



System Administrator's Guide



Contents

Chapter 1

Preparing for Updates

About Upgrades and Updates	8
Preparing for Cloud Connectivity	8
Cloud Reports	8
Performance Profiling	8
Determining the Data Collector Version	9
Data Collector Version via the Portal	9
Data Collector Version via the Command-Line Interface	9
Data Collector Updates with an aptare.jar File	11
Manual Download of the aptare.jar File	11
Portal Updates	11

Chapter 2

Backing Up and Restoring Data

Best Practices for Disaster Recovery	12
Oracle Database Backups	12
File System Backups	13
Backing Up the Oracle Reporting Database	15
Perform a Cold Backup of the Database	15
Reporting Database Export Backups	16
Back Up the Database On Demand	20
Restoring the APTARE IT Analytics System	21
Performing a Full APTARE IT Analytics System Restore	21
Restoring the Oracle Reporting Database	21
Importing the Oracle Database	22
Restoring When a Cold Backup is NOT Available	23
Backing Up the OpenLDAP Database	24
Restoring the OpenLDAP Database	24
Migrating OpenLDAP: Linux to Linux	24
Migrating OpenLDAP: Windows to Linux	25
Migrating OpenLDAP: Linux to Windows	26

Chapter 3

Monitoring APTARE IT Analytics

Starting and Stopping Portal Server Software	27
Starting and Stopping the Reporting Database	28
Starting and Stopping Data Collectors	30
Monitoring Tablespace	31

Chapter 4

Accessing APTARE Reports with the REST API

Setting Up Authentication	32
Extracting Data from Tabular Reports (with pagination)	32
Exporting Reports	33
Exporting Custom Dashboards	33
Sample Client Side Java Code for Calling the REST API	34
Base Class for Testing	34
Class for Paginated Data Extraction from a Tabular Report	35
Class for Exporting Reports and Dashboards	37

Chapter 5

Defining NetBackup Estimated Tape Capacity

NetBackup Estimated Tape Capacity Overview	40
Updating the Estimated Capacity Table	41
Listing Volume Pool IDs and Media Types	41

Chapter 6

Automating Host Group Management

About Automating Host Group Management	42
Task Overview: Managing Host Groups in Bulk	43
Preparing To Use PL/SQL Utilities	44
General Utilities	45
Categorize Host Operating Systems by Platform and Version	45
Identifying a Host Group ID	48
Finding a Host Group ID	48
Move or Copy Clients	49
Organize Clients by Attribute	50
Move Host Group	51
Delete Host Group	51
Move Hosts and Remove Host Groups	51
Organize Clients into Groups by Backup Server	53
Merge Duplicate Backup Clients	54
Bulk Load Utilities	55
Load Host Aliases	55
Load Details of New Hosts or Update Existing Hosts	57
Load Relationships Between Hosts and Host Group	59
Symantec NetBackup Utilities	61
Automating NetBackup Utilities	61
Organize Clients into Groups by Management Server	62
Set Up an Inactive Clients Group	65
Set Up a Host Group for Clients in Inactive Policies	65
Set Up Clients by Policy	66
Set Up Clients by Policy Type	67
IBM Tivoli Storage Manager Utilities	68
Set Up Clients by Policy Domain	68
Set Up Clients by IBM Tivoli Storage Manager Instance	69
Scheduling Utilities To Run Automatically	70
Example—Scheduling Utilities to Run Automatically	70

Chapter 7

Attribute Management

Attribute Bulk Load Utilities	72
Attribute Naming Rules	73
Rename Attributes Before Upgrading	74
Load Host Attributes and Values	75
Create a CSV File	75
Execute the Load Utility	75
Load Attributes and Values and Assign to Hosts	77
Create a CSV File of Hosts, Attributes, and Values	77
Execute the Load Host Attribute Utility	78
Verify the Host Attributes Load	79
Load Array Attributes and Values and Assign to Arrays	80
Create a CSV File of Arrays, Attributes, and Values	80
Execute the Load Array Attribute Utility	81
Verify the Array Attributes Load	82
Overview of Application Attributes and Values	83
Load Application Database Attributes and Values	83
Create a CSV File of Application Database Objects and Attributes	84

Execute the Load Application Database Attribute Utility	85
Verify the Application Database Attributes Load	86
Load MS Exchange Organization Attributes and Values	86
Create a CSV File of Exchange Organization Objects and Attributes.	87
Execute the Load MS Exchange Organization Attribute Utility	88
Verify the MS Exchange Organization Attributes Load	89
Load LUN Attributes and Values	90
Create a CSV File of LUN Objects and Attributes.	90
Execute the Load LUN Attribute Utility	91
Verify the LUN Attributes Load	92
Load Switch Attributes and Values.	93
Create a CSV File of Switches, Attributes, and Values.	93
Execute the Load Switch Attribute Utility.	94
Verify the Switch Attributes Load	95

Chapter 8

Importing Generic Backup Data

About Generic Backup Data Collection	97
Configuring Generic Backup Data Collection.	98
CSV Format Specification	98
Manually Loading the CSV File	99

Chapter 9

Backup Job Overrides

Configure a Backup Job Override	101
---	-----

Chapter 10

Managing Host Data Collection

Identifying Hosts by WWN to Avoid Duplicates	104
Setting a Host's Priority	105
Determining Host Ranking	107
Loading Host and WWN Relationships	108
Loading the Host HBA Port Data	108

Chapter 11

System Configuration in the Portal

System Configuration: Functional Areas	110
System Configuration: Functions.	111
Navigation Overview	111
System Configuration Parameter Descriptions: Additional Info	113
Data Collection: Capacity Chargeback	113
Database Administration: Database	113
Host Discovery: EMC Avamar.	113
Host Discovery: Host.	114
Custom Parameters	115
Adding/editing a custom parameter	115
Portal Customizations	115
Configuring Global Default Inventory Object Selection.	116
Restricting User IDs to Single Sessions	116
Customizing Date Format in the Report Scope Selector	116
Customizing the Maximum Number of Lines for Exported Reports	116
Customizing the Total Label Display in Tabular Reports.	117
Customizing the Host Management Page Size.	117
Customizing the Path and Directory for File Analytics Database	117
Configuring Badge Expiration	117
Configuring the Maximum Cache Size in Memory	118
Configuring the Cache Time for Reports.	118

Chapter 12

Performance Profile Schedule Customization

Customize the Performance Profile Schedule	119
--	-----

Chapter 13

Configuring LDAP

About User Authentication	121
Switching from OpenLDAP to Another LDAP Service	121
User Administration Using an External Authentication Service	124
Creating Portal Super Users	124
Active Directory Tools	125
Using LDP to Find the Base DN	125
Common Active Directory Authentication Errors	126

Chapter 14

Changing Oracle Database User Passwords

Database Connection Properties	128
Modifying the Oracle Database User Passwords	129
Configuring Oracle Passwords in APTARE Configuration Files	129

Chapter 15

Tuning APTARE IT Analytics

Before You Begin Tuning	131
Tuning the Portal Database	131
Performance Recommendations	132
Reclaiming Free Space from Oracle	132

Chapter 16

Defining Report Metrics

Changing Backup Success Percentage	133
Changing Job Status	134
Finding a Host Group ID	134
.	135

Chapter 17

Working with Log Files

About Debugging APTARE IT Analytics	137
Turn on Debugging	137
Database Logging	138
Portal and Data Collector Log Files - Reduce Logging	139
Database SCON Logging - Reduce Logging	141
Refreshing the Database SCON Log	142
Logging User Activity in audit.log	142
Logging Only What a User Deletes	143
Logging All User Activity	143
Data Collector Log Files	144
Data Collector Log File Organization	144
Data Collector Log File Naming Conventions	144
General Data Collector Log Files	149
Find the Event/Meta Collector ID	149
Portal Log Files	150
Database Log Files	153
Installation/Upgrade Log Files	154

Chapter 18

SNMP Trap Alerting

Overview of Alerting	156
SNMP Configurations	156
Standard OIDs	157
Data in an Alerting Trap	157

Chapter 19

SSL Certificate Configuration

SSL Implementation Overview	159
Obtain an SSL Certificate	159
Update the Web Server Configuration to Enable SSL	160
Configure Virtual Hosts for Portal and/or Data Collection SSL	162
If implementing SSL for the Portal Only	162
If implementing SSL for Data Collection Only	163
If implementing SSL for Both the Portal and Data Collection	163
Enable/Disable SSL for a Data Collector	164
Enable/Disable SSL for Emailed Reports	165
Test and Troubleshoot SSL Configurations	165
Create a Self-Signed SSL Certificate	166
Configure the Data Collector to Trust the Certificate	167
Keystore File Locations on the Data Collector Server	167
Import a Certificate into the Data Collector Java Keystore	167
Add a Virtual Interface to a Linux Server	168
Add a Virtual/Secondary IP Address on Windows	170
Default Apache SSL Configuration File	173

Chapter 20

Advanced Configuration for NetBackup Discovery

Discovery Module Overview	183
Activate a Discovery License	184
Modify Discovery System Parameters	185
Why Enable SNMP?	185
About SNMP Probes	186
Enabling SNMP for Windows (NT/2000/XP)	186
Enabling SNMP for Red Hat Linux	187
Enabling SNMP for HP-UX	188
Enabling SNMP for Solaris 8/9	188
Enabling SNMP for Solaris 10	189
Example—Installing Net-SNMP	189
Troubleshooting Net-SNMP Installations	190
.	191

Chapter 21

Data Retention Periods for SDK Database Objects

SDK User-Defined Database Objects	193
Capacity: Default Retention for Basic Database Tables	193
Capacity: Default Retention for EMC Symmetrix Enhanced Performance	195
Capacity: Default Retention for EMC XtremIO	196
Capacity: Default Retention for Dell EMC Elastic Cloud Storage (ECS)	196
Capacity: Default Retention for Microsoft Windows File Services	197
Capacity: Default Retention for Pure Storage FlashArray	197
Cloud: Default Retention for Amazon Web Services (AWS)	197
Cloud: Default Retention for Microsoft Azure	198
Cloud: Default Retention for OpenStack Ceilometer	199
Configure Multi-Tenancy Data Purging Retention Periods	199

Chapter 22

Troubleshooting

Troubleshooting User Login Problems	201
Forgotten Password Procedure	202
Login	202
Connectivity Issues	203
Data Collector and Database Issues	203
Report Emails are not Being Sent	204
General Reporting Issues	206
Performance Issues	207

Copyrights and Trademarks

Legal Notice

Copyright (c) 2019 Veritas Technologies LLC. All rights reserved.

Veritas, and the Veritas Logo, are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at: <https://www.veritas.com/about/legal/license-agreements>

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. VERITAS TECHNOLOGIES LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

<http://www.veritas.com>

Preparing for Updates

This section covers the following topics:

- [About Upgrades and Updates](#)
- [Preparing for Cloud Connectivity](#)
- [Determining the Data Collector Version](#)
- [Data Collector Updates with an aptare.jar File](#)
- [Portal Updates](#)

About Upgrades and Updates

APTARE releases changes to this software through different types of releases:

- **Major release.** Includes all new features and enhancements. If you want to upgrade from to a major release, go to the *APTARE Installation and Upgrade Guide*. If you want to upgrade to the latest major release, you must be running the previous release.
- **Minor release.** Includes mostly fixes and some enhancements to existing features. Minor releases are packaged with an auto-installer.
- **aptare.jar release.** Includes updates to data collectors. This periodically released file encapsulates the main processing logic of the Data Collector.

To receive updates for a minor release, you must upgrade to the corresponding major release. If you want to receive updates, periodically check APTARE's web site for update announcements and instructions.

Preparing for Cloud Connectivity

Cloud Reports

If you have restricted access to the Internet, you will need to enable the following URL for cloud reports:

<https://cloud.aptare.com/remoting/CloudReportService>

Verify the connectivity by entering the URL into a browser window. The following message should display:

"HTTP Status 405 - HessianServiceExporter only supports POST requests"

Performance Profiling

Enable the following URL for Performance Profiling:

<https://cloud.aptare.com/remoting/CommunityService>

Verify the connectivity by enter the URL into a browser window. The following message should display:

"HTTP Status 405 - HessianServiceExporter only supports POST requests"

Determining the Data Collector Version

Two methods are available for checking the version of Data Collectors:

- [Data Collector Version via the Portal](#)
- [Data Collector Version via the Command-Line Interface](#)

Data Collector Version via the Portal

In the Portal, select:

Admin > Data Collection > Collector Updates

Data Collector Version via the Command-Line Interface

To determine your current version of your Data Collector via the command-line interface (CLI)

Linux:

/opt/aptare/mbs/bin/agentversion.sh

Windows:

> C:\opt\aptare\mbs\bin\agentversion.bat

Sample Output:

```
Version information for the Data Collector installed at /opt/aptare on this server DC-
Centos-2
```

```
Version: 9.0.00 08072013-1028
```

```
Version information for datarcvr, aptare.jar and Upgrade Manager at
http://aptareagent.QAtest
```

```
datarcvr Version
```

```
Version: 9.0.0.01
```

```
aptare.jar Version
```

```
Current Version: 9.0.0.03
```

```
Build Number: 12102014-0001
```

```
Upgrade Manager Version
```

```
Current Version: 9.0.0.01
```

```
Build Number: 07032013-1121
```

```
Version information for aptare.jar and Upgrade Manager at /opt/aptare/upgrade on this
server DC-Centos-2
```

```
aptare.jar Version
```

```
Current Version: 9.0.0.01
```

```
Build Number: 08072013-1028
```

```
Upgrade Manager Version
```

```
Current Version: 9.0.0.01
```

Build Number: 07032013-1122

Version information for other jars :

aptare-dc-nbu-col.jar version is: 9.0.0.01|08072013-0003
aptare-dc-confgen.jar version is: 9.0.0.01|08072013-0001
aptare-legacy.jar version is: 9.0.0.01|08072013-0001
aptare-dc-util.jar version is: 9.0.0.01|08072013-0000
aptare-dc-hnas-com.jar version is: 9.0.0.01|06052013-0004
aptare-dc-fw-com.jar version is: 9.0.0.01|08072013-0002
aptare-dc-hnas-col.jar version is: 9.0.0.01|06052013-0004
aptare-dc-fw-col.jar version is: 9.0.0.01|08072013-0002
aptare-dc-nbu-com.jar version is: 9.0.0.01|08072013-0003
aptare-dc-probe.jar version is: 9.0.0.01|08072013-0003
aptare-dc-spi.jar version is: 9.0.0.01|08072013-0001

Validating aptare.jar Version Compatibility - SUCCESS

Data Collector Updates with an aptare.jar File

The Data Collector **aptare.jar** file is periodically updated. The **aptare.jar** encapsulates the main processing logic of the Data Collector.

Data collector updates can happen in the following ways:

- **When data collector services are running:** Data Collectors look for an update every 11 minutes. Once the portal is upgraded, the Data Collector will upgrade automatically.
- **When data collector services are not running:** Data Collectors can be manually updated as mentioned in [Manual Download of the aptare.jar File](#).
- **When data collector services are running and for some reason, such as local changes, the Data Collector must be updated again:** The Portal can be used to start the update from **Admin>Data Collection>Collector Updates**.

Note: The latest distribution of aptare.jar updates is distributed through the regular patch release process.

Manual Download of the aptare.jar File

Use the following procedure to manually update your Data Collector:

1. Use the downloadlib utility to manually download the aptare.jar file. Note that this utility must be run with administrative privileges.
2. If you run the downloadlib utility and you get the following message, it indicates that the restore failed or is in progress: Restore has been running for more than 10 minutes, unable to proceed with collector upgrade.

To proceed, delete the restore.txt file and re-run downloadlib.

Windows: <Home>\upgrade\restore.txt

Linux: <Home>/upgrade/restore.txt

Portal Updates

Portal updates contain feature enhancements and bug fixes. These updates are packaged with an auto-installer.

Once the upgrade package has been installed, perform the upgrade using:

Linux:

/opt/aptare/upgrade/upgrade.sh

Windows:

> C:\opt\aptare\upgrade\upgrade.bat

2

Backing Up and Restoring Data

This section covers the following topics:

- [Best Practices for Disaster Recovery](#)
- [Backing Up the Oracle Reporting Database](#)
- [Restoring the APTARE IT Analytics System](#)
- [Backing Up the OpenLDAP Database](#)

Best Practices for Disaster Recovery

In the event of data loss, for whatever reason, it is critical that you have a backup of the APTARE IT Analytics system. This section lists the key files and data associated with APTARE IT Analytics that you need to protect. These should be backed up regularly to mitigate risk of data loss.

At a high level, your backup and recovery strategy will consist of:

- [Oracle Database Backups](#)—the most critical component of the system
- [File System Backups](#)

Each of these is discussed in detail in subsequent sections.

See [Restoring the APTARE IT Analytics System](#) for steps to recover data that has been backed up.

Oracle Database Backups

Oracle Database – Cold Backup

This should be done about once a month. A cold backup is required of the Oracle data file directories; by default, /data01, /data02, /data03, /data04, /data05, and /data06 for Linux and \oradata for Windows. **Cold backups require Oracle to be shut down**, thereby disrupting the Portal's availability. Perform a cold backup, then back up (export) the database tables on a more regular basis (nightly is recommended). In addition to monthly cold backups, a cold backup is recommended after a significant software upgrade to capture the updated database schema. See [Perform a Cold Backup of the Database](#).

Oracle Database – Export

The reporting database should be exported *nightly*. Exports do not require Oracle to be shut down. See [Backing Up the Oracle Reporting Database](#).

File System Backups

File system backups are required to protect the APTARE IT Analytics application directories, files, and OS-specific settings, such as the registry and services for Windows. The file system backup should also capture the nightly database export, which resides in the file system.

APTARE recommends that you utilize your company's backup method of choice to perform the file system backup. While we recommend a full system backup, we have identified the key files created by APTARE IT Analytics.

APTARE - Created Files and Directory Structures

- The file paths are shown with Linux usage, with the Windows-specific file system noted.

File	Comments
.bash_profile for tomcat and users	
/etc/init.d/*aptare*	
/etc/rc3.d/*aptare*	
/etc/rc5.d/*aptare*	
/data0?	DB server (Linux) Contains the Oracle database files; must be backed up using a Cold Backup. See Perform a Cold Backup of the Database .
\oradata	DB server (Windows) Contains the Oracle database files; must be backed up using a Cold Backup. See Perform a Cold Backup of the Database .
/opt/openldap*, /opt/apache*, /opt/aptare*, /opt/tomcat*	

Other Files

File	Comments
/usr/java	
/etc/profile.d/java.sh	

Note: When backing up the above directories, follow the symbolic links to back up the source directory. For example: /usr/java is typically a symbolic link to /usr/java_versions/jdk<version>

Other Symbolic Links

These symbolic links may vary in your environment. Check the *APTARE Certified Configurations Guide* for the latest third-party and open source versions.

tomcat --> apache-tomcat-5.5.25

openldap --> openldap-2.4.37

apache --> httpd-2.4.6

New Users and Groups

Users: aptare, tomcat (all part of /etc/passwd)

Groups: aptare, dba, tomcat (all part of /etc/group)

Note: Both /etc/passwd and /etc/group should be backed up.

Backing Up the Oracle Reporting Database

As part of your initial installation, you were asked to perform an initial cold backup of your Reporting Database.

For a Cold Backup—stop Oracle and take a backup of the Oracle reporting database by performing a file system backup of /data0?/* for Linux or \oradata for Windows.

Perform a Cold Backup of the Database

Prior to deploying the Portal for operational use and periodically after installation (at least once a month is recommended), it is recommended that you perform a cold backup of the Oracle database. In addition to monthly cold backups, it is also recommended that you take a cold backup after a significant software upgrade to re-capture the updated database schema.

This off-line, cold backup means that you will physically copy or back up the Oracle database data files to another location. This cold backup will simplify the restore process, in the event of unanticipated data loss. With a cold backup, you simply have to restore the files and then import the most recent database export.

To perform a cold backup (Linux)

1. Shutdown the Oracle service:

```
/opt/aptare/bin/oracle stop
```

2. Using your organization's file system backup software, back up all the data files from:

```
$ORACLE_HOME\dbs\initscdb.ora  
/data0?/*
```

To perform a cold backup (Windows)

1. Shut down the Oracle service: **OracleServicescdb** in the Windows Administrative Tools, Component Services window.

2. Backup the following files:

```
$ORACLE_HOME\dbs\iniscdb.ora  
C:\oradata
```

Note: During installation, you could choose a different drive for the `oradata` install, so verify its location before backing up the data.

Reporting Database Export Backups

This method is the preferred method of ensuring that your database is backed up on a regular basis. This is a two-step process:

- [Customizing the Export Script](#)
- [Scheduling the Export Job \(Linux\)](#) or [Scheduling the Export Job \(Windows\)](#)

Customizing the Export Script

A template is provided for automating the database backup process. It must be copied and then customized for your installation.

1. Locate the script template:

Linux: `opt/aptare/database/tools/export_database_template.sh`

Windows: `C:\opt\oracle\database\tools\export_database_template.bat`

2. Before customizing the backup script, `export_database_template.sh|bat`, first **copy** it and then **rename** it to something like: `export_database.sh|bat`

This preserves the template file, which gets overwritten during a Portal upgrade, and provides a file for customization and execution: `export_database.sh|bat`

3. Refer to the relevant steps to customize the script:

- [Linux: Customize the Script](#)
- [Windows: Customize the Script](#)

4. Refer to the relevant steps to schedule the task:

- [Scheduling the Export Job \(Linux\)](#)
- [Scheduling the Export Job \(Windows\)](#)

Important! It is *critical* that the database export file is included in your file system backup policy so that, in the event of a disaster, you can restore and then import the export file.

Linux: Customize the Script

In the `export_database.sh` script:

- Replace `customername` with your relevant company name.
- Replace `/ora_exports` with a directory that is included in your file system backup policy.

```
#!/bin/sh
# The following script is the APTARE IT Analytics database export script for customername

NOTIFY_LIST="support@customername.com"
FILENAME=customername_scdb.exp `date +%m%d%g`
LOGFILENAME=ccustomername_scdb `date +%m%d%g`.log
ORACLE_HOME=/opt/aptare/oracle
ORACLE_SID=scdb
export ORACLE_HOME ORACLE_SID

# Set the export directory
PATHNAME=

# Export the database
/opt/aptare/oracle/bin/exp parfile=/opt/aptare/database/tools/export_scdb.par
file=$PATHNAME/$FILENAME log=$PATHNAME/$LOGFILENAME

if [ $? -eq 0 ]; then
    if [ -f $PATHNAME/$FILENAME ]; then
        if [ -f "$PATHNAME/$FILENAME.gz" ]; then
            rm -f "$PATHNAME/$FILENAME.gz"
        fi
        echo "Done with export"
    fi
else
    echo `date` "Problem with export on customername"
    echo "Problem with export on customername" | mail -s "customername export problem"
$NOTIFY_LIST
    exit 1
fi

gzip -f "$PATHNAME/$FILENAME"

exit 0
```

Windows: Customize the Script

In the `export_database.bat` script:

- Replace **customername** with your relevant company name.
- Replace **C:\tmp** with a directory included in your file system backup policy.
- Customize the **mailto** line to be compatible with your environment.
- If you choose to use a tool other than 7-Zip, change the **software used to zip the file**.

```
@echo off
REM The following script is the APTARE IT Analytics database export script for customername

SET NOTIFY_LIST=support@customername.com

FOR /F "TOKENS=1* DELIMS= " %%A IN ('DATE/T') DO SET CDATE=%%B
FOR /F "TOKENS=1,2 eol=/ DELIMS=/ " %%A IN ('DATE/T') DO SET mm=%%B
FOR /F "TOKENS=1,2 DELIMS=/ eol=/" %%A IN ('echo %CDATE%') DO SET dd=%%B
FOR /F "TOKENS=2,3 DELIMS=/ " %%A IN ('echo %CDATE%') DO SET yyyy=%%B
SET date=%mm%%dd%%yyyy%
set date=%date:=%
REM Set the export directory
SET PATHNAME=
SET FILENAME=aptare_scdb.exp_%date%
SET LOGFILENAME=customername_scdb_date +%m%d%g`.log
SET ZIP_FILENAME=%PATHNAME%\%FILENAME%.zip

REM Export the database
c:\opt\oracle\bin\exp parfile=c:\opt\oracle\database\tools\export_scdb.par
file=%PATHNAME%\%FILENAME% log=$PATHNAME\%LOGFILENAME
ECHO %ZIP_FILENAME%
IF ERRORLEVEL 0 (
    IF exist %PATHNAME%\%FILENAME% (
        IF exist %ZIP_FILENAME% (
            DEL %ZIP_FILENAME%
            echo Done with export
        )
    )
)
IF NOT ERRORLEVEL 0 (
    echo %date% "Problem with export on customername"
    START
    mailto:%NOTIFY_LIST%?subject=20customername%%20export%%20problem^&body=Problem%%20with%%20
    export%%20on%%20customername
)

"c:\Program Files\7-Zip\7z.exe" a %ZIP_FILENAME% %PATHNAME%\%FILENAME%

IF exist %ZIP_FILENAME% (
    IF exist %PATHNAME%\%FILENAME% (
```

```

        DEL %PATHNAME%\%FILENAME%
    )
)

```

Scheduling the Export Job (Linux)

1. Switch to user **aptare**.

```
su - aptare
```

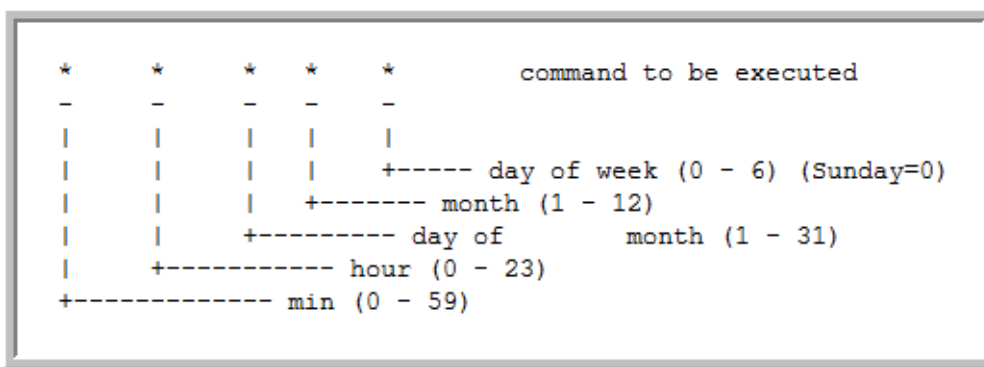
2. Edit or create the crontab file.

```
crontab -e
```

3. Using the following diagram, specify the database export schedule.

Example:

```
04 15 * * * /opt/aptare/utils/export_database.sh 2>&1 >>/tmp/database_export.log
```



4. Verify the newly scheduled job:

```
crontab -l
```

Scheduling the Export Job (Windows)

1. **Start > Programs > Accessories > System Tools > Task Scheduler**
2. Create a new task in the Task Scheduler by specifying the schedule and the script to be run:

```
c:\opt\aptare\utils\export_database.bat
```

Back Up the Database On Demand

This method is useful for cases where an immediate backup/export is required; for example, when Customer Support requests a copy of your database for troubleshooting.

To back up the database tables, APTARE IT Analytics provides an Oracle utility, [exp](#). This utility exports the user `portal`, which contains the database tables. See [Exporting the Oracle Database](#) to create a full export file of all database objects.

For optimum performance, use this utility rather than your favorite backup solution's backup utility (for example, [rman](#)) because most backup solutions require archive logging. APTARE does not enable or expose this setting because archive logging can have a significant, negative impact on performance.

You will import this export in the event that you need to:

- Restore the entire Reporting Database. For details, see [Restoring the APTARE IT Analytics System](#).
- Retrieve a data table that's been corrupted or accidentally deleted. Simply drop the portal user then import the export. See [Importing the Oracle Database](#).

Exporting the Oracle Database

To create a full export file of all objects in the Portal database:

1. Log on to the database server.
 - In a Linux environment, log on to the database server as user `aptare`.
 - In a Windows environment, log on to the database server as a user who is a member of the `ORA_DBA` group.
2. Edit the **export_scdb.par** file to specify a value for `path_to_backup_directory`. The **export_scdb.par** file contains the following parameters:

```
USERID=system/aptaresoftware
BUFFER=128000
GRANTS=Y
ROWS=Y
INDEXES=Y
CONSISTENT=Y
COMPRESS=Y
STATISTICS=NONE
OBJECT_CONSISTENT=Y
FULL=Y
FILE=/path_to_backup_directory/scdb.exp
```

3. Run the following commands:
 - **On Linux** (as user, `aptare`):
`/opt/aptare/oracle/bin/exp parfile=/opt/aptare/database/tools/export_scdb.par`
 - **On Windows**:
`C:\opt\oracle\bin\exp parfile= C:\opt\oracle\database\tools\export_scdb.par`

Restoring the APTARE IT Analytics System

If you experienced data loss due to hardware failure or administrative error, or any of many reasons that may have resulted in a loss that requires some form of restore, APTARE strongly recommends that you contact the APTARE Global Support Services to assist you with determining how to proceed.

The following steps provide guidelines for restoring your system; however, depending on your circumstances, all of these steps may *not* be relevant.

Performing a Full APTARE IT Analytics System Restore

To perform a full system restore, you need to:

1. Follow your company's process to perform a system restore from the full system backup that you took, as described in the previous sections. This should restore the application directories and files, in addition to any OS level-specific files, such as the Windows registry, boot sectors, etc.
2. Restore the Oracle Reporting Database, as described in [Restoring the Oracle Reporting Database](#).

NOTES:

- If you do not have a full system backup, it still may be possible to recover by re-installing the APTARE IT Analytics application, re-installing the Oracle binaries, and then restoring the Oracle Reporting Database. APTARE recommends that you contact the APTARE Global Support Services if you need to follow this recovery method.
- If your data loss is isolated to the Oracle Reporting Database, it may be possible to skip [Step 1](#) above and proceed to [Step 2](#).

Restoring the Oracle Reporting Database

IMPORTANT: Before you try to restore the Reporting Database, contact the APTARE Global Support Services. APTARE prefers to walk you through this process step-by-step. The following steps provide guidance for restoring your database; however, once again, depending on your circumstances, all of these steps may *not* be relevant.

1. Import the most recent version of the database that you exported. See [Importing the Oracle Database](#).
2. If the import of the database fails in [Step 1](#), it is likely that there are issues with your Oracle environment that are preventing Oracle from starting. In this case you will need to restore the database files from your Cold Backup.
 - a. Using the backup software that you used to [Perform a Cold Backup of the Database](#), restore the database with the most recent successful Cold Backup. If you do not have a successful Cold Backup of the Oracle database, see [Restoring When a Cold Backup is NOT Available](#).
 - b. Import the most recent version of the database that you exported. See [Importing the Oracle Database](#).

Importing the Oracle Database

IMPORTANT: The process described below *deletes* your existing APTARE IT Analytics database. Before you try to import the Reporting Database, you should verify that you have no other options for recovery and that you have a valid database export. Contact the APTARE Global Support Services, as APTARE prefers to walk you through this process step-by-step.

Some common problems include:

- **Importing unsuccessful backups.** Ensure that your backups were successful before you accidentally import old data.
- **Importing more than what you need.** Don't restore the entire database or import all database tables if you only need to restore one database table. Import only what you need.

IMPORTANT: Before restoring user objects, stop the Tomcat and Portal processes using [Starting and Stopping Portal Server Software](#).

To import your latest successful export of the Oracle database:

1. Log on to the database server.

- In a Linux environment, log on to the database server as user aptare.
- In a Windows environment, log on to the database server as a user who is a member of the ORA_DBA group.

2. At the command line (**Linux**):

```
sqlplus "/ as sysdba"
SQL> drop user portal cascade;
SQL> drop user aptare_ro cascade;
SQL> @/opt/aptare/database/ora_scripts/create_portal_user.plb;
SQL> @/opt/aptare/database/ora_scripts/create_aptare_ro_user.plb
```

At the command line (**Windows**):

```
sqlplus "/ as sysdba"
SQL> drop user portal cascade;
SQL> drop user aptare_ro cascade;
SQL> @C:\opt\oracle\database\ora_scripts\create_portal_user.plb
SQL> @C:\opt\oracle\database\ora_scripts\create_aptare_ro_user.plb
```

3. Edit the **import_scdb.par** file to specify a value for path_to_backup_directory. The **import_scdb.par** file contains the following parameters:

```
USERID=system/aptaresoftware
FROMUSER=portal, aptare_ro
TOUSER=portal, aptare_ro
BUFFER=128000
IGNORE=Y
COMMIT=N
GRANTS=Y
ROWS=Y
INDEXES=Y
CONSTRAINTS=Y
```

```
LOG=/path_to_log/import_scdb.log  
FILE=/path_to_backup_directory/scdb.exp
```

4. Run the following commands:

- **On Linux** (as user, **aptare**):

```
/opt/aptare/oracle/bin/imp {full_path_and_file_name_of_export_file} parfile=/opt/aptare/  
database/tools/import_scdb.par
```

- **On Windows:**

```
C:\opt\oracle\bin\imp {full_path_and_file_name_of_export_file} parfile= C:\opt\oracle\  
database\tools\import_scdb.par
```

Restoring When a Cold Backup is NOT Available

If you do not have a successful cold backup of your Oracle database, take the following steps to recover your APTARE IT Analytics Oracle database.

1. Re-install the Oracle binaries. See the *APTARE Installation and Upgrade Guide*.
2. Re-install the database schema. See “APTARE IT Analytics Schema Installation” in the *Portal Installation Guide for Linux* or the Portal Install section in the *APTARE Installation and Upgrade Guide for Linux*.
3. Import the latest successful export of your Oracle database to restore the Portal user objects. See [Importing the Oracle Database](#).

Backing Up the OpenLDAP Database

The OpenLDAP database is part of the Portal Server software.

When you do a full system backup (see [File System Backups](#)), your LDAP database should be covered in that backup so these steps may not be necessary.

Windows

1. `c:\opt\openldap\slapcat -f c:\opt\openldap\slapd.conf -l ldap.ldif`
2. Backup the `ldap.ldif` file.

Linux

1. `/opt/openldap/sbin/slappcat -f /opt/openldap/etc/openldap/slapd.conf -l /opt/openldap/ldap.ldif`
2. Backup the `/opt/openladap/ldap.ldif` file.

Restoring the OpenLDAP Database

To **restore** the OpenLDAP database, import it using the commands in [Step 7](#) through [Step 9](#) in [Migrating OpenLDAP: Linux to Linux](#).

Migrating OpenLDAP: Linux to Linux

On your current Linux production Portal Server

1. Log in to your Linux production Portal server as **root**.
2. `cd /opt/openldap`
3. `./sbin/slappcat -f ./etc/openldap/slapd.conf -l /tmp/ldap.ldif`
This will create a dump of your entire LDAP database to the `/tmp/ldap.ldif` file.
4. Copy this file to your *new* Linux system.

On your *new* Linux Portal Server

1. Verify that the file called `ldap.ldif` has been copied to the *new* Linux Portal server.
2. Log in as **root**.
3. `cd /opt/aptare/bin`
4. `./openldap stop`
5. Make a backup of the contents of the OpenLDAP data directory:
`/opt/openldap/var/openldap-data`
6. `rm -f /opt/openldap/var/openldap-data/*`
7. `/opt/openldap/sbin/slappadd -f /opt/openldap/etc/openldap/slapd.conf -l <full_path_to_ldap_ldif>`
8. Verify that the database was imported successfully by executing the command:

```
/opt/openldap/sbin/slapcat -f /opt/openldap/etc/openldap/slapd.conf
```

This will print to the screen a dump of your entire LDAP database.

9. Restart the OpenLDAP service using the command:

```
/opt/aptare/bin/openldap start
```

Migrating OpenLDAP: Windows to Linux

To migrate the OpenLDAP database from Windows to Linux, complete the following steps.

On your current Windows production Portal Server

1. Log in to your Windows production Portal server.
2. Open a DOS command window for execution of the commands in the next steps.
3. `cd C:\opt\openldap`
4. `slapcat -f slapd.conf -l ldap.ldif`

This will create a dump of your entire LDAP database into a file: LDAP.LDIF

5. Copy this file to your *new* Linux Portal Server.

On your *new* Linux Portal Server

1. Verify that the file called LDAP.LDIF has been copied to the *new* Linux Portal Server.
2. Log in as **root**.
3. `cd /opt/aptare/bin`
4. `./openldap stop`
5. Make a backup of the contents of the directory:
`/opt/openldap/var/openldap-data`
6. `rm -f /opt/openldap/var/openldap-data/*`
7. `/opt/openldap/sbin/slapadd -f /opt/openldap/etc/openldap/slapd.conf -l <full_path_to_ldap_ldif>`
8. Verify that the database was imported successfully by executing the command:
`/opt/openldap/sbin/slapcat -f /opt/openldap/etc/openldap/slapd.conf`
This will print to the screen a dump of your entire LDAP database.
9. Restart the OpenLDAP service using the command:
`/opt/aptare/bin/openldap start`

Migrating OpenLDAP: Linux to Windows

To migrate the OpenLDAP database from Linux to Windows, complete the following steps.

On your *new* Windows Portal Server

1. Verify that the file **LDAP.LDIF** has been copied to the new Windows Portal Server.
2. Log in as a Local Administrator user.
3. Execute

```
c:/opt/aptare/utils/stopldap.bat
```

4. Make a backup of the contents of the directory:

```
c:/opt/openldap/var/openldap-data
```

5. Delete the contents of the directory:

```
c:/opt/openldap/var/openldap-data/*
```

6. Execute:

```
c:/opt/openldap/slapadd -f c:/opt/openldap/slapd.conf -l <full_path_to ldap_ldif>
```

7. Verify that the database was imported successfully by executing the command:

```
c:/opt/openldap/slapcat -f c:/opt/openldap/slapd.conf
```

This will print to the screen a dump of your entire LDAP database.

8. Restart the OpenLDAP service using the command:

```
c:/opt/aptare/utils/startldap.bat
```

Monitoring APTARE IT Analytics

This section covers the following topics:

- [Starting and Stopping Portal Server Software](#)
- [Starting and Stopping the Reporting Database](#)
- [Starting and Stopping Data Collectors](#)
- [Monitoring Tablespaces](#)

Starting and Stopping Portal Server Software

Restarting the Portal Server does not have a negative impact on the Data Collector, assuming that the Data Collector established an initial connection to the Portal Server. You do not need to restart the Data Collector after you restart the Portal Server. If the Data Collector is sending data at the time that the Portal Server becomes unavailable, the Data Collector receives an error, and then tries to send the information again. The Data Collector continues to retry and sends alerts until it can reconnect and retransmit.

When you start the Portal Server software, you will start all services that are not already running. How you start and stop the Portal Server software depends on your operating system. Choose the procedure that represents your operating system:

To start Portal Server software on Windows

1. Locate the script to start the Portal Server software:
C:\opt\aptare\utils\startportal.bat
2. Double-click to start the software.
3. Verify the following services are running using the Windows Services Control panel:
 - APTARE Agent Tomcat
 - APTARE Apache
 - APTARE OpenLDAP
 - APTARE Portal Tomcat
 - Oracle Service SCDB
 - OracleSCDBTNSListener

To stop Portal Server software on Windows

1. Locate the script to stop the Portal Server software:
`C:\opt\aptare\utils\stopportal.bat`
2. Double-click to stop the software.
3. Verify the following services are stopped using the Windows Services Control panel:
 - APTARE Portal Tomcat

To start Portal Server software on Linux

As user root, run one of the following commands:

```
# cd /opt/aptare/bin
```

```
./tomcat-portal start|restart
```

Individual component startup scripts can be found in the /opt/aptare/bin directory. Startup log files can be found in the /opt/aptare/logs directory.

To stop Portal Server software on Linux

As user root, run the following commands:

```
# cd /opt/aptare/bin
```

```
./tomcat-portal stop
```

Individual component startup/shutdown scripts can be found in the /opt/aptare/bin directory. Shutdown log files can be found in the /opt/aptare/logs directory.

Starting and Stopping the Reporting Database

Consider restarting the Reporting Database every 4-8 weeks.

To start the Reporting Database on Windows

1. Locate the scripts to start the Reporting Database:
`C:\opt\aptare\utils\`
If all components (Portal Server and Reporting Database) are on the same server and you want to start *all* components including the Reporting Database use:
startallservices.bat
If all components (Portal Server and Reporting Database) are on the same server and you want to only start the Reporting Database use:
startoracle.bat
If the Reporting Database is on a separate server use:
startoracle.bat
2. Verify the following services have started using the Windows Services Control panel:
 - Oracle Service SCDB
 - OracleSCDBTNSListener

To stop the Reporting Database on Windows

1. Locate the scripts to stop the Reporting Database:

C:\opt\aptare\utils

If all components (Portal Server and Reporting Database) are on the same server and you want to stop *all* components including the Reporting Database use:

stopallservices.bat

If all components (Portal Server and Reporting Database) are on the same server and you want to only stop the Reporting Database use:

stoporacle.bat

If the Reporting Database is on a separate server use:

stoporacle.bat

2. Verify the following services have stopped using the Windows Services Control panel:
 - Oracle Service SCDB
 - OracleSCDBTNSListener

To start the Reporting Database on Linux

Do one of the following

- If all components (Portal Server and Reporting Database) are on the same server and you want to start *all* components including the Reporting Database, run the following command:

```
# cd /opt/aptare/bin
```

```
./aptare start|restart
```

- If all components (Portal Server and Reporting Database) are on the same server and you want to only start the Reporting Database, run the following command:

```
# cd /opt/aptare/bin
```

```
./oracle start
```

- If the Reporting Database is on a separate server, run the following command:

```
# cd /opt/aptare/bin
```

```
./oracle start
```

Starting and Stopping Data Collectors

How you start and stop the Data Collector depends on your operating system. Also, the location of the start and stop script/service depends on your backup solution. For most backup solutions, the Data Collector does not run on the backup server (master server).

To start the Data Collector on Windows

1. Start the following services using the Windows Services Control panel:
 - APTARE Agent
 - APTARE WMIServer

To stop the Data Collector on Windows

1. Stop the following services using the Windows Services Control panel:
 - APTARE Agent
 - APTARE WMIServer

To start Data Collector on Linux

As user `root`, run the start or restart command:

```
# cd /etc/init.d
# ./aptare_agent status
# ./aptare_agent start|restart
```

To stop Data Collector on Linux

As user `root`, run the stop command:

```
# cd /etc/init.d
# ./aptare_agent status
# ./aptare_agent stop
```

Monitoring Tablespaces

The Reporting Database contains the user tablespaces outlined in [Table 1](#). During your initial installation, APTARE IT Analytics created these user tablespaces and corresponding data files. These tablespaces have `AUTOEXTEND` turned on, so when a data file fills up, the tablespace increases the data file. You do not need to add any data files. However, you must add disk space to the mount point as needed; otherwise, APTARE IT Analytics cannot extend the data files.

Tablespace	Data Files
aptare_tbs_data_1m	aptare_tbs_data_1m_01.dbf
aptare_tbs_idx_1m	aptare_tbs_idx_1m_01.dbf
aptare_tbs_data_20m	aptare_tbs_data_20m_01-09.dbf
aptare_tbs_idx_10m	aptare_tbs_idx_10m_01-09.dbf
aptare_tbs_data_200m	aptare_tbs_data_200m_01-09.dbf
aptare_tbs_idx_100m	aptare_tbs_idx_100m_01-09.dbf
aptare_tbs_data_200m_lob	aptare_tbs_data_200m_lob_01-09.dbf
aptare_tbs_data_200m_col	aptare_tbs_data_200m_col_01-09.dbf
aptare_undo_tbs	aptare_undo_tbs_01.dbf
aptare_temp_tbs	aptare_tbs_temp_01.dbf

Table 1 User Tablespaces

4

Accessing APTARE Reports with the REST API

The REST API provides external applications programmatic access to APTARE IT Analytics reports and the ability to consume the results in a preset output format. This section covers:

- [Setting Up Authentication](#)
- [Extracting Data from Tabular Reports \(with pagination\)](#)
- [Exporting Reports](#)
- [Exporting Custom Dashboards](#)
- [Sample Client Side Java Code for Calling the REST API](#)

Setting Up Authentication

To use the REST API, you must login to the Portal and pass the following parameter:

```
https://xyz/portal/portal.login?account=admin@etchsketchteam&password=a&isRest=true
```

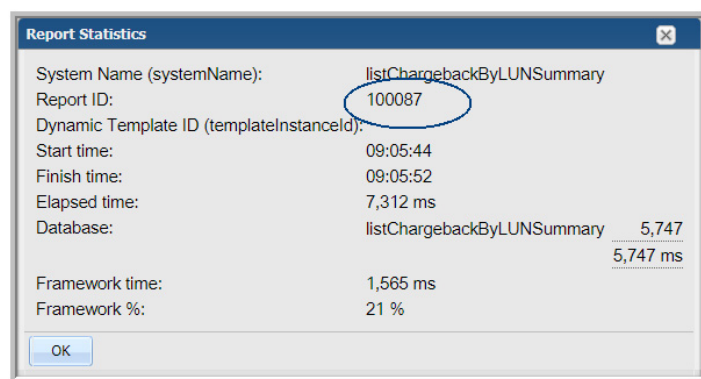
Note: The REST API supports Basic Authentication. Use the same credentials used to log into APTARE IT Analytics when saving the report and dashboard instances.

Extracting Data from Tabular Reports (with pagination)

With the REST API, you can extract data from tabular reports using pagination in JSON and XML formats.

To extract data from tabular reports

1. In the APTARE IT Analytics portal, generate a tabular report and save it. See [Saving Reports](#).
2. Run the saved report.
3. Press **Ctrl + Alt + T** to view the **Report Statistics** and find the **Report ID**.



4. Call the REST API. The format parameter may be set to json or xml. For example:

`https://xyz.com/rest/getReport.ajax?reportId=100087¤tPage=0&format=json`

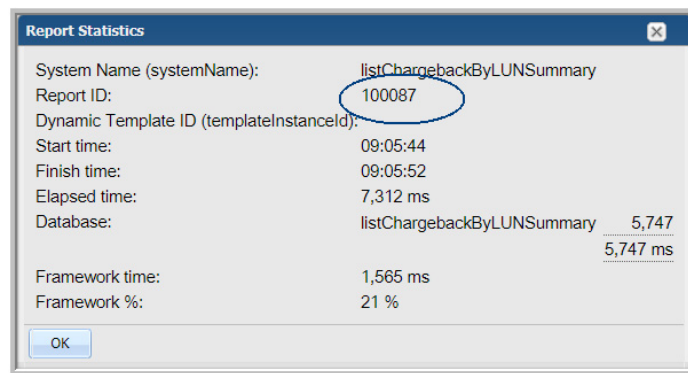
The result set will contain a paging object, which contains an attribute `hasMore`. As long as `hasMore` is true continue calling the REST API with `currentPage=<previous +1>`

Exporting Reports

With the REST API, you can export reports as HTML, PDF and CSV formats.

To extract data from tabular reports

1. In the APTARE IT Analytics portal, generate a tabular report and save it. See [Saving Reports](#).
2. Run the saved report.
3. Press **Ctrl + Alt + T** to view the **Report Statistics** and find the **Report ID**.



4. Call the REST API. The exportFormat parameter may be set to csv, html or pdf. For example:

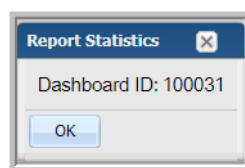
`https://xyz.com/rest/exportReport.ajax?reportId=100087&exportFormat=csv`

Exporting Custom Dashboards

With the REST API, you can export custom dashboards as HTML and PDF formats.

To export custom dashboards

1. In the APTARE IT Analytics portal, generate a custom dashboard and save it. See [Saving Reports](#).
2. Run the saved dashboard.
3. Press **Ctrl + Alt + T** to view the **Report Statistics** and find the **Dashboard ID**.



4. Call the REST API. The exportFormat parameter may be set to html or pdf. For example:

`https://xyz.com/rest/exportDashboard.ajax?dashboardId=100031&exportFormat=html`

Sample Client Side Java Code for Calling the REST API

- [Base Class for Testing](#)
- [Class for Paginated Data Extraction from a Tabular Report](#)
- [Class for Exporting Reports and Dashboards](#)

Base Class for Testing

```
import org.apache.commons.codec.binary.Base64;

import java.io.IOException;
import java.net.URL;
import java.net.URLConnection;

public class BaseRest {

    protected final String baseUrl;
    protected final String username;
    protected final String password;

    public BaseRest(String baseUrl, String username, String password) {
        this.baseUrl = baseUrl;
        this.username = username;
        this.password = password;
    }

    protected URLConnection setUsernamePassword(URL url) throws IOException {
        URLConnection urlConnection = url.openConnection();
        String authString = username + ":" + password;
        String authStringEnc = new String(Base64.encodeBase64(authString.getBytes()));
        urlConnection.setRequestProperty("Authorization", "Basic " + authStringEnc);
        return urlConnection;
    }
}
```

Class for Paginated Data Extraction from a Tabular Report

```
import com.google.gson.Gson;

import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.net.URL;
import java.net.URLConnection;
import java.util.List;
import java.util.Map;

public class TestExtractDataFromReport extends BaseRest{

    public TestExtractDataFromReport(String baseUrl, String username, String password) {
        super(baseUrl, username, password);
    }

    String getDataFromServer(String path) {
        StringBuilder sb = new StringBuilder();
        try {
            URL url = new URL(baseUrl + path);
            URLConnection urlConnection = setUsernamePassword(url);
            BufferedReader reader = new BufferedReader(new
InputStreamReader(urlConnection.getInputStream()));
            String line;
            while ((line = reader.readLine()) != null) {
                sb.append(line);
            }
            reader.close();

            return sb.toString();
        } catch (Exception e) {
            throw new RuntimeException(e);
        }
    }

    //Testing csv
    public static void main(String[] args) {
        TestExtractDataFromReport testRest = new TestExtractDataFromReport("http://
xyz.com","userId","*****");
        String path = "/rest/getReport.ajax?reportId=100063";
        boolean hasMore = true;
```

```

        int page = 0;
        while(hasMore) {
            Result result = execute(testRest, path + "&format=json&currentPage=" + page);
            System.out.println(result.toString());
            ++page;
            hasMore = result.hasMore();
        }
    }

    private static Result execute(TestExtractDataFromReport testRest, String path) {
        String result = testRest.getDataFromServer(path);
        System.out.println(result);
        Gson gson = new Gson();
        Map map = gson.fromJson(result, Map.class);
        Result result1 = new Result();
        result1.reportName = (String) map.get("report_name");
        Map paging = (Map) map.get("paging");
        result1.hasMore = (Boolean) paging.get("hasMore");
        result1.data = (List<Map>) map.get("data");
        return result1;
    }

    static class Result {
        String reportName;
        boolean hasMore;
        List<Map> data;

        @Override
        public String toString() {
            return "Result{" +
                "reportName='" + reportName + '\'' +
                ", hasMore=" + hasMore +
                ", data=" + data.size() +
                '}';
        }
    }
}

```

Class for Exporting Reports and Dashboards

```
import java.io.File;
import java.io.FileOutputStream;
import java.net.URL;
import java.net.URLConnection;
import java.nio.channels.Channels;
import java.nio.channels.ReadableByteChannel;

public class TestRestDownload extends BaseRest {

    public TestRestDownload(String baseUrl, String username, String password) {
        super(baseUrl, username, password);
    }

    void writeDownloadedFile(String path, File folder2Download) {
        try {
            URL url = new URL(baseUrl + path);
            URLConnection urlConnection = setUsernamePassword(url);
            String content = urlConnection.getHeaderField("Content-disposition");
            String fileName = content.replace("attachment;filename=\"", "").replaceAll("\\$","");

            File output = getFileThatDoesNotExist(folder2Download, fileName);
            FileOutputStream fos = new FileOutputStream(output);
            ReadableByteChannel rbc =
Channels.newChannel(urlConnection.getInputStream());
            fos.getChannel().transferFrom(rbc, 0, Long.MAX_VALUE);
            fos.close();
        } catch (Exception e) {
            throw new RuntimeException(e);
        }
    }

    private File getFileThatDoesNotExist(File folder2Download, String fileName) {
        File output = new File(folder2Download.getAbsolutePath() + File.separator +
fileName);
        int index = 0;
        while(output.exists()) {
            ++index;
            String[] parts = fileName.split("[.]");
            if(parts.length == 1) {
                output = new File(folder2Download.getAbsolutePath() + File.separator +
fileName + index);
            }
        }
    }
}
```

```

        break;
    }
    String suffix = parts[parts.length - 1];
    String fileNameNew = fileName.replaceAll("[.]" + suffix, "(" + index + ")" +
    "." + suffix);
    output = new File(folder2Download.getAbsolutePath() + File.separator +
    fileNameNew);
    }
    return output;
}

//Exporting Report
public static void main1(String[] args) throws Exception {
    TestRestDownload testRest = new TestRestDownload("http://
xyz.com","userId","*****");
    String path = "/rest/exportReport.ajax?reportId=100063&exportFormat=csv";
    File file = new File("C:\\tmp");
    testRest.writeDownloadedFile(path, file);
}

//Exporting Dashboard
public static void main(String[] args) throws Exception {
    TestRestDownload testRest = new TestRestDownload("http://
xyz.com","userId","*****");
    String path = "/rest/exportDashboard.ajax?dashboardId=100000&exportFormat=html";
    File file = new File("C:\\tmp");
    testRest.writeDownloadedFile(path, file);
}
}

```


Defining NetBackup Estimated Tape Capacity

This section covers the following topics:

- [NetBackup Estimated Tape Capacity Overview](#)
- [Updating the Estimated Capacity Table](#)

NetBackup Estimated Tape Capacity Overview

For NetBackup, some enterprise environments freeze or suspend tape media and do not allow their backup tapes to fill to capacity. In this situation, a APTARE IT Analytics database table (`apt_nbu_tape_capacity_est`) can be updated to override the standard estimated capacity calculation. In this table, values for Volume Pool ID, Media Type, and Estimated Capacity will be used to override the estimated capacity calculation. See [Estimated Capacity Notes](#).

When values are supplied in this table, the NetBackup estimated capacity calculations will first determine the average size of full tapes—by tape type and volume pool. If this value is less than the value provided in the `apt_nbu_tape_capacity_est` table, the value in the table will be used for the estimated capacity.

Various APTARE IT Analytics backup media reports use an estimated capacity calculation:

- Tape Media Summary
- Tape Media Detail
- Media Availability Forecast
- Media Consumption Forecast

Estimated Capacity Notes

Every time tape data is captured, APTARE IT Analytics recalculates the estimated tape capacity for the tape media type and volume pool combination. It takes into consideration the written KBs for the media type and volume pool for *full* tapes and then stores the average as the estimated tape capacity. Initially, when there is not enough data captured, this value may look low compared to the capacity stated by the vendor. Over time, the estimated capacity improves to the actual number of KBs that is being written to the tapes. Note that the amount of data that fits on the tapes differs based on the compression algorithm used and the type of data that is being backed up, which results in different compression ratios.

Updating the Estimated Capacity Table

Use the following procedure to insert rows into the NetBackup Estimated Capacity database table.

1. Log on to the Portal Server as user `aptare`.
2. Type the following command:

```
sqlplus portal/portal
```
3. Insert a row into the `apt_nbu_tape_capacity_est` table. The following example shows how to insert the values.

```
INSERT INTO apt_nbu_tape_capacity_est (volume_pool_id, media_type,  
estimated_mbyte_capacity)  
VALUES (100304, 10, 35850);  
commit;
```

In this example, both the `volume_pool_id` and `media_type` will be used to establish the estimated capacity.

4. You also can insert a row into this table using `media_type` only (omitting the `volume_pool_id`), as shown in the following example.

```
INSERT INTO apt_nbu_tape_capacity_est (volume_pool_id, media_type,  
estimated_mbyte_capacity)  
VALUES (NULL, 9, 30000);  
commit;
```

In this example, only the `media_type` will be used when the calculation searches for an estimated capacity override.

5. To verify estimated capacities after updating the database table, execute the following commands, supplying the NetBackup Master Server ID:

```
sqlplus portal/portal  
execute media_package.setupTapeMediaCapacity(<master server ID>);
```

Listing Volume Pool IDs and Media Types

Using the Report Template Designer, create a custom report using the following query to identify Volume Pool IDs and Media Type codes:

```
select DISTINCT n.vendor_media_type, t.vendor_media_type_name, n.volume_pool_id  
from apt_v_nbu_tape_media_detail n, apt_v_tape_media t  
where n.tape_media_id = t.tape_media_id  
and t.server_id in ($(hosts))
```

When you create this custom report via the Report Template Designer, configure the Report Designer to include the selection of a host group, enabling users to narrow the scope of the report when they generate the report.

Automating Host Group Management

This section covers the following topics:

- [About Automating Host Group Management](#)
- [Task Overview: Managing Host Groups in Bulk](#)
- [Preparing To Use PL/SQL Utilities](#)
- [General Utilities](#)
- [Bulk Load Utilities](#)
- [Symantec NetBackup Utilities](#)
- [IBM Tivoli Storage Manager Utilities](#)
- [Scheduling Utilities To Run Automatically](#)

About Automating Host Group Management

You can create, move, and organize host groups and link clients/servers to host groups through the Portal. However, you might want to automatically set up your company's host group hierarchy and membership based on unique enterprise business rules and to move or link large quantities of clients/servers in one large [batch](#).

Note: In a Managed Service Provider (MSP) environment, the Application Administrator does not have access to the Reporting Database, so the System Administrator in a MSP environment needs to partner with the Application Administrator, who knows what changes need to be made to the host group hierarchy.

To make host group changes in bulk, use the PL/SQL utilities that APTARE IT Analytics provides. Instead of manually creating and organizing host groups through the Portal, you can run PL/SQL utilities to do the work for you.

These utilities provide the following capabilities:

- **Matching.** You can base your host group management on specific criteria. For example, if you want to organize backup servers by geographical location and your backup servers have a specific naming convention that indicates the servers' region, you need only specify that the SQL utilities to match on that naming convention.
- **Automation.** You can automate how you create and organize host groups. You can automate how you do the following:
 - Move or copy clients.
 - Move and delete host groups.
 - Organize clients into groups by management server and IBM Tivoli Storage Manager server.
 - Set up an inactive clients group.
 - Set up host group for clients in inactive policies.
 - Set up clients by policy, policy type, policy domain, and IBM Tivoli Storage Manager instance.
 - Load details of new hosts or update existing hosts.

- Load relationships between hosts and host groups.

These utilities communicate directly with the Reporting Database to manage and manipulate the host group membership for large quantities of servers. There are two types of utilities:

- **General.** These utilities apply to all backup solutions.
- **Product-specific.** These utilities only apply to a specific backup solution.

Task Overview: Managing Host Groups in Bulk

To manage host groups in large quantities, perform the following sequence of steps:

Task	For Instructions
1. Learn about host groups.	Search the online documentation for <i>Host Group</i> .
2. Learn about <i>bulk</i> host group management.	About Automating Host Group Management
3. Prepare your SQL environment so that you can run the utilities.	Preparing To Use PL/SQL Utilities
4. Based on the type of update you want to make to the Reporting Database, choose the utility that can perform that action.	<ul style="list-style-type: none"> • General Utilities • Merge Duplicate Backup Clients • Symantec NetBackup Utilities • IBM Tivoli Storage Manager Utilities
5. (Optional) Schedule utilities to run automatically.	Scheduling Utilities To Run Automatically

Preparing To Use PL/SQL Utilities

A few things you need to know about running the utilities:

- Any time that you are passing a string value as a parameter, the value must be contained within single quotes. For example: `'text'`
- Some functions require that you pass a `group_id`. To obtain this value, go to [Identifying a Host Group ID](#).

Also, the PL/SQL utilities have functions that need to be executed from within a PL/SQL session, so set up your environment before you begin to use the utilities.

To prepare your SQL environment

1. Start the **sqlplus** session. If any error messages appear, resolve these errors before you continue:
 - If your database server is on a Linux system, log in as the Linux user `aptare`.
 - If your database is on a Windows system, log in as a user who is a member of the `ORA_DBA` group and open a command prompt window.

```
sqlplus portal/<portal_password>
```

2. Enable server output in PL/SQL:

```
SET SERVEROUTPUT ON
```

General Utilities

The utilities contained in this section apply to all host groups and hosts.

- [Categorize Host Operating Systems by Platform and Version](#)
- [Identifying a Host Group ID](#)
- [Move or Copy Clients](#)
- [Organize Clients by Attribute](#)
- [Move Host Group](#)
- [Delete Host Group](#)
- [Move Hosts and Remove Host Groups](#)
- [Organize Clients into Groups by Backup Server](#)
- [Merge Duplicate Backup Clients](#)

Categorize Host Operating Systems by Platform and Version

Host data can be collected from various APTARE IT Analytics products, such as Capacity Manager, Backup Manager, and Virtualization Manager. Data Collectors persist values as they are collected from the subsystems. For a host's operating system, subsystems supply values (operating system names) in a variety of formats that do not lend themselves to *grouping hosts by OS* for reports. For example, Red Hat Linux may be represented as RedHat Linux, rhel, or Red Hat Linux. In order to report on hosts in reasonable groupings, database processing references a set of default regular expressions to parse OS names to categorize the collected host OS data by *platform* and *version*.

The following sections provide the details for maintaining and customizing the default Host OS categorization:

- [Use Regular Expressions to Override or Modify Default Host OS Categorization](#)
- [Host OS Categorization Default Settings](#)
- [Utility to Update Host OS Categorizations](#)
- [Categorize Host Operating Systems On Demand](#)

Use Regular Expressions to Override or Modify Default Host OS Categorization

APTARE IT Analytics supplies a set of regular expressions (Regex) that define the processing used to process the collected Host OS data to glean the platform and version from the text strings.

- The [Host OS Categorization Default Settings](#) can be modified using the [Utility to Update Host OS Categorizations](#).
- Data collection automatically processes the Host OS regular expressions and updates the database with the normalized values. If you want to make immediate changes and not wait for the next collection cycle, you can [Categorize Host Operating Systems On Demand](#).
- Regex processing is case-insensitive.
- To learn more about Regular Expressions, reference Oracle's documentation: [Using Regular Expressions](#).

Host OS Categorization Default Settings

Each row in this table represents a regular expression used to determine a common OS platform and version.

OS Platform Regex	OS Platform	Version Regex	Ignore	Priority	Domain ID	Creation Date	ID
FreeBSD	FreeBSD	\d+\.\?\d?+	(64-bit) (32-bit)	1		15-DEC-15 12.03.33	1
Solaris	Solaris	\d+\.\?\d?+	(64-bit) (32-bit)	1		15-DEC-15 12.03.33	2
AIX	AIX	\d+\.\?\d?+	(64-bit) (32-bit)	1		15-DEC-15 12.03.33	3
Ubuntu	Ubuntu	6.06LTS 8.04LTS 10.04LTS 12.04LTS 14.04LTS 16.04LTS \ d+\.\?\d?+	(64-bit) (32-bit)	1		15-DEC-15 12.03.33	4
Data ONTAP	Data ONTAP	\d+\.\?\d?+	(64-bit) (32-bit)	1		15-DEC-15 12.03.33	5
MAC	MAC	Rhapsody Developer Release Server 1.0 Developer Preview Public Beta \d+\.\? d?+	Linux (64-bit) (32-bit)	1		15-DEC-15 12.03.33	6
HP-UX HPUX	HP-UX	\d+\.\?\d?+	(64-bit) (32-bit)	1		15-DEC-15 12.03.33	7
CentOS	CentOS	\d+?(/?)\d+?(/?)\d?+	(64-bit) (32-bit)	1		15-DEC-15 12.03.33	8
openSUSE SUSE SLES	openSUSE	Leap 42.1 \d+\.\?\d?+	(64-bit) (32-bit) (x86_64)	1		15-DEC-15 12.03.33	9
Windows win	Windows	(\d+? SERVER NT XP Vista)\s?\d?+	(64-bit) (32-bit)	1		15-DEC-15 12.03.33	10
Linux	Linux		(64-bit) (32-bit)	0		15-DEC-15 12.03.33	11
Red Hat RedHat rhel	Red Hat	\d+\.\?\d?+	(64-bit) (32-bit)	1		15-DEC-15 12.03.33	12
vmnix	vmnix		-x86 x86	1		15-DEC-15 12.03.33	13
SunOS	SunOS	\d+\.\?\d?+	(64-bit) (32-bit)	1		15-DEC-15 12.03.33	14
Data Domain	Data Domain		(64-bit) (32-bit)	1		15-DEC-15 12.03.33	15
Fedora	Fedora	\d+\.\?\d?+	(64-bit) (32-bit)	1		15-DEC-15 12.03.33	16
Debian	Debian	\d+\.\?\d?+	(64-bit) (32-bit)	1		15-DEC-15 12.03.33	17

Utility to Update Host OS Categorizations

Use this utility to insert new regular expression rules into the database table or to modify existing rules.

Usage	<p>To <i>insert</i> a regular expression row into the database table, use this command:</p> <pre>execute server_group_package.insertCustomerOsNormData(null, 'os_platform_regex', 'os_platform', 'os_version_regex', 'ignore_string', priority, domain_id);</pre> <p>To <i>update</i> values in a regular expression row into the database table, use this command:</p> <pre>execute server_group_package.insertCustomerOsNormData(os_normalization_id, 'os_platform_regex', 'os_platform', 'os_version_regex', 'ignore_string', priority, domain_id);</pre> <p>Where:</p> <p>os_normalization_id: This value is unique for each Regex row (see Host OS Categorization Default Settings). IDs less than 100000 are system defaults and cannot be removed, but their values can be modified. When inserting a regular expression into the database table, this value must be <i>null</i> because the process assigns this number.</p> <p>os_platform_regex: These strings are used to match a substring in the collected text to identify the platform. This field cannot be null.</p> <p>os_platform: This is the value that is saved to the database when the regular expression is encountered in the collected Host OS. This platform value can never be null, however, the version derived from the version regex may be null.</p> <p>os_version_regex: This is the regular expression used to match a substring in the collected text to identify the version.</p> <p>ignore_string: These strings are ignored and are treated as irrelevant details when determining the platform or version.</p> <p>priority: This value indicates precedence: the higher the value, the higher the priority. For example, Red Hat has a higher priority than Linux, which means that a Host OS that contains a Red Hat substring and a Linux substring will result in a Host OS of Red Hat. User-defined regular expressions must have a priority higher than 1 to override system defaults. This field cannot be null.</p> <p>domain_id: The Domain ID is shipped with a <i>null</i> default value. In multi-tenancy environments, such as Managed Services Providers, the Domain ID can be updated to change the processing for a specific domain/customer.</p> <p>Note that a Creation Date also is saved in the database table. This is the date and time that the Regex record was created in the database.</p>
-------	--

Categorize Host Operating Systems On Demand

Use this utility to process hosts to categorize their operating systems without waiting until the next data collection cycle. This utility uses the regular expressions as described in [Categorize Host Operating Systems by Platform and Version](#).

Usage	<pre>execute server_group_package.updateExisting HostOsinfo(hostGroupId);</pre> <p>Where:</p> <p>host_group_id: This is the numeric identifier of a host group. See Identifying a Host Group ID.</p>
-------	---

Identifying a Host Group ID

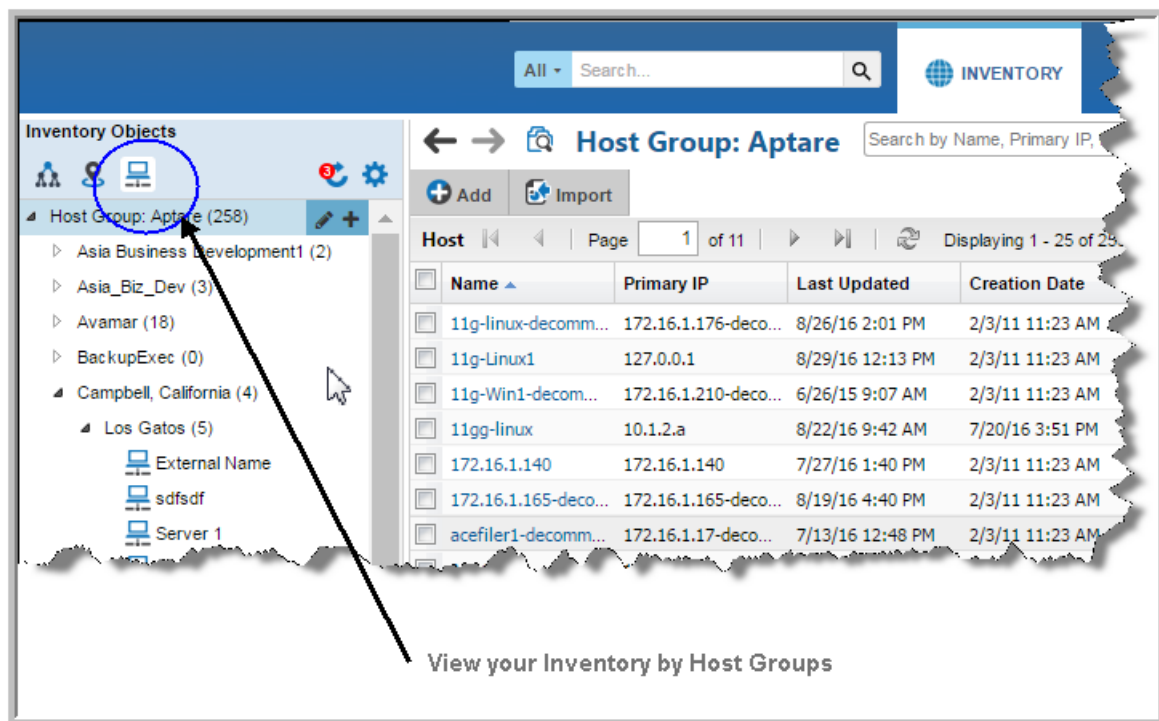
Whenever you want to apply a change to a table in the Reporting Database, you must specify the host group's ID in your SQL utility. For example, you need to identify host group IDs if you intend to delete a host group through the reporting database or if you want to use PL/SQL utilities. The host group ID that you specify in your SQL statement is very important and determines how the change is applied:

- If you are *not* an Managed Services Provider (MSP) and you want to apply a change to a specific host group, determine the group ID for that host group. If you want to apply a change to all host groups, choose the host group ID of the top level folder, the root folder. The group ID for the root folder is always 300000.
- If you are an MSP and you want to apply a change to a specific customer, choose the host group ID of that customer's domain. If you want to apply a change to all customers, choose the group ID of the top-level root folder (ID = 300000).

Finding a Host Group ID

To identify the unique identifier associated with a host group, take the following steps in the Portal.

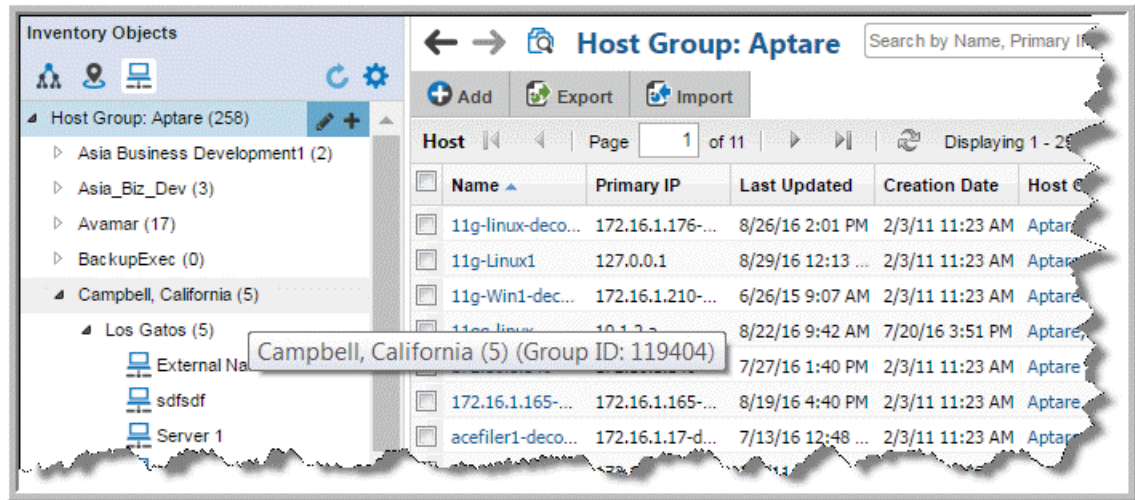
1. Navigate to the **Inventory**.
2. Click the **Host Groups** icon to switch the Inventory view.



3. Verify the Host Group column is displayed on the grid, and optionally, use Advanced Filtering to locate the Host Group.

Note: The **Host Group** column, displayed in the Inventory for the Host Group management view, has sorting disabled to improve portal performance.

4. Hover your mouse over the Host Group folder in which your hosts reside. The Group ID will display in a tooltip.



Move or Copy Clients

Description	This utility enables you to move or link large quantities of clients to different host groups. This tool accepts wildcards for the <code>client_name_mask</code> attribute. This utility will first validate the existence of the two group names passed as the first two parameters (see below). If the groups do not exist, the utility returns an error.
Usage	<pre>execute server_mgmt_pkg.moveOrCopyClients('<source_host_group>', '<destination_host_group>', '<client_name_mask>', <move_or_copy_flag>);</pre> <p>Where:</p> <p>source_host_group is the full pathname to the source host group, for example <code>/Aptare/Masters/GroupA</code></p> <p>destination_host_group is the full pathname to the destination host group.</p> <p>client_name_mask is a string that can contain wildcards (*). For example, <code>abc*</code> indicates all clients that have an <code>internal_name</code> that starts with <code>abc</code>. To process all clients use the value <code>NULL</code> (which should not be within quotes).</p> <p>move_or_copy_flag is 0=copy and 1=move.</p>

Organize Clients by Attribute

Description	<p>This <code>groupClientsbyAttributes</code> utility enables you to organize clients within a host group, based on client attributes. This utility will create host groups named for each attribute value, underneath a parent host group, as shown in the following example.</p> <p>Example of Organizing Clients by Geographical Location:</p> <p>Create a host group named <i>Geography</i>. This will be the destination group that will be used to organize the clients by location.</p> <p>Then, create an attribute named <i>Geography</i>.</p> <p>For a subset of a host group's clients, set their <i>Geography</i> attribute <i>value</i> to <i>London</i> and for another subset of clients, set their <i>Geography</i> attribute to <i>New York</i>.</p> <p>Use the following <code>groupClientsbyAttributes</code> utility to organize the clients that have a <i>Geography</i> attribute configured.</p> <pre>execute server_mgmt_pkg.groupClientsbyAttributes(300000, 302398, 1, StringObjectType(stringObjectType('Geography')));</pre> <p>Where 300000 is the group ID of the root group, <i>Global</i>; 302398 is the ID of the <i>Geography</i> group you just created.</p> <p>So, for this example, the clients in the <i>Global</i> (source) group are organized into the following host group hierarchy:</p> <div data-bbox="430 940 617 1071"><pre>graph TD Global --> Geography Geography --> London Geography --> NewYork[New York]</pre></div> <p>Additional References: See Identifying a Host Group ID.</p>
Usage	<pre>execute server_mgmt_pkg.groupClientsbyAttributes(<source_Group_ID>, <destination_group_ID>, <cascade_Source_Group>, StringObjectType(<attribute_List>));</pre> <p>Where:</p> <p>source_Group_ID is the numeric identifier of the host group for which you want to group the clients. See Identifying a Host Group ID for the steps for finding a group ID.</p> <p>destination_group_ID is the numeric identifier of the group under which you want to group the clients.</p> <p>cascade_Source_Group is a numeric flag that indicates if you want this utility to process the source host group's sub-groups and organize those clients in the destination group.</p> <p>attribute_List is a comma-separated list of attribute names, each enclosed in straight single quotes. These names are used to create the sub-groups that organize the clients underneath the source group.</p>

Move Host Group

Description	This utility enables you to move a host group and all of its hierarchical contents to another host group.
Usage	<pre>execute server_mgmt_pkg.moveServerGroup('<source_host_group>', '<destination_host_group>');</pre> <p>Where:</p> <p>source_host_group is the full pathname to the source host group, for example /Aptare/Masters/GroupA. Be sure to use the host group name, not the host group ID.</p> <p>destination_host_group is the full pathname to the destination host group. Be sure to use the host group name, not the host group ID.</p>

Delete Host Group

Description	<p>There are some occasions where you may wish to remove the entire contents of a host group, including any sub-groups within this group and any clients under the hierarchy. This utility allows administrators to perform this type of delete operation.</p> <p>CAUTION: IF YOU USE THIS COMMAND TO REMOVE A HOST GROUP, AND IF CLIENTS UNDER THE HOST GROUP HIERARCHY DO NOT EXIST IN ANY OTHER GROUP, THE CLIENTS AND ALL OF THEIR ASSOCIATED CONFIGURATIONS WILL BE PERMANENTLY REMOVED FROM THE DATABASE.</p>
Usage	<pre>execute server_group_package.deleteEntireGroupContents(100, <parent_group_id>, <group_to_remove_id>);</pre> <p>Where:</p> <p>parent_group_id is the group id of the parent group which contains the group to be deleted.</p> <p>group_to_remove_id is the group id of the group to be deleted.</p>

Move Hosts and Remove Host Groups

This process, often referred to as Server Group Cleanup, enables removal of backup server groups that had been created automatically in prior APTARE IT Analytics versions. In addition to cleaning up server groups, this process can also be used on other host groups.

Description	<p>Prior versions of IT Analytics automatically created several server/host groups during backup data collection. In certain environments, these auto-generated groups may not be needed, as other host groups are more relevant. This utility can be used to clean up a Portal's host groups by moving servers/hosts and child host groups from a host group and then deleting the source host group. While this utility, by default, is intended for system-created host groups, it can be used for any host group that you want to delete, but retain its contents.</p> <p>Note: Once this process completes, log out of the Portal and log back in before accessing host groups and hosts in the Inventory.</p> <p>Best Practice: In multi-tenancy environments, run this command on a domain-by-domain basis, starting from the bottom of the domain hierarchy to the top IT Analytics domain. This ensures that each domain has been explicitly processed with log messages that confirm the actions taken.</p> <p>CAUTION: THIS COMMAND MOVES CLIENTS TO THE DOMAIN'S HOME HOST GROUP AND THEN PERMANENTLY REMOVES THE SPECIFIED HOST GROUPS FROM THE DATABASE. RUN THIS COMMAND IN VALIDATE MODE FIRST TO VERIFY THAT THE ACTIONS REPRESENT THE INTENDED RESULTS.</p>
Usage	<pre>server_mgmt_pkg.serverGroupCleanup(<processingMode>, '<domain_name>', (<server_group_names_list>), '<log_file_path_name>', '<log_file_name>');</pre> <p>Where:</p> <p>processing_mode is either 1 = Validate or 2 = Execute. Run this command in Validate mode first to understand what hosts will be moved and what host groups will be deleted.</p> <p>domain_name, enclosed in single straight quotes, is the case-insensitive name of the IT Analytics domain for the group to be deleted. See the Best Practice listed above.</p> <p>server_group_names_list is a comma-separated list of host group names to remove, in single straight quotes. This list must be enclosed in parentheses and prefaced with <code>stringListType</code>. If NULL is specified, the utility will process these system-created host groups: NetBackup Policy Types, NetBackup Policies, Inactive Policy Clients, and Policy Domains.</p> <p>log_file_path_name, enclosed in single straight quotes, is the location of the log file for this process.</p> <p>log_file_name, enclosed in single straight quotes, is the name of the log file.</p> <p>Example of Validate Mode:</p> <pre>execute server_mgmt_pkg.serverGroupCleanup(1, 'EMEAfinance', stringListType('NetBackup Policy Types','NetBackup Policies','Inactive Policy Clients', 'Policy Domains'), '/tmp', 'serverGrpCleanup.log');</pre> <p>Example of Execute Mode:</p> <pre>execute server_mgmt_pkg.serverGroupCleanup(2, 'EMEAfinance', stringListType('NetBackup Policy Types','NetBackup Policies','Inactive Policy Clients', 'Policy Domains'), '/tmp', 'serverGrpCleanup.log');</pre> <p>Example of Validate <i>without</i> a list of Host Group Names:</p> <pre>exec server_mgmt_pkg.serverGroupCleanup(1, 'EMEAfinance', NULL, '/tmp', 'serverGrpCleanup.log');</pre>

Organize Clients into Groups by Backup Server

This utility can be used for any backup product, such as IBM Tivoli Storage Manager, Veritas Backup Exec, or HP Data Protector.

Description	<p>This utility enables you to create a hierarchy of servers and links all clients that are members of a server into the respective host group.</p> <p>For example, in an IBM Tivoli Storage Manager environment if you have two IBM Tivoli Storage Manager servers called <code>TSM1</code>, <code>TSM2</code>, this utility creates two host groups, <code>TSM1</code> and <code>TSM2</code>, and links the IBM Tivoli Storage Manager server's clients into the corresponding IBM Tivoli Storage Manager host group.</p>
Usage	<pre>execute common_package.moveClientsIntoServerGroups (<source_group_id>,<destination_group_id>, <move_or_copy_flag>, <latest_server_only>);</pre> <p>Example:</p> <pre>exec common_package.moveClientsIntoServerGroups(300000, 300010, 1, 1), ;</pre> <p>Where:</p> <p>source_group_id is the internal group ID of the group hierarchy to traverse.</p> <p>destination_group_id is the group ID in which host groups by management server will be created. APTARE recommends that you create a host group under <code>source_group_id</code> called <code><vendor_name> Servers</code> and use the group ID of this new host group for the second parameter. See Identifying a Host Group ID.</p> <p>When you organize by server, if a host group exists anywhere under the source group hierarchy with the name of that server, the routine associates the clients with that folder and does not create a new folder under the destination folder. This association occurs whether you explicitly specify the destination folder or if the destination is NULL. However, if you pass a source folder that is at a lower level, the routine only checks for a folder under that hierarchy. If you specify NULL as the destination folder, the routine creates a host group under the <code>source_group_id</code> called Master Servers.</p> <p>move_or_copy_flag can be set to 0=Link (copy) clients or 1=Move clients. If set to 0, the utility links the clients to their respective host groups and keeps the clients in their original group location. If set to 1, the utility moves all clients from the source host group and to their respective host groups.</p> <p>The utility processes and organizes all clients of the source group hierarchy into the target server grouping. However, if the <code>move_or_copy</code> flag is set to 1, the utility removes only clients in the top level <code>source_group_id</code> group—and does not remove those already organized in lower-level sub-groups.</p> <p>latest_server_only, when set to 1, indicates the last server to back up the client; otherwise, set this flag to 0.</p>

Merge Duplicate Backup Clients

ADVANCED USE ONLY - Due to the nature of this utility’s processing, if executed incorrectly, backup clients could be incorrectly moved. This process is particularly risky in a multi-tenancy environment, where multiple IT Analytics domains could have hosts/servers with the same name.

This merge utility can be used for clients that have been collected from the following backup products: Veritas NetBackup, EMC NetWorker, and Commvault Simpana.

Description	<p>Under certain circumstances, backup clients may have duplicate entries in the IT Analytics database. This utility enables you to merge the data of clients that appear more than once in the database.</p> <p>In most cases, it is not necessary to shut down the data receiver while the client records are being merged. Although not required, it is <i>recommended</i> that you shut down the data receiver before executing this utility so that data will not continue to be collected for the hosts that are being merged.</p> <p>Merging of NetBackup master servers is not supported.</p>
Usage	<pre>execute duplicate_package.mergeDuplicateServers(<'host_grp'>,<host_name_type>);</pre> <p>Example:</p> <pre>exec duplicate_package.mergeDuplicateServers('/Corp',1);</pre> <p>Where:</p> <p>host_grp is the explicit host group path and name.</p> <p>host_name_type indicates whether to use only the host’s base name while finding duplicates, or use the fully qualified name. 0 = fully qualified host name, 1 = host base name.</p> <p>Example of a host base name: QAhost1</p> <p>Example of a fully qualified host name: QAhost1.yourcompany.com</p>

Bulk Load Utilities

The utilities contained in this section load hosts and their relationships to host groups into the Reporting Database as a batch process using a comma-delimited file. These utilities load new hosts as well as update existing hosts.

Bulk Load utilities must be run in SQLPLUS as user aptare.

1. Log in to the Portal server as the user aptare for Linux, or an administrator user for Windows.

```
su - aptare
```

2. Open a command-line window.

3. Change the directory to the stored_procedures directory.

```
/opt/aptare/database/stored_procedures (Linux)
```

```
\opt\oracle\database\stored_procedures (Windows)
```

4. Execute the command: sqlplus portal/portal

5. Run the desired command as listed in the following tables.

This section contains the following topics:

- [Load Host Aliases](#)
- [Load Details of New Hosts or Update Existing Hosts](#)
- [Load Relationships Between Hosts and Host Group](#)

Load Host Aliases

Description	Sets up host aliases from a comma-delimited file containing a list of hosts and host aliases. See Host Name Processing - Filters and Aliases for a description of the logic used to process hosts and aliases.									
Usage	<pre>execute load_package.loadHostAliasFile('<file_name>', '<log_path_name>', '<log_file_name>');</pre> <p>Where file_name is the fully qualified path to the csv file that contains the aliases to be loaded.</p> <p>Example of the file_name specification: '/opt/aptare/database/HostAliases.csv'</p> <p>Example of the command execution: execute load_package.loadHostAliasFile('/opt/aptare/database HostAliases.csv', '/ tmp','loadHostAlias.log');</p>									
Load File Specification	<p>The specification for the comma-delimited file is as follows: <domain>, <hostname>, <alias_hostname></p> <p>Example: Enterprise, whitney,182.16.1.101</p> <p>The detailed specification for each field follows:</p> <table><tr><td>domain</td><td>CHAR(128)</td><td>NOT NULL</td></tr><tr><td>hostname</td><td>CHAR(64)</td><td>NOT NULL</td></tr><tr><td>alias_hostname</td><td>CHAR(64)</td><td></td></tr></table> <p>The alias_hostname can be either a host name (up to 64 characters) or an IP address.</p>	domain	CHAR(128)	NOT NULL	hostname	CHAR(64)	NOT NULL	alias_hostname	CHAR(64)	
domain	CHAR(128)	NOT NULL								
hostname	CHAR(64)	NOT NULL								
alias_hostname	CHAR(64)									

Data Constraints	<p>Field values cannot contain embedded commas.</p> <p>The second field, <code>hostname</code>, is the external name, as defined in the Portal database.</p> <p>The csv file must exist and be readable.</p> <p>The csv filename must be specified within single quotes.</p>
Logic Conditions	<p>If the host alias already exists, no updates take place.</p> <p>If the host alias does not already exist in the Reporting Database, the utility adds it.</p> <p>The utility applies case differences in the input file as updates to preexisting rows.</p>
Logging	<p>The utility logs all additions, updates, warnings and errors to the specified log file. Logging strings are typically in the format: <code>Date -> Time -> load_package:sub_routine -> Action</code></p> <p>sub_routine is the sub-routine that is being executed (e.g., <code>loadHostLine</code>).</p>

Load Details of New Hosts or Update Existing Hosts

Description	Imports host details from a comma-delimited file containing a list of hosts and host attributes.																								
Usage	<pre>execute load_package.loadServerFile('<file_name>',['<source_name>']);</pre> <p>file_name is the fully qualified path to the csv file. Example: /opt/aptare/database/hosts.csv</p> <p>source_name is an <i>optional</i>, case-insensitive string, up to 100 characters, representing the source of the host details; for example, CMDB might be relevant for a change management database. This source information is retained for historical purposes, to track how the host was added to the database. If nothing or NULL is provided for this parameter, CSV Load will be inserted as the source into the reporting database.</p>																								
Load File Specification	<p>The specification for the comma-delimited file is as follows: path_to_host_group, internal_name, external_name, description, location, IP_address, make, model, OS</p> <p>Example: /APTARE/ Test,testhost01,testhost01,description,location,172.20.16.1,Sun,E450,Solaris 10 /APTARE/Test,testhost02,testhost02,,location,172.20.16.2,Sun,,Solaris</p> <p>The detailed specification for each field follows:</p> <table><tr><td>internal_name</td><td>CHAR(128)</td><td>NOT NULL</td></tr><tr><td>external_name</td><td>CHAR(128)</td><td>NOT NULL</td></tr><tr><td>description</td><td>CHAR(256)</td><td></td></tr><tr><td>location</td><td>CHAR(64)</td><td></td></tr><tr><td>ip_address</td><td>CHAR(40)</td><td></td></tr><tr><td>make</td><td>CHAR(64)</td><td></td></tr><tr><td>model</td><td>CHAR(64)</td><td></td></tr><tr><td>os_version</td><td>CHAR(128)</td><td></td></tr></table>	internal_name	CHAR(128)	NOT NULL	external_name	CHAR(128)	NOT NULL	description	CHAR(256)		location	CHAR(64)		ip_address	CHAR(40)		make	CHAR(64)		model	CHAR(64)		os_version	CHAR(128)	
internal_name	CHAR(128)	NOT NULL																							
external_name	CHAR(128)	NOT NULL																							
description	CHAR(256)																								
location	CHAR(64)																								
ip_address	CHAR(40)																								
make	CHAR(64)																								
model	CHAR(64)																								
os_version	CHAR(128)																								
Data Constraints	<p>Field values cannot contain embedded commas.</p> <p>The first field, path_to_host_group, must be the full path to an existing host group otherwise the host will not be inserted.</p> <p>The csv file must exist and be readable.</p> <p>The csv filename must be specified within single quotes.</p>																								

Logic Conditions	<p>If the host already exists in the specified host group, the utility updates its details.</p> <p>If the host does not already exist in the Reporting Database, the utility adds the host to the specified host group.</p> <p>If a host attribute field has a <code>NULL</code> value in the input file, the corresponding field in the database will not be updated for a pre-existing row.</p> <p>The utility applies case differences in the input file as updates to preexisting rows.</p> <p>Since the primary key to the record is the <code>internal_name</code>, the <code>internal_name</code> for a host cannot be updated via this utility.</p> <p>If the number of parameters passed in a row exceeds 9, the utility skips the row.</p>
Logging	<p>The utility logs all additions, updates, warnings and errors to the file <code>scon.log</code>, which is located under <code>/tmp</code> by default on Linux systems and <code>C:\opt\oracle\logs</code> on Windows systems. Logging strings are typically in the following format:</p> <p>Date -> Time -> Level -> load_package:sub_routine -> Action</p> <p>Where:</p> <p>Level is DBG, INFO, WARN, or ERR.</p> <p>sub_routine is the sub-routine that is being executed (e.g. <code>loadHostLine</code>).</p> <p>Action is the action that was being reported on.</p> <p>Example:</p> <pre>14-MAY 21:56:08 INFO : updating host: z0001-web0600-s in /APTARE/ Infrastructure</pre>

Load Relationships Between Hosts and Host Group

Description	<p>Imports host-to-host-group relationships from a comma-delimited file. You can choose to audit the host movement, which records the details when a host is removed, added, or moved.</p> <p>See sample output in:</p> <p>Sample Audit File (output from load_package.loadGroupMemberFile).</p>
Usage	<pre>execute load_package.loadGroupMemberFile('<file_name>', '<recycle_group>', <remove_old_entries>, '<audit_pathname>', '<audit_output_file>', <do_log>);</pre> <p>Where:</p> <p>file_name is the fully qualified path to the csv file. For example: /opt/aptare/database/hosts.csv</p> <p>recycle_group is the full path to the group into which deleted hosts will be moved (i.e., the 'recycle bin').</p> <p>remove_old_entries enables you to remove relationships in the Reporting Database that are not in the file. If set to 1 and where there are hosts with a previous relationship to a host group and where that relationship is no longer represented within the file, the utility moves those hosts to the recycle group. If set to 0, the utility does not remove those hosts.</p> <p>audit_pathname is the full path to the audit file, not including the filename.</p> <p>audit_output_file is the name of the audit file where the audit results will be stored.</p> <p>do_log enables you to turn on the auditing function so that all host movements are logged in the audit_output_file. Enter a numeric: 0 or 1, where 0 = No, 1 = Yes.</p> <p>Example command:</p> <pre>execute load_package.loadgroupmemberfile ('/opt/aptare/database/movehosts.csv','Global1/ Recycle',1,'/opt/aptare/database','movehosts.out',1);</pre>
Load File Specification	<p>The specification for the comma-delimited file is as follows:</p> <pre>path_to_host_group, internal_name1, internal_name2, internal_name3, etc.</pre> <p>Where path_to_host_group is the fully qualified path to the host group into which the hosts should be added, and internal_name1 is the internal name of a host within the existing host group hierarchy.</p> <p>Example:</p> <pre>/APTARE/Test, testhost01, testhost02 /APTARE/Infrastructure, testhost02, testhost03</pre> <p>Detailed specification for each field follows:</p> <pre>internal_name CHAR(64) NOT NULL</pre>

Data Constraints	<p>The first field, <code>path_to_host_group</code>, must be the full path to an existing host group. If any host groups in the <code>path_to_host_group</code> field value do not exist, the utility creates them.</p> <p>Field values cannot contain embedded commas.</p> <p>The <code>csv</code> file must exist and be readable.</p> <p>The recycle group folder must exist.</p> <p>Each row must have at least one host specified, otherwise the row will not be processed.</p>
Logic Conditions	<p>If you list hosts after the <code>path_to_host_group</code> field and those hosts are located in the existing host group hierarchy, the utility adds those host groups to the specified host group.</p> <p>If a host with the specified internal name does not exist in the hierarchy, the relationship will not be added. The host must already be configured in the reporting database.</p> <p>If any host groups in the <code>path_to_host_group</code> field value do not exist, the utility creates them.</p> <p>If the <code>removeOldEntries</code> parameter is set to 1, the utility assumes that this file will contain <i>all</i> the required relationships. In other words, for all the host groups that you specify in the file, only those hosts will be in that group after you run this utility. If the host group previously contained other host(s) that are now no longer listed in the file, the utility removes those host(s) from the host group and moves them to the recycle folder.</p> <p>The utility does not delete host groups from the Reporting Database; it only removes members of a host group.</p> <p>If a host group in the Reporting Database is not listed in the file, the utility does not take any processing action against that host group.</p> <p>Host groups with many hosts can be split into multiple lines for ease of file maintenance—for example, the host group and some of the hosts appear on the first line, then the same host group and other hosts appear on subsequent lines.</p>
Logging	<p>The utility logs all additions, updates, warnings, and errors to the <code>scon.log</code> file, which is located under <code>/tmp</code> by default on Linux systems and <code>C:\opt\oracle\logs</code> on Windows systems. Logging strings are typically in the following format:</p> <p>Date -> Time -> Level -> load_package:sub_routine -> Action</p> <p>Where:</p> <p>Level is DBG, INFO, WARN, or ERR.</p> <p>sub_routine is the sub routine that is being executed (e.g. <code>loadServerLine</code>).</p> <p>Action is the action that was being reported on.</p> <p>Example:</p> <pre>14-MAY 19:00:06 ERR load_package:loadServerGroupMembers: Host group / APTARE/Business Views/Regional Offices/Connecticut does not exist on line 6 of the data load file</pre>

Sample Audit File (output from `load_package.loadGroupMemberFile`)

```
27-FEB 14:18:35 Start processing host group membership, filePathname: /opt/mycompany/
database/movehosts.csv recycleGroup: /Global/Recycle , removeOldEntries: 1)
27-FEB 14:18:35 Adding host: Whitney (104637) to group: /Global/Corp (102572)
27-FEB 14:18:35 Adding host: K2(104638) to group: /Global/Corp (102572)
```

```

27-FEB 14:18:35 Adding host: Everest (102573) to group: /Global/Bangalore (104538)
27-FEB 14:18:35 Adding host: McKinley (104637) to group: /Global/United States/
Northwest(104639)
27-FEB 14:18:35 Moving host: testhost (102573) from group: testgroup (102572) to group: /
Global/Recycle (104541)
27-FEB 14:18:35 Completed processing host group membership, filePathname: /opt/mycompany/
database/movehosts.csv recycleGroup: /Global/Recycle , removeOldEntries: 1)

```

Symantec NetBackup Utilities

The following utilities apply only to Symantec NetBackup environments.

- [Automating NetBackup Utilities](#)
- [Organize Clients into Groups by Management Server](#)
- [Set Up an Inactive Clients Group](#)
- [Set Up a Host Group for Clients in Inactive Policies](#)
- [Set Up Clients by Policy](#) and [Set Up Clients by Policy Type](#)

Automating NetBackup Utilities

The Veritas NetBackup utilities listed in this section can be set up to run automatically. A stored procedure can be edited to customize the list of utilities to be run as a background job on a particular schedule.

Windows: C:\opt\oracle\database\stored_procedures\nbu\setup_nbu_jobs_manual.sql

Linux: opt/aptare/database/stored_procedures/nbu/setup_nbu_jobs_manual.sql

All five of the [Symantec NetBackup Utilities](#) are included in this file. To omit a particular utility from the scheduled job, use the following syntax before and after the block of code.

- Before the block of code to be omitted, use: /*
- After the block of code to be omitted, use: */

Example of a Scheduled NetBackup Utility

In a text editor, open the `setup_nbu_jobs_manual.sql` file and modify the schedule to meet your needs. The following example illustrates how to edit syntax to customize the schedule.

```

-----
-- Move clients that are in inactive policies
-- Frequency: Every day at 02:30
-----

jobNo := dba_package.getDatabaseJobID('server_mgmt_pkg.setupInactivePolicyClients');
IF (jobNo IS NOT NULL AND jobNo != 0) THEN
    DBMS_OUTPUT.put_line('setupInactivePolicyClients exists and will first be removed before adding a new
version');
    DBMS_JOB.REMOVE(jobNo);
END IF;

DBMS_JOB.SUBMIT(
    job          => jobNo,

```

```

what      => 'server_mgmt_pkg.setupInactivePolicyClients(NULL, NULL, 0, 0);', -- What to run
next_date => SYSDATE + (5/48), -- First run is 150 mins from initial installation
interval  => 'TRUNC(SYSDATE+1,'DD') + (5/48)'; -- Next run is 2:30 each subsequent day
DBMS_OUTPUT.put_line('setupInactivePolicyClients set to run at 2:30 every day');
COMMIT;

```

Scheduling a NetBackup Utility Job to Run Automatically

Execute the SQL file, as user `aptare` on a Linux system or on a Windows system, as an Administrator who is a member of the `ORA_DBA` group:

```
sqlplus portal/portal_password @setup_nbu_jobs_manual.sql
```

Organize Clients into Groups by Management Server

This utility enables you to create a hierarchy of management servers and links all clients that are members of the management server into the respective host group. For example, in a Symantec NetBackup environment if you have two master servers called `master1` and `master2`, this utility creates host groups named `master1` and `master2` and links the master server's clients into the corresponding group. Two versions of this utility are available:

- Move clients into a Master Server Group: [Basic Usage with 4 Parameters](#)
- Move clients into a Master Server Group & Exclude the Policy Client & Cascade to Sub-groups: [Usage with 6 Parameters](#)

Basic Usage with 4 Parameters

```
execute nbu_adaptor_pkg.moveClientsIntoMasterGroups(  
<source_group_id>,<destination_group_id>, <move_clients>, <latest_master_only>  
) ;
```

Example: execute nbu_adaptor_pkg.moveClientsIntoMasterGroups(300000, 300010, 1, 1) ;

source_group_id is the internal group ID of the host group hierarchy to traverse.

destination_group_id is the group ID in which the host group for your master servers groups will be created. APTARE recommends that you create a host group under source_group_id called Masters or Management Servers and use the group ID of this new host group for the second parameter.

See [Identifying a Host Group ID](#).

When you organize by master server, if a host group exists anywhere under the source group hierarchy with the name of the master server, the routine associates the clients with that folder and does not create a new folder under the destination folder. This association occurs whether you explicitly specify the destination folder or if the destination is NULL. However, if you pass a source folder that is at a lower level, the routine only checks for a folder under that hierarchy. If you specify NULL as the destination, the routine will create (if it does not exist already) a group called “NetBackup” under the Source group ID. It then creates a host group called “Master Servers” under the “NetBackup” group.

move_clients If set to 0, the clients link into the respective host group and remain in their original host group location. If set to 1, all the clients move from the source host group and into the respective host groups.

The utility processes and organizes all clients of the source group hierarchy into the target master server grouping. However, if the move_clients flag is set to 1, the utility removes only clients in the top level source_group_id group—and those already organized in lower level sub-groups remain.

latest_master_only defaults to 0, but can be set to 1, indicating organization by the latest master server. If a client is backed up by two master servers, or if a client was backed up by master server A in the past, but is now backed up by master server B, setting this flag to true will result in the client being organized by the latest master server.

Usage with 6 Parameters

```
execute nbu_adaptor_pkg.moveClientsIntoMasterGroups(  
<source_group_id>,<destination_group_id>, <cascade_source_group>,  
<move_clients>, <latest_master_only>, <exclude_policy_client>);
```

Example: `exec moveClientsIntoMasterGroups(300000, 300010, 1, 1, 1, 0);`

source_group_id is the internal group ID of the host group hierarchy to traverse.

destination_group_id is the group ID in which the new host group for your master servers will be created. APTARE recommends that you create a host group under **source_group_id** called Masters or Management Servers and use the group ID of this new host group for the second parameter.

See [Identifying a Host Group ID](#).

When you organize by master server, if a host group exists anywhere under the source group hierarchy with the name of the master server, the routine associates the clients with that folder and does not create a new folder under the destination folder. This association occurs whether you explicitly specify the destination folder or if the destination is NULL. However, if you pass a source folder that is at a lower level, the routine only checks for a folder under that hierarchy. If you specify NULL as the destination, the routine will create (if it does not exist already) a host group called “NetBackup” under the Source group ID. It then creates a host group called “Master Servers” under the “NetBackup” host group.

cascade_source_group can be set to 0 = Do not include sub-groups, 1 = Include sub-groups. Use **cascade_source_group** to find and re-sort all of the defined host groups that are under the source group. Use this parameter so that you do not have to move all of your clients to the top before re-sorting.

move_clients If set to 0, the clients link into the respective host group and remain in their original host group location. If set to 1, all the clients move from the source group and into the respective management server host groups.

The utility processes and organizes all clients of the source group hierarchy into the target master server grouping. However, if the **move_clients** flag is set to 1, the utility removes only clients in the top-level **source_group_id** group—and those already organized in lower-level sub-groups remain.

latest_master_only defaults to 0, but can be set to 1, indicating organization by the latest master server. If a client is backed up by two master servers, or if a client was backed up by master server A in the past, but is now backed up by master server B, setting this flag to true will result in the client being organized by the latest master server.

exclude_policy_client defaults to 0, but can be set to 1, indicating that you want to organize the clients based on backups and exclude policy-based clients. If this flag is set to 0, the utility finds the clients that are backed up by the master server and also clients that are in the policy that is controlled by the master server.

Set Up an Inactive Clients Group

Description	This utility enables you to automatically generate a list of all clients that are not a member of any policy and move or link the clients into a user-definable host group.
Usage	<pre>execute server_mgmt_pkg.setupInactiveClientsGroup (<host_group_to_traverse>, '<inactive_clients_group>', <move_or_copy_flag>);</pre> <p>Example: <code>exec setupInactiveClientsGroup('/Global/Corp',NULL,0);</code></p> <p>Where:</p> <p>host_group_to_traverse is the full pathname to the host group hierarchy to traverse looking for inactive clients, for example <code>/Aptare/hostgroup1</code>.</p> <p>inactive_clients_group is the full pathname to the host group into which the inactive clients will be moved or linked. The default value for this parameter is <code>NULL</code> (which should not be within quotes). If set to <code>NULL</code>, the utility automatically creates a host group called <code>Clients Not In Policy</code> within <code>host_group_to_traverse</code>.</p> <p>move_or_copy_flag can be set to <code>0=Link (copy) clients</code> or <code>1=Move clients</code>. If set to <code>0</code>, the utility links the clients to the <code>inactive_clients_group</code> and keeps the clients in their original host group location. If set to <code>1</code>, the utility moves all the inactive clients from their current host group location and consolidates them into the <code>inactive_clients_group</code>.</p>

Set Up a Host Group for Clients in Inactive Policies

Description	This utility enables you to automatically generate a list of all clients that are members of a policy, but the policy is NOT active. These clients are then linked or copied into a user-definable host group.
Usage	<pre>execute server_mgmt_pkg.setupInactivePolicyClients (<host_group_to_traverse>, '<inactive_clients_group>', <move_or_copy_flag>, <include_deleted_flag>);</pre> <p>Example: <code>exec setupInactivePolicyClients('/Global/Corp',NULL,1,0);</code></p> <p>Where:</p> <p>host_group_to_traverse is the full pathname to the host group hierarchy to traverse looking for inactive policies, for example <code>/Aptare/hostgroup1</code>.</p> <p>inactive_clients_group is the full pathname to the host group into which the clients in an inactive policy will be moved or linked. The default value for this parameter is <code>NULL</code> (which should not be within quotes). If set to <code>NULL</code>, the utility automatically creates a host group called <code>Inactive Policy Clients</code> within <code>host_group_to_traverse</code>.</p> <p>move_or_copy_flag can be set to <code>0=Link (copy) clients</code> or <code>1=Move clients</code>. If set to <code>0</code>, the utility links the client to the <code>inactive_clients_group</code> and keeps the client in the original host group location. If set to <code>1</code>, the utility moves all the clients in inactive policies from their current host group location and consolidates them into the <code>inactive_clients_group</code>.</p> <p>include_deleted_flag can be used in conjunction with the <code>move_or_copy_flag</code> can be set to <code>1</code> to include policies deleted from NetBackup while organizing inactive policy clients into the <code>inactive_clients_group</code>.</p>

Set Up Clients by Policy

Description	<p>This utility enables you to automatically organize clients by the Symantec NetBackup Policy (or Policies) to which they belong. The utility automatically creates host groups for each Symantec NetBackup Policy and links clients that are members of these policies to the host group(s) accordingly.</p>
Usage	<pre>execute nbu_adaptor_pkg.setupClientsByPolicy ('<source_host_group>', '<destination_host_group>');</pre> <p>Example: <code>exec setupClientsByPolicy('/Global/Corp', NULL);</code></p> <p>Where:</p> <p>source_host_group is the full pathname to the host group hierarchy to traverse for clients, for example <code>/Aptare/hostgroup1</code>. The default value for this parameter is <code>NULL</code> (which should not be within quotes). If set to <code>NULL</code>, the utility automatically locates the highest level host group to traverse.</p> <p>destination_host_group is the full pathname to the host group under which the new groups by policy name will be automatically created. The default value for this parameter is <code>NULL</code> (which should not be within quotes). If set to <code>NULL</code>, the utility automatically creates a host group called <code>NetBackup Policies</code> within <code>source_server_group</code>.</p> <p>If a client is removed from a Symantec NetBackup policy, added to a new policy and the utility is subsequently run again, the client will appear in the new policy group but will not be deleted from the old policy group. To remove the client from the old policy group and completely re-synchronize the grouping structure, simply delete the Policy grouping hierarchy via the <code>deleteEntireGroupContents</code> utility, referenced in Delete Host Group, and then run the <code>setupClientsByPolicy</code> utility again.</p>

Set Up Clients by Policy Type

Description	<p>This utility enables you to automatically organize clients by the type of the Symantec NetBackup policy to which they belong; for example, Standard, NDMP, ORACLE. The utility automatically creates host groups for each Symantec NetBackup policy type and links clients that are members of these policy types to the host group(s) accordingly.</p>
Usage	<pre>execute nbu_adaptor_pkg.setupClientsByPolicyType ('<source_host_group>', '<destination_host_group>');</pre> <p>Example: <code>exec setupClientsByPolicyType('/Global/Corp', NULL);</code></p> <p>Where:</p> <p>source_host_group is the full pathname to the server group hierarchy to traverse for clients, for example <code>/Aptare/hostgroup1</code>. The default value for this parameter is <code>NULL</code> (which should not be within quotes). If set to <code>NULL</code>, the utility automatically locates the highest level host group to traverse.</p> <p>destination_server_group is the full pathname to the server group under which the new groups by Policy type will be automatically created. The default value for this parameter is <code>NULL</code> (which should not be within quotes). If set to <code>NULL</code>, the utility automatically creates a host group called <code>NetBackup Policy Types</code> within <code>source_host_group</code>.</p> <p>If a client is removed from one Symantec NetBackup policy type, added to a new policy type and the utility is subsequently run again, the client will appear in the new policy type host group but will not be deleted from the old policy group. To remove the client from the old policy group and completely re-synchronize the grouping structure, simply delete the Policy Type grouping hierarchy via the <code>deleteEntireGroupContents</code> utility, referenced in Delete Host Group, and then run the <code>setupClientsByPolicy</code> utility again.</p>

IBM Tivoli Storage Manager Utilities

The utilities contained in this section apply only to IBM Tivoli Storage Manager environments and clients that have been backed up by IBM Tivoli Storage Manager.

- [Set Up Clients by Policy Domain](#)
- [Set Up Clients by IBM Tivoli Storage Manager Instance](#)

Set Up Clients by Policy Domain

Description	<p>This utility enables you to automatically organize clients by the IBM Tivoli Storage Manager policy domain(s) to which they belong. The utility automatically creates host groups for each policy domain and links clients that are members of these Policy domain(s) to the host group(s) accordingly.</p>
Usage	<pre>execute tsm_common_pkg.TSMsetupClientsByPolicyDomain ('<source_host_group>', '<destination_host_group>');</pre> <p>Example: <code>exec tsm_common_pkg.TSMsetupClientsByPolicyDomain('/Global', NULL);</code></p> <p>Where:</p> <p>source_host_group is the full pathname to the server group hierarchy to traverse for clients, for example <code>/Aptare/hostgroup1</code>. The default value for this parameter is <code>NULL</code> (which should not be within quotes). If set to <code>NULL</code>, the utility automatically locates the highest level host group to traverse.</p> <p>destination_host_group is the full pathname to the host group under which the new groups by policy domain name will be automatically created. The default value for this parameter is <code>NULL</code> (which should not be within quotes). If set to <code>NULL</code> the utility automatically creates a host group called <code>Policy Domains within source_host_group</code>.</p> <p>If a client is removed from a IBM Tivoli Storage Manager policy domain, added to a new policy domain and the utility is subsequently run again, the client will appear in the new policy group but will not be deleted from the old policy group. To remove the client from the old policy group and completely re-synchronize the grouping structure, simply delete the Policy domain grouping hierarchy via the <code>deleteEntireGroupContents</code> utility, referenced in Delete Host Group, and then run the <code>TSMsetupClientsByPolicyDomain</code> utility again.</p>

Set Up Clients by IBM Tivoli Storage Manager Instance

Description	This utility enables you to automatically organize clients by the IBM Tivoli Storage Manager instance to which they belong. The utility automatically create host groups for each instance, then links clients that are members of the instance into the host group(s) accordingly.
Usage	<pre>execute tsm_common_pkg.TSMsetupClientsByInstance ('<source_host_group>', '<destination_host_group>', <move_or_copy_flag>);</pre> <p>Example: <code>exec tsm_common_pkg.TSMsetupClientsByInstance('/Global', NULL, 1);</code></p> <p>Where</p> <p>source_host_group is the full pathname to the host group hierarchy to traverse for clients, for example <code>/Aptare/hostgroup1</code>. The default value for this parameter is <code>NULL</code> (which should not be within quotes). If set to <code>NULL</code>, the utility automatically locates the highest level host group to traverse.</p> <p>destination_host_group is the full pathname to the host group under which new groups by instance name will be automatically created. The default value for this parameter is <code>NULL</code> (which should not be within quotes). If set to <code>NULL</code> the utility automatically creates a host group called <i>IBM Tivoli Storage Manager instances</i> within <code>source_host_group</code>.</p> <p>move_or_copy_flag can be set to 0=Link (copy) clients or 1=Move clients. If set to 0, the utility links the clients to their respective host groups and keeps the clients in their original host group location. If set to 1, the utility moves all clients from the source host group and to their respective host groups.</p>

Scheduling Utilities To Run Automatically

The utilities can be run on a one-time basis, or scheduled to run every day to automatically keep your hosts and host groups up to date. Scheduling can be accomplished by creating an Oracle job. APTARE IT Analytics already makes use of Oracle jobs to run many background tasks such as purging old data and rebuilding indices.

The sample SQL file in [Example—Scheduling Utilities to Run Automatically](#) sets up an Oracle job to run every day at 5:00 a.m. and call the `moveOrCopyClients` utility to move clients from one folder to another. This example can be used as a template for other automatic jobs you need to set up. Simply customize the text in **bold** for your particular requirements.

To see the Oracle jobs that are automatically configured as part of a new install, review the following files:

- `<database_home>/stored_procedures/setup_base_jobs.plb`
- `<database_home>/stored_procedures/nbu/setup_nbu_jobs.sql`
- `<database_home>/stored_procedures/tsm/setup_tsm_jobs.plb`
- `<database_home>/stored_procedures/tsm/setup_leg_jobs.plb`

Where **database_home** is `/opt/aptare/database` for Linux servers and `C:\opt\oracle\database` for Windows servers.

Example—Scheduling Utilities to Run Automatically

In order to execute the following sample SQL file, as user `aptare` on a Linux system or on a Windows system as an Administrator who is a member of the `ORA_DBA` group execute the following:

```
sqlplus portal/portal_password @setup_ora_job.sql
```

The following example uses two methods:

moveOracleClients	The name you want to assign to this job you are defining.
MoveOrCopyClients	The utility you are calling along with the parameters you are passing.

Note: The parameters passed to the `moveOrCopyClients` method which must be quoted actually have two single quotes. The two single quotes is the standard Oracle syntax to incorporate a literal quote within an already quoted string.

Sample .sql file (setup_ora_job.sql) to set up an automatic job

```
SET SERVEROUTPUT ON
SET ECHO OFF
DECLARE
    jobNo    user_jobs.job%TYPE := NULL;

BEGIN
    -----
    -- Move new clients whose server name ends with 'ORA' into the 'database' host group
    -- Frequency: Every day at 5am (Portal Time)
    -----

    jobNo := dba_package.getDatabaseJobID('moveOracleClients');
    IF (jobNo IS NOT NULL AND jobNo != 0) THEN
        DBMS_OUTPUT.put_line('moveOracleClients exists and will first be removed before
adding a new version');
        DBMS_JOB.REMOVE(jobNo);
    END IF;
    DBMS_JOB.SUBMIT(
        job          => jobNo,
        what          => 'server_mgmt_pkg.moveOrCopyClients('/Aptare','/Aptare/
database',''*ORA'', 1);', -- What to run
        next_date     => SYSDATE + (5/24), -- First run is 5am
server time
        interval      => 'TRUNC(SYSDATE+1,'DD') + (5/24)'); -- Next run is 5am
each subsequent day
        DBMS_OUTPUT.put_line('moveOracleClients job set to run at 5am every day');

    COMMIT;
END;

/
quit;
```


Attribute Management

This section covers the following:

- [Attribute Bulk Load Utilities](#)
- [Attribute Naming Rules](#)
- [Rename Attributes Before Upgrading](#)
- [Load Host Attributes and Values](#)
- [Load Attributes and Values and Assign to Hosts](#)
- [Load Array Attributes and Values and Assign to Arrays](#)
- [Overview of Application Attributes and Values](#)
- [Load Application Database Attributes and Values](#)
- [Load MS Exchange Organization Attributes and Values](#)
- [Load LUN Attributes and Values](#)
- [Load Switch Attributes and Values](#)

Attribute Bulk Load Utilities

The *Attributes* feature provides the ability to define a scope for a report based on specific characteristics, such as operating system or host criticality. In effect, when you generate a report, you can select a set of objects that share the same *attribute* or characteristic.

Often, large enterprise environments need to configure attributes for many *objects*, such as hosts, arrays, and switches. Bulk load utilities assign attributes to objects. While the Portal has capabilities for assigning attributes to certain objects, the utilities described in this section fulfill the large-scale requirement for assigning attributes to a large number of objects.

To facilitate bulk loading and configuration of attributes, several utilities are provided. These utilities load attributes and values into the IT Analytics database from comma-separated-values (CSV) files.

Note: Currently, there are no utilities available for the bulk load of Datastore attributes.

- [Attribute Naming Rules](#)
- [Rename Attributes Before Upgrading](#)
- [Load Host Attributes and Values](#)
- [Load Attributes and Values and Assign to Hosts](#)
- [Load Array Attributes and Values and Assign to Arrays](#)
- [Load Application Database Attributes and Values](#)
- [Load MS Exchange Organization Attributes and Values](#)
- [Load LUN Attributes and Values](#)

- [Load Switch Attributes and Values](#)

For Managed Service Providers (MSPs)

Attributes are APTARE IT Analytics domain-specific; therefore, you can configure different object attributes for different clients without impacting the reports and environments of your other clients.

Attribute Naming Rules

Adhere to the following rules when creating attribute names. Attributes are validated against these rules so that there are no conflicts in the database, such as duplicates or the use of Oracle reserved words.

- Limit the length to 30 characters.
- Begin the name with an alphabetic character.
- Use *only* alpha, numeric, or underscore characters in the name. Spaces and special characters other than underscores are *not* allowed in attribute names, although they are allowed in the list of values (LOV) for an attribute.
- Names are *not* case-sensitive.
- Do *not* use Oracle reserved words. See http://docs.oracle.com/cd/E15817_01/appdev.111/b31231/appb.htm. To list the Oracle reserved words, use this SQLPlus query at the command line:

```
SQL> SELECT * from v$reserved_words;
```
- Attribute names within a domain hierarchy must be unique.

Rename Attributes Before Upgrading

Beginning with APTARE Release Version 10, all attributes are multi-object attributes—that is, a single attribute is defined and that attribute, with its values, can be used for multiple object types. For example, prior to APTARE Release Version 10, you could have a *Location* attribute for a host and a separate *Location* attribute for an array. During the upgrade, a system attribute named *Location* is added to the database and this single attribute can be used for multiple object types—in this example, it would be used for both hosts and arrays.

During the Portal upgrade, if the names of existing attributes match the name of a system attribute introduced with the upgrade, you may want to rename existing attributes so that their values do not get merged into a single attribute. Renaming of attributes, before the upgrade is completed, must be performed using SQL at the command line.

Note: After you rename an attribute, any report templates that used these attributes must be updated via the Portal SQL Template Designer.

To rename existing attributes so that their values do not get merged into a single attribute, take the following steps.

1. Refer to [Attribute Naming Rules](#).

2. Log in to the Portal server.

3. At the command line:

```
su - aptare
```

4. At the command line, launch sqlplus:

```
sqlplus <pwd>/<pwd>
```

- Example: `sqlplus portal/portal`

5. At the command line, execute the following at the SQL prompt:

```
UPDATE apt_attribute
SET attribute_name = '<NewAttributeName>'
WHERE attribute_id = <ExistingAttributeID>;
Commit;
```

Where <NewAttributeName> is the new name you supply and <ExistingAttributeID> is the ID listed during the Portal upgrade process.

Load Host Attributes and Values

Function: This utility provides an efficient method for creating multiple attributes, along with a list of possible values for each attribute. *Note that the result of this process is simply an inventory of attributes with an associated list of values (LOV). These attributes need to be applied to hosts.* This can be accomplished via the Portal or by using other attribute load utilities.

Before You Begin

Bulk Load utilities must be run in SQLPLUS as user APTARE. The load_package utility is located in:

```
/opt/aptare/database/stored_procedures (Linux)
\opt\oracle\database\stored_procedures (Windows)
```

Create a CSV File

In preparation for loading host attributes, enter the information into a spreadsheet from which you will create a comma-separated values file.

The table in the spreadsheet should be in the following format:

- **first column** - list the attribute name
- **subsequent columns** - list the possible values for the attribute

Refer to [Attribute Naming Rules](#).

Table 1: Example of a Table of Attributes and Values

Operating System	Solaris	AIX
Criticality	Mission Critical	Low

↑
Attribute Name

↑
Attribute Value

↑
Attribute Value

Execute the Load Utility

To load attributes and values for a domain:

1. Create a table in a spreadsheet, as shown in the above example. Save the table as a comma-separated file in a temporary directory.
 - **Windows example:** C:\temp\attributes.csv
 - **Linux example:** /tmp/attributes.csv
2. Log in to the Portal server.
3. At the command line:

```
su - aptare
```
4. At the command line, launch sqlplus:

```
sqlplus <pwd>/<pwd>
```

 - **Example:** sqlplus portal/portal

5. At the command line, execute the following at the **SQL** prompt:

```
SQL> Execute load_package.loadAttributeFile('pathname_and_filename', 'domain_name');
```

where:

'pathname_and_filename'	full path + filename (enclosed in single straight quotes) of the CSV file that you created
'domain_name'	name of the domain in which the hosts reside (enclosed in single straight quotes). See Finding the Domain Name .

Example:

```
Execute load_package.loadAttributeFile('c:\temp\attributes.csv', 'APTARE');
```

6. Restart the Portal services so that the newly added attributes become available in the Dynamic Template Designer.

Finding the Domain Name

To identify the domain:

- In the Portal: **Admin > Domains > Domains**

Load Attributes and Values and Assign to Hosts

Function: This utility provides an efficient method of assigning attributes to a large number of hosts.

To create an inventory of a large number of host attributes and associated values using a bulk load utility, see [Rename Attributes Before Upgrading](#).

Before You Begin

Bulk Load utilities must be run in SQLPLUS as user APTARE. The load_package utility is located in:

```
/opt/aptare/database/stored_procedures (Linux)
\opt\oracle\database\stored_procedures (Windows)
```

Take the following steps to load attributes and values and assign those attributes to hosts:

1. [Create a CSV File of Hosts, Attributes, and Values](#)
2. [Execute the Load Host Attribute Utility](#)
3. [Verify the Host Attributes Load](#)
4. Create a report template using a Report Template Designer.

Once attribute values are assigned to hosts, a report can query the database to report on hosts, filtered by the attributes that you've created to categorize them.

Create a CSV File of Hosts, Attributes, and Values

In preparation for loading host attributes, you will need to enter information into a spreadsheet from which you will create a comma-separated values (CSV) file. The table in the spreadsheet should be in the following format:

Columns

- One column lists the hosts, which must already exist in the APTARE IT Analytics database.
- Each additional column lists attributes and values that will be applied to the host.

Rows

- First (Header) Row - Enter the object type—in this case, Host Name—followed by attribute names. Note that any column may be used for the list of host names. When you run the utility, you'll indicate which column contains the host names. The header row is information only and is not processed as a data row.
- Subsequent rows list host names, followed by the attribute values that you are assigning to each host.

Attribute & Values		Attribute & Values
Host Name	Operating System	Criticality
kiwi_server	Solaris	Mission Critical
aardvark_server	AIX	Unknown

Rules for Attributes and Values in the CSV File

- The hosts listed in the CSV must already exist in the Portal database.
- A host should be listed *only once*. If a host name is listed in multiple rows, only the attributes from the last row with the same host name will be saved.
- The Host Name cannot begin with #. Any line that begins with # will be ignored.
- Follow the [Attribute Naming Rules](#) for the attribute name.
- The maximum line size—that is, characters in a row—is 8192 characters.
- Every column must have a value for each row. Those columns that do not have any actual values can be filled with **N/A** or **Unknown** or a period (.). Attribute values of “N/A”, “Unknown”, “.” will be ignored.
- A single attribute **value** cannot include commas. For example: LastName, FirstName
Use spaces instead of commas to separate words. For example: LastName FirstName

Execute the Load Host Attribute Utility

Note: This utility can be used to load new data as well as to update previously loaded data. To revise existing data, simply run the utility with an updated CSV file.

To assign attributes to hosts:

1. Create a table in a spreadsheet, as shown in [Create a CSV File of Hosts, Attributes, and Values](#).
2. Save the table as a comma-separated file (for example, HostAttributes.csv).
3. Log in to the Portal server.
4. At the command line:

```
su - aptare
```
5. At the command line, launch sqlplus:

```
sqlplus <pwd>/<pwd>
```

 - Example:

```
sqlplus portal/portal
```
6. Execute the following at the **SQL prompt**:

```
SQL> Execute load_package.loadServerAttributeFile('pathname_and_filename',  
'domain_name',host_name_column_num,'log_path_name','log_file_name','check_valid_value');
```

Where:

'pathname_and_filename'	Full path + filename (enclosed in single straight quotes) of the CSV file that you created.
'domain_name'	Name (enclosed in single straight quotes) of the APTARE IT Analytics domain in which the host groups and hosts reside. See Finding the Domain Name .
host_name_column_num	Column number in the csv file where the host names are listed. These hosts must already exist in the APTARE IT Analytics database. Typically, this would be column 1.
'log_path_name'	Full path (enclosed in single straight quotes) where the log file will be created/updated. Verify that you have write access to this directory. Example: 'C:\tmp' Optional: If you do not specify a path and log file name, only error messages will be written to the scon.err file. To omit this parameter, enter: "

'log_file_name'	Filename of the log where execution status and errors messages are written. Example: 'HostAttributeLoad.log' Optional: If you do not specify a path and log file name, only error messages will be written to the scon.err file. To omit this parameter, enter: "
'check_valid_value'	'Y' or 'N' Indicates if you want the utility to check if the values provided in this file are among the existing possible values for the attributes. Y or N must be enclosed in single straight quotes.

Example:

```
Execute load_package.loadServerAttributeFile('C:\myfiles\HostAttributes.csv',
'QA_Portal',1,'C:\tmp','HostAttributeLoad.log','Y');
```

- Restart the Portal services so that the newly added attributes become available in the Dynamic Template Designer.

Verify the Host Attributes Load

To verify that the attribute load took effect:

- In the Portal, go to **Reports**.
- Select a blue user folder.
- Select **New SQL Template**.
- With the SQL Template Designer open, click the **Query** tab.
- Enter the following query in the SQL Template Designer to verify Host attributes:

```
select * from apt_v_server_attribute
```


Load Array Attributes and Values and Assign to Arrays

Function: The Load Array Attributes utility provides an efficient method of assigning attributes to a large number of arrays.

Take the following steps to load array attributes and values:

1. [Create a CSV File of Arrays, Attributes, and Values](#)
2. [Execute the Load Array Attribute Utility](#)
3. [Verify the Array Attributes Load](#)
4. Create a report template using a Report Template Designer.

Once attribute values are assigned to hosts, a Report Template Designer report can query the database to report on arrays, filtered by the attributes that you've created to categorize them.

Create a CSV File of Arrays, Attributes, and Values

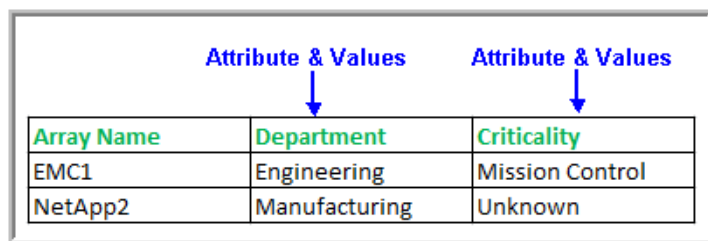
In preparation for loading array attributes, you will need to enter information into a spreadsheet from which you will create a comma-separated values (CSV) file. The table in the spreadsheet should be in the following format:

Columns

- One column lists the arrays, which must already exist in the APTARE IT Analytics database.
- Each additional column lists attributes and values.

Rows

- First (Header) Row - Enter the object type—in this case, Array Name—followed by attribute names. Note that any column may be used for the list of array names. When you run the utility, you'll indicate which column contains the array names. The header row is information only and is not processed as a data row.
- Subsequent rows list arrays, followed by the attribute values that you are assigning to each array.



Array Name	Department	Criticality
EMC1	Engineering	Mission Control
NetApp2	Manufacturing	Unknown

See [Rules for Attributes and Values in the CSV File](#).

Execute the Load Array Attribute Utility

Before You Begin

Bulk Load utilities must be run in SQLPLUS as user APTARE. The load_package utility is located in:

```
/opt/aptare/database/stored_procedures (Linux)
\opt\oracle\database\stored_procedures (Windows)
```

To assign attributes to arrays

Note: This utility only assigns attributes to active arrays. If an array exists in the system, but it is inactive, the log will indicate that no attribute was assigned.

1. Create a table in a spreadsheet, as shown in [Create a CSV File of Arrays, Attributes, and Values](#).
2. Save the table as a comma-separated file (for example, ArrayAttributes.csv).
3. Log in to the Portal server.

4. At the command line:

```
su - aptare
```

5. At the command line, launch sqlplus:

```
sqlplus <pwd>/<pwd>
```

- Example: sqlplus portal/portal

6. Execute the following at the **SQL** prompt:

```
SQL> Execute load_package.loadArrayAttributeFile('pathname_and_filename',
'domain_name',array_name_column_num,'log_path_name','log_file_name','check_valid_value');
```

Where:

'pathname_and_filename'	Full path + filename (enclosed in single straight quotes) of the CSV file you created.
'domain_name'	Name (enclosed in single straight quotes) of the APTARE IT Analytics domain in which the arrays reside. See Finding the Domain Name .
array_name_column_num	Column number in the csv file where the array names are listed. These arrays must already exist in the APTARE IT Analytics database. Typically, this would be column 1.
'log_path_name'	Full path (enclosed in single straight quotes) where the log file will be created/updated. Verify that you have write access to this directory. Example: 'C:\tmp' Optional: If you do not specify a path and log file name, only error messages will be written to the scon.err file. To omit this parameter, enter: "
'log_file_name'	Filename of the log where execution status and errors messages are written. Example: 'ArrayAttributeLoad.log' Optional: If you do not specify a path and log file name, only error messages will be written to the scon.err file. To omit this parameter, enter: "
'check_valid_value'	'Y' or 'N' Indicates if you want the utility to check if the values provided in this file are among the existing possible values for the attributes. Y or N must be enclosed in single straight quotes.

Example:

```
Execute load_package.loadArrayAttributeFile('C:\myfiles\ArrayAttributes.csv',  
'QA_Portal',1,'C:\tmp','ArrayAttributeLoad.log','Y');
```

7. Restart the Portal services so that the newly added attributes become available in the Dynamic Template Designer.

Verify the Array Attributes Load

To verify that the attribute load took effect:

1. In the Portal, go to **Reports**.
2. Select a blue user folder.
3. Select **New SQL Template**.
4. With the SQL Template Designer open, click the **Query** tab.
5. Enter the following query in the SQL Template Designer to verify Array attributes:

```
select * from aps_v_storage_array_attribute
```

Overview of Application Attributes and Values

Applications consume storage on a host and therefore it is often necessary to account for who is using that storage. Since several applications may reside on a host, additional criteria can be used to classify a specific application.

Application attributes provide the mechanism for identifying a host's applications—an Application Database or MS Exchange Organization—enabling reports that:

- Identify the group within your organization that is using an application, to be able to determine accountability.

Example: Which applications are being used by the Engineering department so that I can charge them for capacity usage?

- Identify applications by type/function.

Example: Which applications are used for production and which are development applications?

Note: Currently, application attributes can be used *only* in reports created with the SQL Template Designer.

Load Application Database Attributes and Values

Function: The Load Application Database Attributes utility provides an efficient method of assigning attributes to a large number of application databases.

Take the following steps to load application database attributes and values:

1. [Create a CSV File of Application Database Objects and Attributes](#)
2. [Execute the Load Application Database Attribute Utility](#)
3. [Verify the Application Database Attributes Load](#)
4. Create a report template using the SQL Template Designer.

Once attribute values are assigned to application databases, a SQL Template Designer report can query the database to report on the application databases.

Create a CSV File of Application Database Objects and Attributes

The LoadDBAttribute utility assigns application attribute values to a host's database application. This utility takes as input a comma-separated values (CSV) file.

NOTE: This CSV file becomes the master document of record for Application Database Attributes and therefore should be preserved in a working directory for future updates.

1. Create a spreadsheet table, in the format shown in the following example, and save it as a CSV file in a working directory. This file is specific to application databases.

The diagram shows a table with five columns: Host Name, DB Name, DB Instance, Department, and Function. The first three columns are grouped by a bracket and labeled 'Uniquely identifies an Application Database'. The last two columns are each labeled 'Attribute & Values' with a downward arrow pointing to the column header.

Host Name	DB Name	DB Instance	Department	Function
CorpServer1	FinanceDB	FinanceDBInstance	R&D	Development
CorpServer1	MktDB	MktDBInstance	Marketing	Sales Support
CorpServer2	SalesDB	SalesDBInstance	Marketing	Sales Support
CorpServer2	EngDB	EngDBInstance	Engineering	Production

In the above example:

- The first 3 columns comprise the unique identifier for an Application Database—in this example, CorpServer1, FinanceDB, and FinanceDBInstance.
- Subsequent columns list the attributes and values.

Columns

- Columns list the objects that uniquely identify an application. For an Application Database, the required columns are: Host Name, DB Name, DB Instance.
- Each additional column lists attributes and values.

Rows

- First (Header) Row - Contains the fields that uniquely identify an application, followed by the attribute names. The header row is information only and is not processed as a data row.
- Subsequent rows list the objects that uniquely identify an application database, followed by the attribute values that you are assigning to each application database.

See [Rules for Attributes and Values in the CSV File](#).

Execute the Load Application Database Attribute Utility

Before You Begin

Bulk Load utilities must be run in SQLPLUS as user APTARE. The load_package utility is located in:

```
/opt/aptare/database/stored_procedures (Linux)
\opt\oracle\database\stored_procedures (Windows)
```

To assign attributes to application databases

1. Create a table in a spreadsheet, as shown in [Create a CSV File of Application Database Objects and Attributes](#).
2. Save the table as a comma-separated file (for example, DBAttributes.csv).
3. Log in to the Portal server.

4. At the command line:

```
su - aptare
```

5. At the command line, launch sqlplus:

```
sqlplus <pwd>/<pwd>
```

- Example: sqlplus portal/portal

6. Execute the following at the SQL prompt:

```
SQL> Execute load_package.loadDBAttributeFile('pathname_and_filename','domain_name',
db_name_column_num,db_instance_column_num,host_name_column_num,'log_path_name',
'log_file_name','check_valid_value');
```

Where:

'pathname_and_filename'	Full path + filename (enclosed in single straight quotes) of the CSV file Windows Example: 'c:\config\DBAttributes.csv' Linux Example: '/config/DBAttributes.csv'
'domain_name'	Name (enclosed in single straight quotes) of the domain in which the host groups and hosts reside; Example: 'DomainEMEA' See Finding the Domain Name .
db_name_column_num	Column number in the csv file where the DB Name is listed; Example: 2
db_instance_column_num	Column number in the csv file where the DB Instance is listed; Example: 3
host_name_column_num	Column number in the csv file where the Host Name is listed; Example: 1
'log_path_name'	Full path (enclosed in single straight quotes) where the log file will be created/updated; verify that you have write access to this directory. Optional: If a log path and filename are not specified, log records are written to scon.log and scon.err. To omit this parameter, enter: "" Example: 'c:\configs'

'log_file_name'	Log file name enclosed in single straight quotes. Optional: If a log path and filename are not specified, entries are written to scon.log and scon.err. To omit this parameter, enter: " Example: 'DBAttributes.log'
'check_valid_value'	'Y' or 'N' enclosed in single straight quotes. Y - Checks if the attribute value exists. If the utility determines that the attribute value is not valid, it skips this row and does <i>not</i> assign the attribute value to the application database. N - Updates <i>without</i> checking that the attribute value exists. This option is seldom chosen, but it is available for certain customer environments where attributes may have been created without values (with scripts that bypass the user interface).

Example:

```
SQL> Execute load_package.loadDBAttributeFile('/config/DBAttributes.csv', 'DomainEMEA', 2, 3, 1, '/config/logs', 'DBAttributes.log', 'Y');
```

7. Check the log file for status and errors.
8. Restart the Portal services so that the newly added attributes become available in the Dynamic Template Designer.
9. Go to [Verify the Application Database Attributes Load](#).

Verify the Application Database Attributes Load

To verify that the attribute load took effect:

1. In the Portal, go to **Reports**.
2. Select a blue user folder.
3. Select **New SQL Template**.
4. With the SQL Template Designer open, click the **Query** tab.
5. Enter the following query in the SQL Template Designer to verify Application Database attributes:

```
select * from aps_v_database_attribute
```

Load MS Exchange Organization Attributes and Values

The Load MS Exchange Organization Attributes utility provides an efficient method of assigning attributes to a large number of Exchange Organizations.

Take the following steps to load Exchange Organization attributes and values:

1. [Create a CSV File of Exchange Organization Objects and Attributes](#)
2. [Load MS Exchange Organization Attributes and Values](#)
3. [Verify the MS Exchange Organization Attributes Load](#)
4. Create a report template using the SQL Template Designer.

Once attribute values are assigned to MS Exchange Organizations, a Report Template Designer report can query the database to report on metrics such as capacity usage for chargebacks.

Create a CSV File of Exchange Organization Objects and Attributes

The Load Exchange Organization Attribute utility assigns application attribute values to a host's Microsoft Exchange Organizations. This utility takes as input a comma-separated values (CSV) file.

NOTE: This CSV file becomes the master document of record for MS Exchange Organization Attributes and therefore should be preserved in a working directory for future updates.

1. Create a spreadsheet table, in the format shown in the following example, and save it as a CSV file in a working directory. This file is specific to MS Exchange Organizations.

MS Exchange Org	Host Name	Version
Exchange2010.QAlab.local	QALab1	14.0
Exchange2010SP1.Prod.local	ProdServer1	14.1

In the above example:

- The first 2 columns comprise the unique identifier for a Microsoft Exchange Organization—in this example, Exchange2010.QAlab.local, QALab1.
- Subsequent columns list the attributes and values—in this example, Version.

Columns

- Columns list the objects that uniquely identify an application. For MS Exchange, the required columns are: MS Exchange Organization and Host Name.

Rows

- First (Header) Row - Names the fields that uniquely identify an application, followed by the attribute names.
- Subsequent rows list the objects that uniquely identify an MS Exchange Organization—in this case, MS Exchange Organization and Host Name—followed by the attribute values that you are assigning to each MS Exchange Organization.

See [Rules for Attributes and Values in the CSV File](#).

Execute the Load MS Exchange Organization Attribute Utility

Before You Begin

Bulk Load utilities must be run in SQLPLUS as user APTARE. The load_package utility is located in:

```
/opt/aptare/database/stored_procedures (Linux)
\opt\oracle\database\stored_procedures (Windows)
```

To assign attributes to Microsoft Exchange Organizations

1. Log in to the Portal server.

2. At the command line:

```
su - aptare
```

3. At the command line, launch sqlplus:

```
sqlplus <pwd>/<pwd>
```

- Example: sqlplus portal/portal

4. Execute the following at the SQL prompt:

```
SQL> Execute load_package.loadExchOrgAttributeFile('pathname_and_filename',
'domain_name',exchange_org_column_num,host_name_column_num,'log_path_name',
'log_file_name','check_valid_value');
```

Where:

'pathname_and_filename'	Full path + filename (enclosed in single straight quotes) of the CSV file Windows Example: 'c:\config\MSEExchangeAttributes.csv' Linux Example: '/config/MSEExchangeAttributes.csv'
'domain_name'	Name (enclosed in single straight quotes) of the APTARE IT Analytics Domain in which the host groups and hosts reside; Example: 'DomainEMEA' See Finding the Domain Name .
exchange_org_column_num	Column number in the csv file where the MS Exchange Organization is listed; Example: 1
host_name_column_num	Column number in the csv file where the Host Name is listed; Example: 2
'log_path_name'	Full path (enclosed in single straight quotes) where the log file will be created/updated; verify that you have write access to this directory. Optional: If a log path and filename are not specified, log records are written to scon.log and scon.err. Example: 'c:\configs'

'log_file_name'	Name of the log file enclosed in single straight quotes. Optional: If a log path and filename are not specified, entries are written to scon.log and scon.err. Example: 'MSExchangeAttributes.log'
'check_valid_value'	'Y' or 'N' enclosed in single straight quotes. Y - Checks if the attribute value exists. If the utility determines that the attribute value is not valid, it skips this row and does <i>not</i> assign the attribute value to the Exchange Organization. N - Updates <i>without</i> checking that the attribute value exists. This option is seldom chosen, but is available for certain customer environments where attributes may have been created without values (with scripts that bypass the user interface).

Example:

```
SQL> Execute load_package.loadExchOrgAttributeFile('/config/MSExchangeAttributes.csv',
'DomainEMEA',1,2,'/config/logs',MSExchangeAttributes.log','Y');
```

5. Check the log file for status and errors.
6. Restart the Portal services so that the newly added attributes become available in the Dynamic Template Designer.
7. Go to [Verify the MS Exchange Organization Attributes Load](#).

Verify the MS Exchange Organization Attributes Load

To verify that the attribute load took effect:

1. In the Portal, go to **Reports**.
2. Select a blue user folder.
3. Select **New SQL Template**.
4. With the SQL Template Designer open, click the **Query** tab.
5. Enter use the following query in the SQL Template Designer to verify the MS Exchange Organization attributes:

```
select * from aps_v_exch_org_attribute
```

Load LUN Attributes and Values

Function: The Load LUN Attributes utility provides an efficient method of assigning attributes to a large number of storage array logical units (LUNs).

To load switch attributes and values

1. [Create a CSV File of LUN Objects and Attributes](#)
2. [Execute the Load LUN Attribute Utility](#)
3. [Verify the LUN Attributes Load](#)
4. Create a report template using the SQL Template Designer.

Once attribute values are assigned to application databases, a SQL Template Designer report can query the database to report on the application databases.

Create a CSV File of LUN Objects and Attributes

The loadLunAttributeFile utility assigns attribute values to a list of LUNs. This utility takes as input a comma-separated values (CSV) file.

NOTE: This CSV file becomes the master document of record for LUN Attributes and therefore should be preserved in a working directory for future updates.

1. Create a spreadsheet table, in the format shown in the following example, and save it as a CSV file in a working directory. This file is specific to loading LUN attributes.

		Attribute & Value	Attribute & Value
Array Name	LUN Name	CustomerName	StorageTier
Cluster-1:172.16.1.344	000187880435 1E28	Customer1	Tier1
Array000287890566	000287890566 000A	Customer2	Tier2

Uniquely identifies a LUN

Columns

- The first column lists the Array Name.
- The second column lists the LUN Name.
- Each additional column lists attributes and values that will be applied to the LUN. Multiple attributes can be assigned to a single LUN object.

Rows

- First (Header) Row - Contains the fields that uniquely identify the LUN (array and LUN names), followed by Attribute names. The header row is information only and is *not* processed as a data row.

- Subsequent rows list the Array name and LUN name, followed by the attribute values that you are assigning to each LUN.

See [Rules for Attributes and Values in the CSV File](#).

Execute the Load LUN Attribute Utility

Before You Begin

Bulk Load utilities must be run in SQLPLUS as user APTARE. The load_package utility is located in:

```
/opt/aptare/database/stored_procedures (Linux)
\opt\oracle\database\stored_procedures (Windows)
```

To assign attributes to application databases

1. Create a table in a spreadsheet, as shown in [Create a CSV File of LUN Objects and Attributes](#).
2. Save the table as a comma-separated file (for example, SwitchAttributes.csv).
3. Log in to the Portal server.
4. At the command line:

```
su - aptare
```

5. At the command line, launch sqlplus:

```
sqlplus <pwd>/<pwd>
```

- **Example:** sqlplus portal/portal

6. Execute the following at the **SQL** prompt:

```
SQL> Execute load_package.loadLunAttributeFile('pathname_and_filename',
'domain_name',array_name_column_num, lun_name_column_num
,'log_path_name','log_file_name','check_valid_value');
```

Where:

'pathname_and_filename'	Full path + filename (enclosed in single straight quotes) of the CSV file Windows Example: 'c:\config\SwitchAttributes.csv' Linux Example: '/config/SwitchAttributes.csv'
'domain_name'	Name (enclosed in single straight quotes) of the domain in which the host groups and hosts reside; Example: 'DomainEMEA' See Finding the Domain Name .
array_name_column_num	Column number in the csv file where the Array Name is listed; Example: 1 Note that the Array Name and the LUN Name can be either column 1 or 2 of the CSV. This parameter tells the utility in which column the Array Name will be found.
lun_name_column_num	Column number in the csv file where the LUN Name is listed; Example: 2
'log_path_name'	Full path (enclosed in single straight quotes) where the log file will be created/updated; verify that you have write access to this directory. Optional: If a log path and filename are not specified, log records are written to scon.log and scon.err. To omit this parameter, enter: "" Example: 'c:\config'

'log_file_name'	Log file name enclosed in single straight quotes. Optional: If a log path and filename are not specified, entries are written to scon.log and scon.err. To omit this parameter, enter: " Example: 'SwitchAttributes.log'
'check_valid_value'	'Y' or 'N' enclosed in single straight quotes. Y - Checks if the attribute value exists. If the utility determines that the attribute value is not valid, it skips this row and does <i>not</i> assign the attribute value to the switch object. N - Updates <i>without</i> checking that the attribute value exists. This option is seldom chosen, but it is available for certain customer environments where attributes may have been created without values (with scripts that bypass the user interface).

Example:

```
SQL> Execute load_package.loadLunAttributeFile('/config/LUNAttributes.csv', 'DomainEMEA',
1, 2, '/config/logs', 'LUNAttributes.log', 'Y');
```

7. Check the log file for status and errors.
8. Restart the Portal services so that the newly added attributes become available in the Dynamic Template Designer.
9. Go to [Verify the LUN Attributes Load](#).

Verify the LUN Attributes Load

To verify that the attribute load was successful:

1. In the Portal, go to **Reports**.
2. Select a blue user folder.
3. Select **New SQL Template**.
4. With the SQL Template Designer open, click the **Query** tab.
5. Enter the following query in the SQL Template Designer to verify Switch attributes:

```
select * from aps_v_logical_unit_attribute
```

Load Switch Attributes and Values

Function: The Load Switch Attributes utility provides an efficient method of assigning attributes to a large number of switches. Please note Fabric Manager must be installed or the loading will fail.

To load switch attributes and values

1. [Create a CSV File of Switches, Attributes, and Values](#)
2. [Execute the Load Switch Attribute Utility](#)
3. [Verify the Switch Attributes Load](#)
4. Create a report template using the SQL Template Designer.

Once attribute values are assigned to application databases, a SQL Template Designer report can query the database to report on the application databases.

Create a CSV File of Switches, Attributes, and Values

The loadSwitchAttributeFile utility assigns attribute values to a list of switches. This utility takes as input a comma-separated values (CSV) file.

NOTE: This CSV file becomes the master document of record for Switch Attributes and therefore should be preserved in a working directory for future updates.

1. Create a spreadsheet table, in the format shown in the following example, and save it as a CSV file in a working directory. This file is specific to loading switch attributes.

SAN Name	Switch Name	Region	Department
2000547FEE23CF22	2001002A6F658F93	EMEA	Engineering
3000447FEE23CF23	2001003A6F658F01	ASIA	Engineering
4000547FEE23CF24	2001004A6F658F23	ASIA	Finance

Columns

- The first column lists the SAN Name.
- The second column lists the Switch Name.
- Each additional column lists attributes and values that will be applied to the switch. Multiple attributes can be assigned to a single switch object.

Rows

- First (Header) Row - Contains the fields that uniquely identify the SAN and Switch names, followed by Attribute names. The header row is information only and is *not* processed as a data row.
- Subsequent rows list the SAN Name and Switch Name, followed by the attribute values that you are assigning to each switch.

See [Rules for Attributes and Values in the CSV File](#).

Execute the Load Switch Attribute Utility

Before You Begin

Bulk Load utilities must be run in SQLPLUS as user APTARE. The load_package utility is located in:

```
/opt/aptare/database/stored_procedures (Linux)
\opt\oracle\database\stored_procedures (Windows)
```

To assign attributes to application databases

1. Create a table in a spreadsheet, as shown in [Create a CSV File of Switches, Attributes, and Values](#).
2. Save the table as a comma-separated file (for example, SwitchAttributes.csv).
3. Log in to the Portal server.
4. At the command line:

```
su - aptare
```

5. At the command line, launch sqlplus:

```
sqlplus <pwd>/<pwd>
```

- **Example:** sqlplus portal/portal

6. Execute the following at the SQL prompt:

```
SQL> Execute load_package.loadSwitchAttributeFile('pathname_and_filename','domain_name',
san_name_col_num,switch_name_col_num,'log_path_name',
'log_file_name','check_valid_value');
```

Where:

'pathname_and_filename'	Full path + filename (enclosed in single straight quotes) of the CSV file Windows Example: 'c:\config\SwitchAttributes.csv' Linux Example: '/config/SwitchAttributes.csv'
'domain_name'	Name (enclosed in single straight quotes) of the domain in which the host groups and hosts reside; Example: 'DomainEMEA' See Finding the Domain Name .
san_name_column_num	Column number in the csv file where the SAN Name is listed; Example: 1 Note that the SAN Name and the Switch Name can be either column 1 or 2 of the CSV. This parameter tells the utility in which column the SAN Name will be found.
switch_name_column_num	Column number in the csv file where the Switch Name is listed; Example: 2
'log_path_name'	Full path (enclosed in single straight quotes) where the log file will be created/updated; verify that you have write access to this directory. Optional: If a log path and filename are not specified, log records are written to scon.log and scon.err. To omit this parameter, enter: "" Example: 'c:\config'

'log_file_name'	Log file name enclosed in single straight quotes. Optional: If a log path and filename are not specified, entries are written to scon.log and scon.err. To omit this parameter, enter: " Example: 'SwitchAttributes.log'
'check_valid_value'	'Y' or 'N' enclosed in single straight quotes. Y - Checks if the attribute value exists. If the utility determines that the attribute value is not valid, it skips this row and does <i>not</i> assign the attribute value to the switch object. N - Updates <i>without</i> checking that the attribute value exists. This option is seldom chosen, but it is available for certain customer environments where attributes may have been created without values (with scripts that bypass the user interface).

Example:

```
SQL> Execute load_package.loadSwitchAttributeFile('/config/SwitchAttributes.csv',
'DomainEMEA', 1, 2, '/config/logs', 'SwitchAttributes.log', 'Y');
```

7. Check the log file for status and errors.
8. Restart the Portal services so that the newly added attributes become available in the Dynamic Template Designer.
9. Go to [Verify the Switch Attributes Load](#).

Verify the Switch Attributes Load

To verify that the attribute load was successful:

1. In the Portal, go to **Reports**.
2. Select a blue user folder.
3. Select **New SQL Template**.
4. With the SQL Template Designer open, click the **Query** tab.
5. Enter the following query in the SQL Template Designer to verify Switch attributes:

```
select * from aps_v_switch_attribute
```


Importing Generic Backup Data

This section covers the following topics:

- [About Generic Backup Data Collection](#)
- [Configuring Generic Backup Data Collection](#)
- [CSV Format Specification](#)
- [Manually Loading the CSV File](#)

About Generic Backup Data Collection

APTARE Backup Manager can report on data from backup products that are *not* native to APTARE IT Analytics—such as PureDisk, BakBone, and BrightStor. Using the backup vendor’s export feature, create a comma-separated values (CSV) file. The APTARE IT Analytics Data Collection process will import the data into the Portal database, to be included in APTARE IT Analytics reports, such as the Job Summary report. The data can be scheduled for regular collection intervals.

Note: In addition to the regularly scheduled data collection, the CSV file also can be imported manually. See [Manually Loading the CSV File](#).

Considerations

- Files can be imported more than once. Importing will *not* result in duplicate entries.
- Data is job-centric only—that is, no tape media or tape library information is imported.
- When checking Data Collection Status, the indicator may display a red error status, which for generic backup data collection, may not be a true error condition. The Generic Backup Data Collector checks the timestamp of the CSV file and if it is the same as the last collection, it does not attempt to re-import the data. In this regard, the Generic Backup data collection process differs from other collectors, as it expects to have data provided via the CSV file.
- Data is stored securely and can be used for historical tracking and trending.

Configuring Generic Backup Data Collection

The following tasks must be performed as part of the Generic Backup Data Collection setup:

- In the APTARE IT Analytics Portal, create a host of type: *Generic Backup Server*. This is the server that is managing the backups of the clients for which you will be importing backup data. See [Host Group Membership](#).
- In the APTARE IT Analytics Portal, add a Data Collector Policy of Product Type: *Generic Backup*. In this policy, supply the path to the CSV file. See [Configuring Generic Backup Data Collection](#).
- Create a comma-separated file of the backup/restore data—typically, a file that has been exported using the backup software utilities. See [CSV Format Specification](#).

CSV Format Specification

Using the backup software, create a comma-separated file that contains the following 15 data elements from the backup/restore job(s). Note that each field must have an entry, even if it is a null entry within the commas. Field values cannot contain embedded commas. All string fields must be enclosed within single straight quotes.

Note: The CSV file must be UTF-8 encoded, however be sure to remove any UTF-8 BOMs (Byte Order Marks). The CSV cannot be properly parsed with these additional characters.

Name	Type	Value
VendorName	STRING	The name of the backup application used to perform the backup, enclosed in single straight quotes.
ClientName	STRING	The host name of the machine being backed up, enclosed in single straight quotes.
ClientIPAddress	NUMBER	The IP address of the machine being backed up. If an IP address is not available, simply use two single straight quotes (") or 'null' to indicate a blank/missing value.
VendorJobType	STRING	Valid values include: BACKUP or RESTORE—enclosed in single straight quotes.
StartDateString	DATE	The start date and time of the backup job in the format: YYYY-MM-DD HH:MI:SS (enclosed in single straight quotes). Note: Adhere to the specific date format—number of digits and special characters—as shown above.
FinishDateString	DATE	The end date and time of the backup job in the format: YYYY-MM-DD HH:MI:SS (enclosed in single straight quotes). Note: Adhere to the specific date format—number of digits and special characters—as shown above.
BackupKilobytes	NUMBER	The numeric size of the backup in kilobytes (otherwise use 0). Remember APTARE IT Analytics uses 1024 for a KiB.
NbrOfFiles	NUMBER	The number of files that were backed up (otherwise use 0).
MediaType	STRING	The type of media that was used: T for Tape or D for Disk, enclosed within single straight quotes.

Name	Type	Value
VendorStatus	NUMBER	A numeric job status: 0=Successful, 1=Partially Successful, or 2=Failed.
VendorJobId	STRING	Vendor job ID, enclosed in single straight quotes.
VendorPolicyName	STRING	Vendor policy name, enclosed in single straight quotes.
JobLevel	STRING	Job level, enclosed in single straight quotes. Example: Incremental, Full.
TargetName	STRING	File system backed up by the managed backup system (MBS), enclosed in single straight quotes.
ScheduleName	STRING	Name of the backup schedule, enclosed in single straight quotes.

EXAMPLE: genericBackupJobs.csv

```
'Mainframe Backup','mainframe_name','10.10.10.10','BACKUP','2008-03-24 10:25:00','2008-03-24 11:50:00',3713,45221,'D',0,'413824','Retail_s01002030','Incremental','/I:/Shared/', 'Daily'

'UNIX tar backup','host_xyz.anyco.com','null','BACKUP','2008-03-24 10:22:00','2008-03-24 12:50:00',1713,45221,'T',1,'5201','HQ_Finance','Full','/D:/Backups/', 'Daily'

'ArcServe','host_123.anyco.com','null','RESTORE','2008-03-24 8:22:00','2008-03-24 9:12:00',0,0,'T',0,'2300','Retail_s03442012','Incremental','/I:/Shared/', 'EOM'
```

Manually Loading the CSV File

Use the following procedure to manually load the Generic Backup CSV file into the Portal database.

Prerequisites:

- These scripts must be run on the **Collector Server**.
 - The **checkinstall** script must be run first to register the event collector ID.
1. List the Data Collectors to get the **Event Collector ID** and the **Server ID**, which will be used in step 2.

Windows:

```
C:\opt\APTARE\mbs\bin\listcollectors.bat
```

Linux:

```
/opt/aptare/mbs/bin/listcollectors.sh
```

In the output, look for the Event Collectors section associated with the *Software Home*—the location of the CSV file (the path that was specified when the Data Collector Policy was created). Find the **Event Collector ID** and **Server ID**.

```
==== Event Collectors ===
Event Collector Id: EVENT_1029161_9
Active: true
Active: true
Software Home: C:\gkgenericBackup.csv
Server Address: 102961
Domain: gkdomain
Group Id: 102961
Sub-system/Server Instance/Device Manager Id: 102961
```

Schedule: */10 * * * *

2. Use the following commands to load the data from the CSV file into the Portal database.

Windows:

```
C:\opt\APTARE\mbs\bin\loadGenericBackupData.bat <EventCollectorID> <ServerID> [verbose]
```

Linux:

```
/opt/aptare/mbs/bin/loadGenericBackupData.sh <EventCollectorID> <ServerID> [verbose]
```

Note: If you run the command with no parameters, it will display the syntax.

The load script will check to see if the backup server and client already exist; if not, they will be added to the database. The script then checks for a backup job with the exact same backup server, client, start date and finish date. If no matches are found, the job will be added; otherwise, it will be ignored. This prevents duplicate entries and allows the import of the script to be repeated, if it has not been updated. Once the load is complete, these clients and jobs will be visible via the APTARE IT Analytics Portal and the data will be available for reporting.

Backup Job Overrides

In some backup environments, it is desirable to treat backup warning status messages as successful backups. A configuration modification can change the default behavior of APTARE IT Analytics reports. You may want to override other backup statuses as well. APTARE IT Analytics supports job overrides for all supported backup products.

Use the following procedure to update the job override configuration.

Note: For the purpose of simplicity, only NetWorker and NetBackup job override steps are shown. Similar configuration changes can be done for other backup products.

Configure a Backup Job Override

1. At the command line, log in to the Portal Server as user `aptare`.
2. Make a copy of the following files. Note that in this step, only the NetWorker (leg) override is shown, however, other backup product job overrides can be customized using their relevant .plb files.

Linux:

```
/opt/aptare/database/stored_procedures/job_override.sql  
/opt/aptare/database/stored_procedures/leg/leg_adaptor_pkg.plb
```

Windows:

```
C:\opt\aptare\database\stored_procedures\job_override.sql  
C:\opt\aptare\database\stored_procedures\leg\leg_adaptor_pkg.plb
```

3. On the Portal server, shut down the Data Receiver.
 - **Linux:** `/opt/aptare/bin/tomcat-agent stop`
 - **Windows:** `C:\opt\aptare\utils\stopagent.bat`
4. Edit `job_override.sql` and find the following section.

```

CREATE OR REPLACE PACKAGE BODY job_override AS

    PROCEDURE overrideJobStatus(
        jobID           IN  apt_job.job_id%TYPE,
        productType     IN  apt_job.product_type%TYPE,
        serverID        IN  apt_job.server_id%TYPE,
        clientID        IN  apt_job.client_id%TYPE,
        vendorStatus     IN  OUT NOCOPY apt_job.vendor_status%TYPE,
        summaryStatus    IN  OUT NOCOPY apt_job.summary_status%TYPE) IS
    BEGIN
        NULL;
    END overrideJobStatus;
/*----> overrideJobStatus <----*/

END job_override ;
/*----> END PACKAGE <----*/

/
SHOW ERR

```

Replace this with the relevant lines from the following example.

5. Update the job_override.sql file with code to customize how APTARE IT Analytics will override the backup status. The following example illustrates updates for NetBackup or NetWorker, enabling a warning to be treated as a successful backup. Note that overrides are supported for all backup products.

Example of Job Overrides for NetWorker and NetBackup

```
CREATE OR REPLACE PACKAGE BODY job_override AS
  PROCEDURE overrideJobStatus(
    jobId      IN apt_job.job_id%TYPE,
    productType IN apt_job.product_type%TYPE,
    serverID    IN apt_job.server_id%TYPE,
    clientID    IN apt_job.client_id%TYPE,
    vendorStatus IN OUT NOCOPY apt_job.vendor_status%TYPE,
    summaryStatus IN OUT NOCOPY apt_job.summary_status%TYPE) IS
  BEGIN
    IF productType = constant.PRODUCT_LEGATO_NW THEN
      IF summaryStatus = constant.JOB_STATUS_WARNING THEN
        summaryStatus := constant.JOB_STATUS_OK;
        vendorStatus := constant.JOB_STATUS_OK;
      END IF;
    END IF;

    IF productType = constant.PRODUCT_VERITAS_NBU THEN
      IF summaryStatus = constant.JOB_STATUS_WARNING THEN
        summaryStatus := constant.JOB_STATUS_OK;
        vendorStatus := constant.JOB_STATUS_OK;
      END IF;
    END IF;
  END overrideJobStatus;
  /*---> overrideJobStatus <---*/
END job_override;
/*---> END PACKAGE <---*/
/
SHOW ERR
```

Note: The above example is for illustration purposes only. You may choose to customize job overrides for other backup vendor job statuses.

6. Go to:

- **Linux:** /opt/aptare/database/stored_procedures/
- **Windows:** C:\opt\aptare\database\stored_procedures\

7. Compile the SQL binary (.sql file):

```
sqlplus portal/portal @ job_override.sql
```

8. Go to:

- **Linux:** /opt/aptare/database/stored_procedures/leg/
- **Windows:** C:\opt\aptare\database\stored_procedures\leg

9. Compile the PL/SQL binary (.plb file):

```
sqlplus portal/portal @ leg_adaptor_pkg.plb
```

10. Restart the Data Receiver.

- **Linux:** /opt/aptare/bin/tomcat-agent start
- **Windows:** C:\opt\aptare\utils\startagent.bat

Managing Host Data Collection

This section covers the following topics:

- [Identifying Hosts by WWN to Avoid Duplicates](#)
- [Setting a Host's Priority](#)
- [Loading Host and WWN Relationships](#)

Identifying Hosts by WWN to Avoid Duplicates

By default, APTARE IT Analytics data collection finds hosts based on IP address or host name. Often hosts are collected from multiple sources and these sources have different names for the same host. In such environments, host name or IP address are not sufficient for uniquely identifying a host. In order to prevent duplicate hosts from being created in the database, IT Analytics can use the host's port WWN to uniquely identify a host.

A typical scenario that warrants WWN matching for unique host identification is described in the following example. Host data can be collected in multiple ways; for example, via a manual CSV load, as well as from Virtualization Manager and from Capacity Manager HP 3PAR collection. In this example, all three sources provide different names for the host, which would cause duplicates to be saved in the IT Analytics database. Therefore, in this case, matching on a host port WWN ensures unique hosts. With WWN matching, if different host names are encountered, a host alias record is also created in anticipation of future host data collection.

By default, WWN matching is turned off. A system parameter can be configured to turn on WWN matching *prior* to data collection.

To turn on host WWN matching, type the following command at the command line.

```
update ptl_system_parameter set param_value = '1'
    where param_name = 'SEARCH_HOST_BY_WWN_IS_ENABLED';
COMMIT;
```

A value of 1 turns on WWN matching and 0 turns it off (the default).

Setting a Host's Priority

APTARE IT Analytics can collect host data from multiple vendor products (subsystems), such as Veritas NetBackup and IBM XIV. When host data is collected from more than one subsystem, host reports will display the data from the *primary* subsystem. IT Analytics provides a default ranking for subsystems. When a host is collected, that rank order is referenced to determine if the collected host is coming from the primary subsystem.

An Administrator can override that default ranking and configure a different source subsystem as primary by using the following instructions to customize the ranking for your enterprise.

1. Log on to the Portal Server as user **aptare**.
2. At the command prompt, type: **sqlplus <pwd>/<pwd>**
3. Execute the following at the **SQL** prompt to view the default host ranking. In this table, the Product Types translate to: 1 = backup, 2 = capacity, 4 = virtualization, 8 = replication, 16 = fabric, 32 = file analytics.

```
SQL> SELECT * from apt_host_source_rank;
```

aptare_product_type	product_vendor	priority	product_vendor_name
		100	UI
1	1	202	Veritas NetBackup
1	4	203	Tivoli Storage Manager
1	3	204	EMC NetWorker
1	5	205	CommVault Simpana
1	6	206	HP Data Protector
1	2	207	Veritas Backup Exec
1	9	208	Generic Backup
1	7	209	EMC Avamar
4	51	301	VMware
4	52	302	IBM VIO
2	41	201	Host Resource
2	21	401	Hitachi Data Systems
2	211	402	Hitachi NAS
2	22	403	EMC
2	221	404	EMC CLARiiON
2	222	405	EMC Symmetrix
2	223	406	EMC VNX (Celerra)
2	225	407	EMC Isilon
2	231	408	NetApp Cluster-Mode
2	23	409	NetApp
2	24	410	HP
2	241	411	HP 3PAR

Table 1 Default Host Source Ranking Table

aptare_product_type	product_vendor	priority	product_vendor_name
2	25	412	IBM
2	26	413	NetApp E-Series
2	27	414	IBM SVC
2	28	415	HP EVA
2	254	416	IBM XIV
2	29	417	Dell Compellent
8	61	501	NetApp SnapMirror
8	62	502	NetApp SnapVault
16	701	601	Brocade Switch
16	703	603	Cisco Switch
32	801	700	File Analytics
1	32	701	EMC Data Domain
		800	HBA CSV Load
		801	CSV Load

Table 1 Default Host Source Ranking Table

- Execute the following to customize the host source subsystem ranking for your enterprise. This command can be repeated for as many vendor products (subsystems) as needed in your environment. It updates a custom host source ranking table, which is specific to your environment. See [Determining Host Ranking](#).

```
SQL> INSERT INTO apt_host_user_source_rank (domain_id, aptare_product_type,
product_vendor, priority, product_vendor_name) VALUES (<domain_id_value>,
<aptare_product_type_value>, <product_vendor_value>, <priority_value>,
'<product_vendor_name_value>');
```

```
SQL> Commit;
```

where:

<domain_id_value>	Most environments have only one Domain ID, however, Managed Service Providers (MSPs) will have a different Domain ID for each of their customers. To list the currently configured Domain IDs, use the following SQL SELECT statement: SQL> SELECT * from apt_domain;
<aptare_product_type_value>	The product type is a number that represents the IT Analytics product, such as Capacity Manager. 1 = backup, 2 = capacity, 4 = virtualization, 8 = replication, 16 = fabric, 32 = file analytics
<product_vendor_value>	This number represents the vendor and subsystem from which the host data is collected.

<priority_value>	This number sets the priority ranking for the host. Priority numbers used by customers should be between 1 and 99.
'<product_vendor_name_value>'	<p>This name corresponds to the vendor_number; for example, EMC Avamar. This must be entered exactly as it is listed in the Default Host Ranking Table. See Default Host Source Ranking Table.</p> <p>Note: The product vendor name is <i>not</i> mandatory when the product vendor (number) is available. In this case, a null value within single quotes can be used for the product vendor name value.</p>

Example:

```
INSERT INTO apt_host_user_source_rank (domain_id, aptare_product_type, product_vendor,
priority, product_vendor_name) VALUES (100396, 1, 1, 88, 'Veritas NetBackup');
Commit;
```

5. Execute the following to view the host ranking that you customized for your enterprise:

```
SQL> SELECT * from apt_host_user_source_rank;
```

6. To update a rank that you have customized, use the following steps. Refer to the [Default Host Source Ranking Table](#) for column names.

```
SQL> update apt_host_user_source_rank set <column_name> = <value> where <column_name> =
<Value>;
```

Example:

```
update apt_host_user_source_rank set priority = 91 where product_vendor = 1;
```

Determining Host Ranking

The user-specific host ranking table differs from the default ranking table, as it has a Domain ID column that enables Domain-specific ranking for hosts. You can override host ranking with a Null Domain ID; this becomes a system-wide override.

When determining the priority of a host, APTARE IT Analytics checks the ranking in the following order of priority:

1. User host source rank with a Domain ID populated
2. User host source rank with a Null Domain ID
3. Default host source rank, as defined in the [Default Host Source Ranking Table](#).

Loading Host and WWN Relationships

In environments with firewall restrictions, Capacity Manager Host Resources data cannot be collected. APTARE provides a utility for manually loading host and Worldwide Name (WWN) relationships into the Portal database so that this limited information can be included in the standard Capacity Manager reports.

This utility takes a comma-separated values (CSV) file as input and populates database tables so that the Host Bus Adapter (HBA) data is available in reports.

Loading the Host HBA Port Data

This utility provides an bulk-load method for populating the database with host data.

Create a CSV File

In preparation for loading host data, enter the information into a spreadsheet from which you will create a comma-separated file.

The table in the spreadsheet should be in the following format:

- **first column** - host name
- **second column** - node WWN
- **third column** - port WWN

Example of a Host WWN CSV File

```
test_host, 50:06:0E:80:05:63:B7:20, 50:06:0E:80:05:63:B7:21
```

If a host has multiple HBAs, the CSV should contain a row for every HBA so that all HBAs for the host will be loaded. For example:

```
host123, 50:06:0E:80:05:63:B7:20, 50:06:0E:80:05:63:B7:21
host123, 50:06:0E:80:05:63:B7:21, 50:06:0E:80:05:63:B7:24
host123, 50:06:0E:80:05:63:B7:25, 50:06:0E:80:05:63:B7:26
```

Execute the Script

To load host HBA port data

Note: When running this script, pay attention to the value you supply for the *isIncremental* parameter. When you specify 'N' your existing host data is deleted. When you specify 'Y' your host data is added without removing existing records.

1. Create a table in a spreadsheet, as shown in the above example. Save the table as a comma-separated file (for example, hostWWN.csv).
2. Log on to the Portal Server as user **aptare**.
3. At the command prompt, type: **sqlplus <pwd>/<pwd>**
4. Execute the following at the **SQL** prompt:

```
SQL> Execute srm_load_pkg.loadHBAPortFile('<domainName>', '<isIncremental>', '<CSVfile>',
'<logPathname>', '<logFilename>', [, '<source_name>']);
```

where:

'domainName'	APTARE IT Analytics domain name (enclosed in single straight quotes)
'isIncremental'	'Y' or 'N' (enclosed in single straight quotes) to indicate if it is an incremental load. If 'Y', an HBA port record will be created if none exists. If 'N', old HBA port records will be deleted first and then new records created. Take care when choosing this option, as it will remove existing host data from the database.
'CSVfile'	CSV file path <u>and</u> name (enclosed in single straight quotes)
'logPathname'	Log path name (enclosed in single straight quotes). The audit log file is created only if errors occur. Other status is logged in scon.log.
'logFilename'	Log file name (enclosed in single straight quotes). This audit log file is created only if errors occur. Other status is logged in scon.log.
'source_name'	source_name is an <i>optional</i> , case-insensitive string, up to 100 characters, representing the source of the host details; for example, CMDB might be relevant for a change management database. This source information is retained for historical purposes, to track how the host was added to the database. If nothing or NULL is provided for this parameter, HBA CSV Load will be inserted as the source into the reporting database.

Example:

```
Execute srm_load_pkg.loadHBAPortFile('corpHost1', 'Y', '/tmp/hba_port_data.txt',  
'/tmp', 'hba_port_data.log', 'CMDB');
```

5. **IMPORTANT:** If you created a new **source_name**, you need to insert it into the custom host source ranking table using the instructions provided in [Setting a Host's Priority](#).

System Configuration in the Portal

Configure a number of the components in your system directly from the Portal. Using the System Configuration feature available to Super Users, you can modify default values established during installation for everything from data retention period to how email is setup.

- [System Configuration: Functional Areas](#)
- [System Configuration: Functions](#)
- [System Configuration Parameter Descriptions: Additional Info](#)
- [Custom Parameters](#)

System Configuration: Functional Areas

Functional areas are divided into separate tabs as follows:

- **Data Collection** - Set values for all collection, product-based collection and vendor-based.
- **Data Retention** - Modify default retention periods for systems that are collected by traditional Data Collectors to determine when data is purged from the database. Purging is required to maintain reasonable table sizes. Data types include historical and performance data. Fields are displayed based on what has been installed and collected.

For systems collected by Data Collectors deployed via the SDK, use the procedure described in: [Data Retention Periods for SDK Database Objects](#).

- **Database Administration** - Set values to configure the structure of the database.
- **Host Discovery** - Enable rules for host matching when the system is discovering new hosts/clients.
- **Inventory** - Modify the database polling frequency for Inventory objects.
- **Portal** - Modify default values for a variety of portal properties including host attribute import parameters, maximum number of open tabs, and security settings such as time out values and allowed login attempts.
- **Custom Parameters** - Add, edit and delete custom system parameters, portal properties and their associated values. This area allows free form entry for name/value pairs.

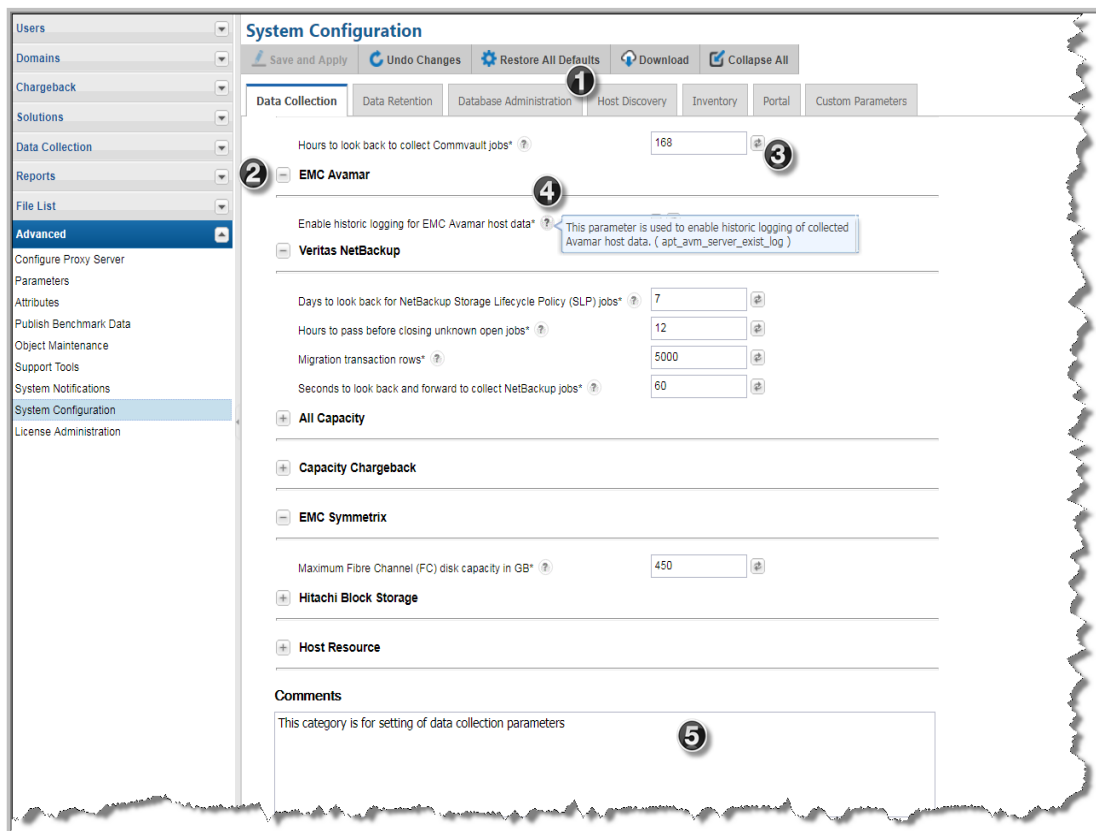
System Configuration: Functions

Buttons available at the top of the tabbed space, apply across all functional tabs.

Save and Apply	Before saving and applying changes, a dialog is displayed to show old values and new values to verify the update. Some changes require a Portal restart. If a restart is required, this is displayed in the confirmation dialog. See Starting and Stopping Portal Server Software for information about restarting systems.
Undo Changes	Cancels changes and resets to the last value across all tabs within the System Configuration area. Use the field level refresh icon to reset values field by field.
Restore All Defaults	Resets default values for all parameters across all tabs within the System Configuration area. Rollover the icons to display the parameters default value.
Download	Click to download a text file of all your system setting values. This includes any custom parameter values.
Expand/Collapse All	Click to expand or collapse all categories on within the System Configuration area. Categories can be expanded or collapsed individually using the icon beside the category title.

Navigation Overview

This self-service portal makes it easy to quickly determine what parameters you are setting. The following graphic outlines some of the built-in features.



1. Functional areas organized into tabs
2. Expand and collapse categories individually
3. Field-level restore icons reset default values per parameter. Default values are displayed in rollover text.
4. Field-level help displays short parameter descriptions for use-case clarification.
5. Free form comments are allowed to enter notes about updates.

System Configuration Parameter Descriptions: Additional Info

Some configuration settings are straight forward and do not require more explanation than is available in the Portal through the field-level help. Other settings require more information. The section covers the additional information not displayed in the Portal.

Data Collection: Capacity Chargeback

- **Drive capacity chargeback range in GB:** When configuring Capacity Chargeback Policies, a Drive Capacity (GB) policy type can be defined. This value is treated as a *range* of capacity, with the default set to: *plus or minus 10 GB*. Often this default is not sufficient for an environment's chargeback policies. Using system parameters, the range for the Drive Capacity policy type can be modified. The value configured in the policy will be treated as a range of values—that is, the *Policy's Drive Capacity plus or minus the Drive Capacity Range* that is configured in the system parameters.
- **Enable chargeback logging:** Enable or disable capacity chargeback logging. This allows data to be collected and then custom report templates developed with one of the report template designers can query this data to generate chargeback reports. Capacity chargeback logging is enabled by default. If this is not a requirement for your environment, disable it.

Database Administration: Database

- **Large index number leaf blocks:** In large environments, to improve the performance of index builds, a system parameter can be configured to define the number of leaf blocks for a large index. The default value is 10,000 leaf blocks. This parameter configures the number of leaf blocks in a database index.
- **Maximum number of large indexes for rebuild:** To improve the performance of index recreation, modify this parameter to change the number of large database indexes that will be processed in a single run. The default value is 10.
- **Rebuild indexes schedule (days):** In large environments, if report generation performance begins to degrade, database indexes can be built more frequently. The default is to rebuild indexes every 60 days.
- **Maximum time in minutes for large index rebuilds:** To improve the performance of index recreation, configure this parameter to define the number of minutes the index rebuild should run. The default value is 10 minutes. If the rebuild takes longer than this time, the job will stop. In very large environments, it may be necessary to increase this time to accommodate large indexes.

Host Discovery: EMC Avamar

In a specific circumstance, EMC Avamar data collection can persist *duplicate* clients in the Portal database. This occurs in the following case:

- Multiple enterprise domains are configured.
- The same host name is used in multiple domains, but for different hosts.

If your Portal has the above configuration, configure the following to prevent the creation of duplicate Avamar clients. And, logging can be configured to identify how a host is determined and persisted in the Portal database.

Note: Another parameter, **Enable IP address matching for Host search**, is also used by the Avamar host-matching algorithm. If your environment has already enabled this parameter, it will be honored by the host-matching algorithm.

- **Enable short name matching for Avamar Host Search:** This parameter is used to enable comparisons of a client's base name. During data collection, the data persistence logic will compare the short name retrieved by data collection and compare it to what exists in the Portal database. This parameter currently is used only while searching for a host in Avamar data. For example, the host name in the database might be `xyz.aptare.com`, but the collected host name is `xyz.apr.com`. If this parameter is enabled, the host-matching algorithm will find the host with the name, `xyz.aptare.com`, based on matching the short name, `xyz`, thereby preventing the creation of a duplicate host.
- **Remove patterns in host matching:** This parameter will enable the stripping of unwanted suffixes while searching for hosts based on host name. This parameter is currently used only while searching for a host in Avamar data.
 - **Prerequisite:** Any suffix that needs to be ignored must first be inserted into the `apt_host_name_exclد_suffix` database table, as described in the following procedure. When the parameter is enabled, the host-matching algorithm searches this table for suffixes that should be ignored.

Add suffixes to the database table:

```
INSERT INTO apt_host_name_exclد_suffix (exclد_suffix, suffix_length, priority) VALUES
(<<excludeSuffixInitials>>,<<totalSuffixLength - lengthOfexcludeSuffixInitials>>,
<<priority>>);
COMMIT;
```

Examples

The data searching logic used when this system parameter is enabled is described in the following examples.

- Host name in the database is `xyz` and the collected host name is `xyz_UCMAAZWlR6kihBHN5R8iA`. The host-matching algorithm will find the host with the name `xyz` and `_UCMAAZWlR6kihBHN5R8iA` will be removed while searching.
- Host name in the database is `xyz` and the collected host name is `xyz_UA3rT06VdULrQyViIxEFuQ2011.07.22.16.05.49`. The host-matching algorithm will find the host with the name `xyz` and `_UA3rT06VdULrQyViIxEFuQ2011.07.22.16.05.49` will be removed while searching. The time portion, `2011.07.22.16.05.49`, is automatically removed if the parameter is enabled.
- Host name in the database is `xyz` and the collected host name is `xyz2011.07.22.16.05.49`. The host-matching algorithm will find the host with the name `xyz` and `2011.07.22.16.05.49` will be removed while searching. The time portion, `2011.07.22.16.05.49`, is automatically removed if the parameter is enabled.
- Host name in database is `xyz` and the collected host name is `xyz2011.07.22.16.05.49_UA3rT06VdULrQyViIxEFuQ`. The host-matching algorithm will find the host with the name `xyz` and `2011.07.22.16.05.49_UA3rT06VdULrQyViIxEFuQ` will be removed while searching. The time portion, `2011.07.22.16.05.49`, is automatically removed if the parameter is enabled.

Host Discovery: Host

- **Enable IP address matching for Host search:** In certain environments, where hosts or VMs are frequently provisioned and/or decommissioned causing IP addresses to be re-used, these duplicate IP addresses can result in multiple aliases for a single host. Use this parameter to activate/deactivate IP address matching. By default, this value is active. When the parameter is disabled, a collected host with an IP address that matches a host in the database, but that has a different host name, will result in the creation of a new host in the database.

Custom Parameters

Customizations to the Portal extend beyond what is available in the System Configuration. When working with Services and APTARE Global Support Services, you may be required to add or edit custom parameters to address a particular issue. The **Custom Parameters** tab enables free-form key value pairs to further customize APTARE IT Analytics.

Note: Prior to version 10.3, customizations to the Portal were made using a file, portal.properties. Not all of those settings are displayed in the **System Configuration** feature. If you upgrade from a version prior to 10.3, those properties are displayed and automatically populated in the **Custom Parameters**.

Adding/editing a custom parameter

1. Navigate to **Admin>Advanced>System Configuration>Custom Parameters**.
2. Select a custom parameter if editing.
3. Click **Add/Edit**. The **Add Custom Parameters** dialog is displayed.
4. Enter the **Custom Parameter Name** and **Custom Parameter Value**.
5. Click **Save**. The parameter is added to the list and available for you to revise in future sessions.

Portal Customizations

This section covers customizations for the portal that are not available through the user interface. Use Custom Parameters to add/edit and delete these properties.

- [Configuring Global Default Inventory Object Selection](#)
- [Restricting User IDs to Single Sessions](#)
- [Customizing Date Format in the Report Scope Selector](#)
- [Customizing the Maximum Number of Lines for Exported Reports](#)
- [Customizing the Total Label Display in Tabular Reports](#)
- [Customizing the Host Management Page Size](#)
- [Customizing the Path and Directory for File Analytics Database](#)
- [Configuring Badge Expiration](#)
- [Configuring the Maximum Cache Size in Memory](#)
- [Configuring the Cache Time for Reports](#)

Configuring Global Default Inventory Object Selection

To globally configure the selection of default Inventory objects for users, modify the `portal.properties` files. This is useful for filtering environments with large volumes of data that may be impacted by browser limitations. For new users who have never logged into the portal, the objects defined with this setting are shown selected when they log in. For existing users, this property can be used to reset a users environment when large volumes of data can present issues with certain browsers.

- Use the following:

```
portal.ocn.defaultVisibleObjectType=HOST,ARRAY,SWITCH,BACKUPSERVER,VM_SERVER,VM_GUEST,
DEDUPLICATION_APPLIANCE,DATASTORE,EC2_INSTANCE,S3_BUCKET,AZURE_STORAGE_ACCOUNT,
AZURE_VIRTUAL_MACHINE
```

Restricting User IDs to Single Sessions

To restrict a user ID from signing on multiple times using different browsers on the same machine or the same browser on different machines, modify the `portal.properties` file. The last browser session with the user ID to login will have access to the portal. Other browser sessions with same user ID will be logged out.

- Use the following:

```
portal.security.allowUserToLoginMultipleTimes=false
```

Customizing Date Format in the Report Scope Selector

To customize the date format displayed in the report scope selector for all Portal users, you can modify the `portal.properties` file. For example, you can set the date to display: `dd/MM/yyyy` or `MM/dd/yyyy`

- Use the following:

```
#Formatters that define specific presentations of numbers and dates
formatter.decimalPlaces=2
fileSize.base2=true
formatter.number=###,###,##0
formatter.date=MMM dd, yyyy hh:mm:ssa
formatter.dateZone=MMM dd, yyyy hh:mm:ssa z
formatter.yearMonth=MMM dd
formatter.groupByDate=MMM dd
formatter.designerDate=MM/dd/yyyy
formatter.currency=$ ###,###,##0.00
```

Customizing the Maximum Number of Lines for Exported Reports

When you export or email a large report, IT Analytics limits the maximum number of lines to 20,000. The report truncates when that value is exceeded. The report can still be exported or emailed, but will contain a message that the report has been truncated.

- Use the following:

```
portal.report.maxRowsExported=<enter new limit value here>
```

Where the <new limit value> is the number of rows greater than 20,000 that your report export requires. For example, if your report has 36,000 rows enter a number greater than 36000. Note that the new limit value cannot contain commas or decimal points. Keep in mind that Portal server performance can degrade considerably for very large reports. For very large reports, you may want to segment the scope into multiple reports.

Customizing the Total Label Display in Tabular Reports

To customize the minimum number of records needed to display the **Total** label in a report, you can modify the portal.properties file. The default value is 10.

- Use the following:

```
portal.rowCountDisplayMinimum = <enter numeric value>
```

Customizing the Host Management Page Size

In the Portal, the Host Management page (**Admin > Advanced > Host Management**) displays 200 rows by default. You can change the default value by modifying the portal.properties file. System performance will be impacted if you increase the number of rows past the 200 value.

- Use the following:

```
portal.hostManagementPageSize=xxxx
```

Customizing the Path and Directory for File Analytics Database

You can customize the location of the File Analytics database. The default paths are:

- **Linux:** /opt/aptare/fa
- **Windows:** C:\opt\aptare\fa

Use the following to revise the path:

```
fa.root=/opt/aptare/fa
```

For example:

Linux:

```
fa.root=/opt/aptare/fa_db
```

Windows:

```
fa.root= D:\opt\aptare\fa
```

Configuring Badge Expiration

Configure the expiration of **NEW** badges in the **Home** section of the **Reports** tab. By default, **NEW** badges will no longer display after 14 days.

- Use the following:

```
cloudTemplateNewBadgeExpireInDays = 14
```

Configuring the Maximum Cache Size in Memory

The cache can retain up to 0.5 GB of reporting data and if it reaches capacity, it frees up space for new reports by purging the data for the least frequently used reports.

- Use the following:

```
portal.reports.cache.maxSizeInMemory
```

The unit of measure for the cache `maxSizeInMemory` value is *bytes*.

Example: `portal.reports.cache.maxSizeInMemory=536870912`

Configuring the Cache Time for Reports

The cache retains reporting data and if it reaches capacity, it frees up space for new reports by purging the data for the least frequently used reports. Purging also occurs when a cached report is more than 24 hours old.

6. Use the following:

```
portal.reports.cache.timeOut
```

The unit of measure for the cache `timeOut` value is *seconds*.

Example: `portal.reports.cache.timeOut=86400`

Performance Profile Schedule Customization

Array Performance Profiling enables you to monitor performance over time and to compare your enterprise-specific performance with the performance found in a broader community. You can customize the time of day when your environment's profiling job will run.

Customize the Performance Profile Schedule

To customize the time period for profiling the collected performance data, take the following steps.

1. On the Portal server, go to the database procedures directory.

Windows: C:\opt\oracle\database\stored_procedures\srm

Linux: /opt/aptare/database/stored_procedures/srm

2. Edit the script: **setup_srm_jobs.plb**.
3. Note the parameters shown in red and modify them accordingly.

```

jobNo :=
dba_package.getDatabaseJobID('srm_array_perf_report_pkg.recalIntPerformanceProfile');
  IF (jobNo IS NOT NULL AND jobNo != 0) THEN
      DBMS_OUTPUT.put_line('srm_array_perf_report_pkg.recalIntPerformanceProfile
exists and will first be removed before adding a new version');
      DBMS_JOB.REMOVE(jobNo);
  END IF;

  DBMS_JOB.SUBMIT(
      job          => jobNo,
      what         =>
'srm_array_perf_report_pkg.recalIntPerformanceProfile(dateRangeType(null,null,null,SY
SDATE-2/24, SYSDATE, null, 0));',
      next_date    => SYSDATE + (3/24),
      interval     => 'TRUNC(SYSDATE+1, 'DD') + (10/24)';
      DBMS_OUTPUT.put_line('srm_array_perf_report_pkg.recalIntPerformanceProfile set to
run on daily at 10am');

  COMMIT;

```

- Three hours after a Portal Installation or Upgrade, this job runs for the first time. See the parameter: (SYSDATE + (3/24))
- After the first run, this job will run at 10:00 a.m. every day. See the parameter: (TRUNC(SYSDATE+1, "DD") + (10/24))

- This Performance Profiler will calculate the last two hours of statistics. See the parameter: SYSDATE-2/24

4. Execute the following command to activate your new schedule:

```
su - aptare  
sqlplus portal/portal @setup_srm_jobs.plb
```


13

Configuring LDAP

This section covers the following topics:

- [About User Authentication](#)
- [Switching from OpenLDAP to Another LDAP Service](#)
- [User Administration Using an External Authentication Service](#)
- [Creating Portal Super Users](#)
- [Active Directory Tools](#)
- [Common Active Directory Authentication Errors](#)

About User Authentication

APTARE IT Analytics supports the following user authentication methods:

- **Local LDAP.** APTARE IT Analytics bundles OpenLDAP to manage user login authentication. For information about OpenLDAP, go to <http://www.openldap.org/>.
- **Enterprise LDAP.** Refers to any standard LDAP service, including Active Directory. For information about Active Directory, go to [Microsoft's Active Directory](#) web site.

By default, APTARE IT Analytics uses OpenLDAP to manage user login authentication.

- If your company uses a different LDAP service, such as Active Directory, configure APTARE IT Analytics to use that solution.
- If your company does not have an LDAP service, use OpenLDAP.

Switching from OpenLDAP to Another LDAP Service

By default, APTARE IT Analytics uses OpenLDAP to manage user login authentication. If your company uses a different LDAP service, such as Active Directory, you have the option to configure APTARE IT Analytics to use that solution, though if you're not intimately familiar with Active Directory, you'll find that you'll save lots of time if you use OpenLDAP. See also, [About User Authentication](#) and [User Administration Using an External Authentication Service](#).

Note: Only a single LDAP search base is supported.

To use your enterprise LDAP

1. Update the default Administrator login.

The Portal Installation Wizard created a user account in the form **admin@yourdomain.com** in the Reporting Database. You must update this user record in the Reporting Database to match an existing user account in your Enterprise Authentication directory. Otherwise, you will not be able to log in to the Portal.

2. Determine and record the login attribute and login attribute value of your Enterprise LDAP directory, which is used for authentication to your company's other enterprise systems.

This attribute might be employee ID or user name. In [Step 8](#) you will update the `loginAttribute` in the Portal LDAP configuration with this value.

3. Do one of the following:

- In a Linux environment, log in to the Oracle database server as user `aptare`. If you already are logged in as root, use: **`su - aptare`**
- In a Windows environment, log in to the Oracle database server as a user who is a member of the `ORA_DBA` group.

4. Identify your system's admin account `user_id` and corresponding `ldap_id` using:

```
select ldap_id, user_id from ptl_user where user_id=100000
```

5. On the Oracle database server, update the existing record where, *for example*, the login attribute is `user_name` and the actual value is `Admin`.

```
sqlplus portal/portal password
UPDATE ptl_user SET ldap_id = 'Admin'
WHERE user_id = 100000;
commit;
```

This is the user name that you would use to log in to the external directory. Do *not* use the name, `aptare`. The user account, `aptare` (`user_id=100`), is an internal bootstrap user required to maintain referential integrity among database tables and therefore the name should *not* be changed or used for external LDAP integration.

Note: `user_id = 100000` is always the default `user_id` for the super user account.

6. Back up the `/opt/aptare/portalconf/portal.properties` file, which contains the Portal's OpenLDAP configuration settings. You need to change these settings in [Step 8](#).

7. If you require SSL support, run the following command to generate the keystore file:

```
/usr/java/bin/keytool -import -file certificate_file -alias alias_name -keystore
keystore_file
```

Note that for Windows Portals, the `keytool` executable is located in: `C:\opt\jre\bin`

`certificate_file` is the path and file name for the X.500 CA certificate.

`alias_name` explicitly assign an alias to the certificate (choose a unique name) to ensure that there are no conflicts with existing aliases. This is an essential parameter when importing multiple certificates.

`keystore_file` is the target path and filename for the keystore file being generated.

Example of Keystore Generation

```
/usr/java/bin/keytool -import -file HQLDAP.crt -alias HQCertAlias -keystore /opt/aptare/
portalconf/portal.keystore
```

8. On the Portal Server, change the following configuration settings in the `/opt/aptare/portalconf/portal.properties` file.

By default the `/opt/aptare/portalconf/portal.properties` file, contains the following entries:

```
#LDAP
ldap.external=false
ldap.context=com.sun.jndi.ldap.LdapCtxFactory
ldap.searchBase=dc=localhost
ldap.url=ldap://localhost:389
```

```

ldap.dn=cn=Manager, dc=localhost
ldap.password=
ldap.password.encrypted=t2Hrjn38M+ubi5tklqTd3Q==
ldap.loginAttribute=uid
ldap.keystore=c:\\opt\\aptare\\portalconf\\portal.keystore

```

Note: If you set `ldap.external` to `true`, either comment out the `ldap.keystore` parameter or set it to a valid keystore.

ldap_url	<ul style="list-style-type: none"> Set to the host and port of your external authentication service. Note that this url value has a prefix of: <code>ldap:</code> If using SSL, change the prefix to <code>ldaps</code> If you are using Active Directory for your external LDAP configuration, you may want to use the global catalog port of 3268 instead of port 389. If using SSL, you may to use the secure global catalog port of 3269 or 636 for standard <code>ldaps</code>. For information on the global catalog, see http://technet.microsoft.com/en-us/library/cc978012.aspx.
ldap.dn ldap.password ldap.password.encrypted	<p>Set to the id and password of a user who has permission to search the <code>SEARCHBASE</code>. This user must be able to search all LDAP directory servers.</p> <p>APTARE IT Analytics requires a user that has privileges to search under the Base DN (Distinguished Name) within the Active Directory structure. This needs to be an account that has administrative privileges, typically Administrator. It can be the Administrator account that was created when Active Directory was installed or it can be an account that was created and either was given administrative privileges, or was placed into a group with administrative privileges.</p> <p>If you use Active Directory, specify this setting because Active Directory services do not allow anonymous binds. Microsoft Active Directory requires the username and password of a user that has sufficient privileges to search the LDAP directory.</p>
ldap.searchBase	<p>Location from which the search will be performed to locate users in the authentication directory.</p> <p>Often referred to as the Active Directory (AD) Search Base, this is the starting point in the Active Directory tree for searching for LDAP users. This search base, in LDAP distinguished name format, contains a fully qualified domain name. APTARE IT Analytics supports only one Search Base.</p> <p>The distinguished name is derived from a company's DNS domain. This naming structure has the following format:</p> <p>cn specifies the Common Name or Relative Distinguished Name. This is the User's given name plus surname, for example, a User would be specified as: <code>cn=Ellen Doe</code></p> <p>dc specifies the Domain Controller or Domain Component</p> <p>So, for example, <code>aptare.com</code> would have the following DN format: <code>dc=aptare, dc=com</code></p> <p>Note that a Common Name (<code>cn</code>) is not required for the Base DN.</p>

Table 1 Definitions of Portal LDAP Configuration Settings

ldap.external	Set to TRUE because you want to use an external Enterprise LDAP, not OpenLDAP. If you set <code>ldap.external</code> to true, either comment out the <code>ldap.keystore</code> parameter or set it to a valid keystore.
ldap.loginAttribute	The login attribute used for login authentication. This is the column in Active Directory that specifies the user name. The default value, <code>uid</code> , seldom needs to be customized.
ldap.keystore	Keystore file location, if the external authentication service uses SSL. The APTARE-provided default seldom needs to be customized.

Table 1 Definitions of Portal LDAP Configuration Settings

9. Do one of the following to restart the APTARE Portal Tomcat service:

- In a Linux environment, run the following command:

```
# /opt/aptare/bin/tomcat-portal restart
```

- In a Windows environment, using the Windows Services Console, locate and restart the APTARE Portal Tomcat service.

10. Log in to Portal using the Admin user account that you set up in [Step 1](#), then add new user accounts to the Portal.

User Administration Using an External Authentication Service

Using the Portal, you can add users and update passwords. However, when using an external authentication service, the user must already exist in the external directory before you can add a record for this user via the Portal. Note also that you will not be able to change a user's password via the Portal.

Creating Portal Super Users

A super user (**admin@yourdomain.com**) was automatically created during your initial installation. To learn about the privileges of a super user, see [About User Privileges](#).

For security purposes, you cannot add additional super users through the Portal. To add a new super user requires that you log on to the Oracle database server.

To create a super user account:

1. Create a new user, or identify an existing user that requires super user privileges and record the user ID. To create a new user, see [Creating Portal User Accounts](#).

2. On the Oracle database server (typically, the Portal server), log on as user `aptare`.

3. Start `sqlplus`, then log on to the database using the following command:

```
# sqlplus portal/portalPassword
UPDATE ptl_user
SET user_type=3
WHERE email_address='emailaddress@companyname.com';
```

4. Save your changes.

Active Directory Tools

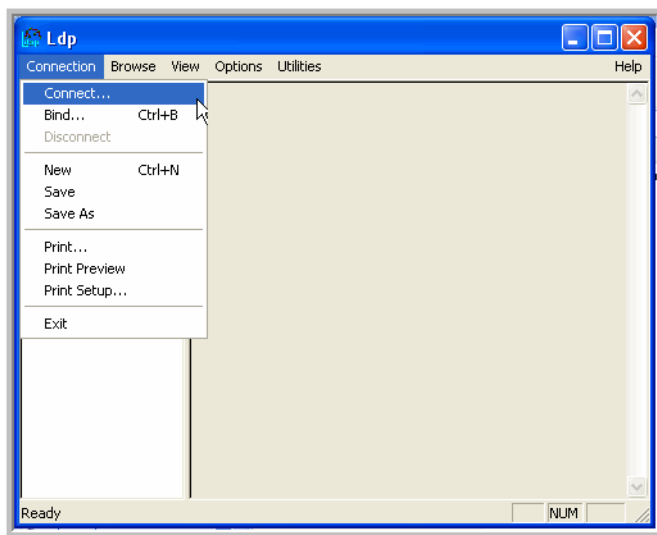
Several tools are available for identifying the Active Directory details. If these tools are not present on the Active Directory server, download them from the Microsoft web site and use the following links to access the documentation.

- Microsoft's LDP (ldp.exe): <http://support.microsoft.com/kb/224543>
- Microsoft's Active Directory Interface Editor (adsiedit.msc): [http://technet.microsoft.com/en-us/library/cc773354\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc773354(Ws.10).aspx)

Using LDP to Find the Base DN

Use the following procedure to search the Active Directory hierarchy.

1. Execute **ldp.exe** to log in to the Active Directory server.
2. Choose **Connection -> Connect** and enter the Server and Port number.



3. Choose **Connection -> Bind** and enter the Administrator for the User ID and then the password to authenticate the user access.
4. Choose **View -> Tree** to browse the Active Directory tree.
5. The Tree View window expects a **BaseDN** entry. The Tree View displays a tree hierarchy with the settings of the users under the Base DN. Most environments have Exchange Objects located in:

CN=Services, CN=Configuration, DC=<yourdomain>, DC=com

Alternatively, try one of the following:

- DC=<yourdomain>, DC=com
- DC=<yourdomain>, DC=local
- CN=Users, DC=<yourdomain>, DC=com

Example

If your domain is **support.aptare.com**, your Base DN would be:

DC=support, DC=aptare, DC=com

Using LDP to Search Active Directory

To confirm the Base DN, use the LDP Search option.

1. In LDP, choose **Browse -> Search**.
2. Use the **Sub-tree Scope** for all searches.
3. Leave the BASE DN entry untouched and enter the following **Filter**:

```
(&(objectClass=msExchExchangeServer)(cn=<serverShortName>))
```

where <serverShortName> is the name before the dot (.) of a fully qualified domain name
The filtered attributes of interest are: legacyExchangeDN and serialNumber
4. If the filter in the previous step does not result in what you need, try the following **Filter**:

```
(&(objectClass=msExchExchangeServer)(cn=<serverName>))
```

where <serverName> is the fully qualified domain name of the server
5. A Group search will display the DN.

```
(objectClass=msExchStorageGroup)
```
6. A Stores search will display the DN.

```
(objectClass=msExchMDB)
```

Common Active Directory Authentication Errors

When troubleshooting external Active Directory integration, these error code descriptions can be useful for isolating issues.

Error	Description
525	User not found
52e	User credentials not valid
530	User is not allowed to log in at this time
531	User is not allowed to log in at this workstation
532	Password has expired
533	User account has been disabled
701	User account has expired
773	User must reset his/her password
775	User account has been locked

Changing Oracle Database User Passwords

These instructions are for modifying the Oracle database user passwords for access to the APTARE IT Analytics database. **You can modify the user passwords, but do not modify the user names without the assistance of Professional Services.**

This section covers:

- [Database Connection Properties](#)
- [Modifying the Oracle Database User Passwords](#)
- [Configuring Oracle Passwords in APTARE Configuration Files](#)

Database Connection Properties

The following table summarizes the portal.properties values for the Oracle users and passwords that are used by the portal.

Portal Property	Description
db.driver	This value is customized by the Portal installer and should <i>not</i> be modified.
db.url	This is the address where the IT Analytics database resides. Depends on what was entered during the installation. This may need to be modified when there is a host name change.
db.user	Use this property to change the DB User ID for logging in to access the database. The default value is portal .
db.password db.password.encrypted=	Enter a password to be used with the DB user. The default value is portal . The password initially is stored in clear text, but after the restart of the Tomcat Portal services, the password is saved in the encrypted format and the clear text password is removed from portal.properties.
db.connection.max	Use this property to specify the maximum database connections allowed. The default value is 25 .
db.connection.min	Use this property to specify the minimum number of database connections that the Portal can have. The default value is 25 .
db.connection.expiration	When a Portal report initiates a long-running database query, this value (in minutes) establishes when the report will time out if the query takes too long to complete. The default value is 5 .

Portal Property	Description
db.ro_user_password db.ro_user_password.encrypted=	Enter a password to be used with the DB read-only user. The default value is aptaresoftware123 . The password initially is stored in clear text, but after the restart of the Tomcat Portal services, the password is saved in the encrypted format and the clear text password is removed from portal.properties.
db.ro_user_password db.ro_user_password.encrypted=	The Oracle database read-only user password for the APTARE IT Analytics database tables. The preset value is aptaresoftware123.
db.sysdba_user	The Oracle database System DBA for the APTARE IT Analytics database tables. The preset value is system.

Modifying the Oracle Database User Passwords

Complete these steps to modify passwords for the Oracle database user. These instructions apply to users **portal**, **aptare_ro** and **sysdba**. Replace user_name with the relevant user.

1. Log in with root access.
2. Stop the portal and data receiver Tomcat services.
3. Change the user password.

At the command line, execute the following commands:

```
su - aptare
sqlplus / as sysdba
SQL> alter user <user_name> identified by <new_password>;
SQL> commit;
WHERE:
      user_name = portal, aptare_ro or system
      new_password = new password
```

For example:

```
SQL> alter user portal identified by newportalpass;
```

4. Follow the instructions in [Configuring Oracle Passwords in APTARE Configuration Files](#) to update the portal configuration files with the new passwords.

Configuring Oracle Passwords in APTARE Configuration Files

Once you've made the change in Oracle, [Modifying the Oracle Database User Passwords](#), changes must be made in two files: datrarcvrproperties.xml and portal.properties.

In the portal.properties file

1. Revise the credentials using the portal.properties file:

Linux:

```
/opt/aptare/portalconf/portal.properties
```

Windows:

```
C:\opt\aptare\portalconf\portal.properties
```

2. Modify the following lines (for the Database User ID):

```
db.user=portal(preset value)
db.password=portal
db.password.encrypted=
```

Modify the following lines (for the System DBA):

```
db.sysdba_user=system (preset value)
db.sysdba_password=
db.sysdba_password.encrypted=
```

Note: For encryption, the system completes the part after the “=” sign and removes the clear text password entry once Tomcat portal services are restarted.

In the datarcvrproperties.xml

3. Revise the credentials using the datarcvrproperties.xml file:

Linux:

```
/opt/aptare/datarcvrconf/datarcvrproperties.xml
```

Windows:

```
C:\opt\aptare\datarcvrconf\datarcvrproperties.xml
```

4. Add the following lines (for the Database User ID):

```
db.user=portal(preset value)
db.password=portal
db.password.encrypted=
```

Add the following lines (for the System DBA):

```
<sysdba_user>system</sysdba_user>
<sysdba_password>new_password</sysdba_password>
<oracle_service_name>SCDB</oracle_service_name>
```

5. Restart the portal and data receiver Tomcat services.

Note: When the Tomcat service is restarted, credentials will be replaced with the encrypted string, so it's important to make note of the original values.

For example:

```
<db.user>Tij0nQG/IWdtAjwPmFX8xw==</db.user>
<db.password>hs47wbzenhnzTgI0JP62kw==</db.password>
and
```

For example:

```
<sysdba_user>Tij0nQG/IWdtAjwPmFX8xw==</sysdba_user>
<sysdba_password>hs47wbzenhnzTgI0JP62kw==</sysdba_password>
<oracle_service_name>SCDB</oracle_service_name>
```

15

Tuning APTARE IT Analytics

This section covers the following topics:

- [Before You Begin Tuning](#)
- [Tuning the Portal Database](#)
- [Performance Recommendations](#)
- [Reclaiming Free Space from Oracle](#)

Before You Begin Tuning

You should rarely need to tune any factory-default settings. If you determine that degraded system performance warrants an examination of certain configurations such as memory, take the following steps.

Note: If you encounter any issues following these directions contact APTARE Global Support Services for further guidance.

1. Before modifying your configuration, **make a copy of all files you plan to edit.**
2. Consider tuning to be a *process*—that is, increase/decrease a number slightly, then monitor system performance. If your modification results in improvement, you may consider additional adjustments later.
3. Whenever you undertake this tuning process, consider the potential negative impact of settings that are either too high or too low, within the resource constraints of your environment.

Tuning the Portal Database

Note: Only 64-bit Operating Systems are supported for the Oracle Database.

Database Cache and Shared Pool Size Recommendation:

- Comment out the following lines in **initscdb.ora**:

- `#db_cache_size = 400M`
- `#shared_pool_size = 256M`

Windows: C:\opt\oracle\database\initscdb.ora

Linux: /opt/aptare/oracle/dbs/initscdb.ora

Memory Recommendation: If your database server has sufficient memory, you may consider making the changes listed below.

- Increase the values for the following fields in **initscdb.ora**:
 - `pga_aggregate_target` from 1000 MB to 1500 MB
 - `sga_target` from 1228 MB to 2048 MB

Windows: C:\opt\oracle\database\initscdb.ora

Linux: /opt/aptare/oracle/dbs/initscdb.ora

Number of Connections Recommendation: On a Windows server, the number of Oracle connections is specified in the script: setupservices.bat. To modify the number of connections, take the steps listed below.

1. Edit/view the script that sets up the number of connections:

```
C:\opt\aptare\utils\setupservices.bat
```

2. Note that in this file, the following commands specify the number of connections:

```
C:\opt\oracle\bin\oradim -new -sid scdb -maxusers 60 -startmode auto -pfile
```

```
C:\opt\oracle\database\initscdb.ora
```

To change the number of Oracle connections, you must remove the service and then re-add it.

3. To remove the service:

```
C:\opt\oracle\bin\oradim -delete -sid scdb
```

4. To re-add the service, execute the following command, substituting the new connection values:

```
C:\opt\oracle\bin\oradim -new -sid scdb -maxusers 60 -startmode auto -pfile
```

Performance Recommendations

To optimize database performance:

- Use your fastest disk storage for the portal database. When choosing the device for your Oracle database and if you have a choice between RAID1 - RAID5, choose RAID1.
- Minimize I/O wait time. Use the **top** command to determine the I/O wait time.

Reclaiming Free Space from Oracle

You may occasionally need to reclaim space from Oracle before additional storage can be provisioned. You can run the following script at any time to reclaim space. It examines every Oracle database file (DBF) for “white space” at the end of the file. If the script discovers more than 256 MB of white space, it re-sizes the DBF file to remove the trailing space. This white space is a result of many insertions and deletions; in addition, white space can occur if you have truncated tables or purged a lot of data.

1. Log in to the database server as **aptare**.

2. Go to the tools directory:

- **Linux:** cd /opt/aptare/database/tools
 - **Windows:** cd C:\opt\oracle\database\tools
- ```
sqlplus / as sysdba
@ reclaim_aptare_tablespace
commit;
exit
```

# 16

## Defining Report Metrics

This section covers the following topics:

- [Changing Backup Success Percentage](#)
- [Changing Job Status](#)

### Changing Backup Success Percentage

---

By default the Backup Status Report defines the `Success Percentage` metric as 85%. Although this percentage is typical, your SLA might require a different percentage. You can change this percentage for specific host groups or for all host groups.

To change the success percentage metric:

1. Determine the host group's ID. See [Finding a Host Group ID](#).
2. Log on to the Portal Server as user `aptare`.
3. Type the following command:

```
sqlplus portal/portal_password
```

4. Insert a row into the `ptl_sla_group_policy` table. The following example assumes that you want to change the success percentage to 95% for all host groups.

```
INSERT INTO ptl_sla_group_policy (group_id,
successful_backups_objective,
successful_restores_objective)
VALUES (300000, 95.0, 95.0);
commit;
```

# Changing Job Status

---

By default, the Job Summary Report defines the job status as follows:

| Metric                 | Default Value             |
|------------------------|---------------------------|
| LONG_JOB_HOURS_DEFAULT | 12 hours                  |
| SLOW_JOB_DEFAULT       | <200 kilobytes per second |
| STALLED_JOB_DEFAULT    | 1800 seconds (30 minutes) |

Table 1 Job Summary Metrics

Although these values are typical, your SLA might require a different values. You can change these metrics for specific host groups or for all host groups.

To change the job status:

1. Determine the host group’s ID. See [Finding a Host Group ID](#).
2. Log on to the Portal Server as user `aptare`.
3. Type the following command:

`sqlplus portal/portal_password`

4. Insert a row into the `ptl_sla_group_policy` table. The following example assumes that you want to change the metric to 1MB per second for all host groups.

```
INSERT INTO ptl_group_policy (group_id, policy_name,
display_name, numeric_value)
VALUES (300000,'SLOW_JOB_KB_PER_SEC', 'Slow
Running Job', 1000);
commit;
```

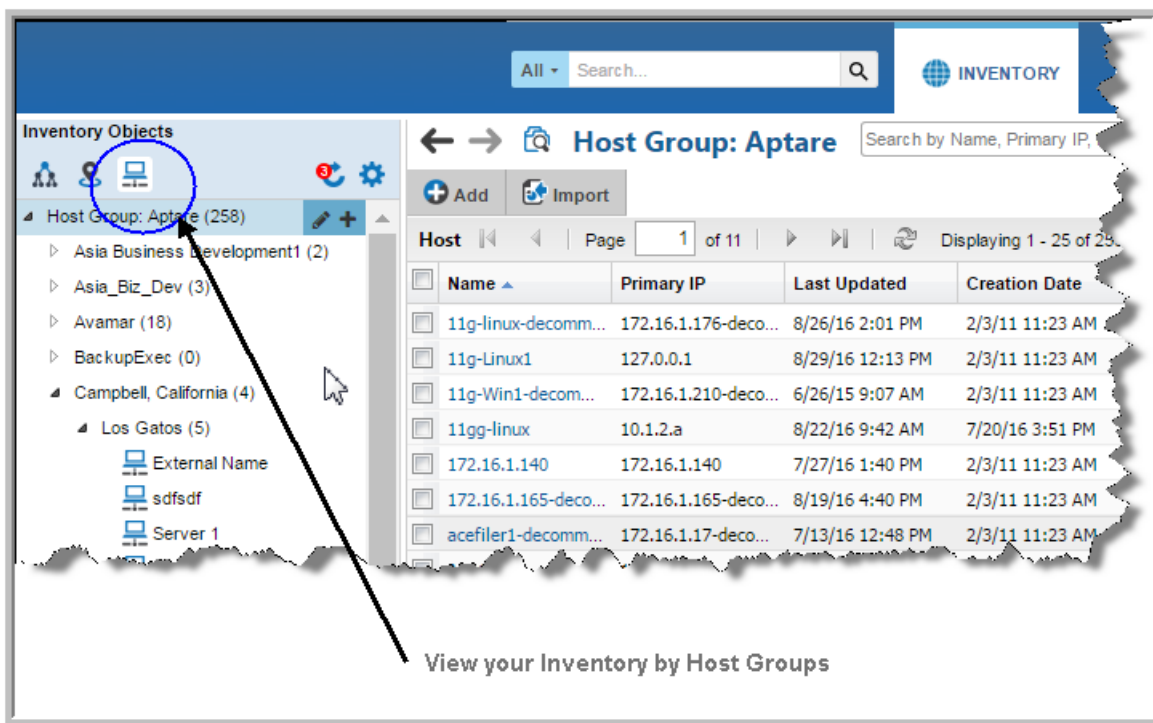
## Finding a Host Group ID

---

To identify the unique identifier associated with a host group, take the following steps in the Portal.

1. Navigate to the **Inventory**.

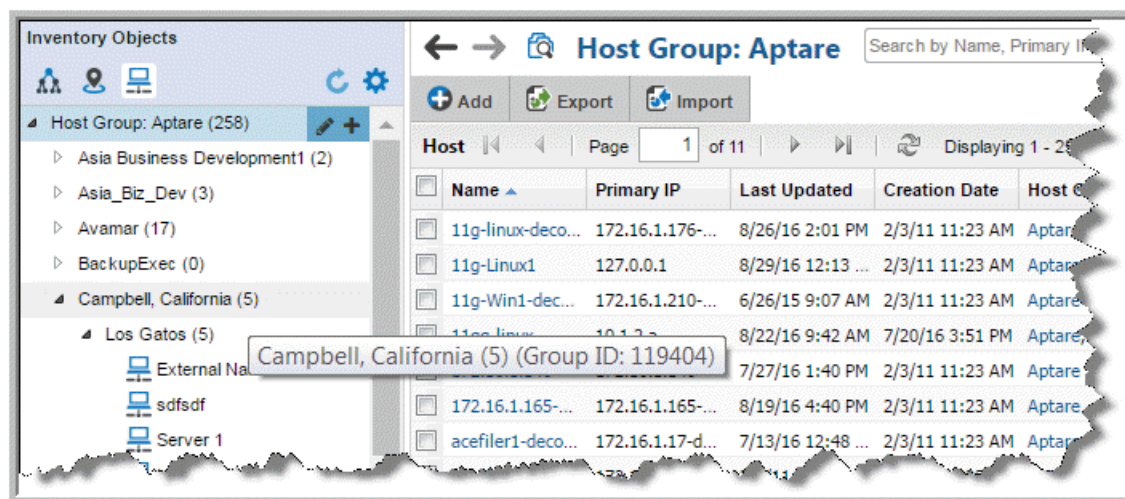
- Click the **Host Groups** icon to switch the Inventory view.



- Verify the Host Group column is displayed on the grid, and optionally, use Advanced Filtering to locate the Host Group.

**Note:** The **Host Group** column, displayed in the Inventory for the Host Group management view, has sorting disabled to improve portal performance.

- Hover your mouse over the Host Group folder in which your hosts reside. The Group ID will display in a tooltip.



# 17

## Working with Log Files

This section covers the following topics:

- [About Debugging APTARE IT Analytics](#)
- [Turn on Debugging](#)
- [Database Logging](#)
- [Portal and Data Collector Log Files - Reduce Logging](#)
- [Database SCON Logging - Reduce Logging](#)
- [Refreshing the Database SCON Log](#)
- [Logging User Activity in audit.log](#)
- [Data Collector Log Files](#)
- [Portal Log Files](#)
- [Database Log Files](#)
- [Installation/Upgrade Log Files](#)

### About Debugging APTARE IT Analytics

---

APTARE IT Analytics logs exceptions. Often these exceptions do not indicate a problem with APTARE IT Analytics. However, if you experience system problems, APTARE Global Support Services wants to help you troubleshoot your problem and interpret information in the log files. To speed up troubleshooting, provide the APTARE Global Support Services with the appropriate log files. These log files are often specific to your operating system.

Log files are managed by a logging subsystem, which manages log file size and rolls and deletes old files. Log files are used only for audit trail or troubleshooting purposes and can be safely deleted.

**Note:** When the portal/receiver or collector is upgraded, the logging configuration will be reset to the default values.

### Turn on Debugging

---

When you turn on debugging, additional entries are logged to provide troubleshooting details.

1. In the Portal, within a report window, enter the following key combination:

Ctrl+Alt+D

This turns on debugging for the current report and it logs messages to both of the following log files:

**Linux:** /tmp/scon.log and /opt/tomcat/logs/portal.log

**Windows:** C:\tmp\scon.log and C:\opt\tomcat\logs\portal.log



2. See also [Portal Log Files](#) and [Database Log Files](#).

## Database Logging

---

The `/tmp/scon.log` file (on Linux systems) or `C:\opt\oracle\logs\scon.log` (on Windows systems) contains a database audit trail and troubleshooting messages. You can control database logging by editing the following file, which contains instructions on what to modify in the file.

**Linux:** `/opt/aptare/database/stored_procedures/config.sql`

**Windows:** `C:\opt\oracle\database\stored_procedures\config.sql`

## Portal and Data Collector Log Files - Reduce Logging

---

To manage the maximum file size and threshold parameter, edit the file:

**Linux:** /opt/aptare/mbs/conf/systemlogger.xml

**Windows:** C:\opt\aptare\mbs\conf\systemlogger.xml

```
<param name="MaxFileSize" value="10MB" />
<param name="MaxBackupIndex" value="10" />
<!--The Threshold param can either be debug/info/warn/error/fatal.-->
<param name="Threshold" value="debug"/>
```

### Portal Log Files

For **Portal Tomcat**, edit this file:

**Linux:** /opt/aptare/portalconf/systemlogger.xml

**Windows:** C:\opt\aptare\portalconf\systemlogger.xml

```
<param name="MaxFileSize" value="10MB" />
<param name="MaxBackupIndex" value="10" />
```

For the **Data Receiver Tomcat**, edit this file:

**Linux:** /opt/aptare/dataarcvrconf/systemlogger.xml

**Windows:** C:\opt\aptare\dataarcvrconf\systemlogger.xml

```
<rollingPolicy class="ch.qos.logback.core.rolling.FixedWindowRollingPolicy">
<fileNamePattern>/opt/tomcat/logs/dataarcvr_%i.log</fileNamePattern>
 <minIndex>1</minIndex>
 <maxIndex>10</maxIndex>
</rollingPolicy>
<triggeringPolicy class="com.aptare.dc.util.LogbackSizeBasedTriggeringPolicy">
 <maxFileSize>20MB</maxFileSize>
</triggeringPolicy>
<!--The Threshold param can either be debug/info/warn/error/fatal.-->
<param name="Threshold" value="debug"/>
```

### Data Collector Log Files

For the **Data Collector** the file:

**Linux:** /opt/aptare/mbs/conf/metadatalogger.xml

**Windows:** C:\Program Files\Aptare\mbs\conf\metadatalogger.xml

```
<rollingPolicy class="ch.qos.logback.core.rolling.FixedWindowRollingPolicy">
<fileNamePattern>/opt/aptare/agent_version/DemoDC/mbs/logs/metadata${mdc_key}_%i.log</
fileNamePattern>
 <minIndex>1</minIndex>
 <maxIndex>20</maxIndex>
</rollingPolicy>
```

```
<triggeringPolicy class="com.aptare.dc.util.LogbackSizeBasedTriggeringPolicy">
 <maxFileSize>50MB</maxFileSize>
</triggeringPolicy>
```

## Database SCON Logging - Reduce Logging

To minimize output to the scon.log file, you can prune the content using this procedure:

1. Edit the config.sql file.

**Linux:** /opt/aptare/database/stored\_procedures/config.sql

**Windows:** C:\opt\oracle\database\stored\_procedures\config.sql

2. Change the output setting to LOW, as shown in **red** in the following example.

```
set Echo Off
set Feedback Off

CREATE OR REPLACE PACKAGE config AS
-- Valid APTARE IT Analytics Logging levels are as follows:
-- constant.DEBUG_OFF
-- constant.DEBUG_LOW
-- constant.DEBUG_MEDIUM
-- constant.DEBUG_HIGH

-- To change the global APTARE IT Analytics logging level, change the
following constant
 globalDebugLevel PLS_INTEGER := constant.DEBUG_LOW;

 reportTransLongerThan FLOAT := 0.85; -- Transactions that take
longer than this number of seconds will be reported in aptare-trans.log
-- The following directory will be used to store the APTARE IT
Analytics
-- database logfiles scon.log and scon.err. On a Windows portal
server,
-- this will default to C:\opt\oracle\logs
LOGDIRECTORY CONSTANT VARCHAR2(64) := '/tmp' ;

END config;
/
SHOW ERRORS;
```

3. Apply and validate new settings with the following utilities:

**Linux:**

```
sqlplus portal/<portal_password>@/opt/aptare/database/stored_procedures/config.sql
```

```
sqlplus portal/<portal_password>@/opt/aptare/database/tools/validate_sp
```

**Windows:**

```
sqlplus portal/<portal_password>@C:\opt\oracle\database\stored_procedures\config.sql
```

```
sqlplus portal/<portal_password>@C:\opt\oracle\database\tools\validate_sp
```

## Refreshing the Database SCON Log

---

Even when the amount of data written to the scon.log file is minimal, over time this file can reach a limit that causes processing to cease. The following instructions provide the steps for a utility that copies the existing log file and then empties scon.log, without impacting APTARE IT Analytics processing.

The utility to refresh scon.log executes automatically according to the following rules:

- Utility executes monthly to refresh the scon.log file
- First run executes 30 days after portal installation
- Production run is scheduled for the first Tuesday of every month

The utility searches for the following directory paths until an scon.log file is found:

```
'C:\opt\oracle\logs', 'C:\opt\aptare\oracle\logs', 'C:\opt\aptare\oracle\log', '/tmp'
```

To refresh the scon.log file, use the following utility:

1. Log in to SQLPLUS, as shown below.

**Linux & Windows:**

```
sqlplus portal/<portal_password>
```

2. Execute the log cleanup utility,

**Linux & Windows:**

```
exec logfile_cleanup_pkg.cleanupLog('Y','Y');
```

- Two parameters are required, as described in the following table:

Backup Flag	Save in Backup File	Description
Y	Y	scon.log file emptied backup in scon_<month>.log file
Y	N	scon.log file emptied backup in scon1.log file; all backups will overwrite scon1.log
N	Y	scon.log file emptied no backup of the scon.log file
N	N	scon.log file emptied no backup of the scon.log file

- **NOTE:** This utility is intended to be run no more than once a month. If you plan to run it more than once in a month, be aware of the naming convention for the backup scon.log file, as shown with the parameters in the above table.

## Logging User Activity in audit.log

---

By default, the audit.log captures:

- User login
- User impersonate

Modify the logging level of the `systemlogger.xml` file to provide additional information about a user's activity in the Portal. You can set the level to *info* to capture only what a user deletes OR set it to *debug* to capture all the user activity (including all deletes).

## Logging Only What a User Deletes

---

To log all deletes made by a user in `audit.log`, edit the following file:

**Linux:** `/opt/aptare/portalconf/systemlogger.xml`

**Windows:** `C:\opt\aptare\portalconf\systemlogger.xml`

```
<logger name="com.aptare.sc.gwt.shared.server.GwtSpringAdapter" additivity="false">
 <level value="info"/>
 <appender-ref ref="SECURITY" />
</logger>

<logger name="com.aptare.sc.presentation.filter.AuthorizationFilter" additivity="false">
 <level value="info"/>
 <appender-ref ref="SECURITY" />
</logger>
```

## Logging All User Activity

---

To log all the activity of a user (including what they delete) in `audit.log`, edit the following file:

**Linux:** `/opt/aptare/portalconf/systemlogger.xml`

**Windows:** `C:\opt\aptare\portalconf\systemlogger.xml`

```
<logger name="com.aptare.sc.gwt.shared.server.GwtSpringAdapter" additivity="false">
 <level value="debug"/>
 <appender-ref ref="SECURITY" />
</logger>

<logger name="com.aptare.sc.presentation.filter.AuthorizationFilter" additivity="false">
 <level value="debug"/>
 <appender-ref ref="SECURITY" />
</logger>
```

# Data Collector Log Files

---

Before resorting to examining Data Collector logs, use the following System Administration reports to check collection status:

- Collection Message Summary
- Data Collection Schedule Summary
- Data Collector Status Summary
- File Analytics Collection Status

You can also view live collection status using the **Collection Status** page on the **Admin** tab.

The data collection process logs activity to provide additional processing details that support troubleshooting. Use the **Admin > Advanced > Support Tools** feature to request a support package that contains Data Collector Server files. To identify specific files, it may be helpful to have some knowledge of the logging structure and naming conventions.

Refer to the following sections to understand the logging structure.

- [Data Collector Log File Organization](#)
- [Data Collector Log File Naming Conventions](#)
- [General Data Collector Log Files](#)

## Data Collector Log File Organization

---

Data Collector logs are organized into two directory hierarchies:

### Checkinstall and Validation Probes

- /opt/aptare/mbs/logs/validation/
- C:\Program Files\Aptare\mbs\logs\validation\

### Scheduled Probes (such as running as a service)

- /opt/aptare/mbs/logs/scheduled/
- C:\Program Files\Aptare\mbs\logs\scheduled\

Within this directory structure, there is a `framework` sub-directory. The `framework` sub-directory is used in the beginning of the collection process, before the Data Collector type has been identified. Once IT Analytics knows the type of collector (for example, EMC Isilon), logging is recorded in the main `scheduled` directory using the naming convention described in [Data Collector Log File Naming Conventions](#).

## Data Collector Log File Naming Conventions

---

Within the directory structure described in [Data Collector Log File Organization](#), log files have the following naming convention:

```
<vendor.product>/<subsystem>#META_<ID>/Probe.log
```

For example, an EMC Isilon probe from checkinstall would result in a file name similar to:

```
/opt/aptare/mbs/logs/validation/emc.isilon/
alphpeifr023#META_EA1BA380E95F73C72A72B3B0792111E5/IsilonClusterDetailProbe.log
```

Some collectors may have a period of time when they are not processing a specific subsystem. For those periods, logging will occur in an aggregate log file similar to:

```
/opt/aptare/mbs/logs/validation/emc.isilon/#META_EA1BA380E95F73C72A72B3B0792111E5/
IsilonClusterDetailProbe.log
```

## Sample Vendor.Product Naming Convention

Examples of vendor.product folder names within this directory structure include:

```
cisco.cisco
commvault.simpana
dell.compellent
emc.avamar
emc.clariion
generic.host (Valid for a host resources discovery policy)
hp.3par
symantec.bue
```

Additionally, each Java Virtual Machine (JVM) creates its own logging file(s) when starting up. This is necessary because multiple processes logging to the same file could overwrite each other's log messages. These log files can be found in the framework sub-directory, as described in [Data Collector Log File Organization](#). See also, [Checkinstall Log](#).

## Log File Names Based on Data Collector Generation

Throughout the APTARE IT Analytics life cycle, some collectors have been upgraded to include new functionality and new Data Collectors have been designed with an improved architecture. The log file naming convention depends on the generation of the Data Collector that you are using. You do not need to know the generation of the Data Collector to find relevant log files.

When running a scheduled data collection, the following log files are created, depending on the generation of the Data Collector. For technical reasons, the following naming conventions are used for data collection logs:

- older-generation collectors follow the convention, {scheduled, validation}/vendor.product/#META\_ or {scheduled, validation}/vendor.product/EVENT\_, where EVENT\_ or META\_ is prepended to the collector policy ID; for example, META\_CA6EC7685A9E6330EC3BBFC0DD4811E4.
- newer-generation collectors share a single file named with the main collector ID, for example, {scheduled, validation}/vendor.product/#<Collector\_PolicyID>

Several log file names include a specific ID. This ID can be found in a System Administration report, *Data Collection Schedule Summary*. See also, [Find the Event/Meta Collector ID](#).

### Examples

- /opt/aptare/mbs/logs/scheduled/dell.compellent/#META\_EA1BA380E95F73C72A72B3B0792111E5/  
META\_EA1BA380E95F73C72A72B3B0792111E5.log
- /opt/aptare/mbs/logs/scheduled/emc.avamar/#HQBackupCollector/HQBackupCollector.log

## Checkinstall Log

The checkinstall process produces its own log file, but in most cases, there is very little to report in this log. For example, the checkinstall creates:

```
/opt/aptare/mbs/logs/validation/framework/#checkinstall/checkinstall.log
```



## Test Connection Log

When you initiate a Test Connection action from within a Data Collector policy, a `TestConnection.log` file captures the steps and their status.

- `/opt/aptare/mbs/logs/validation/<vendor.product>/#TestConnection/TestConnection.log`
- `C:\Program Files\Aptare\mbs\logs\validation\<vendor.product>\#TestConnection\TestConnection.log`

## Log File Naming Convention by Collected System

The log file names will have one of the following prefixes substituted for the `<policyID>`:

- `#EVENT_<policyID>`
- `#META_<policyID>`
- `#<policyID>`

**Example:** `scheduled\legato.nw\#META_D922ACBCCFFA2933A301A530A0E011E4`

**Note:** Some collectors may have both a `#META_` and an `#EVENT_` log file.

APTARE IT Analytics Product	Collected System	Where to find the logs (Linux syntax)
Backup Manager	Commvault Simpana	<code>scheduled/commvault.simpana/#&lt;policyID&gt;</code> <code>validation/commvault.simpana/#&lt;policyID&gt;</code>
	EMC Avamar	<code>scheduled/emc.avamar/#&lt;policyID&gt;</code> <code>validation/emc.avamar/#&lt;policyID&gt;</code>
	EMC Data Domain Backup	<code>scheduled/emc.datadomain/#&lt;policyID&gt;</code> <code>validation/emc.datadomain/#&lt;policyID&gt;</code>
	EMC NetWorker	<code>scheduled/legato.nw/#&lt;policyID&gt;</code> <code>validation/legato.nw/#&lt;policyID&gt;</code>
	HP Data Protector	<code>scheduled/hp.dp/#&lt;policyID&gt;</code> <code>validation/hp.dp/#&lt;policyID&gt;</code>
	IBM Spectrum Protect (TSM)	<code>scheduled/ibm.tsm/#&lt;policyID&gt;</code> <code>validation/ibm.tsm/#&lt;policyID&gt;</code>
	Oracle Recovery Manager (RMAN)	<code>scheduled/oracle.rman/#&lt;policyID&gt;</code> <code>validation/oracle.rman/#&lt;policyID&gt;</code>  <b>Note:</b> In addition to the <code>hostname#&lt;productId&gt;/</code> directories, RMAN also creates directories for each <code>INSTANCE.SCHEMA</code> from which it collects.
	Veeam Backup & Replication	<code>scheduled/veeam.backupandreplication/#&lt;policyID&gt;</code> <code>validation/veeam.backupandreplication/#&lt;policyID&gt;</code>
	Veritas Backup Exec	<code>scheduled/symantec.bue/#&lt;policyID&gt;</code> <code>validation/symantec.bue/#&lt;policyID&gt;</code>
	Veritas NetBackup	<code>scheduled/symantec.netbackup/#&lt;policyID&gt;</code> <code>validation/symantec.netbackup/#&lt;policyID&gt;</code>

APTARE IT Analytics Product	Collected System	Where to find the logs (Linux syntax)
<b>Capacity Manager</b>	Dell Compellent	scheduled/dell.compellent/#<policyID> validation/dell.compellent/#<policyID>
	EMC Data Domain Storage	scheduled/emc.datadomain/#<policyID> validation/emc.datadomain/#<policyID>
	EMC Isilon	scheduled/emc.isilon/#<policyID> validation/emc.isilon/#<policyID>
	EMC Symmetrix	scheduled/emc.symmetrix/#<policyID> validation/emc.symmetrix/#<policyID>
	EMC VNX (Celerra)	scheduled/emc.celerra/#<policyID> validation/emc.celerra/#<policyID>
	EMC VNX (CLARiiON)	scheduled/emc.clariion/#<policyID> validation/emc.clariion/#<policyID>
	EMC VPLEX	scheduled/emc.vplex/#<policyID> validation/emc.vplex/#<policyID>
	EMC XtremIO	scheduled/emc.xtremio/#<policyID> validation/emc.xtremio/#<policyID>
	HP 3PAR	scheduled/hp.3par/#<policyID> validation/hp.3par/#<policyID>
	HP EVA	scheduled/hp.eva/#<policyID> validation/hp.eva/#<policyID>
	Hitachi Block	scheduled/hds.hds/#<policyID> validation/hds.hds/#<policyID>
	Hitachi HCP	scheduled/hds.hcp/#<policyID> validation/hds.hcp/#<policyID>
	Hitachi NAS	scheduled/hitachi.hnas/#<policyID> validation/hitachi.hnas/#<policyID>
	Huawei Ocean Stor	scheduled/huawei.oceanstor/#<policyID> validation/huawei.oceanstor/#<policyID>
	IBM Enterprise	scheduled/ibm.ent/#<policyID> validation/ibm.ent/#<policyID>
	IBM SVC	scheduled/ibm.svc/#<policyID> validation/ibm.svc/#<policyID>
	IBM XIV	scheduled/ibm.xiv/#<policyID> validation/ibm.xiv/#<policyID>
	INFINIDAT InfiniBox	scheduled/infinidat.infinibox/#<policyID> validation/infinidat.infinibox/#<policyID>
	NetApp 7-Mode	scheduled/netapp.netapp/#<policyID> validation/netapp.netapp/#<policyID>
	NetApp Cluster	scheduled/netapp.netapp/#<policyID> validation/netapp.netapp/#<policyID>

APTARE IT Analytics Product	Collected System	Where to find the logs (Linux syntax)
	NetApp E-Series	scheduled/netapp.netapp/#<policyID> validation/netapp.netapp/#<policyID>
	Pure Storage FlashArray	scheduled/purestorage.flasharray/ #<policyID> validation/purestorage.flasharray/ #<policyID>
<b>Cloud</b>	Amazon Web Services	scheduled/amazon.webservices/#<policyID> validation/amazon.webservices/#<policyID>
	Microsoft Azure	scheduled/microsoft.azure/#<policyID> validation/microsoft.azure/#<policyID>
	OpenStack Ceilometer	scheduled/openstack.ceilometer/#<policyID> validation/openstack.ceilometer/#<policyID>
	OpenStack Swift	scheduled/openstack.swift/#<policyID> validation/openstack.swift/#<policyID>
<b>Fabric Manager</b>	Brocade	scheduled/brocade.brocadeswitch/#<policyID> validation/brocade.brocadeswitch/ #<policyID>
	Brocade Zone Alias	scheduled/brocade.brocade/#<policyID> validation/brocade.brocade/#<policyID>
	Cisco	scheduled/cisco.ciscoswitch/#<policyID> validation/cisco.ciscoswitch/#<policyID>
	Cisco Zone Alias	scheduled/cisco.cisco/#<policyID> validation/cisco.cisco/#<policyID>
<b>File Analytics</b>	Hosts	scheduled/generic.fa/#<policyID> validation/generic.fa/#<policyID>
<b>Host Collection</b>	Hosts	scheduled/generic.host/#<policyID> validation/generic.host/#<policyID>
<b>Virtualization Manager</b>	IBM VIO	scheduled/cisco.cisco/#<policyID> validation/cisco.cisco/#<policyID>
	VMware	scheduled/vmware.esx/ validation/vmware.esx/

## General Data Collector Log Files

Locations in this table represent the default locations, but these may have been modified for your environment.

Log File Name	Default Location	Description	Component
<b>start_watchdog.log</b>	/opt/aptare/mbs/logs	Logging for the high-level management of the Watchdog component. Management includes startup, shutdown, and initialization.	Watchdog
<b>wrapper.log</b>	C:\Program Files\Aptare\mbs\logs		
<b>watchdog.log</b>	C:\Program Files\Aptare\mbs\logs /opt/aptare/mbs/logs		
<b>upgradeMgr.log</b> <b>upgrade_&lt;version&gt;.log</b>	C:\Program Files\Aptare\upgrade\upgradeManager\logs  /opt/aptare/upgrade/upgradeManager/logs	Detailed logging for the Data Collector Upgrade Manager. <version> refers to the version of the aptare.jar to which the Data Collector is being upgraded. <b>Note:</b> The logs directory will not exist for a new installation of the Data Collector. The logs directory will only be created once the collector goes through an aptare.jar upgrade cycle.	Upgrade Manager

Table 1 General Data Collector Logs

## Find the Event/Meta Collector ID

This ID is displayed in the *Data Collection Schedule Summary*, but you can also use the following script to list the IDs.

1. List the Data Collectors to get the Event/Metadata Collector ID.

Windows:

```
C:\Program Files\APTARE\mbs\bin\listcollectors.bat
```

Linux:

```
/opt/aptare/mbs/bin/listcollectors.sh
```

In the output, look for the Event Collectors section associated with the Software Home—the path that was specified when the Data Collector Policy was created.

```
==== Event Collectors ===
Event Collector Id: EF14CEE486DF781F312E5D40411C11E5
Active: true
Active: true
Software Home: C:\Program Files\EMC NetWorker\nsr\bin
Server Address: networker3
Domain: 100000
Sub-system/Server Instance/Device Manager Id: 110050
Schedule: 10
```

## Portal Log Files

Key log files are managed by a logging subsystem, which manages the log size, and rolls and deletes old files. Log files are used only as an audit trail for troubleshooting, so they can be deleted safely.

Locations in this table represent the default locations, but these may have been modified for your environment.

Log File Name	Default Location	Description
<b>access.log</b>	C:\opt\apache\logs /opt/apache/logs	Standard Web server access log. Use this log to analyze request processing time, request method, page hit count, and session activity.
<b>aptareagent-access*.log</b>	C:\opt\apache\logs /opt/apache/logs	Standard Web Server access log. Logs all http transactions between the Data Collector and the Web Server.
<b>aptareagent-error*.log</b>	C:\opt\apache\logs /opt/apache/logs /opt/tomcat/logs	Standard Web Server error log file. Logs http transaction errors between the Data Collector and the Web Server.
<b>aptareportal-access*.log</b>	C:\opt\apache\logs /opt/apache/logs	Standard Web Server access log. Logs all http transactions between the browser based Portal application and the Web Server.
<b>aptareportal-error*.log</b>	C:\opt\apache\logs /opt/apache/logs	Standard Web Server error log file. Logs http transaction errors between the browser-based Portal application and the Web Server.
<b>aptareStartup.log</b>	/opt/aptare/logs	Contains startup and shutdown information for the Portal services (e.g., from running /opt/aptare/bin/xxx start stop). If a service fails to start, check this log file for details.
<b>audit.log</b>	C:\opt\tomcat\logs\ /opt/tomcat/logs/	By default, logs portal login requests and user impersonations in the Portal web browser window. Modifications can be made to log additional user activity. See <a href="#">Logging User Activity in audit.log</a> .
<b>catalina.out</b>	C:\opt\tomcat\aptare-instances\portal\logs /opt/tomcat/aptare-instances/portal/logs	For Tomcat, this is the standard destination log file for System.out and System.err console messaging.
<b>datacivr*.log</b>	C:\opt\tomcat\logs /opt/tomcat/logs	Detailed logging for the data receiver - the servlet that receives data from the Data Collectors on the Master Server(s). Logs Data Collector connection requests/issues, data received, and database interaction.  See also, <a href="#">Portal and Data Collector Log Files - Reduce Logging</a> .
<b>error.log</b>	C:\opt\apache\logs /opt/apache/logs	Standard Web Server error log file.

Table 2 Portal Log Files

Log File Name	Default Location	Description
<b>portal*.log</b>	C:\opt\tomcat\logs\ /opt/tomcat/logs/	Detailed logging for the Portal servlet. Logs portal login requests, user impersonations, portal reports that are run - basically all actions in the Portal web browser window. Database problems are displayed as SQL exceptions and often list the associated Oracle error number (ORA nnn). See also, <a href="#">Portal and Data Collector Log Files - Reduce Logging</a> .
<b>stderr.log</b>	C:\opt\tomcat\logs\ /opt/tomcat/logs/	High-level log messaging for Tomcat.

**Table 2 Portal Log Files**

Log File Name	Default Location	Description
<b>Tomcat Standard Log Files (Portal)</b>		
<b>admin*.log</b>	C:\opt\tomcat\aptare-instances\portal\logs /opt/tomcat/aptare-instances/portal/logs	Apache Tomcat provides several file handlers that write messages to application-specific log files. The date is appended to <i>admin</i> in the name of the file.
<b>catalina*.log</b>	C:\opt\tomcat\aptare-instances\portal\logs /opt/tomcat/aptare-instances/portal/logs	Apache Tomcat provides several file handlers that write messages to application-specific log files. The date is appended to <i>catalina</i> in the name of the file.
<b>host-manager*.log</b>	C:\opt\tomcat\aptare-instances\portal\logs /opt/tomcat/aptare-instances/portal/logs	Apache Tomcat provides several file handlers that write messages to application-specific log files. The date is appended to <i>host-manager</i> in the name of the file.
<b>manager*.log</b>	C:\opt\tomcat\aptare-instances\portal\logs /opt/tomcat/aptare-instances/portal/logs	Apache Tomcat provides several file handlers that write messages to application-specific log files. The date is appended to <i>manager</i> in the name of the file.
<b>Tomcat Standard Log Files (Data Receiver)</b>		
<b>admin*.log</b>	C:\opt\tomcat\aptare-instances\agent\logs /opt/tomcat/aptare-instances/agent/logs	Apache Tomcat provides several file handlers that write messages to application-specific log files. The date is appended to <i>admin</i> in the name of the file.
<b>catalina*.log</b>	C:\opt\tomcat\aptare-instances\agent\logs /opt/tomcat/aptare-instances/agent/logs	Apache Tomcat provides several file handlers that write messages to application-specific log files. The date is appended to <i>catalina</i> in the name of the file.
<b>host-manager*.log</b>	C:\opt\tomcat\aptare-instances\agent\logs /opt/tomcat/aptare-instances/agent/logs	Apache Tomcat provides several file handlers that write messages to application-specific log files. The date is appended to <i>host-manager</i> in the name of the file.
<b>manager*.log</b>	C:\opt\tomcat\aptare-instances\agent\logs /opt/tomcat/aptare-instances/agent/logs	Apache Tomcat provides several file handlers that write messages to application-specific log files. The date is appended to <i>manager</i> in the name of the file.

Table 2 Portal Log Files

## Managing Apache Log Files

Even if you set up Apache logs for a regularly scheduled rotation, space issues can still occur. You must purge older files if maintaining space is more important than preserving logs. Logs are *not* automatically deleted.

Set up a cron job to remove older apache logs. By default, these logs rotate, but they are not removed. Create scheduled jobs to delete logs that are <XX> days old.

## Database Log Files

Locations in this table represent the default locations, but these may have been modified for your environment.

Log File Name	Location	Description
<b>aptare-trans.log</b>	C:\tmp  /tmp	Records long-running transactions.
<b>scon.err</b>	C:\tmp  /tmp	Error messages from the database stored procedures. Oracle errors are prefixed with ORA-nnnn, where nnnn is the APTARE or Oracle error number. On Windows, if the directory C:\tmp exists, the file will be written there. Otherwise, it will be written to C:\opt\oracle\logs.
<b>scon.log</b>	C:\tmp  /tmp	Detailed logging from database stored procedures. Shows input and output values, and timing of queries. Oracle errors are prefixed with ORA-nnnn, where nnnn is the APTARE or Oracle error number. On Windows, if the directory C:\tmp exists, the file will be written there. Otherwise, it will be written to C:\opt\oracle\logs.
<b>sqlnet.log</b>	C:\opt\oracle\network\log  /opt/aptare/oracle/network/log	Oracle listener log file. Logs information about connection requests made to the Reporting Database.
<b>alert_scdb.log</b>	C:\opt\oracle\rdbms\log\diag\rdbms\scdb\scdb\trace  /opt/aptare/oracle/rdbms/log/diag/rdbms/scdb/scdb/trace	Oracle alert log file. Logs information on startup and shutdown of oracle instance, and also critical Oracle problems (such as disk I/O failures, out of disk space, system resource issues etc.)

Table 3 Reporting Database Log Files



## Installation/Upgrade Log Files

---

Log File Name	Location	Description
<b>aptare_installer*.log</b>	C:\opt\oracle\logs /tmp	Database installation log files.
<b>install.log</b>	C:\opt\installlogs /opt/aptare/installlogs	Log of high-level installation tasks.
<b>installer_debug.txt</b>	C:\opt\installlogs /opt/aptare/installlogs	Log of install tasks.
<b>upgrade.log</b>	C:\opt\aptare\upgrade\logs /opt/aptare/upgrade/logs	Log of upgrade tasks performed by the upgrader

Table 4 Installation Log Files

# 18

## SNMP Trap Alerting

This section covers the following topics:

- [Overview of Alerting](#)
- [SNMP Configurations](#)
- [Standard OIDs](#)
- [Data in an Alerting Trap](#)

### Overview of Alerting

---

Tabular Reports can be configured to alert users via a number of options:

- Email
- Script
- SNMP
- Native log

Typically, notifications are expected when a report's content indicates a threshold crossing or an error state. For example, a Job Summary report can be configured to trigger an alert when failed backup events are reported.

### SNMP Configurations

---

SNMP traps can be issued from any saved tabular report instance, including custom reports that have been created via the Report Template Designer.

Traps have the following characteristics:

- A trap is sent for each row in a report; therefore, if a table is empty, no traps are sent.
- The name of the report is included in the trap.
- The trap includes data for each column in a row.

# Standard OIDs

APTARE IT Analytics does not include a static MIB, however, a standard set of Object IDs can be used to create a MIB.

APTARE\_ENTERPRISE\_TRAP\_OID = "1.3.6.1.4.1.15622.1.1.0.1"

SNMP\_TRAP\_OID = "1.3.6.1.6.3.1.1.4.1.0"

SYS\_UP\_TIME\_OID = "1.3.6.1.2.1.1.3.0"

COLUMN\_OID\_PREFIX = "1.3.6.1.4.1.15622.1.2"

# Data in an Alerting Trap

The data from each row in the report’s table is packed into a single SNMP trap as follows:

ObjectId COLUMN_OID_PREFIX + .0	Contains the saved report instance name, such as Job Summary
ObjectId COLUMN_OID_PREFIX + .1	Column 1 data
ObjectId COLUMN_OID_PREFIX + .2	Column 2 data
ObjectId COLUMN_OID_PREFIX + .n	Each column’s data is included

# Example of a Job Summary Alerting Trap

In the following example, a Job Summary report was generated for All Backups with an Event Status of *Failed*. This report was then filtered on *Type equals Full Backup*. A sample of the saved report instance is shown below.

Failed Full Backups											
Global   Jul 17, 2009 12:00:00AM - Sep 14, 2009 04:09:37PM											
Total Jobs: 64 - This report has a filter applied											
Client	Server	Product	Type	Start Date	Finish Date	Duration	MBytes	MBytes/Sec	Exit Code	# of Files	Tapes
syria	everest	Veritas NetBackup	Full Backup	Jul 27, 2009 12:47:57PM	Jul 27, 2009 12:54:13PM	00:06:16	0.00	N/A	Failed	0	
monaco	everest	Veritas NetBackup	Full Backup	Jul 27, 2009 12:47:57PM	Jul 27, 2009 12:48:41PM	00:00:44	0.00	N/A	Failed	0	
uganda	everest	Veritas NetBackup	Full Backup	Jul 27, 2009 09:27:51AM	Jul 27, 2009 09:34:17AM	00:06:26	0.00	N/A	Failed	0	
syria	everest	Veritas NetBackup	Full Backup	Jul 27, 2009 07:17:47AM	Jul 27, 2009 07:30:13AM	00:12:26	0.00	N/A	Failed	0	
syria	everest	Veritas NetBackup	Full Backup	Jul 26, 2009 07:17:48AM	Jul 26, 2009 05:40:15PM	10:22:27	3,204.00	0.09	Failed	232,500	
moldova	everest	Veritas NetBackup	Full Backup	Jul 26, 2009 07:17:48AM	Jul 26, 2009 05:40:14PM	10:22:26	4,925.25	0.13	Failed	24,275	

For the above example, the data is delivered in the trap as follows:

ObjectId COLUMN\_OID\_PREFIX + .0 contains the saved report instance name—Failed Full Backups

ObjectId COLUMN\_OID\_PREFIX + .1 contains the Client

ObjectId COLUMN\_OID\_PREFIX + .2 contains the Server

ObjectId COLUMN\_OID\_PREFIX + .3 contains the Product

## SSL Certificate Configuration

The following sections provide the steps for implementing the Secure Socket Layer (SSL) protocol within APTARE IT Analytics. SSL can be used when communicating with the Portal and for data collection communication. In addition to SSL configuration details, this section provides instructions to create a self-signed certificate and to add a virtual interface to a Linux server. A sample of a default Apache SSL configuration file is also provided.

APTARE validated these instructions, but there are many variations in the method used to implement SSL. This document is meant only as a guide to one implementation approach and it may not be applicable in all situations. Implementing SSL requires knowledge of the underlying technology.

**Note:** While these steps include directions for generating a temporary, self-signed certificate, APTARE recommends obtaining the certificate from a third-party provider rather than using the self-signed certificate.

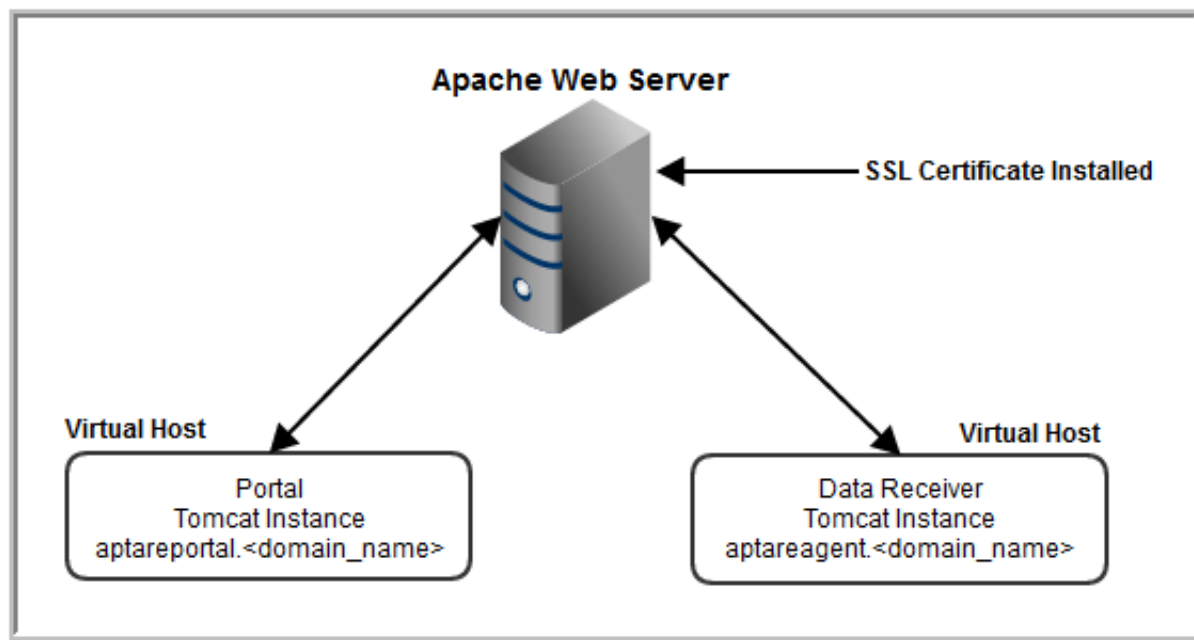
This section covers the following topics:

- [SSL Implementation Overview](#)
- [Obtain an SSL Certificate](#)
- [Update the Web Server Configuration to Enable SSL](#)
- [Enable/Disable SSL for a Data Collector](#)
- [Enable/Disable SSL for Emailed Reports](#)
- [Test and Troubleshoot SSL Configurations](#)
- [Create a Self-Signed SSL Certificate](#)
- [Configure the Data Collector to Trust the Certificate](#)
- [Add a Virtual Interface to a Linux Server](#)
- [Add a Virtual/Secondary IP Address on Windows](#)
- [Default Apache SSL Configuration File](#)

## SSL Implementation Overview

---

The Secure Socket Layer (SSL) protocol enables corporations to leverage standards-based security to protect and encrypt traffic between the APTARE IT Analytics Portal, the Data Collector, and the client browser. The following diagram illustrates how SSL is implemented for APTARE IT Analytics. The Apache Web Server typically resides on the Portal Server.



**Note:** The actual SSL certificates get installed and configured within the Apache Web Server, however, in cases where the issuing certificate authority (CA) is not automatically trusted (for example, self-signed or a one-off domain reseller), the certificates will need to be imported and configured to be trusted on the Data Collector Server. In this case, follow the process to import certificates into the keystore for both the Data Collector and the Upgrade Manager: [Configure the Data Collector to Trust the Certificate](#).

Implementing SSL involves these main tasks:

- [Obtain an SSL Certificate](#)
- [Update the Web Server Configuration to Enable SSL](#)
- [Enable/Disable SSL for a Data Collector](#)
- [Enable/Disable SSL for Emailed Reports](#)

## Obtain an SSL Certificate

---

APTARE, Inc. recommends obtaining a third-party certificate from a certificate authority (CA) such as VeriSign, Thawte, or GeoTrust. The methods for obtaining a certificate vary. Therefore, refer to the vendor's web site for specific instructions.

You may, for testing purposes or as a permanent solution, use a self-signed certificate. This is not recommended as it makes the implementation slightly more complex and may limit access to APTARE IT Analytics to some of your users. To create a self-signed or unknown certificate, see [Create a Self-Signed SSL Certificate](#).

# Update the Web Server Configuration to Enable SSL

These instructions apply to Apache version 2.4.xx and the steps should be taken on the designated Web server.

1. Copy the certificate files, typically generated via a certificate authority (CA), to a folder in the Web server's Apache configuration folder.

**Note:** Configuration files shipped with APTARE licensed modules may use path names with recommended folder names. To use folders with different names, be sure to update all references to the recommended name in the default configuration files.

Linux, APTARE recommends using:	Windows, APTARE recommends using:
/opt/apache/conf/ssl_cert	C:\opt\apache\conf\ssl_cert

2. Stop the Apache and Tomcat services. From a terminal console, enter the following commands.

Linux	Windows
/opt/aptare/bin/tomcat-agent stop	C:\opt\aptare\utils\stopagent.bat
/opt/aptare/bin/tomcat-portal stop	C:\opt\aptare\utils\stopportal.bat
/opt/aptare/bin/apache stop	C:\opt\aptare\utils\stopapache.bat

3. Update the Apache configuration file to enable SSL.

**Linux:** /opt/apache/conf/httpd.conf

**Windows:** C:\opt\apache\conf\httpd.conf

Un-comment the following lines by removing the # character.

Linux	Windows
#LoadModule ssl_module modules/mod_ssl.so	#LoadModule ssl_module modules/mod_ssl.so
#Include conf/extra/httpd-ssl.conf	#Include conf/extra/httpd-ssl.conf
#LoadModule socache_shmcb_module modules/mod_socache_shmcb.so	

4. Update the Apache SSL configuration file. See [Default Apache SSL Configuration File](#) for the sample SSL configuration file shipped with APTARE installations. Note that some of these lines may not be present in your configuration.

**Linux:** /opt/apache/conf/extra/httpd-ssl.conf

**Windows:** C:\opt\apache\conf\extra\httpd-ssl.conf

	Linux	Windows
1.	Disable the SSLMutex by adding a # at the beginning of the SSLMutex line (if this line is listed in your configuration).	Disable the SSLMutex by adding a # at the beginning of the SSLMutex line (if this line is listed in your configuration).
2.	Ensure that an IP address is available for the Portal and/or Data Collection, as required.	

## Examples:

Linux: #SSLMutex "file:/opt/apache/logs/ssl\_mutex"

Windows: #SSLMutex "file:c:\opt\apache\logs\ssl\_mutex"

5. If any of the above configurations are missing for either the Portal or Data Collector, the host configuration information must be added to enable SSL. Refer to the [Default Apache SSL Configuration File](#) as a guide and proceed with the following steps.
6. If a Virtual Host declaration is missing from the default Apache SSL configuration file, add the missing virtual host declaration to the configuration file. See the relevant section for instructions in [Configure Virtual Hosts for Portal and/or Data Collection SSL](#):
  - [If implementing SSL for the Portal Only](#)
  - [If implementing SSL for Data Collection Only](#)
  - [If implementing SSL for Both the Portal and Data Collection](#).
7. For each active virtual host section in the Apache SSL configuration file (httpd-ssl.conf), ensure that declaration lines beginning with the following are un-commented (they do not have a # at the beginning of the line):

```

SSLEngine
SSLCipherSuite
SSLCertificateFile (update certificate file details)
SSLCertificateKeyFile (update certificate key file details)

```

8. For a Linux Web Server only, update the Apache script used to start Apache, /opt/aptare/bin/apache, to include the **-D SSL** parameter:

```
Ret="$APACHE_HOME/bin/apachectl -D SSL -k start 2>&1"
```

9. **If implementing SSL for Data Collection, complete the following steps:**

- a Ensure that the Data Collector global properties file does not have the protocol (http or https) in the URL specified in that file.

Linux	Windows
/opt/aptare/dataarcvrconf/ collectorConfig.global.properties	C:\opt\aptare\dataarcvrconf\ collectorConfig.global.properties

- b If using a self-signed certificate, run the **InstallCert** utility on the Data Collection server to allow the background data collection processes to automatically accept the unsigned, unverified certificate.

The **InstallCert** utility is *not* shipped with APTARE products. Contact the APTARE Global Support Services to obtain a copy of this utility.

Linux Data Collector Server Command	Windows Data Collector Server Command
java -classpath /opt/aptare/mbs/bin InstallCert aptareagent.<domain_name>.com:443	"C:\program files\aptare\jre\bin\java" - classpath "C:\program files\aptare\mbs\ bin" InstallCert aptareagent.<domain_name>:443

**Warning:** If you are using a self-signed certificate and the Data Collector is upgraded, the validation of the certificate may be lost and you may have to rerun the InstallCert utility for data collection to work.

- c Verify the **Trust all certificates** is enabled in the System Configuration settings. Locate the parameter here: **Admin>Advanced>System Configuration> Portal**.

10. Restart Apache and both Tomcat (Portal and Data Collector) services.

Linux	Windows
/opt/aptare/bin/apache start	C:\opt\aptare\utils\startapache.bat
/opt/aptare/bin/tomcat-portal start	C:\opt\aptare\utils\startagent.bat
/opt/aptare/bin/tomcat-agent start	C:\opt\aptare\utils\startportal.bat

## Configure Virtual Hosts for Portal and/or Data Collection SSL

Refer to the following sections that are relevant for your environment. These instructions are referenced in [Step 6](#) of [Update the Web Server Configuration to Enable SSL](#).

- [If implementing SSL for the Portal Only](#)
- [If implementing SSL for Data Collection Only](#)
- [If implementing SSL for Both the Portal and Data Collection](#)

### If implementing SSL for the Portal Only

1. Verify that there is a VirtualHost section with the **IP address assigned to the Portal host**. This section starts with the following lines. These lines must be present and enabled.

```
<VirtualHost IP_ADDRESS_PORTAL:443>
ServerName aptareportal.domainname:443
Document Root /opt/aptare/portal
```

2. In the VirtualHost declaration, replace IP\_ADDRESS\_PORTAL with the IP address assigned to the Portal server.
3. If the Portal VirtualHost section is not found, the configuration for the Portal VirtualHost must be added.
4. If there is a configuration section for the Data Collection virtual host, ensure that this section is disabled by adding a # to the beginning of each line in the section, as shown below.

```
#<VirtualHost aptareagent.domainname:443>
```

5. Set the Document Root path to a valid path for the Web Server's OS.

Linux	Windows
/opt/aptare/portal	C:\opt\aptare\portal



## If implementing SSL for Data Collection Only

1. Verify that there is a VirtualHost section for the data collection with the **IP address of the Data Receiver**. This section starts with the following lines. These lines must be present and enabled.

```
<VirtualHost IP_ADDRESS_DATARCVR:443>
ServerName aptareagent.domainname:443
DocumentRoot /opt/aptare/datarcvr
```

2. Replace IP\_ADDRESS\_DATARCVR in the VirtualHost declaration with the IP address assigned to the Data Receiver.
3. If the data collection VirtualHost section is not found, the configuration for the data collection VirtualHost must be added.
4. If there is a configuration section for the Portal virtual host, ensure that this section is disabled by added a # to the beginning of each line in the section, as shown below.  
#<VirtualHost aptareportal.domainname:443>
5. Set the Document Root path to a valid path for the Web Server's OS.

Linux	Windows
/opt/aptare/datarcvr	C:\opt\aptare\datarcvr

## If implementing SSL for Both the Portal and Data Collection

To implement SSL for both the Portal and Data Collection, the Portal server must be configured with two IP addresses, one for the Portal and one for Data Collection. The two required IP addresses may be implemented using two NICs. If only a single NIC is available, a virtual interface may be added for the second IP address. See [Add a Virtual Interface to a Linux Server](#) and [Add a Virtual/Secondary IP Address on Windows](#).

1. Verify there is a VirtualHost section with the **IP address assigned to the Portal host**. This section starts with the following lines. These lines must be present and enabled.

```
<VirtualHost IP_ADDRESS_PORTAL:443>
ServerName aptareportal.domainname:443
DocumentRoot /opt/aptare/portal
```

2. Replace IP\_ADDRESS\_PORTAL in the VirtualHost declaration with the IP address assigned to the Portal server.
3. Verify there is a VirtualHost section with the **Data Receiver IP address**. This section starts with the following lines. These lines must be present and enabled.

```
<VirtualHost IP_ADDRESS_DATARCVR:443>
ServerName aptareagent.domainname:443
DocumentRoot /opt/aptare/datarcvr
```

4. Replace IP\_ADDRESS\_DATARCVR in the VirtualHost declaration with the IP address assigned to the Data Receiver.
5. Set the Document Root paths to valid paths for the Web Server's OS.

Linux	Windows
/opt/aptare/portal	C:\opt\aptare\portal
/opt/aptare/datarcvr	C:\opt\aptare\datarcvr

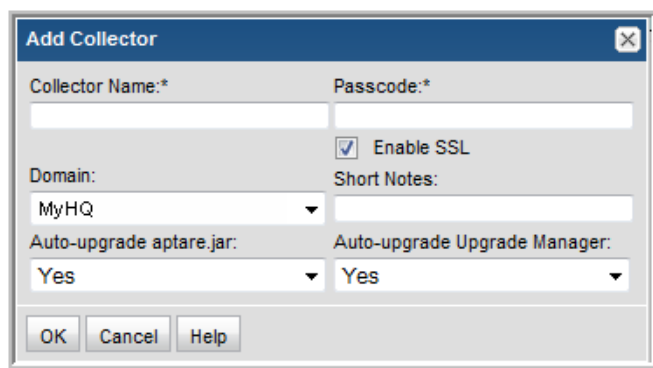
## Enable/Disable SSL for a Data Collector

Once you globally configure SSL, you can change the settings for individual Data Collectors. This provides the capability of supporting a mix of both http and https among your Data Collector servers.

A system property **-Dhttps.protocols=TLSv1,TLSv1.1,TLSv1.2** is included in the startup and checkinstall scripts (aptaredc.bat/sh, checkinstall.bat/sh) to support TLS 1.1, TLS 1.2.

To enable and disable SSL for a specific Data Collector:

1. If you are using a self-signed certificate, verify the **Trust all certificates** is enabled in the System Configuration settings. Locate the parameter here: **Admin>System Configuration> Portal**.
2. In the APTARE IT Analytics Portal, go to **Admin > Data Collection>Collector Administration**.
3. Double-click a Data Collector to view the existing settings or click **Add** to add a Data Collector.



4. Check the **Enable SSL** checkbox.

Both secure (SSL) and non-secure Data Collectors can send data to the same Portal. Check this box to select the secure communication protocol (https) that the Data Collector will use.

This check box will *not* appear in the dialog box if SSL is not enabled in your environment. The Portal data receiver must be listening for https traffic; for example:  
<https://agent.mycollector.com>

5. Click **OK** to save the setting.

## Enable/Disable SSL for Emailed Reports

---

When emailing reports, an *Add a Live Link* option provides the capability of having a hyperlink (View this report in the Portal) in the email to take the user directly to the Portal. In environments where SSL is enabled, a configuration change is required in the `portal.properties` file to ensure that this link is secure.

**Linux:** `/opt/aptare/portalconf/portal.properties`

**Windows:** `C:\opt\aptare\portalconf\portal.properties`

1. In the `portal.properties` file, find the following section and update the `portal.applicationUrl` to replace *http* with *https*.

### Example:

```
#The Portal environment
portal.sessionTimeout=3600
portal.applicationUrl=https://aptareportal.mycompany.com
```

2. Restart the Portal service. See [Starting and Stopping Portal Server Software](#).

## Test and Troubleshoot SSL Configurations

---

### Test if SSL is set up for the Portal

1. Enter `https://aptareportal.domain.com/` in a browser.  
The Portal login page should display.

### Test if SSL is set up for Data Collection

1. Enter `https://aptareagent.domain.com/` in a browser. The default Tomcat page should display.
2. Enter `https://aptareagent.domain.com/servlet/util/` in a browser.  
The error message, **GET not SUPPORTED. Illegal Operation!!!**, should display.

### Workaround for Missing Library Errors

While configuring SSL on a Portal, when starting Apache and/or checking syntax, you may encounter missing library errors for `libssl.so.X` and `libcrypto.so.X`.

1. Create symbolic links in `/usr/lib64` to the actual files, as shown in the following example.  

```
root@aptare01 lib64# ln -s libssl.so.1.0.1e libssl.so.6
```

# Create a Self-Signed SSL Certificate

---

APTARE recommends using OpenSSL open source software to create your self-signed certificate. For more information on creating self-signed certificates using OpenSSL, refer to the FAQs and documentation on the OpenSSL site at [www.openssl.org](http://www.openssl.org).

The instructions and examples in this section are applicable for the Linux operating system. OpenSSL also may be used with the Windows operating system. Check the OpenSSL web site for specific instructions. Note that the certificate is independent of the operating system under which it was created. A self-signed certificate created on a Linux computer may be installed on a Windows web server.

You can create a self-signed certificate with multiple options depending on how you want to configure your certificate. APTARE recommends the following OpenSSL command to create a self-signed certificate. The command creates two files: `server.key` and `server.crt`. You must install these files on the IT Analytics web server.

```
openssl req -x509 -days 365 -sha1 -newkey rsa:1024 -nodes
-keyout server.key -out server.crt
-subj '/O=<CompanyName>/OU=<Department>/CN=<CommonName>'
```

## where

**-x509** is used to create a certificate as opposed to a certificate request that is sent to a certificate authority

**-days** determines the number of days that the certificate is valid

**-sha1** specifies the type of encryption to be used

**-newkey rsa:1024** sets the key as 1024-bit RSA

**-nodes** specifies that no passkey will be used

**-keyout** specifies the name of the key file

**-out** specified the name of the certificate file

**<CompanyName>** is the name of your company

**<Department>** is the name of your department

**<CommonName>** is the URL of the site that the certificate will be installed at. This may be the full URL, such as `aptareportal.site.com`, or a partial URL, such as `*.site.com`. APTARE, Inc. recommends using the latter; the latter must be used if the certificate is to be used when accessing both the Portal and Data Collection.

## Example:

```
openssl req -x509 -days 365 -sha1 -newkey rsa:1024 -nodes
-keyout server.key -out server.crt
-subj '/O=ABC Company/OU=IT/CN=*.abc.com'
```

**Note:** The use of the **-nodes** option in the previous example creates a certificate that does *not* require a pass phrase. This makes it easier to install and use the certificate, but weakens the security of the certificate. If the certificate is created with a pass phrase, it must be entered when the certificate is installed and used.

The actual certificates get installed and configured on the Apache web server, however, in cases where the issuing certificate authority (CA) is not automatically trusted (such as self-signed certificates), the certificates need to be imported and trusted on the Data Collector server.

Once the self-signed certificates have been created, [Configure the Data Collector to Trust the Certificate](#).

# Configure the Data Collector to Trust the Certificate

---

In cases where the certificate authority (CA) is not trusted, as may be the case when using a self-signed or unknown certificate, both the Data Collector and the Upgrade Manager will need to have the certificate imported into the keystore to ensure that the Data Collector can communicate using SSL. See [Keystore File Locations on the Data Collector Server](#) and [Import a Certificate into the Data Collector Java Keystore](#).

## Keystore File Locations on the Data Collector Server

---

**Note:** For the following commands, if you are not running in the default collector location (/opt/aptare or C:\opt\aptare), substitute the appropriate APTARE\_HOME in the command path. See [Import a Certificate into the Data Collector Java Keystore](#).

**Linux Data Collector:** /opt/aptare/jre/lib/security/cacerts

**Windows Data Collector:** C:\opt\aptare\jre\lib\security\cacerts

**Linux Upgrade Manager:** /opt/aptare/upgrade/upgradeManager/jre/lib/security/cacerts

**Windows Upgrade Manager:** C:\opt\aptare\upgrade\upgradeManager\jre\lib\security\cacerts

## Import a Certificate into the Data Collector Java Keystore

---

Use the following steps to add an SSL certificate to the Java keystore for a Data Collector. Some servers, such as vSphere, require a certificate for connection while communicating with SSL. See also, [Configure the Data Collector to Trust the Certificate](#) and [Keystore File Locations on the Data Collector Server](#).

1. Copy the certificate file (certfile.txt) to the Data Collector.
2. Run the following command to add the certificate:

**Linux:**

```
/usr/java/bin/keytool -import -alias "somealias" -file certfile.txt -keystore /opt/
aptare/jre/lib/security/cacerts
```

**Windows:**

```
C:\opt\jre\bin\keytool -import -alias "somealias" -file certfile.txt -keystore C:\opt\
aptare\jre\lib\security\cacerts
```

3. When prompted, enter the default password to the keystore:

```
changeit
```

The results will be similar to the following example:

```
Enter keystore password:
```

```
.....
```

```
Certificate Shown here
```

```
.....
```

```
Trust this certificate? [no]: yes
```

4. Once completed, run the following keytool command to view a list of certificates from the keystore and confirm that the certificate was successfully added. The certificate fingerprint line displays with the alias name used during the import.

**Linux:**

```
/usr/java/bin/keytool -list -keystore /opt/aptare/jre/lib/security/cacerts
```

## Windows:

```
C:\opt\jre\bin\keytool -list -keystore C:\opt\aptare\jre\lib\security\cacerts
```

## Sample Linux Output

```
Enter keystore password:
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 79 entries
digicertassuredidrootca, Apr 16, 2008, trustedCertEntry,
Certificate fingerprint (SHA1):
05:63:B8:63:0D:62:D7:5A:BB:C8:AB:1E:4B:DF:B5:A8:99:B2:4D:43
trustcenterclass2caii, Apr 29, 2008, trustedCertEntry,
Certificate fingerprint (SHA1):
AE:50:83:ED:7C:F4:5C:BC:8F:61:C6:21:FE:68:5D:79:42:21:15:6E
.....
```

## Add a Virtual Interface to a Linux Server

---

The standard APTARE server configuration uses two virtual hosts on the server. One host, identified by the sub-domain **aptareportal**, handles Portal requests to deliver APTARE IT Analytics administration and reporting functionality. The second host, identified by the sub-domain **aptareagent**, handles data collection functionality between the data collection agent and the various devices that report to the agent. These virtual hosts are defined in the Apache configuration file; the sub-domain names are used to identify the each host.

When using SSL, unique IP addresses must be assigned to each virtual host. Therefore, if SSL is to be enabled for both the Portal and Data Collection, two IP addresses are required. Two IP addresses can be assigned using two NICs or, on a Linux server, a virtual interface can be created to assign two IP addresses to a single NIC. See also, [Configure Virtual Hosts for Portal and/or Data Collection SSL](#) and [Add a Virtual/Secondary IP Address on Windows](#).

1. To verify the number of IP addresses assigned to a Linux server, use the following command:

```
ifconfig -a
```

Example result of the `ifconfig -a` command:

```
eth0 Link encap:Ethernet HWaddr 08:00:27:71:44:C4
 inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:310 errors:0 dropped:0 overruns:0 frame:0
 TX packets:372 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:63235 (61.7 KiB) TX bytes:28143 (27.4 KiB)

lo Link encap:Local Loopback
 inet addr:127.0.0.1 Mask:255.0.0.0
 UP LOOPBACK RUNNING MTU:16436 Metric:1
 RX packets:8762 errors:0 dropped:0 overruns:0 frame:0
 TX packets:8762 errors:0 dropped:0 overruns:0 carrier:0
```

```
collisions:0 txqueuelen:0
RX bytes:5422509 (5.1 MiB) TX bytes:5422509 (5.1 MiB)
```

2. You must have two Ethernet connections, identified by the `eth0` label. To add a virtual interface on a Linux server, with a second IP address, to the existing Ethernet interface, use the following command:

```
ifconfig eth0:0 111.222.333.444
```

where

111.222.333.444 is the new IP address for the virtual interface.

3. You must add a file to the network scripts to recreate the virtual interface when the server is rebooted. If the IP address assigned to the `eth0` interface is static, make a copy of the `ifcfg-eth0` file in `/etc/sysconfig/network-scripts` and name it `ifcfg-eth0:0`.
4. Update the IP address in `ifcfg-eth0:0` to be the new IP address assigned to the virtual interface.
5. If the IP address in the `eth0` interface is dynamically assigned, as indicated by the line `BOOTPROTO=dhcp` in the `ifcfg-eth0` file, create a file named `ifcfg-eth0:0` with the following lines:

```
DEVICE=eth0:0
IPADDR=111.222.333.444
```

6. Finally, update your DNS server so that the new IP address is mapped to the data collection URL (for example, `aptareagent.company.com`).

## Add a Virtual/Secondary IP Address on Windows

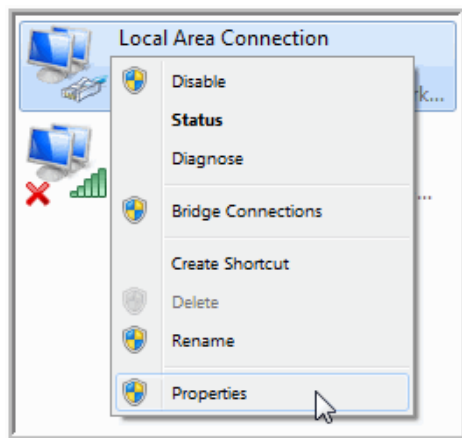
---

See also, [Configure Virtual Hosts for Portal and/or Data Collection SSL](#) and [Add a Virtual Interface to a Linux Server](#).

To add a Virtual IP Address on Windows, go to:

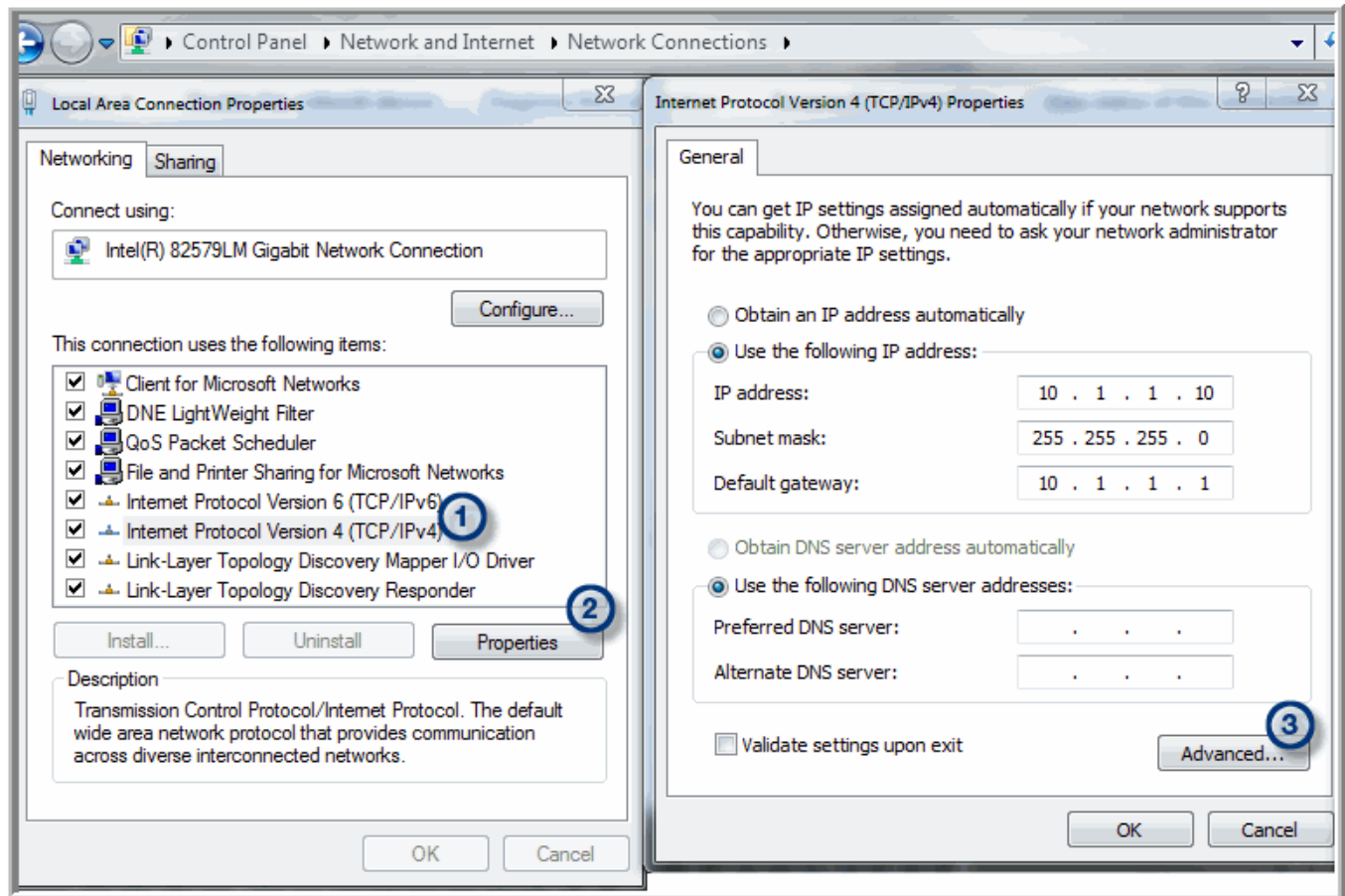
**Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings**

Right-click on a Network connection and select **Properties**.

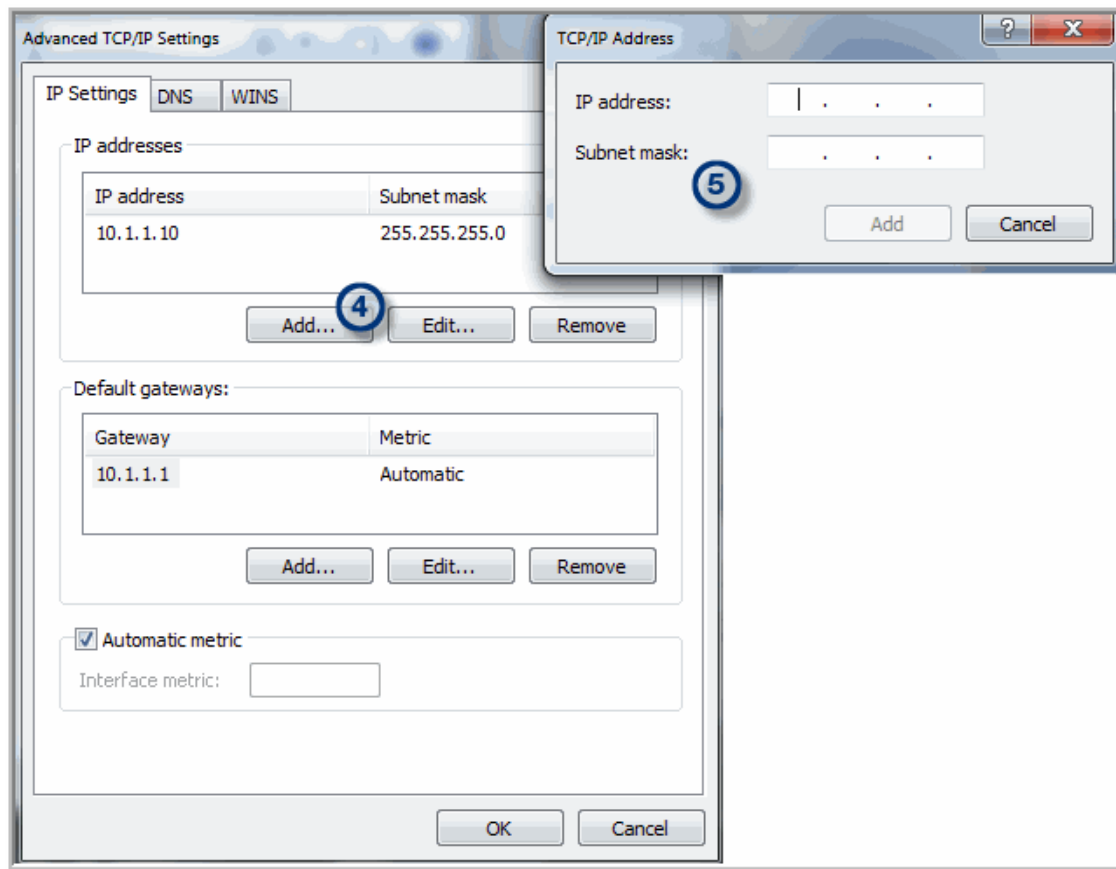


Take the following steps to configure a secondary IP address.





1. Select the TCP/IP connection.
2. Click **Properties**.
3. For the configured IP address, click **Advanced**.



4. In the Advanced TCP/IP Settings window, click **Add**.
5. Enter the **IP address** and **Subnet mask** and click **Add**.

# Default Apache SSL Configuration File

---

This section lists the content of the default Apache SSL configuration file:

/opt/apache/conf/extra/httpd-ssl.conf

C:\opt\apache\conf\extra\httpd-ssl.conf

```
#
This is the Apache server configuration file providing SSL support.
It contains the configuration directives to instruct the server how to
serve pages over an https connection. For detailing information about these
directives see <URL:http://httpd.apache.org/docs/2.2/mod/mod_ssl.html>
#
Do NOT simply read the instructions in here without understanding
what they do. They're here only as hints or reminders. If you are unsure
consult the online docs. You have been warned.
#
#
Pseudo Random Number Generator (PRNG):
Configure one or more sources to seed the PRNG of the SSL library.
The seed data should be of good random quality.
WARNING! On some platforms /dev/random blocks if not enough entropy
is available. This means you then cannot use the /dev/random device
because it would lead to very long connection times (as long as
it requires to make more entropy available). But usually those
platforms additionally provide a /dev/urandom device which doesn't
block. So, if available, use this one instead. Read the mod_ssl User
Manual for more details.
#
#SSLRandomSeed startup file:/dev/random 512
#SSLRandomSeed startup file:/dev/urandom 512
#SSLRandomSeed connect file:/dev/random 512
#SSLRandomSeed connect file:/dev/urandom 512

#
When we also provide SSL we have to listen to the
standard HTTP port (see above) and to the HTTPS port
#
Note: Configurations that use IPv6 but not IPv4-mapped addresses need two
Listen directives: "Listen [::]:443" and "Listen 0.0.0.0:443"
#
Listen 443
##
SSL Global Context
##
```

```

All SSL configuration in this context applies both to
the main server and all SSL-enabled virtual hosts.
##
#
Some MIME-types for downloading Certificates and CRLs
#
AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl .crl

Pass Phrase Dialog:
Configure the pass phrase gathering process.
The filtering dialog program ('builtin' is a internal
terminal dialog) has to provide the pass phrase on stdout.
SSLPassPhraseDialog builtin

Inter-Process Session Cache:
Configure the SSL Session Cache: First the mechanism
to use and second the expiring timeout (in seconds).
#SSLSessionCache "dbm:/opt/apache/logs/ssl_scache"
SSLSessionCache "shmcb:/opt/apache/logs/ssl_scache(512000)"
SSLSessionCacheTimeout 300

Semaphore:
Configure the path to the mutual exclusion semaphore the
SSL engine uses internally for inter-process synchronization.
SSLMutex "file:/opt/apache/logs/ssl_mutex"
##
SSL Virtual Host Context
##
<VirtualHost 10.2.2.1:443>
 ServerName ~AGENT_HOST~.~DOMAIN_NAME~:443
 DocumentRoot ~PORTAL_BASE~/datarcvr
 DirectoryIndex index.jsp
 ErrorLog "|/opt/apache/bin/rotatelogs /opt/apache/logs/aptareportalSSL-error_%Y-%m-%d-%H_%M_%S.log 50M"
 CustomLog "|/opt/apache/bin/rotatelogs /opt/apache/logs/aptareportalSSL-access_%Y-%m-%d-%H_%M_%S.log 50M" common
 Alias / ~PORTAL_BASE~/datarcvr/
 JkMount /*.jsp agent
 JkMount /*.do agent
 JkMount /servlet/* agent

SSL Engine Switch:
Enable/Disable SSL for this virtual host.

```

SSL Engine on

```
SSL Cipher Suite:
List the ciphers that the client is permitted to negotiate.
See the mod_ssl documentation for a complete list.
SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL

Server Certificate:
Point SSLCertificateFile at a PEM encoded certificate. If
the certificate is encrypted, then you will be prompted for a
pass phrase. Note that a kill -HUP will prompt again. Keep
in mind that if you have both an RSA and a DSA certificate you
can configure both in parallel (to also allow the use of DSA
ciphers, etc.)
SSLCertificateFile "/opt/apache/conf/ssl_cert/server.crt"

Server Private Key:
If the key is not combined with the certificate, use this
directive to point at the key file. Keep in mind that if
you've both a RSA and a DSA private key you can configure
both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile "/opt/apache/conf/ssl_cert/server.key"

Server Certificate Chain:
Point SSLCertificateChainFile at a file containing the
concatenation of PEM encoded CA certificates which form the
certificate chain for the server certificate. Alternatively
the referenced file can be the same as SSLCertificateFile
when the CA certificates are directly appended to the server
certificate for convenience.
#SSLCertificateChainFile "/opt/apache/conf/server-ca.crt"

Certificate Authority (CA):
Set the CA certificate verification path where to find CA
certificates for client authentication or alternatively one
huge file containing all of them (file must be PEM encoded)
Note: Inside SSLCACertificatePath you need hash symlinks
to point to the certificate files. Use the provided
Makefile to update the hash symlinks after changes.
#SSLCACertificatePath "/opt/apache/conf/ssl.crt"
#SSLCACertificateFile "/opt/apache/conf/ssl.crt/ca-bundle.crt"

Certificate Revocation Lists (CRL):
```

```

Set the CA revocation path where to find CA CRLs for client
authentication or alternatively one huge file containing all
of them (file must be PEM encoded)
Note: Inside SSLCARevocationPath you need hash symlinks
to point to the certificate files. Use the provided
Makefile to update the hash symlinks after changes.
#SSLCARevocationPath "/opt/apache/conf/ssl.crl"
#SSLCARevocationFile "/opt/apache/conf/ssl.crl/ca-bundle.crl"

Client Authentication (Type):
Client certificate verification type and depth. Types are
none, optional, require and optional_no_ca. Depth is a
number which specifies how deeply to verify the certificate
issuer chain before deciding the certificate is not valid.
#SSLVerifyClient require
#SSLVerifyDepth 10

Access Control:
With SSLRequire you can do per-directory access control based
on arbitrary complex boolean expressions containing server
variable checks and other lookup directives. The syntax is a
mixture between C and Perl. See the mod_ssl documentation
for more details.
#<Location />
#SSLRequire (%{SSL_CIPHER} !~ m/^(EXP|NULL)/ \
and %{SSL_CLIENT_S_DN_O} eq "Snake Oil, Ltd." \
and %{SSL_CLIENT_S_DN_OU} in {"Staff", "CA", "Dev"} \
and %{TIME_WDAY} >= 1 and %{TIME_WDAY} <= 5 \
and %{TIME_HOUR} >= 8 and %{TIME_HOUR} <= 20) \
or %{REMOTE_ADDR} =~ m/^192\.76\.162\. [0-9]+$/
#</Location>

SSL Engine Options:
Set various options for the SSL engine.
o FakeBasicAuth:
Translate the client X.509 into a Basic Authorisation. This means that
the standard Auth/DBMAuth methods can be used for access control. The
user name is the `one line' version of the client's X.509 certificate.
Note that no password is obtained from the user. Every entry in the user
file needs this password: `xxj31ZMTZzkVA'.
o ExportCertData:
This exports two additional environment variables: SSL_CLIENT_CERT and
SSL_SERVER_CERT. These contain the PEM-encoded certificates of the

```

```

server (always existing) and the client (only existing when client
authentication is used). This can be used to import the certificates
into CGI scripts.
o StdEnvVars:
This exports the standard SSL/TLS related `SSL_*' environment variables.
Per default this exportation is switched off for performance reasons,
because the extraction step is an expensive operation and is usually
useless for serving static content. So one usually enables the
exportation for CGI and SSI requests only.
o StrictRequire:
This denies access when "SSLRequireSSL" or "SSLRequire" applied even
under a "Satisfy any" situation, i.e. when it applies access is denied
and no other module can change it.
o OptRenegotiate:
This enables optimized SSL connection renegotiation handling when SSL
directives are used in per-directory context.
#SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
<FilesMatch "\.(cgi|shtml|phtml|php)$">
 SSLOptions +StdEnvVars
</FilesMatch>
<Directory "/opt/apache/cgi-bin">
 SSLOptions +StdEnvVars
</Directory>

SSL Protocol Adjustments:
The safe and default but still SSL/TLS standard compliant shutdown
approach is that mod_ssl sends the close notify alert but doesn't wait for
the close notify alert from client. When you need a different shutdown
approach you can use one of the following variables:
o ssl-unclean-shutdown:
This forces an unclean shutdown when the connection is closed, i.e. no
SSL close notify alert is send or allowed to received. This violates
the SSL/TLS standard but is needed for some brain-dead browsers. Use
this when you receive I/O errors because of the standard approach where
mod_ssl sends the close notify alert.
o ssl-accurate-shutdown:
This forces an accurate shutdown when the connection is closed, i.e. a
SSL close notify alert is send and mod_ssl waits for the close notify
alert of the client. This is 100% SSL/TLS standard compliant, but in
practice often causes hanging connections with brain-dead browsers. Use
this only for browsers where you know that their SSL implementation
works correctly.
Notice: Most problems of broken clients are also related to the HTTP

```

```

keep-alive facility, so you usually additionally want to disable
keep-alive for those clients, too. Use variable "nokeepalive" for this.
Similarly, one has to force some clients to use HTTP/1.0 to workaround
their broken HTTP/1.1 implementation. Use variables "downgrade-1.0" and
"force-response-1.0" for this.
BrowserMatch ".*MSIE.*" \
 nokeepalive ssl-unclean-shutdown \
 downgrade-1.0 force-response-1.0

Per-Server Logging:
The home of a custom SSL log file. Use this when you want a
compact non-error SSL logfile on a virtual host basis.
CustomLog "/opt/apache/logs/ssl_request_log" \
 "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>

<VirtualHost 10.2.2.1:443>
General setup for the virtual host
ServerName ~PORTAL_HOST~.~DOMAIN_NAME~:443
DocumentRoot ~PORTAL_BASE~/portal
DirectoryIndex index.jsp
ErrorLog "|/opt/apache/bin/rotatelog /opt/apache/logs/aptareportalSSL-error_%Y-%m-%d-%H_%M_%S.log 50M"
CustomLog "|/opt/apache/bin/rotatelog /opt/apache/logs/aptareportalSSL-access_%Y-%m-%d-%H_%M_%S.log 50M" common
Alias / ~PORTAL_BASE~/portal/
ErrorDocument 503 /maintenance.html
JkMount /*.jsp portal
JkMount /*.do portal
JkMount /servlet/* portal
JkMount /chart* portal
JkMount /*.mvc portal
JkMount /*/bundles/*.css portal
JkMount /*.download portal
JkMount /*.login portal
JkMount /*.ajax portal
JkMount /*/bundles/*.js portal
JkMount /*.jawr-css portal
JkMount /*.jawr-js portal
JkMount /*.httprpc portal
JkMount /*.rpc portal

SSL Engine Switch:
Enable/Disable SSL for this virtual host.

```



SSL Engine on

```
SSL Cipher Suite:
List the ciphers that the client is permitted to negotiate.
See the mod_ssl documentation for a complete list.
SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL

Server Certificate:
Point SSLCertificateFile at a PEM encoded certificate. If
the certificate is encrypted, then you will be prompted for a
pass phrase. Note that a kill -HUP will prompt again. Keep
in mind that if you have both an RSA and a DSA certificate you
can configure both in parallel (to also allow the use of DSA
ciphers, etc.)
SSLCertificateFile "/opt/apache/conf/ssl_cert/server.crt"

Server Private Key:
If the key is not combined with the certificate, use this
directive to point at the key file. Keep in mind that if
you've both a RSA and a DSA private key you can configure
both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile "/opt/apache/conf/ssl_cert/server.key"

Server Certificate Chain:
Point SSLCertificateChainFile at a file containing the
concatenation of PEM encoded CA certificates which form the
certificate chain for the server certificate. Alternatively
the referenced file can be the same as SSLCertificateFile
when the CA certificates are directly appended to the server
certificate for convenience.
#SSLCertificateChainFile "/opt/apache/conf/server-ca.crt"

Certificate Authority (CA):
Set the CA certificate verification path where to find CA
certificates for client authentication or alternatively one
huge file containing all of them (file must be PEM encoded)
Note: Inside SSLCACertificatePath you need hash symlinks
to point to the certificate files. Use the provided
Makefile to update the hash symlinks after changes.
#SSLCACertificatePath "/opt/apache/conf/ssl.crt"
#SSLCACertificateFile "/opt/apache/conf/ssl.crt/ca-bundle.crt"

Certificate Revocation Lists (CRL):
```

```

Set the CA revocation path where to find CA CRLs for client
authentication or alternatively one huge file containing all
of them (file must be PEM encoded)
Note: Inside SSLCARevocationPath you need hash symlinks
to point to the certificate files. Use the provided
Makefile to update the hash symlinks after changes.
#SSLCARevocationPath "/opt/apache/conf/ssl.crl"
#SSLCARevocationFile "/opt/apache/conf/ssl.crl/ca-bundle.crl"

Client Authentication (Type):
Client certificate verification type and depth. Types are
none, optional, require and optional_no_ca. Depth is a
number which specifies how deeply to verify the certificate
issuer chain before deciding the certificate is not valid.
#SSLVerifyClient require
#SSLVerifyDepth 10

Access Control:
With SSLRequire you can do per-directory access control based
on arbitrary complex boolean expressions containing server
variable checks and other lookup directives. The syntax is a
mixture between C and Perl. See the mod_ssl documentation
for more details.
#<Location />
#SSLRequire (%{SSL_CIPHER} !~ m/^(EXP|NULL)/ \
and %{SSL_CLIENT_S_DN_O} eq "Snake Oil, Ltd." \
and %{SSL_CLIENT_S_DN_OU} in {"Staff", "CA", "Dev"} \
and %{TIME_WDAY} >= 1 and %{TIME_WDAY} <= 5 \
and %{TIME_HOUR} >= 8 and %{TIME_HOUR} <= 20) \
or %{REMOTE_ADDR} =~ m/^192\.76\.162\.[0-9]+$/
#</Location>

SSL Engine Options:
Set various options for the SSL engine.
o FakeBasicAuth:
Translate the client X.509 into a Basic Authorisation. This means that
the standard Auth/DBMAuth methods can be used for access control. The
user name is the `one line' version of the client's X.509 certificate.
Note that no password is obtained from the user. Every entry in the user
file needs this password: `xxj31ZMTZzkVA'.
o ExportCertData:
This exports two additional environment variables: SSL_CLIENT_CERT and
SSL_SERVER_CERT. These contain the PEM-encoded certificates of the

```

```

server (always existing) and the client (only existing when client
authentication is used). This can be used to import the certificates
into CGI scripts.
o StdEnvVars:
This exports the standard SSL/TLS related `SSL_*' environment variables.
Per default this exportation is switched off for performance reasons,
because the extraction step is an expensive operation and is usually
useless for serving static content. So one usually enables the
exportation for CGI and SSI requests only.
o StrictRequire:
This denies access when "SSLRequireSSL" or "SSLRequire" applied even
under a "Satisfy any" situation, i.e. when it applies access is denied
and no other module can change it.
o OptRenegotiate:
This enables optimized SSL connection renegotiation handling when SSL
directives are used in per-directory context.
#SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
<FilesMatch "\.(cgi|shtml|phtml|php)$">
 SSLOptions +StdEnvVars
</FilesMatch>
<Directory "/opt/apache/cgi-bin">
 SSLOptions +StdEnvVars
</Directory>

SSL Protocol Adjustments:
The safe and default but still SSL/TLS standard compliant shutdown
approach is that mod_ssl sends the close notify alert but doesn't wait for
the close notify alert from client. When you need a different shutdown
approach you can use one of the following variables:
o ssl-unclean-shutdown:
This forces an unclean shutdown when the connection is closed, i.e. no
SSL close notify alert is send or allowed to received. This violates
the SSL/TLS standard but is needed for some brain-dead browsers. Use
this when you receive I/O errors because of the standard approach where
mod_ssl sends the close notify alert.
o ssl-accurate-shutdown:
This forces an accurate shutdown when the connection is closed, i.e. a
SSL close notify alert is send and mod_ssl waits for the close notify
alert of the client. This is 100% SSL/TLS standard compliant, but in
practice often causes hanging connections with brain-dead browsers. Use
this only for browsers where you know that their SSL implementation
works correctly.
Notice: Most problems of broken clients are also related to the HTTP

```

```

keep-alive facility, so you usually additionally want to disable
keep-alive for those clients, too. Use variable "nokeepalive" for this.
Similarly, one has to force some clients to use HTTP/1.0 to workaround
their broken HTTP/1.1 implementation. Use variables "downgrade-1.0" and
"force-response-1.0" for this.
BrowserMatch ".*MSIE.*" \
 nokeepalive ssl-unclean-shutdown \
 downgrade-1.0 force-response-1.0

Per-Server Logging:
The home of a custom SSL log file. Use this when you want a
compact non-error SSL logfile on a virtual host basis.
CustomLog "/opt/apache/logs/ssl_request_log" \
 "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>

```

## Advanced Configuration for NetBackup Discovery

This section covers the following topics:

- [Discovery Module Overview](#)
- [Activate a Discovery License](#)
- [Modify Discovery System Parameters](#)
- [Why Enable SNMP?](#)

### Discovery Module Overview

---

The Discovery module, specific to Veritas NetBackup, uses discovery policies to illuminate risk and exposure within the corporate IT backup and recovery environment. Three different Discovery types can be configured to collect additional NetBackup data. See the *APTARE Data Collector Installation Guide for Backup Manager* for details.

#### Client Drive Discovery

- *This feature requires a Discovery license and SNMP.* This discovery process seeks out hosts and devices in your environment. The process identifies all hosts in your environment, in particular those that are not currently stored in the reporting database and are therefore potentially not being backed up. This probe uses SNMP to probe the IP address range for drive utilization; therefore, SNMP must be enabled.

#### Media Server Disk Discovery

- This discovery process probes all the media servers associated with the management server to gather disk-based information such as capacity and free space on the media server file systems. This information is then displayed in the *Disk Usage and Performance* report. If the Media Server Disk Discovery process is not enabled, disk-based information will show as **Unknown** in reports. If you have several master servers in your environment, and they have media servers and disk storage units attached to them, you must enable the Media Server Disk Discovery module on each of the master servers.

#### Backup Policy Coverage

- *This feature requires a Discovery license and SNMP.* This discovery process, probes all the NetBackup clients known to the NetBackup database that are associated with the management server. It queries NetBackup to discover if there are backup policies that cover the client. A client is determined to be associated with the NetBackup management server if it belongs to a policy associated with the management server. This probe uses SNMP to probe for drive utilization; therefore, SNMP must be enabled.

# Activate a Discovery License

---

You need to activate your Discovery license so that you can access the additional discovery features beyond the Media Server Disk Discovery component.

A Discovery license is required for the following Discovery types:

- Client Drive Discovery
- Backup Policy Coverage

## To activate the Discovery license:

1. Go to the utilities directory.

**Linux:** /opt/aptare/Utils

**Windows:** C:\opt\aptare\utils

2. Run the following license utilities to view the status of your current license or to install your updated license.

### Linux:

```
./printLicense.sh
./installLicense.sh
```

### Windows:

```
printlicense.bat
installlicense.bat
```

# Modify Discovery System Parameters

---

Many of the default settings for discovery processes are maintained in the Reporting Database. Occasionally, you might need to adjust some of the default settings. For example, if you want to adjust the default timeout values used for the various probes, you need to edit the default settings. You can update these settings by loading a new set of settings from an XML file that you maintain on the Portal Server.

Each host group folder that a master server references, using the `ServerGroupId` parameter in the `bnrtriggerconfig.xml` file on the master server, has its own set of configuration parameters. Therefore to change the settings for a Data Collector running on a master server, you must first find the value of the `ServerGroupId` parameter.

This procedure assumes that the `ServerGroupId` value is 300000, and the Portal Server is installed on a Linux system. However, for Windows installations, simply replace the forward slashes with backslashes and the `.sh` with `.bat`.

## To modify discovery system parameters

1. On the Portal Server, make a copy of the default discovery settings file.

```
cd /opt/aptare/utlis
cp DiscoverProperties.xml DiscoverProperties_new.xml
```

2. In the new discovery settings file, change `public` to your SNMP community string value:

```
vi DiscoverProperties_new.xml
```

3. Save and close the file.
4. Go to the `utlis` directory:

```
cd /opt/aptare/utlis
```

5. From the `utlis` directory and to load the new configuration settings into the Reporting Database for the appropriate `ServerGroupId`, type the following line as one continuous line:

```
./updDiscoverProperties.sh 300000 ../portalconf\
systemlogger.xml DiscoverProperties.xml
```

The configuration will always load from: `/opt/aptare/portalconf/portal.properties`

## Why Enable SNMP?

---

**Note:** The information contained in this section is intended for the administration of Discovery functionality. APTARE provides this SNMP configuration guidance for informational purposes only. APTARE Global Support Services will not provide assistance with the installation, configuration, and troubleshooting of SNMP subsystems on your Master Servers.

The Simple Network Management Protocol (SNMP) is an Internet standard that provides a common way to query, monitor, and manage devices connected to IP networks. The protocol is defined in RFC 2571. For additional information, see <http://www.ietf.org/rfc/rfc2571.txt>.

To capture filesystem level information on your media servers and any other servers in your environment, you must enable SNMP.

Using SNMP v2c messaging, Discovery queries all media servers and other servers or devices and retrieves information about the physical attributes of their configured storage units and file systems. The SNMP probe uses UDP and the standard SNMP Port 161 by default.

There are different SNMP probes for different operating systems. The way that you enable and configure SNMP services on your servers to take advantage of these probes depends on your operating system.

- Windows
- Red Hat Linux
- HP-UX
- Solaris 8/9
- Solaris 10

## About SNMP Probes

---

To take full advantage of the Discovery functionality, the SNMP subsystem must be configured to respond to the following probes:

### First Probe (sysObjectOID)

This probe is sysObjectOID (.1.3.6.1.2.1.1.2). This probe returns an OID that conforms to the enterprise OIDs allocated by the Internet Assigned Numbers Authority. Be aware that the SNMP agent resident on the device returns this number, and this number might not be the same number as the hardware manufacturer. For example an HP N-class server may return the enterprise OID of 1.3.6.1.4.1.11 or 1.3.6.1.4.1.2021.250.14 depending on whether the SNMP agent is provided by HP or is the open source NET-SNMP package. The number returned is matched against a lookup table to try and determine the company value of the OID. (For example, IBM or Sun).

### Second Probe (sysDescr OID)

This probe is made for the sysDescr OID (.1.3.6.1.2.1.1.1). This probe returns a description of the device or agent. This string is matched against a lookup table to try and determine the system description value. (For example, Windows 2000 or Solaris).

Lastly, if configured, a query is made against the Device and Storage section of the Host Resources Management Information Block (MIB). Specific information retrieved is the file system mount point, storage type, storage description, allocation units, size in storage units, and storage units used. Before this information is returned, calculations are made to convert the values into kilobytes. Only fixed disk storage units are returned.

## Enabling SNMP for Windows (NT/2000/XP)

---

This procedure assumes that you have Windows 2000/XP. However, the process is very similar on Windows NT. For more information about setting up SNMP on Windows, go to the following Microsoft articles:

- *How To Configure Security for a Simple Network Management Protocol Service in Windows 2000* (<http://support.microsoft.com/default.aspx?scid=KB;EN-US;q315154>)
- *SNMP Storage Information Is Not Updated Dynamically* (<http://support.microsoft.com/kb/q295587/>)
- *Management information base support in Windows 2000, Windows XP, Windows Server 2003, and Windows Vista* (<http://support.microsoft.com/kb/q237295/>)



To install the SNMP on Windows 2000/XP:

You might need to install the CD for your operating system, so have the recovery CD available.

1. Click **Start > Settings > Control Panel**.
2. Double-click **Add/Remove Programs**.
3. Click **Add/Remove Windows Components**.
4. Click **Management and Monitoring Tools** and click **Details**.  
The Management and Monitoring Tools window appears.
5. Select **Simple Network Management Protocol** check box and click **OK**.
6. Click **Next** to initiate the installation.
7. After the installation completes and from the Control Panel, double-click on **Administrative Tools**.
8. Double-click on **Computer Management**.
9. In the navigation tree on the left, expand Services and Applications, then click on **Services**.
10. In the Services contextual frame, scroll down to SNMP Service, then double-click **SNMP Service**.
11. In the General tab, select **Automatic** for Startup Type.
12. In the Security tab, do one of the following:
  - Leave the default community name public.
  - To improve security, choose your own name. Click on Add... for accepted community names, leave Community Rights as Read-Only, pick a secure Community Name, and click on OK. Remove the public entry. Modify the default Discovery properties configuration file to match this value.
13. In the Security tab, choose which IP addresses can access the SNMP service. You must choose at least the IP address of the Master Server that runs APTARE IT Analytics.
14. In the Agent tab, specify the values for all fields, and select the Internet check box to make all SNMP values available.

## Enabling SNMP for Red Hat Linux

---

Red Hat Linux has an SNMP agent, ucd-snmp, preinstalled. Ucd-snmp is the pre-cursor to net-snmp. You need to configure the ucd-snmp agent to return the host resource information and to ensure that it executes at system startup. This procedure provides the steps for enabling SNMP in a Red Hat Linux environment.

To enable SNMP for Red Hat Linux:

1. Locate the SNMPD configuration file in `/etc/snmp/snmpd.conf` and the executable at `/usr/sbin/snmpd`.
2. Configure the SNMP agent as shown in the following example, which shows read-only access to the system and host resource storage portions of the MIB.

```
####
First, map the community name "public" into a "security name"
sec.name source community
com2sec notConfigUser default public
####
Second, map the security name into a group name:
```

```
groupName securityModel securityName
group notConfigGroup v1 notConfigUser
group notConfigGroup v2c notConfigUser
####
Third, create a view for us to let the group have rights to:
name incl/excl subtree mask(optional)
#view systemview included .1
view APTARE IT Analytics included
.iso.org.dod.internet.mgmt.mib-2.system fe
view APTARE IT Analytics included
.iso.org.dod.internet.mgmt.mib-2.host.hrStorage ff
view APTARE IT Analytics included
.iso.org.dod.internet.mgmt.mib-2.host.hrDevice ff
.iso.org.dod.internet.mgmt.mib-2.system = .1.3.6.1.2.1.1
.iso.org.dod.internet.mgmt.mib-2.host.hrStorage = .1.3.6.1.2.1.25.2
####
Finally, grant read-only access to the system and storage portions of
the MIB2 tree
group context sec.model sec.level prefix read write
notif
#access notConfigGroup "" any noauth exact systemview none
none
access notConfigGroup "" any noauth exact APTARE IT Analytics
none none
```

## Enabling SNMP for HP-UX

---

Although HP-UX 11.00 has an SNMP agent installed, it does not provide access to the Host Resource MIB, so Discovery cannot use this agent to find storage units. However, net-snmp is supported on HP-UX 10.20, 11.00 and 11.11.

To install and configure SNMP for HP-UX 11.00:

1. Read the Net-SNMP HP-UX README.
2. Download and the net-snmp binaries
3. Install the net-snmp binaries. For an example, go to [Example—Installing Net-SNMP](#).

## Enabling SNMP for Solaris 8/9

---

The Solstice Enterprise Agent does not support the Host Resource MIB, so Discovery cannot use this agent to find storage units. However, net-snmp is supported on Solaris 5.6, 5.7, 5.8, and 5.9.

To install and configure SNMP for Solaris:

1. Read the Net-SNMP Solaris README.

2. Download and the net-snmp binaries. For an example, go to [Example—Installing Net-SNMP](#).
3. Install the net-snmp binaries. For an example, go to [Example—Installing Net-SNMP](#).

## Enabling SNMP for Solaris 10

---

The Solaris System Management Agent (SMA) is an SNMP agent that Sun Microsystems offers, and it is based on the Net-SNMP open source implementation version 5.0.9.

To install and configure SNMP for Solaris 10:

1. Install the SMA packages just as you would install bundled products as outlined in the *Solaris 10 Installation Guide: Basic Installations* and in the *Solaris 10 Installation Guide: Custom JumpStart and Advanced Installations*.
2. Configure the SMA agent as outlined in the *Solaris System Management Agent Administration Guide*.

## Troubleshooting

If you have problems installing and configuring SMA, go to SunSolve.

## Example—Installing Net-SNMP

---

Net-SNMP is an open source implementation of the Simple Network Management Protocol.

Net-SNMP provides an extensible agent for responding to SNMP queries for management information, and this functionality is important to the Media Discovery module Net-SNMP includes built-in support for a wide range of MIB information modules, specifically the Host Resource MIB. Net-SNMP is available for many Linux and Linux-like operating systems and also for Microsoft Windows, though functionality can vary depending on the operating system.

To install net-snmp:

1. Download and install Perl 5.6 or above, if the package is not already installed.
2. Install net-snmp as outlined in the following example:

```
/usr/local/bin/snmpconf -g basic_setup
*** Beginning basic system information setup ***
Do you want to configure the information returned in the system MIB group
(contact info, etc)? (default = y): no
Do you want to properly set the value of the sysServices.0 OID (if you don't know, just
say no)? (default = y): no
*** BEGINNING ACCESS CONTROL SETUP ***
Do you want to configure the agent's access control? (default = y):
Do you want to allow SNMPv3 read-write user based access (default = y): no
Do you want to allow SNMPv3 read-only user based access (default = y): no
Do you want to allow SNMPv1/v2c read-write community access (default = y): no
Do you want to allow SNMPv1/v2c read-only community access (default = y): yes
Configuring: rocommunity
```

Description:

a SNMPv1/SNMPv2c read-only access community name arguments: community [default|hostname|network/bits] [oid]

The community name to add read-only access for: public

The hostname or network address to accept this community name from [RETURN for all]:

The OID that this community should be restricted to [RETURN for norestriction]:

Finished Output: rocommunity public

Do another rocommunity line? (default = y): no

\*\*\* Beginning trap destination setup \*\*\*

Do you want to configure where and if the agent will send traps? (default= y): no

\*\*\* Beginning monitoring setup \*\*\*

Do you want to configure the agent's ability to monitor various aspects of your system? (default = y): no

The following files were created:

snmpd.conf

3. Move the **snpd.conf** file to one of the following locations:

- If you want this file used by everyone on the system, moved the file to **/usr/local/share/snmp**. Next time, use the **-i** option if you want the command to copy the files to that location automatically.
- If you want the file for your personal use only, copy the file to your HOME directory. Next time, use the **-p** option if you want the command to copy the file to that location automatically.

4. Ensure that user **root** starts the snmpd executable that is located in **/usr/local/sbin/snmpd**.

## Troubleshooting Net-SNMP Installations

---

The **/usr/local/bin/snmpconf** file requires Perl v5.6 and above.

Replace the line:

```
#!/usr/local/bin/perl
```

in **/usr/local/bin/snmpconf** to reference your Perl installation:

If your version of Perl is 5.0 or before then you might receive a runtime error when the **snmpconf** file executes. To correct this problem, edit the **snmpconf** file and make the following changes:

```
#!/usr/local/bin/perl
- if (! (-d "$opts{'I'}") && ! (mkdir ("$opts{'I'}"))) {
+ if (! (-d "$opts{'I'}") && ! (mkdir ("$opts{'I'}", 0755))) {
print "\nCould not create $opts{'I'} directory: $!\n";
print ("File $didfile{$i} left in current directory\n");
}
@@ -198,7 +198,7 @@
}
}
} elsif ($opts{'p'}) {
- if (! (-d "$home") && ! (mkdir ("$home"))) {
+ if (! (-d "$home") && ! (mkdir ("$home", 0755))) {
print "\nCould not create $home directory: $!\n";
```

```
print ("File $didfile{$i} left in current directory\n");
```

---

## Data Retention Periods for SDK Database Objects

This section covers the procedure for modifying data retention periods for systems collected by Data Collectors deployed via the SDK.

Because data collection continuously adds data to the database, management of the database size becomes an essential task. **For objects created via the SDK**, a data retention period can be defined along with the database schema, to align with your IT Analytics reporting requirements. Data retention (purging rules) described in this section apply only to user-defined objects defined by an SDK project; API and database objects are handled by system parameters.

Purging rules (data retention periods) are specific to an object, such as array disk performance, and they are used to maintain corresponding database tables. These rules are configured at the beginning of the object's definition in the schema template json file.

**Best Practice:** Configure retention days for objects that accumulate historical data over time, such as array performance. Other objects should not have data retention days.

In multi-tenancy environments, where IT Analytics domains partition client data, data retention periods can be configured for each domain. The data retention period for a domain applies to that domain and all of its sub-domains. For systems collected by traditional Data Collectors, use the **Data Retention** tab located:

**Admin>Advanced>System Configuration.**

To enable purging for a user-defined object for a specific domain, take the following steps.

1. Log in to the Portal Server as user aptare.
2. Type the following command:  

```
sqlplus <portal_user>/<portal_password>
```

where <portal\_user> and <portal\_password> are portal credentials to connect to the database.
3. At the command line, execute the following SQL statement, substituting relevant values for the variables shown <> in the syntax. See also, [Find the Domain ID and Database Table Names, Retention Period Update for Multi-Tenancy Environments Example](#), and [Retention Period Update for SDK User-Defined Objects Example](#).

```
INSERT INTO apt_purge_rules (table_name, product_type, table_description,
date_column_name, retention_days, default_retention_days, domain_id, creation_date,
last_updated)
SELECT table_name, product_type, table_description, date_column_name, <NewRetentionDays>,
default_retention_days, <domain_id_value>, SYSDATE, SYSDATE
FROM apt_purge_rules
WHERE domain_id IS NULL
AND table_name = <tableName>;
Commit;
```

## Find the Domain ID and Database Table Names

<domain_id_value>	Most environments have only one Domain ID; however, multi-tenancy environments, such as Managed Service Providers (MSPs), will have a different Domain ID for each of their customers.  To list the currently configured Domain IDs, use the following SQL SELECT statement: <b>SQL&gt; SELECT * from apt_domain;</b>
<tableName>	Find the relevant database table name for the retention period you want to change <a href="#">SDK User-Defined Database Objects</a> .

## Retention Period Update for SDK User-Defined Objects Example

The following example illustrates an update for a Pure Storage performance database table.

```
INSERT INTO apt_purge_rules (table_name, product_type, table_description,
date_column_name, retention_days, default_retention_days, domain_id, creation_date,
last_updated)
SELECT table_name, product_type, table_description, date_column_name, 50,
default_retention_days, 100007, SYSDATE, SYSDATE
FROM apt_purge_rules
WHERE domain_id IS NULL
AND table_name = 'SDK_PURE_STORAGEARRAY_PERF';
Commit;
```

## SDK User-Defined Database Objects

The data retention period for various database tables often can be modified to maintain reasonable table sizes. Data retention periods can be modified for historical and performance data. Reference the following sections for details:

- [Capacity: Default Retention for Basic Database Tables](#)
- [Capacity: Default Retention for EMC Symmetrix Enhanced Performance](#)
- [Capacity: Default Retention for EMC XtremIO](#)
- [Capacity: Default Retention for Dell EMC Elastic Cloud Storage \(ECS\)](#)
- [Capacity: Default Retention for Microsoft Windows File Services](#)
- [Capacity: Default Retention for Pure Storage FlashArray](#)
- [Cloud: Default Retention for Amazon Web Services \(AWS\)](#)
- [Cloud: Default Retention for Microsoft Azure](#)
- [Cloud: Default Retention for OpenStack Ceilometer](#)

## Capacity: Default Retention for Basic Database Tables

Table Description	Table Name	Default Retention	Notes
File system log	aps_file_system_log	6 months	KEEP_FILE_SYSTEM_LOG_MONTHS

LUN performance log	apt_lun_perform_log	504 hours	KEEP_LUN_RAW_PERFORM_HOURS
Array group log	aps_array_group_log	12 months	KEEP_ARRAY_GROUP_LOG_MONTHS
Array port statistics log	aps_array_port_stats_log	1 day	KEEP_ARRAY_PORT_STAT_LOG_DAYS
Array port statistics daily log	aps_array_port_stats_daily_log	2 months	KEEP_ARRAY_PORT_STAT_DAILY_LOG_MONTHS
Capacity chargeback log	aps_chargeback_log	24 months	KEEP_SRM_CHARGEBACK_LOG_MONTHS
Host processing log	apt_host_process_log	15	KEEP_HOST_PROCESS_LOG_DAYS



## Capacity: Default Retention for EMC Symmetrix Enhanced Performance

Table Description	Table Name	Default Retention	Notes
Array Performance	sdk_esym_array_perf	21 days	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a> .
Back-end Director Performance	sdk_esym_be_director_perf	21 days	
Database Performance	sdk_esym_database_perf	21 days	
Device Group Performance	sdk_esym_device_group_perf	21 days	
Disk Group Performance	sdk_esym_disk_group_perf	21 days	
Disk Performance	sdk_esym_disk_perf	21 days	
Disk Tech Pool Performance	sdk_esym_disk_tchpool_perf	21 days	
Front-end Director Performance	sdk_esym_fe_director_perf	21 days	
Front-end Port Performance	sdk_esym_fe_port_perf	21 days	
Storage Group Performance	sdk_esym_storage_grp_perf	21 days	
Storage Tier Performance	sdk_esym_storage_tier_perf	21 days	
Thin Pool Performance	sdk_esym_thin_pool_perf	21 days	
Thin Tier Performance	sdk_esym_thin_tier_perf	21 days	
Array's Cache Usage Performance	sdk_esym_array_cache_usage	21 days	

## Capacity: Default Retention for EMC XtremIO

---

Table Description	Table Name	Default Retention	Notes
XtremIO Data Reduction Rate	sdk_exio_datareductionrate	15	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a> .

## Capacity: Default Retention for Dell EMC Elastic Cloud Storage (ECS)

---

Table Description	Table Name	Default Retention	Notes
ECS Storage Array Performance	sdk_decs_ecsstg_ary_stats	21	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a>
ECS Replication Group Performance	sdk_decs_ecsrep_grp_stats	21	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a>
ECS Node Performance	sdk_decs_ecsnode_stats	21	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a>
ECS Node's Disk Performance	sdk_decs_ecsnodedisk_stats	21	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a>
ECS Storage Pools Performance	sdk_decs_ecsstg_pls_stats	21	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a>

## Capacity: Default Retention for Microsoft Windows File Services

Table Description	Table Name	Default Retention	Notes
History and Performance Table for Windows File Systems	sdk_msws_filesystem_perf	21 months	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a> .
History and Performance Table for Windows Cifs Shares	sdk_msws_cifsshare_perf	21 months	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a> .
History and Performance Table for Windows NFS Server	sdk_msws_nfs_statistics	21 months	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a> .
History and Performance Table for Windows Event Log Details	sdk_msws_eventlog_details	30 months	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a> .

## Capacity: Default Retention for Pure Storage FlashArray

Table Description	Table Name	Default Retention	Notes
Array Performance	sdk_pure_storagearray_perf	21 days	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a> .

## Cloud: Default Retention for Amazon Web Services (AWS)

Table Description	Table Name	Default Retention	Notes
Billing Record Tag	sdk_aws_billing_rec_tag	366 days	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a> .
Mapping from any resource ID or name to one of many different entities (or none at all)	sdk_aws_resource_map	999999 days	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a> .
S3 bucket usage	sdk_aws_s3_bucket_usage	999999 days	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a> .

Billing Record	sdk_aws_billing_record	367 days	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a> . Note: The retention period for the billing record data must be one day more than the billing record tag data to ensure that the dependent tag data is removed before purging the billing record.
----------------	------------------------	----------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Cloud: Default Retention for Microsoft Azure

---

Table Description	Table Name	Default Retention	Notes
Resource Mapping from any resource ID or name to one of many different entities (Virtual Machines or Storage Accounts)	sdk_msaz_resourcemap	999999 days	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a> .

## Cloud: Default Retention for OpenStack Ceilometer

---

Table Description	Table Name	Default Retention	Notes
Instance Metrics	sdk_oscm_instance_metrics	15	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a> .
Network Metrics	sdk_oscm_network_metrics	15	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a> .
Disk Metrics	sdk_oscm_disk_metrics	15	To modify the retention period, see <a href="#">Data Retention Periods for SDK Database Objects</a> .

## Configure Multi-Tenancy Data Purging Retention Periods

---

In multi-tenancy environments, where APTARE IT Analytics domains partition client data, data retention periods can be configured for each domain. The data retention period for a domain applies to that domain and all of its sub-domains. For systems collected by traditional Data Collectors, use the procedure described in: [System Configuration: Functions](#). This is modified through the System Configuration section in the Portal.

To enable purging for a user-defined object for a specific domain, take the following steps.

1. Log in to the Portal Server as user aptare.
2. Type the following command:  
`sqlplus portal/<portal_password>`
3. At the command line, execute the following SQL statement, substituting relevant values for the variables shown <> in the syntax. See also, [Find the Domain ID and Database Table Names](#) and [Retention Period Update for Multi-Tenancy Environments Example](#).

```
INSERT INTO apt_purge_rules (table_name, product_type, table_description,
date_column_name, retention_days, default_retention_days, domain_id, creation_date,
last_updated)
SELECT table_name, product_type, table_description, date_column_name, <NewRetentionDays>,
default_retention_days, <domain_id_value>, SYSDATE, SYSDATE
FROM apt_purge_rules
WHERE domain_id IS NULL
AND table_name = <tableName>;
Commit;
```

## Find the Domain ID and Database Table Names

<domain_id_value>	<p>Most environments have only one Domain ID; however, multi-tenancy environments, such as Managed Service Providers (MSPs), will have a different Domain ID for each of their customers.</p> <p>To list the currently configured Domain IDs, use the following SQL SELECT statement:</p> <p><b>SQL&gt; SELECT * from apt_domain;</b></p>
<tableName>	<p>Find the relevant database table name for the retention period you want to change in <a href="#">SDK User-Defined Database Objects</a>.</p>

## Retention Period Update for Multi-Tenancy Environments Example

The following example illustrates an update for a Pure Storage performance database table.

```
INSERT INTO apt_purge_rules (table_name, product_type, table_description,
date_column_name, retention_days, default_retention_days, domain_id, creation_date,
last_updated)
SELECT table_name, product_type, table_description, date_column_name, 50,
default_retention_days, 100007, SYSDATE, SYSDATE
FROM apt_purge_rules
WHERE domain_id IS NULL
AND table_name = 'SDK_PURE_STORAGEARRAY_PERF';
Commit;
```

# 22

## Troubleshooting

This section covers the following topics:

- [Troubleshooting User Login Problems](#)
- [Forgotten Password Procedure](#)
- [Connectivity Issues](#)
- [Data Collector and Database Issues](#)
  - [Data Collector: Changing the Name and Passcode](#)
  - [Insufficient Privileges](#)
  - [Remove an Inactive Hitachi Array from the Database](#)
  - [Report Emails are not Being Sent](#)
- [General Reporting Issues](#)
- [Performance Issues](#)

### Troubleshooting User Login Problems

---

To troubleshoot LDAP/login issues, use the `findUser` tool.

1. Launch the tool's usage instructions.

**Linux:**

```
cd /opt/aptare/utils/
./findUser.sh
```

**Windows:**

```
C:\opt\aptare\utils\finduser.bat
```

2. Use any of the following commands:

Add User	<b>Linux:</b> <code>./addUser.sh &lt;userId&gt; &lt;lastName&gt; &lt;password&gt; &lt;restoreWizPassword&gt;</code>
	<b>Windows:</b> <code>adduser.bat &lt;userId&gt; &lt;lastName&gt; &lt;password&gt; &lt;restoreWizPassword&gt;</code>
Delete User	<b>Linux:</b> <code>./delUser.sh &lt;userId&gt;</code>
	<b>Windows:</b> <code>deluser.bat &lt;userId&gt;</code>

<b>Find User</b>	<b>Linux:</b> <code>./findUser.sh &lt;userId&gt;</code> <b>Windows:</b> <code>finduser.bat &lt;userId&gt;</code>
<b>Modify User</b>	<b>Linux:</b> <code>./updateUser.sh &lt;currentUserId&gt; &lt;modUserId&gt; &lt;modLastName&gt; &lt;modPassword&gt; &lt;modRestoreWizPassword&gt;</code> <b>Windows:</b> <code>updateuser.bat &lt;currentUserId&gt; &lt;modUserId&gt; &lt;modLastName&gt; &lt;modPassword&gt; &lt;modRestoreWizPassword&gt;</code> See <a href="#">Forgotten Password Procedure</a> .

## Forgotten Password Procedure

---

If a user forgets a user ID or password, they can be reset using the following command, run with root/administrator privileges:

### Linux:

```
cd /opt/aptare/utils
./updateUser.sh <currentUserId> <modLastName> <modPassword> <modRestoreWizPassword>
```

### Windows:

```
C:\opt\aptare\utils
updateuser.bat <currentUserId> <modLastName> <modPassword> <modRestoreWizPassword>
```

For example:

```
./updateUser.sh admin@domain.com adminguy@domain.com Administrator newpwd newrestpwd
```

## Login

---

### Portal Login Errors

- File system is out of disk space.
- Fully qualified URL incorrectly set up
- URL not in the local hosts file or in DNS.
- Domain incorrectly specified
- Values in Tomcat Application Server and Apache Web Server do not match what's in DNS.

### Cannot Log On To Portal

When a user can't log in to the Portal, the reasons are usually one of the following:

- User forgot password. Change the user's password. See [Setting/Resetting Passwords](#).
- LDAP service is not running.
- There is a port conflict. Another program is listening on port 80, resulting in a port conflict. Apache Web Server needs port 80. Use the `netstat` command to determine the other application that's listening on port 80, then assign that application a different port.

### Troubleshooting Recommendations

The following list suggests actions you can take to determine what is causing the issue.

- Review the portal log file: `/opt/tomcat/logs/portal.log`. Check for "Exception" or "ERROR."



## Database Tools

C:\opt\oracle\database\tools  
/home/oracle/database/tools

## Telnet

- Use port 80 to test connectivity to web server.
- Use port 25 to test connectivity to email server.

## Connectivity Issues

---

### No Connectivity

A number of conditions can disrupt connectivity, including:

- Firewall issues can prevent connectivity.
- A network change occurred. Typically a DNS, system domain, or hostname change is the culprit.
- Oracle service is not running.
- LDAP service is not running.
- Network timeouts

### Troubleshooting Recommendations

The following list suggests actions you can take to determine what is causing the issue.

- Ping **aptareagent.mydomain.com** from the master server.
- Check if you can connect to **aptareagent.mydomain.com** telnet port 80.

## Data Collector and Database Issues

---

### Data Collector: Changing the Name and Passcode

The Data Collector uses a name and a passcode to identify itself with the Data Receiver. If this name or passcode is changed on the Portal, it needs to be changed on the Data Collector side.

To find and update name and passcode information on the Data Collector server, follow these steps:

#### On a Windows Data Collector Server

1. Edit the following file:

`$APTARE_HOME/mbs/conf/wrapper.conf`

by modifying the following entries accordingly:

```
wrapper.app.parameter.2="$COLLECTOR_NAME$"
wrapper.app.parameter.3="$COLLECTOR_PASSWORD$"
```

2. Edit the following file:

`$APTARE_HOME/mbs/bin/updateconfig.bat`

to modify the name and passcode. They are the two parameters immediately following "com.storage.mbs.watchdog.ConfigFileMonitorThread".

## On a Linux Data Collector Server

1. Edit the following files:

```
$APTARE_HOME/mbs/bin/updateconfig.sh
```

```
$APTARE_HOME/mbs/bin/startup.sh
```

- The name and the passcode will be passed as program arguments to the Java program in the above two scripts.
- In `updateconfig.sh`, the name and passcode are the two parameters immediately following `"com.storage.mbs.watchdog.ConfigFileMonitorThread"`.
- In `startup.sh`, the name and passcode follow `"com.storage.mbs.watchdog.WatchDog"`.

## Insufficient Privileges

When creating the database, you may get an insufficient privileges message when the Windows user is not local, or is not a member of the `ORA_DBA` group. In this case, you receive an `insufficient privileges` error when you create the database.

## Remove an Inactive Hitachi Array from the Database

In Capacity Manager, if an array has been removed from Hitachi Device Manager (HDvM), it remains in the APTARE IT Analytics database as an inactive array and it will continue to be included in reports. Take the following command-line steps to delete the array.

1. Log in to SQLPlus and set the user to `aptare`.

2. Execute the query:

```
select storage_array_id from aps_storage_array where array_name='<ARRAY NAME>;
```

3. Using the `storage_array_id` from the above query to execute this code:

```
Begin
 srm_common_pkg.deleteStorageArray(<STORAGEARRAYID>);
End;
/
```

4. Verify that the array was deleted successfully using this query (should return 0).

```
select count(*)
FROM aps_storage_array
WHERE storage_array_id = <STORAGEARRAYID>;
```

## Report Emails are not Being Sent

---

If Report Emails are not being sent:

The `SMTP_HOST` value in the **System Configuration** does not have a running mailer.

You can also set the authentication mode under **Admin>Advanced>System Configuration>Portal**.

As shown in the following table, several properties can be customized:

<b>Email SMTP authentication</b>	Set to true to enable email authentication.
<b>Email SMTP host IP address</b>	Make sure this references a running mail server.
<b>Email debug mode</b>	Used for product developers to debug mail transmission issues.
<b>Email enable Transport Layer Security (TLS)</b>	The SMTP Transport Layer Security extension—the encryption and authentication protocol. When a client and server that support TLS talk to each other, they can encrypt the data channel to guard against eavesdroppers.
<b>Email from address</b>	The email address for a reply back.
<b>Email from name</b>	The name associated with the reply back email address.
<b>SMTP User</b>	User name used for authentication on the email server.
<b>SMTP password</b>	Password required by email server.

## Additional Email Troubleshooting Recommendations

To determine what is causing the issue.

- Telnet to port 25 to test connectivity to the email server.

```
Typed text is in bold.
$ telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 www.aptare.com ESMTP Sendmail 8.11.6/8.11.6; Wed, 26 Jan 2008 10:16:10 -0800
hello aptare
250 www.aptare.com Hello localhost.localdomain [127.0.0.1], pleased to meet you
mail from: gthom@aptare.com
250 2.1.0 gthom@aptare.com... Sender ok
rcpt to: gthom@aptare.com
250 2.1.5 gthom@aptare.com... Recipient ok
data
354 Enter mail, end with "." on a line by itself
this is the email body
.
250 2.0.0 j0QIMUQ10566 Message accepted for delivery
$
```

## General Reporting Issues

---

### Reports with Graphs Fail to Load

Certain reports that include graphs may result in a report failing to load due to an “out-of-memory: Java heap space” error. This may occur when generating a report for a large set of data or exporting it to a PDF. For example, the following reports are known to occasionally encounter this condition: Tape Library and Drive Utilization for one year grouped by hours, Job Volume Summary for three years of daily data, and Data Domain Filesystem Capacity & Forecast for two months grouped by hours.

To work around this condition, try these changes in the Report Designer:

- reduce the number of selected objects (for example, servers or arrays)
- limit the time period to a shorter timeframe
- select a less granular “group by” option (for example, *by days* instead of *by hours*)

### Missing backups from clients

- Typically, this is a Data Collector issue.

### Charts Don't Appear

- File system is out of disk space.

# Performance Issues

---

Performance can be impacted by a number of issues. Use the following checklist to help you isolate problems.

- Check the number of backup jobs that have been processed in the last 24-hour period.
- Determine the level of database logging that has been enabled in **scon.log**. If DBG level messages have been enabled, this can negatively impact performance. INFO and WARNING messages have negligible impact.
- Check if anything else is running on the server.
- Note if performance suffers at specific times of the day and determine which processes are running during those times.
- Verify the server's configuration: memory and CPU size
- Check if Oracle has been tuned or if the default file (**initscdb.ora**) is in use.
  - On Windows, by default, Oracle can use only 1 GB of memory. If the system has more memory available, use the /3GB option to tell windows to allocate 2 GB to the Oracle process.
- Determine the top running processes—run **top**.
  - What are the top running processes and what is the average CPU Utilization?
  - Is a lot of Virtual Memory being consumed?
  - Is there a high I/O Wait? (This implies a disk bottleneck.)
  - If oraclescdb is the top running process, using a lot of CPU resources:

Run: **sqlplus portal/portal @/opt/aptare/database/tools/list\_quiery\_by\_pid**

This task will prompt for the process id (pid) and show the query that is running. If you run this several times over the course of 5-10 minutes and it returns the same query, you have a long-running query. Note that this will only work if you use process IDs associated with oraclescb processes.

- Query the report database for long-running jobs.
  - Select from **apt\_query\_execution** table to see what reports have been running and for how long. This will help identify a report that someone may have inadvertently scheduled to run every five minutes.
  - In **/opt/aptare/database/tools**, use other sql queries:

**list\_long\_running\_queries.sql**

**list\_running.sql**

**list\_running\_queries.sql**

**long\_running.sql**

Run the above queries and capture the output to send to the APTARE Global Support Services.