Authenticator to map authenticated LDAP users into Viewpoint roles based on group membership recorded on a user entry. The relevant XML attributes:

As a reminder, following is the LDIF for Joe:

```ldif
dn: cn=joec,dc=User Accounts,dc=acme,dc=com
cn: joec
givenName: Joe
sn: Customer
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: joe.customer@acme.com
sAMAccountName: customerjoe
objectClass: inetOrgPerson
memberOf: cn=Sales,ou=Groups,dc=acme,dc=com
memberOf: cn=DBA,ou=Groups,dc=acme,dc=com
...
```

The `memberOf` attribute is used to specify Joe's membership in two groups whose names are specified with a full DN: `(cn=Sales,ou=Groups,dc=acme,dc=com and cn=DBA,ou=Groups,dc=acme,dc=com)`. To map those two groups onto two Viewpoint roles, **SALES_ROLE** and **DBA_ROLE**, the XML would be as follows:
First role mapping
- Type: ATTRIBUTE
- Attribute name: memberOf
- LDAP value: cn=Sales,ou=Groups,dc=acme,dc=com
- Viewpoint role: SALES_ROLE

Second role mapping
- Type: ATTRIBUTE
- Attribute name: memberOf
- LDAP value: cn=DBA,ou=Groups,dc=acme,dc=com
- Viewpoint role: DBA_ROLE

Example 2
1. Configure the Viewpoint Authenticator to map authenticated LDAP users into Viewpoint roles based on group membership maintained in a static group. A static group is a separate entity in LDAP that maintains its own list of members.

Assume the following is the LDIF for a static group ‘Sales’:

```
dn: cn=sales,dc=Groups,dc=acme,dc=com
  cn: sales
  objectClass: groupOfUniqueNames
  uniqueMember: cn=joec,dc=User Accounts,dc=acme,dc=com
  uniqueMember: cn=janed,dc=User Accounts,dc=acme,dc=com
...
```

The `uniqueMember` attribute is used to specify two members of the group with full DNs of: `(cn=joec,dc=User Accounts,dc=acme,dc=com)` and `(cn=janed,dc=User Accounts,dc=acme,dc=com)`. To map these two users into the Viewpoint role **SALES_ROLE**, the configuration would be as follows:

Role mapping global settings
- Group search base: ou=Groups,dc=acme,dc=com
- Group search subtree: (unchecked)
- Group attribute name: uniqueMember
Configure Viewpoint LDAP

**Role mapping**
- Type: GROUP
- LDAP value: cn=Sales,ou=Groups,dc=acme,dc=com
- Viewpoint role: SALES_ROLE

**LDAP Over SSL (LDAPS)**

For LDAP over SSL (also knows as LDAPS) support, ensure the URL in the LDAP Servers portlet reads ldaps://ldap.acme.com:636. The prefix is ldaps instead of ldap, and the port number is 636 instead of 389.

If the Certification Authority (CA) of the LDAP server is not trusted by the Viewpoint server, use the following procedure to store the CA certificate for the LDAP server into the cacerts keystore on the Viewpoint server.

1. Log on to the **Teradata Viewpoint** server (Linux) as root.
2. Install the SSL Certificate by typing the following commands:
   
   ```bash
   keytool -import -alias <your_alias> -keystore $JDK5_64_HOME/jre/lib/security/cacerts -trustcacerts -file <your_certificate_filename>
   ```
3. Enter the password as: `changeit`.

Refer to the Java keytool command documentation for additional configuration steps and options if necessary: [http://java.sun.com/j2se/1.5.0/docs/tooldocs/solaris/keytool.html](http://java.sun.com/j2se/1.5.0/docs/tooldocs/solaris/keytool.html)

**Enable Debug Logging**

If using the new test functionality in the LDAP Servers portlet is not sufficient to troubleshoot a specific LDAP issue, **Teradata Viewpoint** can be configured to output detailed log information to help diagnose the issue.

You can change back the logging levels when the troubleshooting is complete.

1. Make a copy of `log4j.xml`. For example: `log4j.xml.old`.
   This file is located at: `/opt/teradata/viewpoint/common/classes`.
2. Insert the following XML stanzas into `log4j.xml`. Comment out any similar stanzas, if present.
3. Restart Viewpoint for the logging changes to take effect.
Add Teradata Viewpoint Roles

4. View the log output located at `VIEWPOINT_DIR/logs/viewpoint.log`. Following is an example:

```xml
<!--=======================================================================
LDAP / Authentication
==========================================================================--> 

<logger name="com.teradata.viewpoint.security.container.tomcat.authn">
  <!-- Set the level value to DEBUG to investigate LDAP/JNDI authentication issues.-->
  <level value="DEBUG"/>
</logger>

<logger name="com.teradata.viewpoint.security.config.XmlConfigLoader">
  <!-- Set the level value to DEBUG to investigate LDAP/JNDI authentication issues.-->
  <level value="DEBUG"/>
</logger>

<logger name="org.apache.catalina.realm">
  <!-- Set the level value to DEBUG to investigate LDAP/JNDI authentication issues.-->
  <level value="DEBUG"/>
</logger>

<logger name="org.apache.catalina.realm.RealmBase">
  <!-- Generally leave this level value at WARN, even when investigating LDAP issues.-->
  <level value="WARN"/>
</logger>
```

Add Teradata Viewpoint Roles

**Teradata Viewpoint** allows System Administrators to assign permissions by creating classes of users called *roles*. Various roles are created and each user is assigned to a role, allowing each portlet to be controlled with a high level of granularity. For example, a DBA can have permission to abort a query in the My Queries portlet, but other classes of users do not have permission.

**Teradata Viewpoint** includes two pre-configured roles called Administrator and User. Each role can be tailored as needed and additional roles can be added.

Roles can also be modified, deleted, or copied and then modified. To modify, delete, or copy a role, see **Teradata Viewpoint** Help.

To add a role, assign users to a role, and then enable portlets for a role, see **Teradata Viewpoint** Help.
Add Teradata Viewpoint Users

Before assigning a role to a user, verify the role and user exists. Users can be assigned to roles using either Roles Manager or User Manager. You can also use the LDAP interface. See Configure Managed Servers on page 38.

Teradata Viewpoint can be configured to monitor certain system level metrics for managed servers, including Teradata Viewpoint itself. These metrics include data on CPU usage, memory usage, system load, swap space usage, and I/O activity. Data that is collected from different managed servers can be viewed using the Viewpoint Monitoring portlet.

Configure Teradata Viewpoint Security

Control Access to Portlets

The Portlet Library allows administrators to globally enable or disable portlets. This setting takes precedence over every other portlet permission level. You can browse the list of installed portlets by category, name, and software version, and see if the portlet is enabled or disabled.

To enable or disable portlets, see Teradata Viewpoint Help.

Control Access within Portlets

The Roles Manager portlet allows Teradata Viewpoint Administrators to configure what roles have permission to access specific functionality for a specific system in each portlet.

To enable or disable permissions, see Teradata Viewpoint Help.

Configure Viewpoint to Log to TVI

The default TVI logging configuration assumes Teradata Viewpoint is running on a managed server. If this is the case, no special configuration is needed for logging Alert/Event information, but it is still recommended that you configure TVI to log errors. If Teradata Viewpoint is running on an unmanaged server, or if you want to log asset information, TVI logging must be configured to send information to TVI through a queue table.

Before starting, contact the administrator who set up the TVI Administration Software (TAS) for your system. Ask if the system supports logging to TVI using a queue table. If a queue table has been set up for your system, ask for the login information for this queue table.

1. Locate the file tvilogoer.properties within the /opt/teradata/dcs/config directory.
Back Up Teradata Viewpoint Databases

2. Copy this properties file to
   /etc/opt/teradata/tvilogger/tvilogger.properties.

3. If **Teradata Viewpoint** is running on an unmanaged server, or if asset logging is required, you must modify the properties to specify login information for queue table logging. Follow the instructions provided within the properties file.

4. Restart the **Teradata Viewpoint** services for the changes in the properties file to take effect.

5. Do the following:
   a. Open the **Teradata Viewpoint** log file located at:
      /opt/teradata/viewpoint/logs/viewpoint.log
   b. Look for messages that state the following:
      TVILogger will write to queue table

   Serious errors in **Teradata Viewpoint** are sent through TVI.

---

**Back Up Teradata Viewpoint Databases**

The **Teradata Viewpoint** DCS automatically creates snapshot dumps of the **Teradata Viewpoint** databases on a daily basis. The backup process can be managed in the Backup administration portlet. The following options can be specified using this portlet.

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Description</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Checked to enable the backup process and unchecked to disable it.</td>
<td>checked</td>
</tr>
<tr>
<td>Location</td>
<td>The location of the backup files, either on the Viewpoint server or on a networked file server. The location of the local backup files is always /data/backup. If local backups are performed, keep a copy of the files off the Viewpoint server to prevent data loss in the event of a catastrophic failure. For a networked backup, enter the host name (or IP address) of the NFS server and the absolute path to where the backups will be written. Note: The postgresql user on the Viewpoint server must have write access to this location.</td>
<td>Local</td>
</tr>
<tr>
<td>Backup time</td>
<td>The time of day that the backup process begins.</td>
<td>12:00 AM (midnight)</td>
</tr>
<tr>
<td>Retention days</td>
<td>The number of days to keep backups before they are removed.</td>
<td>7</td>
</tr>
</tbody>
</table>

---

**Restore a Teradata Viewpoint Database**

Five databases are stored on a **Teradata Viewpoint** server:

- lportal
Change the Session Timeout

- td_portal
- td_portlets
- dcsdb
- cam

Each database has its own nightly backup file.

1. Navigate to the directory where the database backup files are located.
2. Type the following commands:
   
   ```
   su postgres
   pg_restore --clean -d <database_name> <name_of_backup_file>
   ```

**Change the Session Timeout**

The default session timeout in **Teradata Viewpoint** is 90 minutes.

To check the session timeout value, run:

```
/opt/teradata/viewpoint/bin/vpadmin.sh -t
```

To set the session timeout, run (where `[timeout]` is the wanted timeout value):

```
/opt/teradata/viewpoint/bin/vpadmin.sh -T [timeout]
```

The maximum recommended timeout is 1440 (1 day).

**Set the Default Locale**

The default locale in **Teradata Viewpoint** is `en_US`. To check the default locale value, run:

```
/opt/teradata/viewpoint/bin/vpadmin.sh -l
```

To set the default locale, run (where `[localecode]` is a valid locale code):

```
/opt/teradata/viewpoint/bin/vpadmin.sh -L [locale]
```

The valid locale codes are as follows:

<table>
<thead>
<tr>
<th>Locale Code</th>
<th>Language/Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>en_US</td>
<td>English US</td>
</tr>
<tr>
<td>en_GB</td>
<td>English UK</td>
</tr>
<tr>
<td>zh_CN</td>
<td>Chinese China</td>
</tr>
<tr>
<td>zh_TW</td>
<td>Chinese Taiwan</td>
</tr>
<tr>
<td>fr_FR</td>
<td>French</td>
</tr>
<tr>
<td>de_DE</td>
<td>German</td>
</tr>
<tr>
<td>ja_JP</td>
<td>Japanese</td>
</tr>
<tr>
<td>ko_KR</td>
<td>Korean</td>
</tr>
</tbody>
</table>
Reset the Admin User Password

If you ever forget the Viewpoint admin user password, reset it to teradata by running the following command:

```
/opt/teradata/viewpoint/bin/vpadmin.sh -R
```

Ports Used by Teradata Viewpoint

Following is a list of ports used by Teradata Viewpoint. Additional ports are required for Teradata Viewpoint clustering. See Additional Considerations on page 72.

Incoming Ports
- 22 (SSH)
- 80 (HTTP)
- 443 (HTTPS)
- 5432 (Cache Database)
- 8888 (optional for monitoring Viewpoint server – tmsmonitor)
- 22000-22010 (only required for clustering)
- 61616 (optional for Teradata Alerting)

Outgoing Ports
- 389 (optional for LDAP authentication)
- 1025 (JDBC)
- 8888 (optional for monitoring Teradata Managed Servers - tmsmonitor)
- 22000-22010 (only required for clustering)

Set Teradata Viewpoint Server Time

The preferred way to set the Teradata Viewpoint server time is to use NTP. See Configure NTP Time Synchronization on page 54.

Caution: If setting the time manually, shut down the DCS before changing the time to prevent possible data loss that could result if the date is set incorrectly. Ensure the date is correct before restarting the DCS.

1. Type the following command:

```
yast timezone
```
Configure NTP Time Synchronization

2. Select the region using the arrow key.

3. Tab to the **Time Zone** field and use the arrow key to select the appropriate time zone.

4. Tab to the **Change Time or Date** field and press **Enter**.

5. Tab to the appropriate time and date entries and use the backspace key to delete the old value.

6. Enter the new value.

7. Tab through the subsequent entries until finished.

8. Tab to **Apply** and press **Enter**.

9. Tab to **Accept** and press **Enter** to accept the change.

**Configure NTP Time Synchronization**

To ensure the time on the **Teradata Viewpoint** server is always accurate, you can configure NTP time synchronization. This is especially important if setting up a Viewpoint cluster because the time between the servers needs to be in sync.

This setup assumes a time server is available on the LAN. If no time server is available, then time is only synchronized between the Viewpoint servers in a cluster and not a master time source. Use the following procedure for each Viewpoint server.

1. Enable the ntp service by typing:
   ```
   chkconfig ntp on
   ```

2. If the customer has a time server:
   a. Open **edit /etc/ntp.conf**.
   b. Add the following line to the end of the file where [host] is the host name of the time server:
      ```
      server [host]
      ```

3. If **Teradata Viewpoint** is configured in a cluster:
   a. Open **/etc/ntp.conf**.
   b. Add the following line to the end of the file for each **Teradata Viewpoint** server in the cluster, excluding the current host, where [address] is the IP address of another **Teradata Viewpoint** server:
      ```
      peer [address]
      ```
4. Start the ntp service by typing:
   
   /etc/init.d/ntp start

**Teradata Viewpoint Clustering**

Starting with **Teradata Viewpoint** 13.0.1, multiple **Teradata Viewpoint** servers can be clustered together for purposes of high availability and scalability. Each **Teradata Viewpoint** server in a cluster shares the same users, roles, permissions, preferences, and collected data from monitored Teradata systems. This topic covers:

- Cluster Configurations
- Failure Scenarios
- Creating a **Teradata Viewpoint** Cluster
- Adding Additional **Teradata Viewpoint** Servers to the Cluster
- Promoting the Standby Cache Database
- Upgrading PostgreSQL to Enable Clustering
- Additional Considerations

**Cluster Configurations**

This topic contains the supported **Teradata Viewpoint** cluster configurations. This includes:

- High Availability configuration
- High Usage configuration
- Advanced configuration
High Availability Configuration: Two Teradata Viewpoint Servers

This is the base configuration for customers that want to set up a Teradata Viewpoint cluster.

The following diagram shows two Teradata Viewpoint servers configured in a cluster. Both Teradata Viewpoint instances point at the same active cache database. A standby cache database is kept up to date with the last minute of data if a failure occurs. An active Data Collection Service (DCS) runs on the same Teradata Viewpoint server as the active cache database. The other Teradata Viewpoint server contains a standby DCS that takes over data collection when the active DCS goes down. The Teradata Viewpoint servers share a distributed cache so the state between the Teradata Viewpoint portals remains consistent.
High Usage Configuration: Three or More Teradata Viewpoint Servers

This configuration extends the High Availability configuration to allow Teradata Viewpoint to scale to thousands of concurrent users by adding Teradata Viewpoint servers to the cluster. These added Teradata Viewpoint servers only run the Teradata Viewpoint portal and not the DCS or cache database. Instead, they point to the cluster-wide cache database to access users, permissions, preferences, and collected data. The two additional Teradata Viewpoint servers shown in the following diagram are marked optional as they are not required for high availability. Even though these added servers only run the Teradata Viewpoint portal, they are staged the same as any Teradata Viewpoint server and have the DCS and cache database installed, but not enabled.
Advanced Configuration: Three or More Teradata Viewpoint Servers with Dedicated Cache Database Server

This configuration is for customers that require better cache database performance because of high use or because multiple large/high use Teradata systems are being monitored.

In this configuration, the Teradata Viewpoint portal is not run on the same machine as the active cache database. This provides the cache database more system resources.
Failure Scenarios

Data Collection Service (DCS) Failure (Scenario 1)

If the active DCS goes down, the standby DCS automatically takes over data collection and logs an error to TVI and optionally sends out an email. When the standby DCS detects the active DCS is back online, it stops data collection and continues to operate in standby mode.
Cache Database Failure (Scenario 2)

If the DCS detects that the active cache database is down, the DCS logs an error to TVI and optionally sends out an email. If the problem is not trivial to solve, the System Administrator can promote the standby cache database. Promoting the standby cache database makes the standby cache database become the active cache database. The promotion is broadcast to all Teradata Viewpoint servers and they are automatically redirected to the new active cache database. The standby DCS automatically becomes the new active DCS. After the standby machine is promoted, a new standby cache database needs to be set up by the System Administrator. See Create a Teradata Viewpoint Cluster on page 62.

If the cluster is set up using the Advanced configuration, stop the Teradata Viewpoint portal on the new active cache database server so that it continues to run on a dedicated machine.
Active Teradata Viewpoint Server Failure

This failover scenario is the combination of scenario 1 and 2. The standby DCS detects that the active DCS and cache database are down and logs an error to TVI and optionally sends out an email. If the problem is not trivial to solve, the System Administrator can promote the standby cache database to the active cache database. A notification is broadcast to all Teradata Viewpoint portals so that they are automatically redirected to the new active cache database. The standby DCS becomes the new active DCS. After the standby machine is promoted, a new standby cache database needs to be set up by the System Administrator. See Create a Teradata Viewpoint Cluster on page 62.

If the cluster is set up using the Advanced configuration, stop the Teradata Viewpoint portal on the new active cache database server so that it continues to run on a dedicated machine.
Create a Teradata Viewpoint Cluster

This topic describes how to create a Teradata Viewpoint cluster. Two Teradata Viewpoint servers are required. One is configured with the active cache database and the other is configured with the standby cache database. To add additional Teradata Viewpoint servers to the cluster, see Add Additional Teradata Viewpoint Servers to the Cluster on page 68.

Before you proceed with Teradata Viewpoint clustering configuration, review Additional Considerations on page 72.

System Preparation

1. Check the Teradata Viewpoint software version installed on both servers. Ensure the installed versions are the same and the version installed is at least 13.0.1.

   If the version numbers are not the same or the installed version is less than 13.0.1, upgrade the servers to 13.0.1 or later version. See Upgrade to Teradata Viewpoint 13. on page 86. The Teradata Viewpoint versions on all servers in a Teradata Viewpoint cluster must be identical.

2. Check the PostgreSQL versions.

   Teradata Viewpoint servers staged before the Teradata Viewpoint 13.0.1 release have an older version of PostgreSQL installed that is incompatible with clustering.

   Creating a cluster requires PostgreSQL 8.3.5 be installed on both servers.

   a. To check the version number of a running PostgreSQL instance, use the following commands:

      su postgres
      psql
      SELECT version();

   b. If the PostgreSQL version is not equal to 8.3.5, see Upgrade PostgreSQL to Enable Clustering on page 70.

3. Determine which server is going to host the active cache database and which one is going to host the standby cache database. The server that is going to host the active cache database can already have existing users, roles, permissions, preferences, and collected data from monitored Teradata systems that is shared by all Teradata Viewpoint servers in the cluster. Any data on the server hosting the standby cache database is lost.

Set Up Cluster Configuration Files

1. On both servers, copy cluster configuration files to /etc/opt/teradata/viewpoint/ by typing the following commands:
   - `cp /opt/teradata/dcs/config/local.cluster.properties /etc/opt/teradata/viewpoint/
   - `cp /opt/teradata/dcs/config/distributed.cluster.properties /etc/opt/teradata/viewpoint/
   - `cp /opt/teradata/dcs/config/cluster-protocol-stacks.xml /etc/opt/teradata/viewpoint/

2. Check the file permissions on the copied files and their parent directory, and ensure they are readable by everyone.
   - `chmod 744 /etc/opt/teradata/viewpoint
   - `chmod 744 /etc/opt/teradata/viewpoint/*

3. Edit /etc/opt/teradata/viewpoint/distributed.cluster.properties on both servers.
   a. Set the value of the `active.database.host` property to the host name or IP address of the active cache database server.
   b. Set the value of the `standby.database.host` to the host name or IP address of the standby cache database server.

   For example:
   - `active.database.host=viewpoint1
   - `standby.database.host=viewpoint2

   **Note:** You can inspect the contents of the `distributed.cluster.properties` file at any time to determine which cache database server is currently the active server and which is the standby server.

4. Edit /etc/opt/teradata/viewpoint/local.cluster.properties on both servers.
   a. Set the value of the `cluster.hosts` property equal to the host names or IP addresses of both Teradata Viewpoint servers separated by a comma. If enabling host authentication (see *Additional Considerations* on page 72), the `cluster.hosts` property must only include IP addresses and not host names.

   For example:
   - `cluster.hosts=viewpoint1,viewpoint2

   b. Set the value of the `tcp.bind_addr` property equal to the public IP address of the host where the file resides. This is the IP address that other servers in the cluster use to connect to this host. Do not set the IP address to a private server management IP address.

   For example:
   - `tcp.bind_addr=192.168.0.1`
5. Test the cluster configuration.
   a. Run `/opt/teradata/dcs/bin/clustertest.sh` on both servers. This command reads in data from the console.
   b. Enter console input and ensure that when `Enter` is pressed, the text appears on the other server’s console.
   c. Enter text on both servers and ensure it appears on the other server when Enter is pressed. If this does not work, check the configuration again in `/etc/opt/teradata/viewpoint/local.cluster.properties` to see if the `cluster.hosts` property was set correctly.
   d. To enable more debug information, set the `cluster.debug.enabled` property to true in `/etc/opt/teradata/viewpoint/local.cluster.properties` and run `/opt/teradata/dcs/bin/clustertest.sh` again.
   e. Press `Ctrl-D` on each console to exit.

6. After the test succeeds of the cluster configuration:
   a. Edit `/etc/opt/teradata/viewpoint/local.cluster.properties` on both servers.
   b. Set the `cluster.enabled` property to `true`.

7. Restart Viewpoint and the DCS to start them in clustered mode as discussed in Start and Stop Teradata Viewpoint Services on page 7.

   **Note:** All of the Viewpoint services listed under Start and Stop Teradata Viewpoint Services on page 7 must be running on both servers.

### Enable PostgreSQL Replication

1. Enable public-key authentication for the postgres user between both servers. On each server, perform the following commands:
   a. Assume the postgres user by typing the following commands:
      ```
      cd /data
      su postgres
      ```
   b. Generate a public/private key pair:
      ```
      ssh-keygen -t rsa
      ```
   c. Press `Enter` three times to accept the defaults.
   d. Copy public key to alternate server by replacing `[host]` with an alternate server’s host name by typing the following command. Note that the command must be typed on a single line:
Teradata Viewpoint Clustering

scp /var/lib/pgsql/.ssh/id_rsa.pub root@[host]:/var/lib/pgsql/.ssh/authorized_keys

e. Accept alternate servers’ authenticity by typing yes and press Enter.

f. Enter root password for alternate server.

g. Test public-key authentication by replacing [host] with an alternate server’s host name by typing:
   ssh [host]

h. Verify the above command logged into the alternate host without requiring a password.
   - If it does not work, check the file permissions on the /var/lib/pgsql/.ssh/authorized_keys file on the remote host by typing:
     chmod 744 /var/lib/pgsql/.ssh/authorized_keys
     Ensure the file is readable by all.

i. Exit from ssh:
   exit

j. Exit postgres user:
   exit

2. Prepare the standby cache database server.

   **WARNING:** Only run the following command on the standby cache database server and not on the active cache database server otherwise you will lose all your data!

   a. Stop PostgreSQL by typing:
      
      /etc/init.d/postgresql stop

   b. Delete existing data on the standby cache database server:
      
      rm -rf /data/postgresql/*
      rm -rf /data/archive/*

3. On the active cache database server, enable WAL archiving.

   a. Edit /data/postgresql/postgresql.conf and look for the WRITE AHEAD LOG section:
      
      - Set archive_mode = on and remove "#" comment from beginning of line.
      - Set archive_command = '/opt/teradata/dcs/bin/archive.sh %p %f' and remove "#" comment from beginning of line.
      - Set archive_timeout = 60 and remove "#" comment from beginning of line.
b. Restart postgresql:
   /etc/init.d/postgresql restart

4. Ensure the active cache database server WAL logs are being sent to the standby cache database server's /data/archive folder.

   a. On the standby cache database, type:
      
      ```
      ls /data/archive
      ```
      
      Files are copied and displayed (with names such as "00000001000000000000000000000000").

   b. Open the PostgreSQL log file for the active cache database server located at, where DAY is the current day of the week:
      
      ```
      /data/postgresql/pg_log/postgresql.log.DAY
      ```

   c. Look for archive-related errors.

5. Create a base backup of the active cache database on standby cache database server.

   a. On the active cache database, start the base backup:
      
      ```
      cd /data
      su postgres
      psql
      SELECT pg_start_backup('viewpoint');
      \
      q
      exit
      ```

   b. Copy cache database on active cache database server to standby cache database server. This could take some time, depending on the size of the database. The `rsync` command below can be cancelled and restarted at any time; it starts transferring the database where it left off. Replace the [host] value with the standby cache database server host name. Note that the `rsync` through `/data/postgresql` code must be typed on a single line.

      ```
      cd /data
      su postgres
      rsync -avtrz --exclude=pg_xlog/* -e ssh /data/postgresql/ [host]:/data/postgresql
      exit
      ```

   c. On the active cache database, stop the base backup:
      
      ```
      cd /data
      su postgres
      psql
      SELECT pg_stop_backup();
      \q
      exit
      ```

6. Start standby cache database in recovery mode. All the following commands must be performed on the standby cache database server.
a. On the standby cache database server, set up the recovery configuration file:

```bash
rm -f /data/postgresql/recovery.done
cp /opt/teradata/dcs/config/recovery.conf /data/postgresql/
cp /opt/teradata/dcs/bin/recover.sh /data/postgresql/
```

b. Check the file permissions on the copied files and ensure they are readable, and that the postgres user is able run them.

```bash
chmod 744 /data/postgresql/recovery.conf
chmod 755 /data/postgresql/recover.sh
```

c. Modify the PostgreSQL init script to not wait for start up.

- Open `/etc/init.d/postgresql` and remove the `-w` option from where `pg_ctl start` is called.

d. Disable WAL archiving.

- Open `/data/postgresql/postgresql.conf` and look for the WRITE AHEAD LOG section.

- Set `archive_mode` to `off`.

e. Start PostgreSQL:

```bash
/etc/init.d/postgresql start
```

f. Open the postgresql log file for the standby cache database server located at, where DAY is the current day of the week:

```bash
/data/postgresql/pg_log/postgresql.log.DAY
```

If using SSL for PostgreSQL connections on the active cache database, follow step 3 in the Cluster Security section for the new standby cache database. See *Cluster Security on 73.*
The creation of a Viewpoint cluster is now complete. See the next section to add additional Viewpoint servers to the cluster or the Additional Considerations sections for additional configuration options.

Add Additional Teradata Viewpoint Servers to the Cluster

After a cluster has been configured with an active and a standby cache database, additional Teradata Viewpoint servers can be added to the cluster to support a growing number of end users.

1. On the server being added to the cluster, stop and disable the DCS by typing the following commands:
   
   ```
   /etc/init.d/dcs stop
   chkconfig dcs off
   ```

   The DCS runs only on the servers hosting the active and standby cache databases.

2. On each existing server in the cluster, edit
   
   ```
   /etc/opt/teradata/viewpoint/local.cluster.properties
   ```

   and append a comma to the cluster.hosts property followed by the host names or IP address of the Teradata Viewpoint server being added. If using host authentication (see Additional Considerations on page 72), specify the IP address and not the host name.

3. Copy the current cluster configuration from another Teradata Viewpoint server in the cluster. Replace the [host] value in the following command with the host name or IP address of an existing Teradata Viewpoint server in the cluster. When prompted, enter the root password for the specified host.

   ```
   scp root@[host]:/etc/opt/teradata/viewpoint/* /etc/opt/teradata/viewpoint/
   ```

4. Edit /etc/opt/teradata/viewpoint/local.cluster.properties on the new server.

   Set the value of the tcp.bind_addr property equal to the public IP address of the host where the file resides. This is the IP address that other servers in the cluster use to connect to this host. Do not set the IP address to a private server management IP address.

   For example:

   ```
   tcp.bind_addr=192.168.0.1
   ```

5. Test communication with the rest of the cluster.

   a. Run /opt/teradata/dcs/bin/clustertest.sh on all the servers in the cluster. This command reads in data from the console.

   b. Enter console input and ensure that when Enter is pressed, the text appears on the other server’s console.
c. Enter text on each server and ensure it appears on the other servers console when Enter is pressed. If this is does not work, check the configuration in /etc/opt/teradata/viewpoint/local.cluster.properties to see if the cluster.hosts property is set correctly.

d. To enable more debug information, set the cluster.debug.enabled property in /etc/opt/teradata/viewpoint/local.cluster.properties to true and run /opt/teradata/dcs/bin/clustertest.sh again.

e. Press Ctrl-D on each console to exit.

6. Restart the Teradata Viewpoint portal on the newly configured server.

Promote the Standby Cache Database

In situations where the active cache database goes down and cannot easily be restarted, the standby cache database can be promoted to the new active cache database. After the standby cache database is promoted to the active cache database, the Teradata Viewpoint portals in the cluster and the active DCS automatically starts using the newly promoted cache database.

To promote the standby cache database, log on to the Teradata Viewpoint server hosting the standby cache database and type the following command to promote the standby cache database:

```
/opt/teradata/dcs/bin/promote.sh
```

After the script completes, Teradata Viewpoint is available again. After the promotion, the follow maintenance tasks must be performed.

1. Modify the PostgreSQL init script on the newly promoted server to wait for start up.

   a. Open /etc/init.d/postgresql.

   b. Add the -w option to the pg_ctl start command on line 131 as follows:

```
pg_ctl start -s -w -p $H -D $DATADIR -o "\"$OPTIONS\""
```

2. Follow the instructions in Create a Teradata Viewpoint Cluster on page 62 to set up a new standby cache database. This can be done on the server that was previously hosting the active cache database or on an additional Teradata Viewpoint server.

3. If the standby server was set up on an additional Teradata Viewpoint server already in the cluster, re-enable and start the DCS by typing the following commands:

```
chkconfig dcs on
/etc/init.d/dcs start
```
4. If the cluster was set up using the Advanced configuration, disable the Teradata Viewpoint portal on the newly promoted cache database host:
   
   ```
   /etc/init.d/viewpoint stop
   chkconfig viewpoint off
   ```

### Upgrade PostgreSQL to Enable Clustering

Creating a Teradata Viewpoint cluster requires installing PostgreSQL 8.3.5 on the Teradata Viewpoint servers hosting the active and standby cache databases.

Teradata Viewpoint servers staged prior to the release of Teradata Viewpoint 13.0.1 have an older version of PostgreSQL installed that is not compatible with clustering so the PostgreSQL databases on these servers need to be upgraded.

If the server being upgraded has pre-existing data on it that is used to seed the cluster’s active cache database, this data can be migrated to a Teradata Viewpoint 13.0.1 or later server. See Migrate Pre-Existing Data on page 70.

The destination server must be a properly staged Teradata Viewpoint server with PostgreSQL 8.3.5 installed. Do not upgrade the version of PostgreSQL on the source server until the data migration is complete.

### Migrate Pre-Existing Data

This procedure can take a couple of days, depending on how much data has been collected. As a shortcut, skip the DCS collected data migration and only migrate the Teradata Viewpoint users, roles, permissions, preferences, and configuration. Skipping the migration of DCS data makes the migration process relatively quick.

1. Check to ensure the source and destination servers have the same version of Teradata Viewpoint installed. If the source server has an older version of Teradata Viewpoint installed, upgrade the Teradata Viewpoint software on the source server before continuing with the data migration.

2. On the source server, edit `/data/postgresql/pg_hba.conf` to allow access from the destination server by adding the following line (replace [IP ADDRESS] with the IP address of the destination server):
   ```
   host    all    postgres    [IP ADDRESS]/32       trust
   ```

   **Note:** If it is not the first entry in the `pg_hba.conf` file, the migration fails.

3. Reload postgresql configuration on the source server by typing:
   ```
   /etc/init.d/postgresql reload
   ```

4. Check to ensure the Teradata Viewpoint portal and DCS are stopped on the destination server.
5. On the destination server, migrate all of the configuration data from the source server by typing the following command (replace [SOURCE] with the IP address or hostname of the source server):

```
/opt/teradata/dcs/bin/migrateconfig.sh [SOURCE]
```

6. On the destination server, run the DCS database setup script:

```
/opt/teradata/dcs/bin/setupdb.sh
```

7. Start the Teradata Viewpoint portal and DCS.

**Note:** If continuing on with the next step, the portal might be slow to function as the data is loaded. During the data migration, historical data slowly starts to appear.

8. [Optional] On the destination server, migrate all of the performance and monitoring data collected by the DCS on the source server by typing the following command (replace [SOURCE] with the IP address or the hostname of the source server):

```
/opt/teradata/dcs/bin/migratedata.sh [SOURCE]
```

Depending on how much data has been collected, this could take a couple of days. You can safely ignore any warnings during the restore.

**Upgrade to PostgreSQL 8.3.5**

1. Ensure postgresql is stopped by typing:

```
/etc/init.d/postgresql stop
```

2. Uninstall postgresql-server:

```
rpm -e postgresql-server
```

3. Uninstall postgresql:

```
rpm -e postgresql
```

4. Uninstall postgresql-libs:

```
rpm -e postgresql-libs
```

5. Obtain the postgresql 8.3.5 packages from one of the following sources:

   o Copy packages from **Teradata Viewpoint – Open Source Install Packages** CD.
   
   o Download packages from the **Teradata Software Server**. The Teradata Software Server can be accessed from **Teradata @Your Service** (log on and click the **Teradata Software Server** link).

     a. Select **Certified Configs**.

     b. From the menu on the left, select **Software Patches>Teradata Applications**.

     c. Select Sub Category **Viewpoint** and Release **13.0.1**.
d. Click **Submit**.

e. Select the packages specified below and enter the required fields.

f. Click **Submit** to download.

g. Extract the PostgreSQL packages from the downloaded archive.

The **postgresql** package includes:
- postgresql-8.3.5-2.1.x86_64.rpm
- postgresql-libs-8.3.5-2.1.x86_64.rpm
- postgresql-server-8.3.5-2.1.x86_64.rpm
- postgresql-contrib-8.3.5-2.1.x86_64.rpm

6. Install the following **postgresql** packages:

   - rpm -ivh postgresql-libs-8.3.5-2.1.x86_64.rpm
   - rpm –ivh postgresql-8.3.5-2.1.x86_64.rpm
   - rpm –ivh postgresql-server-8.3.5-2.1.x86_64.rpm
   - rpm –ivh postgresql-contrib-8.3.5-2.1.x86_64.rpm

7. From the command prompt, type:

   ```
   chkconfig postgresql on
   ```

8. Follow the steps in *Create a Teradata Viewpoint Cluster* on page 62.

### Additional Considerations

**LAN or WAN**

The recommended setup of a **Teradata Viewpoint** cluster is that all cluster members be located on the same LAN.

A **Teradata Viewpoint** cluster can be set up over a WAN, but a minimum of 16MB of data is transferred between the active cache database and standby cache database every minute. This amounts to about 23GB a day. Only consider setting up a Viewpoint cluster spanning a WAN if there is adequate bandwidth available.

**Disk Capacity**

The disk capacity available to different generations of Viewpoint servers might be different. When clustering, if the active cache database has more disk capacity than the standby cache database, set a disk quota so that the active cache database does not use up more space than is available on the standby cache database.
To check the capacity available to the cache database, run `df -h /data`. If the capacity on the active cache database is greater than on the standby cache database, run the following command on the active cache database server to limit the capacity used (replace `<number of GBs>` with the limit, in Gigabytes, for the drive):

```
setquota -u postgres 0 <number of GBs>000000 0 0 /data
```

The `setquota` command is available only on staged 13.02 Viewpoint servers and later. All Viewpoint servers staged prior to this time had the same disk capacity, therefore it is not necessary to run the `setquota` command on those machines. Later releases always have a larger disk capacity.

### Cluster Security

Encryption and authentication between the hosts in the Teradata Viewpoint cluster is disabled, by default.

To encrypt all communications between hosts in a cluster and restrict the hosts that are able to participate in a cluster:

1. Stop all Teradata Viewpoint portals and DCS in the cluster.
2. Enable encryption for messages sent between the hosts in the cluster.
   a. Open the following file on every server in the cluster:
      `/etc/opt/teradata/viewpoint/cluster-protocol-stacks.xml`
   b. Uncomment the following line:
      ```
      <!-- ENCRYPT encrypt_entire_message="true" sym_init="128"
      sym_algorithm="AES/ECB/PKCS5Padding" asym_init="512"
      asym_algorithm="RSA" /-->
      ```
3. Enable SSL access to the cache database by running the following commands on the Teradata Viewpoint server hosting the active cache database and the standby cache database:
   a. Change to the postgresql directory:
      ```
      cd /data/postgresql
      ```
   b. Assume the postgres user:
      ```
      su postgres
      ```
   c. Generate a certificate signing request:
      ```
      openssl req -new -text -out server.req
      ```
   d. Enter a PEM pass phrase. It can be anything, but must be at least four characters in length.
   e. Press **Enter** to the rest of the questions. There is no need to enter input.
Teradata Viewpoint Clustering

f. Generate the server key:
   openssl rsa -in privkey.pem -out server.key

g. Enter the same pass phrase as above.

h. Remove privkey.rpm:
   rm privkey.pem

i. Create the certificate:
   openssl req -x509 -in server.req -text -key server.key -out server.crt

j. Change the permissions on the key:
   chmod og-rwx server.key

k. Open and edit /data/postgresql/postgresql.conf and change the line from #ssl = off to ssl = on.

l. Exit postgres user:
   exit

m. Restart postgresql:
   /etc/init.d/postgresql restart

4. Enable the use of SSL when Teradata Viewpoint or the DCS connects to the active cache database.
   a. Open the following file on every server in the cluster:
      /etc/opt/teradata/viewpoint/local.cluster.properties
   b. Uncomment the following line:
      #jdbc.options=ssl\=true&sslfactory\=org.postgresql.ssl.
      NonValidatingFactory

5. Enable host authentication to prevent unknown hosts from joining the cluster.
   a. Open the following file on every server in the cluster:
      /etc/opt/teradata/viewpoint/cluster-protocol-stacks.xml
   b. Uncomment the following line:
      <!-- AUTH auth_class="org.jgroups.auth.FixedMembershipToken"
      fixed_members_value="${cluster.hosts}" fixed_members_seperator="","
      /-->

To enable cluster authentication, the cluster.hosts property in
/etc/opt/teradata/viewpoint/local.cluster.properties must only contain IP addresses and not host names.

6. Test cluster communication with security enabled.
   a. Run /opt/teradata/dcs/bin/clustertest.sh on all the servers in the cluster. This command reads in data from the console.
b. Enter console input and ensure that when Enter is pressed, the text appears on the other server’s console.

c. Enter text on each server and ensure it appears on the other server’s console when Enter is pressed. If this does not work, check the configuration in /etc/opt/teradata/viewpoint/local.cluster.properties to see if the cluster.hosts property is set with the correct IP addresses.

d. To enable more debug information, set the cluster.debug.enabled property to true and run /opt/teradata/dcs/bin/clustertest.sh again.

e. Press Ctrl-D on each console to exit.

7. After the cluster communication test succeeds, restart all Teradata Viewpoint portals and DCS in the cluster.

Getting Notifications of Failures

When Teradata Viewpoint detects a failure has occurred that requires the attention of a Teradata Viewpoint administrator, an email can be sent out to a configured list of recipients. Emails are sent out for the following conditions:

- The active DCS is down.
- The active DCS is restored.
- The active cache database is down.
- The active cache database is restored.
- Cache database replication is not working.

1. To configure email alerts, modify the following properties in the /etc/opt/teradata/viewpoint/local.cluster.properties file on the active and standby cache database servers.

   - alert.enabled – Set to true to turn on email alerting.
   - alert.smtpHost - The hostname of the SMTP server is used to send emails.
   - alert.fromAddress – [Optional] Set the from address that appears the email.
   - alert.recipients – A comma-separated list of the email addresses that receive alerts.
Configure Teradata Viewpoint SSL Support

2. Test if notifications are working.  
   **Note:** Firing a test alert is not available.
   
   a. Stop the active DCS.
   b. After 30 seconds, restart the DCS.
   
   An email is sent for the active DCS going down and another one for the active DCS recovering. The standby DCS must be up and running for the alerts to be sent.

**Ports Used for Clustering**

Besides the normal ports required by Teradata Viewpoint, a Teradata Viewpoint cluster uses the ports in the range 22000 to 22010 for cluster communications.

**Load Balancing**

To make all Teradata Viewpoint portals in a cluster appear as a single host and to protect end-users from a single host failure, a third-party load balancer can be set up to split traffic between the running Teradata Viewpoint portals.

Configuration of a third-party load balancer is outside the scope of this guide.

**Configure Teradata Viewpoint SSL Support**

Enable users to access the Viewpoint server using an HTTPS connection. If clustering is used, perform this step on all Viewpoint servers in the cluster.

**Configure Viewpoint for SSL support**

To allow HTTPS communication to the Viewpoint server on port 443:

1. Log on to the Teradata Viewpoint server (Linux) as root.
   
   a. Open the following file:
      
      ```
      /opt/teradata/viewpoint/conf/server.xml
      ```
   
   b. Search for an XML block similar to the following and uncomment it by removing the surrounding <!--and -->:
      
      ```
      <!--
      <Connector port="443" maxHttpHeaderSize="8192"
      maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
      enableLookups="false" disableUploadTimeout="true"
      acceptCount="100" scheme="https" secure="true"
      clientAuth="false" sslProtocol="SSL" algorithm="IbmX509"/>
      -->
      ```
Configure Teradata Viewpoint SSL Support

2. Save the server.xml file.

[Optional] Configure All Viewpoint Access to be Over SSL

To force all users of Teradata Viewpoint to access the server using HTTPS:

1. Log on to the Teradata Viewpoint server (Linux) as root.

2. Open /opt/teradata/viewpoint/conf/web.xml.

3. Add the following XML block to the end of the file, immediately before the existing </web-app> tag at the end of the file:

   <security-constraint>
     <web-resource-collection>
       <web-resource-name>Viewpoint</web-resource-name>
       <url-pattern>/*</url-pattern>
     </web-resource-collection>
     <user-data-constraint>
       <transport-guarantee>CONFIDENTIAL</transport-guarantee>
     </user-data-constraint>
   </security-constraint>


Create a Self-Signed Certificate

If you already have a trusted certificate from a certificate authority such as VeriSign®, skip to Import a Certificate on page 78 to import it. If you do not have a trusted certificate, use the following procedure to create your own self-signed certificate.

1. If you have not already done so, complete the steps to Configure Viewpoint for SSL support on page 76.

2. Log on to the Teradata Viewpoint server (Linux) as root.

3. Enter the following command and then follow the instructions on the screen:

   keytool -genkey -alias tomcat -keyalg RSA

4. Enter the password: changeit.

5. In the What is your first and last name field, enter your server domain name.

6. In the organization unit field, enter your division name.

7. In the organization field, enter your company name.

8. In the city, state, and country field, enter your city, state, and country.
Configure Teradata Viewpoint SSL Support

9. Type yes, and press Enter if the entered information is correct.

10. When prompted for a password, press Enter.

11. Restart Viewpoint with the following command:

   /etc/init.d/viewpoint restart


   Your self-signed certificate is created and installed.

Create a Certificate Signing Request

When using a self signed certificate, a warning message is displayed to end users about the server’s security certificate not being trusted. To avoid this message, you can obtain a trusted certificate by generating a Certificate Signing Request (CSR) and submitting the request to a trusted Certification Authority (CA).

1. Log on to the Teradata Viewpoint server (Linux) as root.

2. Create a CSR in a file called viewpoint.csr:

   $JDK5_64_HOME/bin/keytool –certreq –alias tomcat –file viewpoint.csr

3. Enter the password: changeit.

4. Submit the generated CSR to a trusted Certification Authority.

5. When you get the trusted certificate, follow the steps in Import a Certificate on page 78.

Import a Certificate

After you have a signed certificate, use the following procedure to import it into the Java keystore. In the steps below, type the keytool command all on one line with a space where the line breaks are shown.

1. Log on to the Teradata Viewpoint server (Linux) as root.

2. Install the Signed Certificate generated from the Certificate Signing Request:

   $JDK5_64_HOME/bin/keytool -import -alias tomcat -trustcacerts -file <your_certificate_filename>

3. Enter the password: changeit.

Install a CA Certificate in Cacerts Keystore

If you receive any errors when installing the certificate, they are most likely the result of not having the CA certificate installed in the cacerts keystore.

1. Log on to the Teradata Viewpoint server (Linux) as root.
Configure Teradata Viewpoint SSL Support

2. Install the trusted CA certificate:

   $JDK5_64_HOME/bin/keytool -import -alias tomcat -keystore
   $JDK5_64_HOME/jre/lib/security/cacerts -trustcacerts -file
   <your_certificate_filename>

3. Enter the password: **changeit**.

Certificates have different requirements for installation; therefore, refer to the documentation for the Java **keytool** command for additional configuration steps and options: [http://java.sun.com/j2se/1.5.0/docs/tooldocs/solaris/keytool.html](http://java.sun.com/j2se/1.5.0/docs/tooldocs/solaris/keytool.html)
## Teradata Viewpoint Properties

**Teradata Viewpoint** has a simple key-value properties table which is used to set various configuration options.

### Available Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Values</th>
<th>Default</th>
<th>Effect</th>
<th>Restart Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>viewpoint.shareableportlets.enabledbydefault</code></td>
<td>true or false</td>
<td>false</td>
<td>When true, shareable portlets are enabled by default; that is, it is not necessary for an <strong>Teradata Viewpoint</strong> Administrator to enable the portlet in the Portlet Library.</td>
<td>No</td>
</tr>
<tr>
<td><code>viewpoint.web.caching.dailyexpiry.enable</code></td>
<td>true or false</td>
<td>true</td>
<td>When true, web assets such as JS and CSS are given an expiration date of 2:00 a.m. the next morning. The browser does not check again for those assets until that time.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>When false, the expiration caching is disabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>When disabling caching (for example, before upgrading <strong>Teradata Viewpoint</strong>), the web assets change, but the browser does not check for new assets because of the expired tag.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>When caching is enabled, <strong>Teradata Viewpoint</strong> only checks this property (to determine whether caching should be disabled) at the switchover time (that is, every day at 2:00 a.m.). Disabling caching only takes effect after 2:00 a.m., unless <strong>Teradata Viewpoint</strong> is restarted. However, this does not change the fact that the browser keeps caching until 2:00 a.m. If caching is disabled, <strong>Teradata Viewpoint</strong> frequently checks if caching has been re-enabled. Enabling caching takes effect immediately.</td>
<td></td>
</tr>
</tbody>
</table>
### Accessing Properties

These Teradata Viewpoint properties (specifically the property table in the td_portal database), can be accessed programmatically using a Java DAO or a command-line utility.

**PropertyDao**

The com.teradata.commons.util.property.PropertyDao interface in the CommonsSecurity project (which should ultimately be moved into CommonsUtils) provides a simple interface for the basic property CRUD operations. An implementation is provided by com.teradata.commons.util.property.impl.JdbcPropertyDao, and that Spring bean can be referenced as sfPropertyDao.

**vp-property.sh**

The vp-property.sh script in the $CATALINA_HOME/bin directory is a utility to read, write, delete, list, and load Teradata Viewpoint properties. Run `vp-property.sh help` for extensive online help. The help content is noted below for reference. Consult the online help for the latest and most accurate information.

**NAME**

vp-property.sh - access the Viewpoint property table

**SYNOPSIS**

vp-property.sh read key

vp-property.sh write key value

vp-property.sh delete key
Teradata Viewpoint Properties

vp-property.sh list [file.props]
vp-property.sh load file.props
vp-property.sh loadnice file.props
vp-property.sh usage|help
vp-property.sh config

DESCRIPTION

vp-property.sh allows administrators to read, write, delete, list and load Viewpoint "properties", as set in the 'property' table of the 'td_portal' database. This executable, a shell/batch file that executes Java code, is typically located in /opt/teradata/viewpoint/bin/vp-property.sh and should be executed from that directory, as the script relies upon the exact location of certain JAR files.

Also, note that in order to connect to the 'td_portal' database, this program needs to gather database connectivity information, which can be automatically gleaned from the server.xml file in the viewpoint/conf directory. This program uses the following strategy to locate the server.xml file:

1. Check if there exists a file $VP_PROPERTY_XML. The user can set this environment variable to point at a preferred server.xml file.
2. If not, check if there exists a file ../conf/server.xml relative to the current working directory (which should be the viewpoint/bin dir).
3. If not, check if there exists a file $CATALINA_HOME/conf/server.xml
4. Failed to find server.xml, display error message to user.

The commands are as follows:

read key print the value for the property identified by key.
write key value set the value for the property identified by key.
delete key remove the property identified by key.
list [file.props] print all properties, optionally outputting to the specified file.
load file.props set all properties loaded from file.props, which must be in the standard Java properties file format.
loadnice file.props set new properties loaded from file.props, which must be in the standard Java properties file format, but without overwriting existing properties.
Teradata Viewpoint Properties

usage|help  
the usage or help commands print help content.

config  
prints the location of the server.xml file that is being used, and the database config options gathered from that file.

EXAMPLES

vp-property.sh read viewpoint.version
[property found]
viewpoint.version=13.0.0.1

vp-property.sh write viewpoint.version 14.0
[overwrote property, previous value: 13.0.0.1]

vp-property.sh load my.props
[wrote 5 properties total, overwrote 5, from my.props]

NOTES

The first line of output from this program is always a status line.

*Escape characters* may not be properly rendered to the shell by the read and list commands under certain rare circumstances. If this occurs, use the 'list [file.props]' command to output to a file which will be formatted per the Java properties file spec.

A property can have, according to the table schema, a *null value*. However, this utility renders null values as 'null', and does not have a facility to set a null property value. It is recommended that a property be deleted rather than use null.

HISTORY

Added in Viewpoint 13.0.
Client-PC Recommendations

Browser Requirements

Teradata Viewpoint 13.10 supports the following browsers:

- Mozilla Firefox 3.5 (recommended)
- Internet Explorer 7
- Internet Explorer 6

Recommendations by PC Class

For PCs below the minimum recommended configuration (for example, 800MHz PIII, 512MB memory):

- Usable with a maximum of one portlet per page.
- Usable with two low-impact portlets per page.

For PCs with the minimum recommended configuration (for example, 1.8GHz Pentium M or 3GHz Pentium 4, 1GB memory):

- Usable with up to four portlets per page.
- Poor load times (such as 30 seconds) when using Internet Explorer and multiple high-impact portlets on a page.

For PCs above the minimum recommended configuration (for example, 2GHz or better Core 2 Duo, 1GB memory), expect:

- Good load times with multiple portlets on a page and a quick response when drilling down.
- Possible performance problems with Microsoft Internet Explorer; switch to Mozilla Firefox for best performance.

Portlet Load Times

All portlets have a similar load time when they are alone on a page. Load time is similar for Microsoft Internet Explorer and Mozilla Firefox. When there are several portlets on a page, high-impact portlets slow the load time more than low-impact portlets. Also, Mozilla Firefox loads multiple portlets faster than Microsoft Internet Explorer.

There is no value in putting more than four portlets on a page because you cannot see them all at once.
Portlet Load Times

Portlets in the medium-impact and high-impact class run time-consuming queries to collect their data. The results are cached to improve load time, but occasionally a user has to wait up to 30 seconds longer than usual if their query is the one loading the cache.

The portlet categories are:

**Low impact**
- My Queries
- Query Monitor (unless a very large number of queries is displayed)
- Remote Console
- SQL Scratchpad
- System Health
- Today's Statistics

**Medium impact**
- Alert Viewer
- Calendar
- Canary Response Times
- Lock Viewer
- Metrics Analysis
- Node Resources
- Productivity
- Space Usage
- Viewpoint Monitoring
- Workload Health

**High impact**
- Capacity Heatmap
- Metrics Graph
- Workload Designer
- Workload Monitor
Install Teradata Viewpoint for Electronic Software Distribution

If Teradata Viewpoint was purchased under the Teradata Electronic Software Distribution Management (ESDM) program, then the Teradata Viewpoint packages have not yet been installed on the Teradata Viewpoint server. To install the Teradata Viewpoint packages, go to Upgrade to Teradata Viewpoint 13.10.xx.xx on page 86, and follow the instructions starting with step 3.

Upgrade to Teradata Viewpoint 13.10.xx.xx

Starting with the Teradata Viewpoint 13.03 release, an install script is available to simplify the upgrade the process. This script does the following:

1. Checks for an appropriate version of Java.
2. Ensures the required packages are located in the same directory as the script.
3. Stops any running Teradata Viewpoint services.
4. Installs the new Teradata Viewpoint packages if they are not already installed.
5. [Optional] Starts Teradata Viewpoint services.
6. [Optional] Uninstalls and cleans up older versions of Teradata Viewpoint.

Upgrade Teradata Viewpoint

1. Download the Teradata Viewpoint 13.10 software and install script.
2. Run the install script.
3. Apply customizations.

Download the Teradata Viewpoint 13.10 Software

1. Log on to the Teradata Software Server. The Teradata Software Server can be accessed from Teradata @Your Service (log on and click the Teradata Software Server link).
2. Select Certified Configs.
3. From the menu on the left, go to Software Patches > Teradata Applications.
Upgrade to Teradata Viewpoint 13.10.xx.xx

5. Click **Submit**.

6. Check **Select all packages for download**.

7. Enter your personal **User Name, E-Mail, Site ID, and Change Control Number** fields.

8. Click **Submit**.

9. Click **Download** to download an archive containing the **Teradata Viewpoint** packages.

10. Extract the **Teradata Viewpoint** software and install script from the download archive.

### Run the Install Script

1. Place all the downloaded packages and install script in the same folder on the Viewpoint server.

2. Log on to the Viewpoint server as the root user and change directory to where the Viewpoint packages and install script are located.

3. Ensure the install script has permission to run (replace **xx** with correct patch version).

   ```
   chmod +x install-viewpoint-13.10.xx.xx.sh
   ```

4. Run the install script (replace **xx** with correct patch version).

   ```
   ./install-viewpoint-13.10.xx.xx.sh
   ```

5. Press **Y** for yes or **N** for no, when prompted about being licensed and current with the appropriate subscriptions for certain packages.

6. Press **Y** and then **Enter** when asked to start the **Teradata Viewpoint** Services.

7. Press **Y** and then **Enter** when asked about uninstalling and cleaning up previously installed versions of **Teradata Viewpoint**.

8. Before accessing **Teradata Viewpoint**, clear the cache of the web browser to ensure that new versions of all files will be retrieved.

9. If **Teradata Viewpoint** is not accessible one minute after start up, do the following:

   a. Open the Teradata Viewpoint log file located at

      ```
      /opt/teradata/viewpoint/logs/viewpoint.log
      ```

   b. Look for any errors.

      All errors include the keyword **ERROR**
10. If no data shows up in **Teradata Viewpoint**, do the following:

   a. Open the Data Collection log file located at
      `/opt/teradata/dcs/logs/dcs.log`

   b. Look for any startup or collection errors.
      All errors include the keyword `ERROR`

### Install and Uninstall Teradata Viewpoint Packages Manually

#### Handle Failed Upgrades of Teradata Viewpoint

During the installation of the dcs, viewpoint, and camalert RPMs, modifications might be made to the tables and data within the Postgres database. These modifications are necessary to ensure the database is synchronized with the version of the software you are installing.

When installing these RPMs (either manually or using the installation script), ensure that there are no errors reported as a part of any database modifications.

If errors are reported as a part of the installation, uninstall the RPM and fix the situation that caused the error. The resolution of the error depends upon the problem. The discussion of what the resolution might be is outside the scope of this document.

After you have uninstalled the RPM and solved the problem, install the same RPM again to successfully upgrade the database and the software.

### Install Teradata Viewpoint Packages Manually

The install script automatically installs and uninstalls all **Teradata Viewpoint** packages. If necessary, you can also install the **Teradata Viewpoint** packages manually. Use the `rpm -ivh` command to install each package. For example, to install the 13.03.00.01 version of the camactivemq package, run the following command:

```
rpm -ivh camactivemq_SLES10_x8664.13.03.00.01-1.rpm
```

Install the packages in the following order:

1. camactivemq
2. camalert
3. camnotification
4. dcsopen
5. dcs
6. tmsmonitoropen
Uninstall Teradata Viewpoint Packages Manually

If necessary, you can also uninstall the Teradata Viewpoint packages manually. Use the `rpm -e` command to uninstall each package. For example, to uninstall the 13.10.00.00 version of the tasmportlets package, run the following command:

```
rpm -e tasmportlets-13.10.00.00-1
```

Uninstall the packages in the following order:

1. tasmportlets
2. tdmgmtportlets
3. camportlets
4. tdselfsrvportlets
5. viewpoint
6. viewpointopen
7. tmsmonitor
8. tmsmonitoropen
9. dcs
10. dcsopen
11. camnotification
12. camalert
13. camactivemq
Apply Customizations

Some custom configuration changes applied in the previous version of Teradata Viewpoint must also be applied to the newly installed version. This includes:

- Enabling SSL (https).
- Installing additional portlets, including TMSM or any other portlet bundles previously installed in Teradata Viewpoint.

**Note:** This is only necessary if upgrading from an earlier release than 13.02.00.03. In 13.02.00.03 and later, deployed portlets are redeployed on upgrade.

- Changing the session timeout.

**Note:** This is only necessary if upgrading from an earlier release than 13.03.00.00. In 13.03.00.00 and later, the session timeout settings remain on upgrade. See Change the Session Timeout on page 52.

- Setting up TVI logging to a Teradata TVI queue table.

**Note:** This is only necessary if upgrading from an earlier release than 13.03.00.00. In 13.03.00.00 and later, the session timeout settings remain on upgrade. See Configure Viewpoint to Log to TVI on page 50.

Set Up New Collectors

Teradata Viewpoint 13.10 contains new data collectors that require new permissions to Teradata. For information about these new collectors, see Teradata System Preparation on page 8 and Configure Viewpoint to Monitor a Teradata Database System on page 14.

Apply LDAP Customizations

If upgrading from Teradata Viewpoint 13.0.0 or earlier and LDAP authentication is used, the LDAP configuration that was previously stored in server.xml needs to be manually transferred to the LDAP SERVERS view of the new Viewpoint LDAP Servers portlet.

1. Use the following table to map the old server.xml configuration parameters to the new Viewpoint Configuration portlet fields.

<table>
<thead>
<tr>
<th>server.xml Parameter</th>
<th>Viewpoint Configuration Portlet Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>jndiConnectionURL</td>
<td>URL</td>
</tr>
<tr>
<td>jndiUserPattern</td>
<td>Name Matching -&gt; DN Pattern Bind</td>
</tr>
<tr>
<td>jndiConnectionName</td>
<td>Name Matching -&gt; User Search -&gt; Service account DN</td>
</tr>
<tr>
<td>jndiConnectionPassword</td>
<td>Name Matching -&gt; User Search -&gt; Service account password</td>
</tr>
<tr>
<td>jndiUserSearch</td>
<td>Name Matching -&gt; User Search -&gt; Search pattern</td>
</tr>
<tr>
<td>jndiUserBase</td>
<td>Name Matching -&gt; User Search -&gt; Search base</td>
</tr>
<tr>
<td>jndiUserSubtree</td>
<td>Name Matching -&gt; User Search -&gt; Search extent</td>
</tr>
<tr>
<td>server.xml Parameter</td>
<td>Viewpoint Configuration Portlet Field</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>jndiFirstNameAttribute</td>
<td>LDAP first name attribute</td>
</tr>
<tr>
<td>jndiLastNameAttribute</td>
<td>LDAP last name attribute</td>
</tr>
<tr>
<td>jndiEmailAttribute</td>
<td>LDAP email attribute</td>
</tr>
<tr>
<td>autoProvision</td>
<td>Turn on auto-provisioning</td>
</tr>
<tr>
<td>autoProvisionRoles</td>
<td>Automatically assign these roles</td>
</tr>
<tr>
<td>autoProvisionEmailDomain</td>
<td>Default email domain</td>
</tr>
<tr>
<td>jndiUserRoleName</td>
<td>Role mapping -&gt; Attribute name</td>
</tr>
<tr>
<td>jndiRoleMappings</td>
<td>Role mapping -&gt; LDAP value &amp; Viewpoint role</td>
</tr>
</tbody>
</table>