Oracle® Enterprise Manager

System Monitoring Plug-in for Microsoft SQL Server User's Guide

Release 12.1.0.6.0 for Windows

E35211-13

August 2015

ORACLE®

Oracle Enterprise Manager System Monitoring Plug-in for Microsoft SQL Server User's Guide, Release 12.1.0.6.0 for Windows

E35211-13

Contents

Preface

This document provides a description about the Oracle System Monitoring plug-in for Microsoft SQL Server, details on the versions the plug-in supports, prerequisites for installing the plug-in, and step-by-step instructions on how to download, install, verify, and validate the plug-in.

Audience

This document is intended systems and database administrators tasked with monitoring Microsoft SQL Server through Enterprise Manager Cloud Control.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
`http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit
`http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit
`http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Related Documents

For information about the troubleshooting scenarios that you might encounter while working with the System Monitoring plug-ins, see the *Oracle® Enterprise Manager System Monitoring Plug-in Troubleshooting Guide for Third-Party Database Plug-ins*:

`http://docs.oracle.com/cd/E24628_01/em.121/e35212/toc.htm`

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

Convention	Meaning
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's Changed

This table provides a brief overview of the document changes for the latest publication of the *Oracle Enterprise Manager System Monitoring Plug-in Installation Guide for Microsoft SQL Server*:

Part Number	Change Summary
E35211-13	Corrected to the file names of the JDBC files provided. See Added Support for Microsoft SQL Server 2014.
E35211-12	Updated with new features. See What's New in This Release for more information.
	Updated Prerequisites to include new patch requirements.
	Added new content for Adding Targets with EMCLI.
	Updated the Using the Backup and Restore Jobs section.
	Added new content for Deploying Reports After BI Publisher is Configured.
	Updated the Using the Microsoft SQL Server Plug-in Reports section.
	Added new content for Chargeback Functionality.
	Added new content for Compliance Management.
	Added new content for Inventory and Usage Details.

1

Microsoft SQL Server Plug-in Overview and Prerequisites

This chapter describes the system monitoring plug-in for Microsoft SQL Server and provides a list of available features. Review the summary of prerequisites required before configuring Microsoft SQL Server for monitoring by Oracle Enterprise Manager Cloud Control.

The following topics are provided:

- Microsoft SQL Server Plug-in Overview and Feature Summary
- What's New in This Release
- Supported Versions
- Prerequisites
- Downloading the Plug-in
- Deploying the Plug-in
- Upgrading the Plug-in
- Undeploying the Plug-in

1.1 Microsoft SQL Server Plug-in Overview and Feature Summary

The system monitoring plug-in for Microsoft SQL Server extends Oracle Enterprise Manager Cloud Control 12*c* to add support for managing Microsoft SQL Server instances. By deploying the plug-in within your Cloud Control environment, you gain the following management features:

- Monitor SQL Server instances.
- Supports both SQL Authentication and Windows Integrated Authentication.
- Gather configuration data and track configuration changes for SQL Server instances.
- Raise alerts and violations based on thresholds set on monitored metrics and configuration data.
- Provide rich out-of-box reports through Enterprise Manager's BI Publisher reports feature based on the gathered data.
- Support monitoring by a local or remote Windows Agent. Local Windows Agent is an agent running on the same host as the Microsoft SQL Server. Remote Windows Agent is an agent running on a host that is different from the host where SQL Server is running.

- Out-of-the-box monitoring templates for Microsoft SQL Server Cluster monitoring and Microsoft SQL Server AlwaysOn (HADR) monitoring.

- Oracle Enterprise Manager Jobs are made easy-to-access by being accessible from the plug-in's UI. These jobs allow for the following management of Microsoft SQL Server:

  - Backup, restore, schedule, and naming of Microsoft SQL Server database backups.

  - Start, stop, pause, and resume of SQL Server Instances.

  - Killing of sessions that are high in CPU or memory usage.

- Provide chargeback functionality for resource usage metering, consumption reports, and charge plans to define the resources to charge for and their associated rates.

- Provide compliance management to evaluate the compliance of targets and systems.

- Provide inventory and usage details for inventory summaries of your Microsoft SQL Server database.

1.2 What's New in This Release

This release of the Microsoft SQL Server plug-in for Oracle Enterprise Manager Cloud Control 12*c* includes many new features for better visibility into your Microsoft SQL Server environment. Highlighted below are some of the new features included in this release:

- Added Support for Microsoft SQL Server 2014

- Updated User Interface

- Business Intelligence Publisher Reports

- Chargeback Functionality

- SQL Server Compliance Standard

1.2.1 Added Support for Microsoft SQL Server 2014

Microsoft SQL Server plug-in for Oracle Enterprise Manager Cloud Control 12*c* supports a wide range of Microsoft SQL Server versions (Figure 1–1). This plug-in release adds support for the latest version of Microsoft SQL Server - SQL Server 2014. The plug-in supports not only standalone but also the cluster configuration of this version.

This release provides support for JDBC 4.0. The sqljdbc_auth.dll files are now prepackaged with the plug-in.

Figure 1–1   Microsoft SQL Server Database Instances
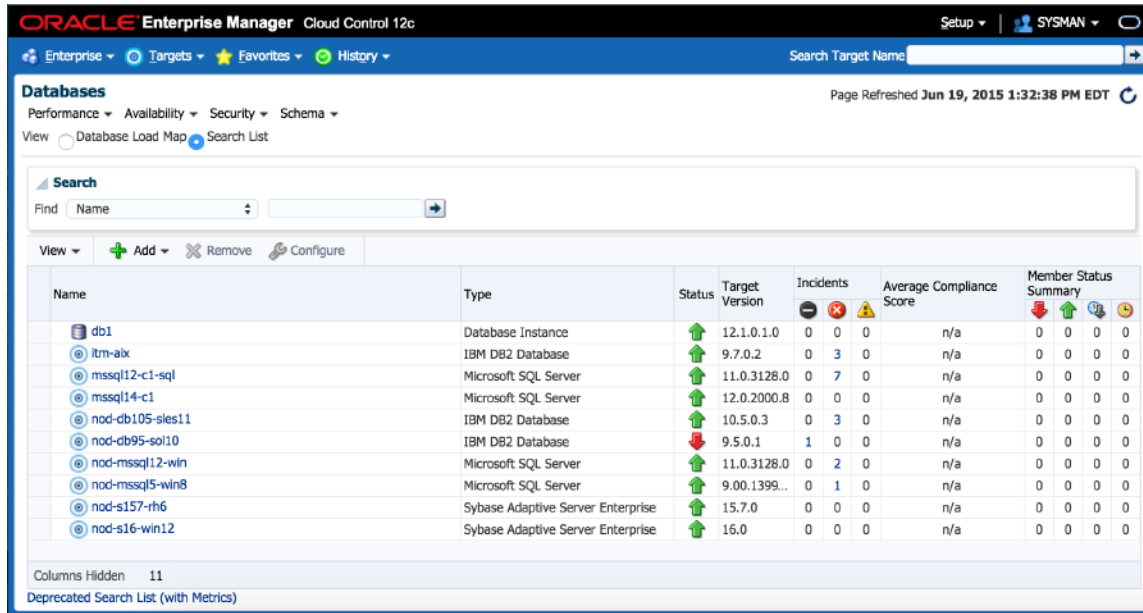
1.2.2 Updated User Interface

The user interface has been updated to add an index page and a new link to the home page.

The home page (Figure 1–2) has been enhanced with the addition of a link in the Summary section to the all new indexes page. This enables quicker navigation throughout the plug-in.

Figure 1–2   Microsoft SQL Server Plug-in Target Home Page
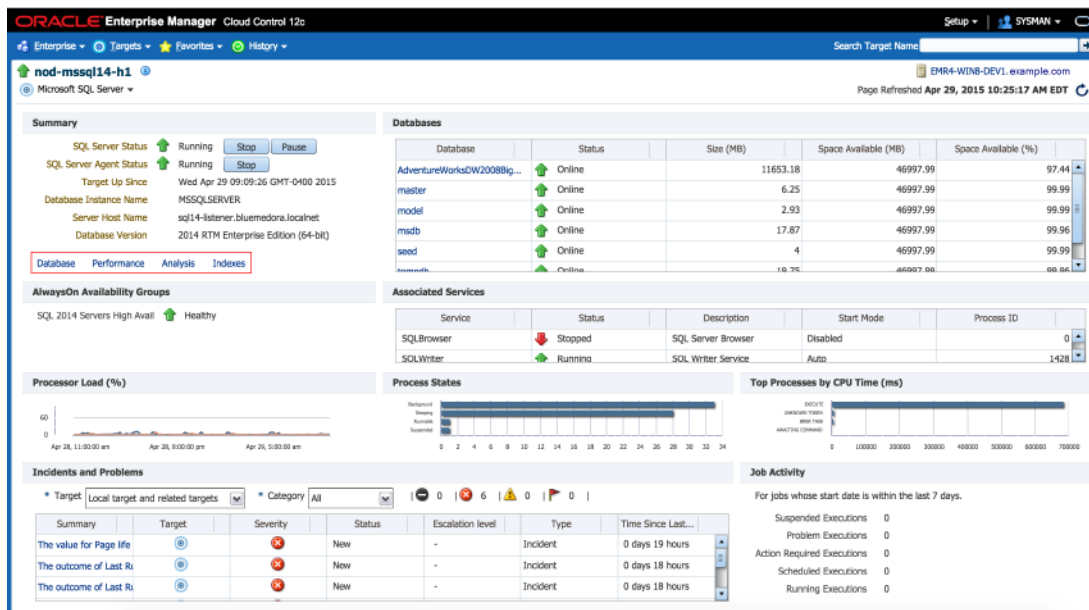
The all-new indexes page (Figure 1–3) has been added to the plug-in to give greater insight into the monitored SQL Server indexes. This includes an indexes by usage

graph and table, index fragmentation table, recommended missing indexes, and a job to create indexes.

Figure 1–3 Microsoft SQL Server Plug-in Indexes Page
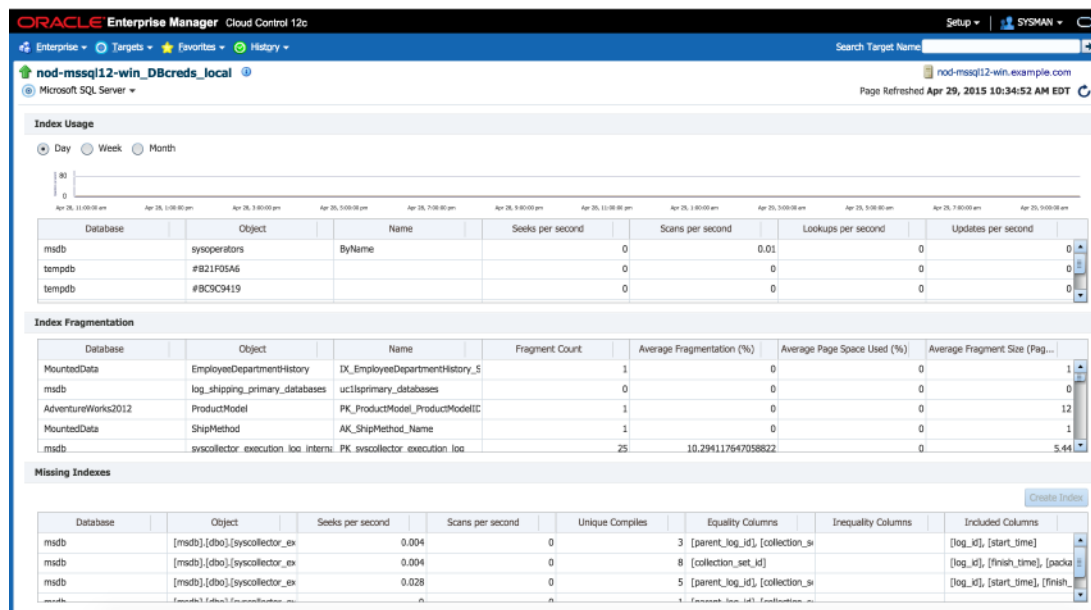
1.2.3 Business Intelligence Publisher Reports

In this release Information Publisher Reports included in the previous release of the MS SQL Server Plug-in have been migrated to BI Publisher Reports. BI Publisher Reports eliminate complexity and simplify report development and maintenance.

See Using Reports and Monitoring Templates for more information on using these reports.

1.2.4 Chargeback Functionality

New to this version is Chargeback functionality (Figure 1–4). Chargeback allows users to gather data on resource use, allocate charges for the use of these resources, and present the results in an intelligible format. Using Chargeback assists consumers in monitoring and controlling their IT costs.

Figure 1–4   Microsoft SQL Server Plug-in Chargeback Funtionality
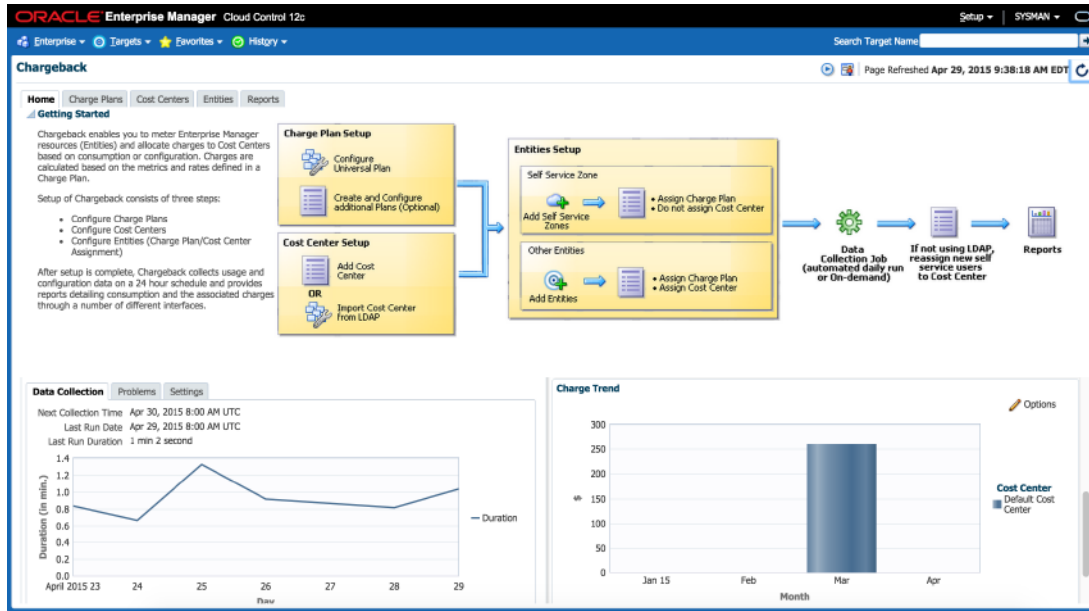
For more information on how to implement Chargeback services, see the *Oracle Enterprise Manager Cloud Administration Guide*:

http://docs.oracle.com/cd/E24628_01/doc.121/e28814/chargeback_cloud_admin.htm#EMCLO917

1.2.5 SQL Server Compliance Standard

Another new feature in this release is the Microsoft SQL Server Compliance Standard (Figure 1–5). Associating a Compliance Standard with targets allows an administrator to track and monitor the adherence of managed targets. This will assist in revealing the least compliant targets, so measures can be taken to correct them.

Figure 1–5   SQL Server Configuration Compliance Standard
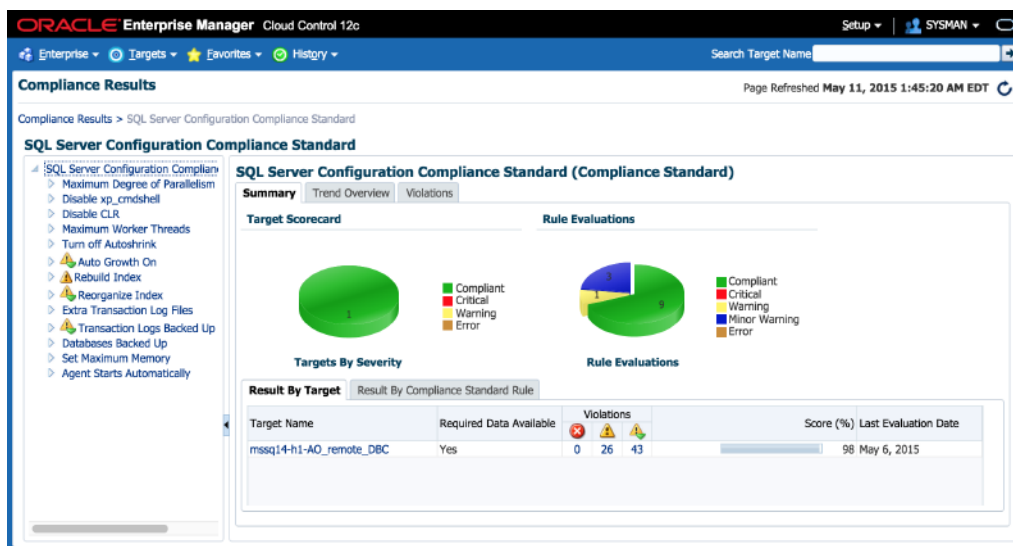
For more information on how to implement Compliance Standards to targets, see the *Oracle Enterprise Manager Cloud Control Oracle Database Compliance Standards Guide*:

http://docs.oracle.com/cd/E24628_01/doc.121/e36074/db_comp_intro.htm#EMDBC108

1.3 Supported Versions

This plug-in supports the following versions of products:

- Enterprise Manager Cloud Control 12*c* Release 4 (12.1.0.4.0) or higher (Oracle Management Server and Oracle Management Agent).

- Standard, Enterprise, and Workgroup editions of Microsoft SQL Server 2005, Microsoft SQL Server 2008, Microsoft SQL Server 2012, and Microsoft SQL Server 2014 as detailed below:

  - Microsoft SQL Server 2005 (32-bit or 64-bit).

  - Microsoft SQL Server 2008 (32-bit or 64-bit).

  - Microsoft SQL Server 2008 R2 (32-bit or 64-bit) including Failover Cluster support.

  - Microsoft SQL Server 2012 (32-bit or 64-bit) including Failover Cluster and AlwaysOn Availability Groups support.

  - Microsoft SQL Server 2014 (32-bit or 64-bit) including Failover Cluster and AlwaysOn Availability Groups support.

Note: Monitoring of Microsoft SQL Server Clusters are only supported with a remote monitoring configuration. The Oracle Management Agent used in monitoring cannot be installed to one of the cluster nodes.

1.4 Prerequisites

The following prerequisites must be met before you can deploy the plug-in. Patches are available from My Oracle Support (https://support.oracle.com):

1. Enterprise Manager Cloud Control 12*c* (Oracle Management Server and Oracle Management Agent) must be installed. Choose from:

   - *Recommended:* Enterprise Manager Cloud Control 12*c* Release 5 (12.1.0.5).

   - Enterprise Manager Cloud Control 12*c* Release 4 (12.1.0.4.0) or higher **and** install Patch 20870437 to upgrade to version 12.1.0.4.4.

     To correct a deployment issue, install system patch 20645335: *On Windows Server OMS side plug-in deployment was stuck at OUI step*.

2. The following patches must be installed:

   - Configuration Management Patch 18140699.

   - Inventory and Usage Patch 20692416.

   - Chargeback Patch:

     - For Enterprise Manager Cloud Control 12*c* Release 5 (12.1.0.5.0), which contains Chargeback plug-in version 12.1.0.7.1, apply patch 21420915: *Enterprise Manager for OMS Plug-ins 12.1.0.5.1*.

     - For Enterprise Manager Cloud Control 12*c* Release 4 (12.1.0.4.0), which contains Chargeback plug-in version 12.1.0.6.2, apply patch 21415432: *Enterprise Manager for OMS Plug-ins 12.1.0.4.14*.

3. The plug-in is only supported when running the Oracle Management Agent on 32-bit or 64-bit Windows.

4. Access privileges required for non-admin System user to perform Remote Monitoring of SQL Server instance.

   For more information, see Configuring Remote Connections to Monitor Targets.

5. Windows Management Instrumentation Service is up and running.

6. Enable TCP/IP for the SQL Server instance. For more information, see Enabling and Finding TCP/IP Port Information.

7. Enable SQL or Mixed Authentication on the SQL Server instance. For more information, Enabling SQL Authentication or Mixed Authentication.

8. Create a suitable DB user with a sysadmin fixed server role. To monitor the SQL Server instance using non-sysadmin user, create a user with non-sysadmin role and provide the following access to it:

   a. Execute this command to give access to the user:

      ```
      GRANT VIEW SERVER STATE TO "login name"
      ```

   b. Provide database access to the user.

   c. Provide SQLAgentOperatorRole fixed database role in msdb to the user.

9. Preferred credentials are set and validated on all Agents where you want to deploy the plug-in.

10. The OS privileges for the user (set in the Preferred Credentials for the Agent) must meet the requirements documented in the "*Setting Credentials for the Job System to Work with Enterprise Manager*" section of the *Oracle Database Installation Guide for Microsoft Windows* available at:

    http://docs.oracle.com/cd/E11882_01/install.112/e24186/postcfg.htm#BABFAEIG

    Note: If you do not assign the correct privileges for users, the deployment will fail.

    ---

11. As part of JDBC URL, either IP Address or host name can be provided. Ensure that the host name can be resolved consistently on the network. Standard TCP tools such as nslookup and traceroute can be used to verify the host name. Validate using the following commands on Management Agent where plug-in is deployed:

    - nslookup <hostname>

      This returns the IP address and fully qualified host name.

    - nslookup <IP>

      This returns the IP address and fully qualified host name.

12. To enable the use of the Backup, Delete Backup, and Restore jobs, the following SQL commands must be processed on the monitored SQL Server database:

    ```
    EXEC sp_configure 'show advanced options', 1
    RECONFIGURE
    EXEC sp_configure 'xp_cmdshell', 1
    RECONFIGURE
    ```

1.5 Downloading the Plug-in

You can download plug-ins in online or offline mode. *Online mode* refers to an environment where you have Internet connectivity, and can download the plug-in directly through Enterprise Manager from My Oracle Support. *Offline mode* refers to an environment where you do not have Internet connectivity, or where the plug-in is not available from My Oracle Support.

See the *Managing Plug-ins* chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for details on downloading the plug-in in either mode:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mngr.htm#CJGBEAHJ

1.6 Deploying the Plug-in

You can deploy the plug-in to an Oracle Management Service instance using the Enterprise Manager Cloud Control console, or using the EM Command Line Interface (EMCLI). While the console enables you to deploy one plug-in at a time, the command line interface mode enables you to deploy multiple plug-ins at a time, thus saving plug-in deployment time and downtime, if applicable.

See the *Managing Plug-ins* chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for instructions on deploying the plug-in:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mngr.htm#CJGCDHFG

1.7 Upgrading the Plug-in

The Self Update feature allows you to expand Enterprise Manager's capabilities by updating Enterprise Manager components whenever new or updated features become available. Updated plug-ins are made available via the Enterprise Manager Store, an external site that is periodically checked by Enterprise Manager Cloud Control to obtain information about updates ready for download. See the *Updating Cloud Control* chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for steps to update the plug-in:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/self_update.htm

1.8 Undeploying the Plug-in

See the *Managing Plug-ins* chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for steps to undeploy the plug-in:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mngr.htm#CJGEFADI

2

Configure Microsoft SQL Server for Authentication

This chapter provides the instructions for configuring Microsoft SQL Server for authentication for access through Oracle Enterprise Manager Cloud Control. Starting first with enabling and finding TCP/IP port information, the chapter ends with a set of authentication configuration scenarios that you can modify for your own environment.

The following topics are provided:

- Enabling and Finding TCP/IP Port Information
- Modifying the Permissions for Database Authentication
- Enabling SQL Authentication or Mixed Authentication
- Authentication Configuration Scenarios

2.1 Enabling and Finding TCP/IP Port Information

The following sections provide information you require to enable the TCP/IP port and to find the TCP/IP port for a particular SQL server instance:

- Enabling TCP/IP Port
- Finding the TCP/IP Port

2.1.1 Enabling TCP/IP Port

1. From the SQL Server Configuration Manager, select your appropriate SQL Server Network Configuration in the left panel and navigate to the SQL Server instance.

   The right panel displays all protocols for the specified SQL Server instance and their status.

2. Ensure that TCP/IP is enabled.

3. If TCP/IP is disabled, right-click **TCP/IP** and select **Properties.** The TCP/IP Properties dialog box appears.

4. In the Protocol tab, select **enabled,** and click **Apply.**

5. Restart the SQL Server instance.

2.1.2 Finding the TCP/IP Port

After enabling the TCP/IP protocol, restart the SQL Server to apply the changes.

From the SQL Server Configuration Manager, select the appropriate SQL Server Network Configuration in the left panel and navigate to the SQL Server instance:

The right panel displays all protocols for the specified SQL Server instance and their status.

In the **IP Addresses** tab, TCP Dynamic Ports row of IP All will give the TCP/IP port of instance.

2.2 Modifying the Permissions for Database Authentication

Modify the permissions for database authentication so that you enable SQL authentication or Windows authentication, and set sysadmin role for the database user that you are going to use for discovering the target and running jobs.

On the SQL Server, for the user you are going to use for monitoring and running jobs, set the write permissions by following these steps:

Note: If you do not have a user for Windows Authentication, then create one. To do so, from the task bar, go to **Start**, select **Settings**, and then **Control Panel**. In the Control Panel, double-click **Users and Passwords** and click **Add** in the Users tab.

---

1. Log in to the Microsoft SQL Server Management Studio with a predefined user account, or if one was not setup for SQL authentication, use Windows Authentication (Figure 2–1):

Figure 2–1   Log In to Microsoft SQL Server
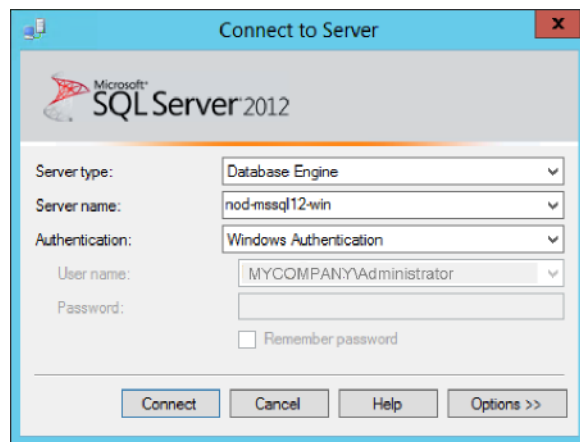
2. Right-click **Logins** and select **New Login…** (Figure 2–2):

Figure 2–2   New Login Menu
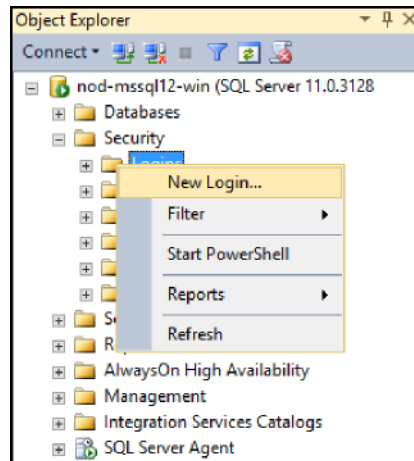
3. Select either **Windows authentication** and select a predefined user, or select **SQL Server authentication** to specify a new user (Figure 2–3):

Figure 2–3   Select User
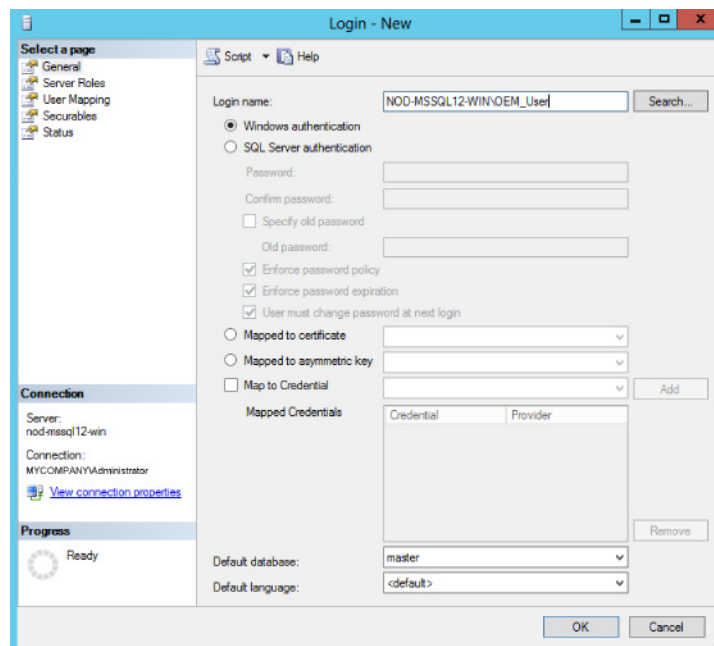
4. Under the Server Roles page, click the check box for the **sysadmin** server role (Figure 2–4):

Figure 2–4   Select sysadmin Server Role
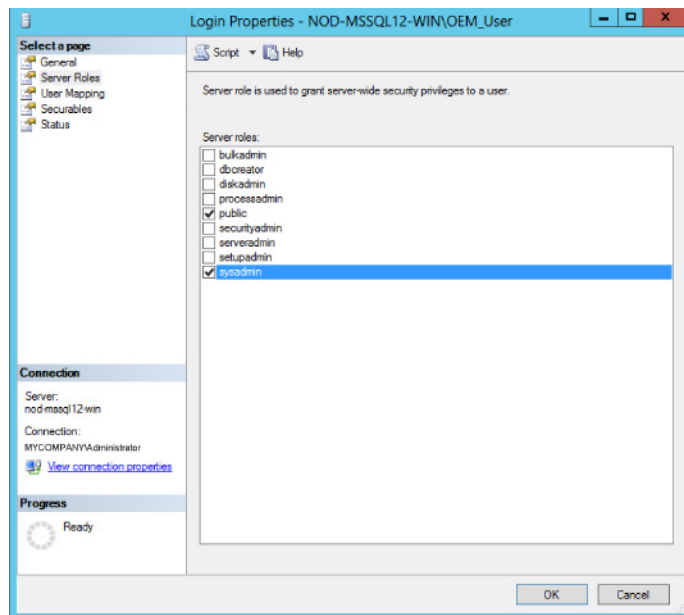
5. Click **OK**.

2.3 Enabling SQL Authentication or Mixed Authentication

1. Log in to the Microsoft SQL Server Management Studio with a predefined user account, or if one was not set up for SQL authentication, use Windows Authentication.

2. Right-click the server you wish to modify and then click **Properties**.

3. Select the **Security Page**.

4. Under the Server authentication heading choose either the desired authentication: **Windows Authentication** or **SQL Server and Windows Authentication** mode.

5. Click **OK**.

6. At this point the SQL server must be restarted. To do so, right-click the server you have just modified and select **Restart**.

7. If SQL Server Agent is running, it must also be restarted.

2.4 Authentication Configuration Scenarios

The examples listed below describe supported configuration details for Microsoft SQL Server. Follow the examples and choose the configuration options best suited for your environment.

- Local monitoring with SQL Authentication

- Local monitoring with Windows Integrated Authentication (WIA)

- Remote monitoring with SQL Authentication

- Remote monitoring with Windows Integrated Authentication (WIA)

- Cluster remote monitoring with SQL Authentication

- Cluster remote monitoring with Windows Integrated Authentication

> **Note:** Before proceeding with target discovery, manually verify the authentication mode used by manually logging in to the target SQL Server's management tool or request WIA/SQL Authentication credentials from the SQL Server administrator.

Example 2–1   Local monitoring with SQL Authentication

```
EM Agent                              : MACHINE_1
JDBC URL                              : jdbc:sqlserver://MACHINE_1:<PORT>
Database Username                     : Database_Username
Password of Database User             : Database_Password
System Password                       : <BLANK>
System Username                       : <BLANK>
Connect Using WIA (Yes/No)            : No
```

`Database_Username` can manually log in to the SQL Server management tool and be granted Sysadmin or correct SQL Server privileges.

Windows OS user is configured to run the Enterprise Manager Agent service and is granted advanced privileges.

Example 2–2   Local monitoring with Windows Integrated Authentication (WIA)

```
EM Agent                              : MACHINE_1
JDBC URL                              : jdbc:sqlserver://MACHINE_1:<PORT>
Database Username                     : <BLANK>
Password of Database User             : <BLANK>
System Password                       : <BLANK>
System Username                       : <BLANK>
Connect Using WIA (Yes/No)            : Yes
```

Windows OS User can manually log in to the SQL Server management tool using WIA, is configured to run Enterprise Manager Agent service, is granted advanced privileges, and is granted Sysadmin or correct SQL Server privileges.

Example 2–3   Remote monitoring with SQL Authentication

```
EM Agent                              : MACHINE_1
JDBC URL                              : jdbc:sqlserver://MACHINE_REMOTE:<PORT>
Database Username                     : Database_Username
Password of Database User             : Database_Password
System Username                       : REMOTE_Windows_OS_User
System Password                       : REMOTE_Windows_OS_Password
Connect Using WIA (Yes/No)            : No
```

Sysadmin or SQL Server privileges are granted to the `Database_Username`.

Advanced privileges granted to `REMOTE_Windows_OS_User` within the SQL Server host machine, and can log in to SQL Server host machine.

Example 2–4   Remote monitoring with Windows Integrated Authentication (WIA)

```
EM Agent                              : MACHINE_1
JDBC URL                              : jdbc:sqlserver://MACHINE_REMOTE:<PORT>
Database Username                     : <BLANK>
Password of Database User             : <BLANK>
System Username                       : REMOTE_Windows_OS_User
System Password                       : REMOTE_Windows_OS_Password
Connect Using WIA (Yes/No)            : Yes
```

`REMOTE_Windows_OS_User` can log in to SQL Server host machine, can manually login to the SQL Server management tool using WIA, granted advanced privileges, granted Sysadmin or correct SQL Server privileges, and must be a Windows Domain account with access to OMA host and target database.

The host with the Oracle Management Agent (OMA) must be a member of the same Windows domain as the SQL Server host.

Example 2–5 Cluster remote monitoring with SQL Authentication

```
Cluster  = SQLServer_Cluster_Hostname
Nodes    = Node1_Hostname
           Node2_Hostname
           etc..

EM Agent                      : ANY MACHINE
JDBC URL                      : jdbc:sqlserver://SQLServer_Cluster_Hostname:<PORT>
Database Username             : Database_Username
Password of Database User     : Database_Password
System Username               : REMOTE_Windows_OS_User
System Password               : REMOTE_Windows_OS_Password
Connect Using WIA (Yes/No)    : No
```

Sysadmin or SQL Server privileges are granted to the `Database_Username`.

`REMOTE_Windows_OS_User` granted advanced privileges within the SQL Server nodes and can log in to SQL Server cluster hostname. Test the login by using Windows Remote Desktop.

`SQLServer_Cluster_Hostname` is virtual hostname or IP of the SQL Server Clustered Service and not the Windows Cluster Hostname.

Example 2–6 Cluster remote monitoring with Windows Integrated Authentication

```
Cluster  = SQLServer_Cluster_Hostname
Nodes    = Node1_Hostname
           Node2_Hostname
           etc..

EM Agent                      : ANY MACHINE
JDBC URL                      : jdbc:sqlserver://SQLServer_Cluster_Hostname:<PORT>
Database Username             : <BLANK>
Password of Database User     : <BLANK>
System Username               : REMOTE_Windows_OS_User
System Password               : REMOTE_Windows_OS_Password
Connect Using WIA (Yes/No)    : Yes
```

`REMOTE_Windows_OS_User` can log in to SQL Server cluster hostname, can manually login to the SQL Server management tool using WIA, granted advanced privileges, granted Sysadmin or correct SQL Server privileges, and must be a Windows Domain account with access to OMA host and target database.

`SQLServer_Cluster_Hostname` is virtual hostname or IP of the SQL Server Clustered Service and not the Windows Cluster Hostname.

> **Note:** Where a User account requires Advanced Privileges, this includes the following Operation System rights:
>
> - Act as part of the operating system.
> - Adjust memory quotas for a process.
> - Log on as batch job.
> - Replace a process-level token.

The host with the Oracle Management Agent (OMA) must be a member of the same windows domain as the SQL Server host.

3

Discovery of the Microsoft SQL Server Target

This chapter describes how to add a Microsoft SQL Server target to Enterprise Manager Cloud Control.

The following topics are provided:

- Discovering Targets
- Verifying and Validating the Plug-in

3.1 Discovering Targets

After successfully deploying the plug-in, follow these steps to add the plug-in target to Cloud Control for central monitoring and management:

1. From the **Setup** menu, select **Add Target** and then **Add Targets Manually** as shown in Figure 3–1:

   Figure 3–1 Add Targets Manually Menu
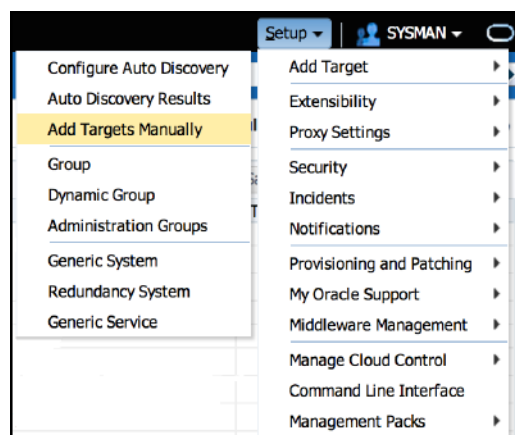
2. In the Add Targets Manually page, select **Add Targets Declaratively by Specifying Target Monitoring Properties**, select **Target Type** as **Microsoft SQL Server**, select a **Monitoring Agent** and click **Add Manually**.

   In the Add Microsoft SQL Server page (Figure 3–2), provide the following information for the properties:

   - **Target Name**: Unique target name across all Cloud Control targets, such as `MSSQL_Hostname`. This is the display name in Cloud Control. It represents this SQL Server target across all user interfaces within Cloud Control.

- **Monitoring Database Host Credentials**

  – **Target System Username** (Needed when SQL Server is at remote location): Valid host user name. Required only for remote Agent monitoring. When using WIA remotely this account must be a Windows Domain account with access to the OMA host and target database. For more information, see Configuring Remote Connections to Monitor Targets. The system user name must be fully qualified. For example:

    ```
    hostname.domainname.com\Administrator
    ```

  – **Target System Password**: Password for the System Username. Required only for remote Agent monitoring.

  – **Confirm Target System Password**: Confirm the password entered for the System Username.

- **Monitoring Database Credentials**

  – **Database Username** (Required for SQL Authentication): Valid user for the database in sysadmin fixed server role.

  – **Database Password** (Required for SQL Authentication): Corresponding password for the database user.

  – **Confirm Database Password** (Required for SQL Authentication): Confirm the password entered for the database user.

  – **Database Role** (Optional): Role assigned to the database user.

  – **Confirm Database Role**: Confirm database role entered for database user.

- **Properties**

  – **Connect Using Windows Integrated Authentication** (Yes/No): Select **Yes** for Windows Integrated Authentication, or select **No** for SQL Authentication.

  – **JDBC Driver**: (Optional) Microsoft SQL Server 2005 JDBC driver class name.

    For example,

    ```
    com.microsoft.sqlserver.jdbc.SQLServerDriver
    ```

  – **JDBC URL**: URL for JDBC. It is recommended that the host name provided in the JDBC URL should be a fully qualified domain name (FQDN). The default port number for Microsoft SQL Server is **1433**. You can specify either IP Address or host name. If you are monitoring a Microsoft SQL Server Cluster, then specify the IP address or host name of the virtual SQL server of the cluster (**Note:** this is not the same as the IP address or host name of the Windows cluster). For example:

    ```
    jdbc:sqlserver://<hostname.domain.com>:<port>
    ```

    You do not need to include the port number if your instance is using the default of **1433**.

> **Note:** Specifying a Named Instance is possible for the URL of the JDBC, however consider the following when building the JDBC URL string:
>
> - Microsoft recommend method for SQL Server hosts with multiple instances of SQL Server installed is to specify unique port numbers for each instance and only specify `hostname:port` for each URL string.
>
> - Optionally, to make use of the Instance Name in the URL use the following supported URL format:
>
>   `jdbc:sqlserver://hostname:port;instanceName=nameofinstance`
>
> - Building JDBC connection URLs with backslashes "\" or without the port number, is not supported by the Microsoft SQL Server plug-in.

3. Click **Test Connection** to make sure the parameters you entered are correct.

Figure 3–2   Add Microsoft SQL Server

3.2 Adding Targets with EMCLI

To add Microsoft SQL Server targets with EMCLI, use the `add_target` verb, as shown in Example 3–1.

You will need to specify the following options:

- **Target name:** `*-name*`

  It must begin with an alphabetic character contain only alphanumeric characters, multibyte characters, a space, -, _, ., :, /, (,) and have a maximum length of 256 characters.

- **Target type:** `*-type*`

Always use `"microsoft_sqlserver_database"` (including the quotes).

- **Host name:** `*-host*`

  Network name of the machine running the Management Agent that is collecting data for this target instance.

- **Target instance properties:** `*-properties*`

  Name-value pair list of properties for the target instance. The available property names are as follows.

  ```
  SysUserName
  SysPassword
  DBUserName
  DBpassword
  Role
  dbBackupPath
  WinSecurityEnabled
  jdbcdriver
  url
  ```

- **Properties separator delimiter:** `*-separator=properties*`

  Specify a string delimiter to use between name-value pairs for the value of the -properties option. The default separator delimiter is ";".

- **Properites subseparator delimiter:** `*-subseparator=properties*`

  Specify a string delimiter to use between name and value in each name-value pair for the value of the -properties option. The default subseparator delimiter is ":″. For the SQL Server plug-in, it is recommended that a plus "+" sign be used.

Example 3–1   Adding Microsoft SQL Server Targets Using EMCLI

```
emcli.bat add_target
          -name="SqlServerTarget"
          -type="microsoft_sqlserver_database"
          -host="HostTargetName"
          -properties="jdbcdriver+com.microsoft.sqlserver.jdbc.SQLServerDriver;
                      url+jdbc:sqlserver://SqlServerHost.domain.localnet:1433;
                      DBUserName+sa;DBpassword+password;
                      SysUserName+SqlServerHost.domain.localnet\Administrator;
                      SysPassword+password;WinSecurityEnabled+No;"
          -subseparator=properties="+"
```

3.3 Verifying and Validating the Plug-in

After waiting a few minutes for the plug-in to start collecting data, use the following steps to verify and validate that Enterprise Manager is properly monitoring the plug-in target:

1. Click the Microsoft SQL Server target link from the All Targets page. The Microsoft SQL Server home page appears as shown in Figure 3–3:

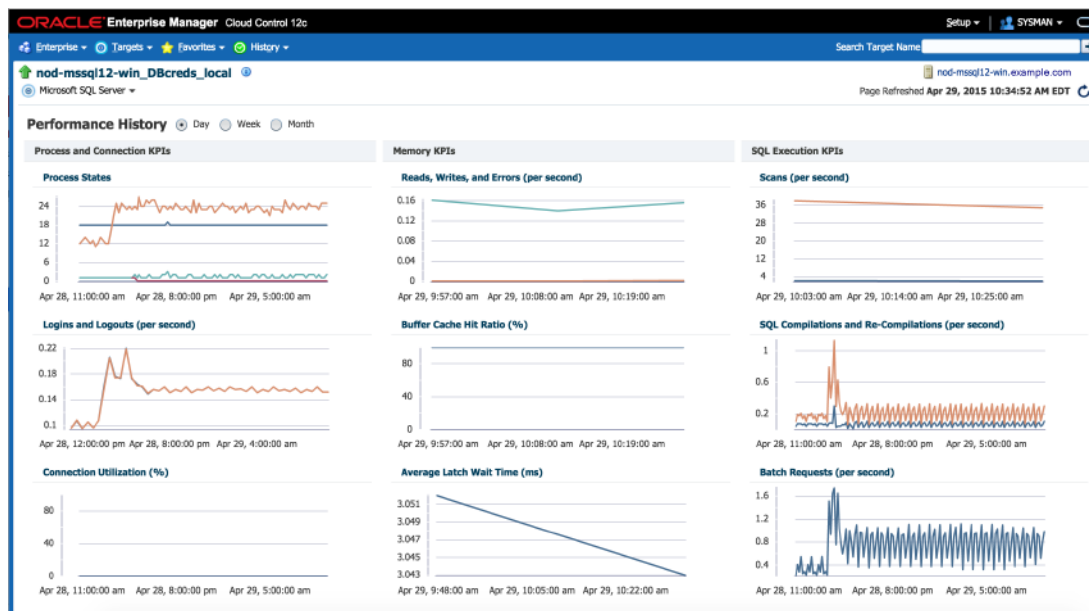*Figure 3–3   Microsoft SQL Server Target Home Page*
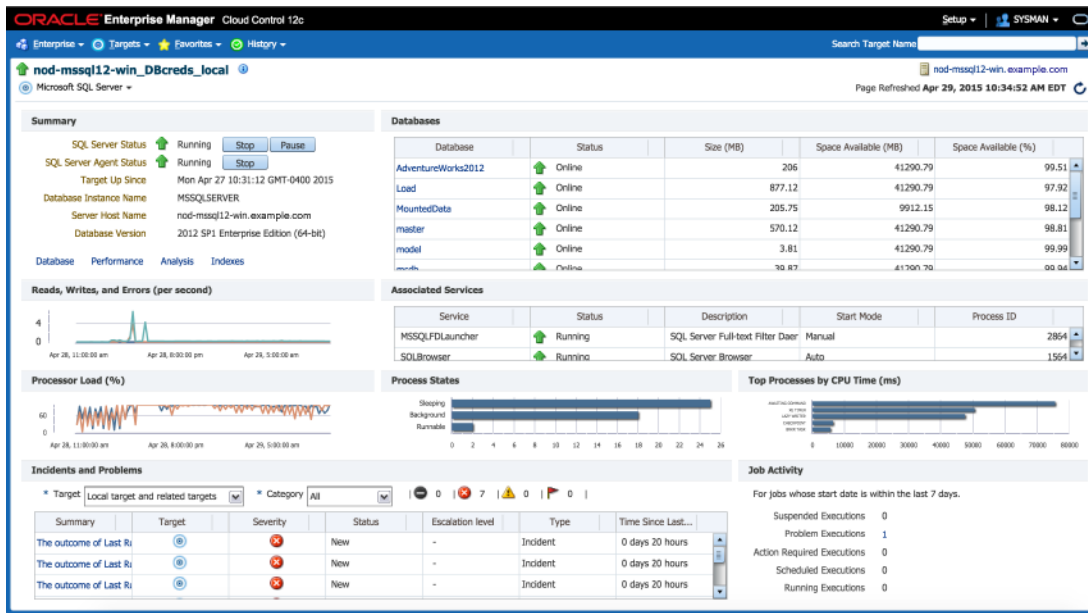
2. Verify that no metric collection errors are reported by clicking **Monitoring** and then **Metric Collection Errors** from the **Target** menu.

3. Ensure that reports can be seen and no errors are reported by clicking **Information Publisher Reports** in the **Target** menu and viewing reports for the Microsoft SQL Server target type.

4. Ensure that configuration data can be seen by clicking **Configuration** and then **Last Collected** in the **Target** menu. If configuration data does not immediately appear, click **Refresh** in the Latest Configuration page.

5. View the Database Page by selecting the **Microsoft SQL Server** drop down under the target name and selecting **Database**. The database page appears (Figure 3–4). The database page contains database specific performance and configuration metrics as well as backup and restore functionality. The database will be selected from a drop-down menu.
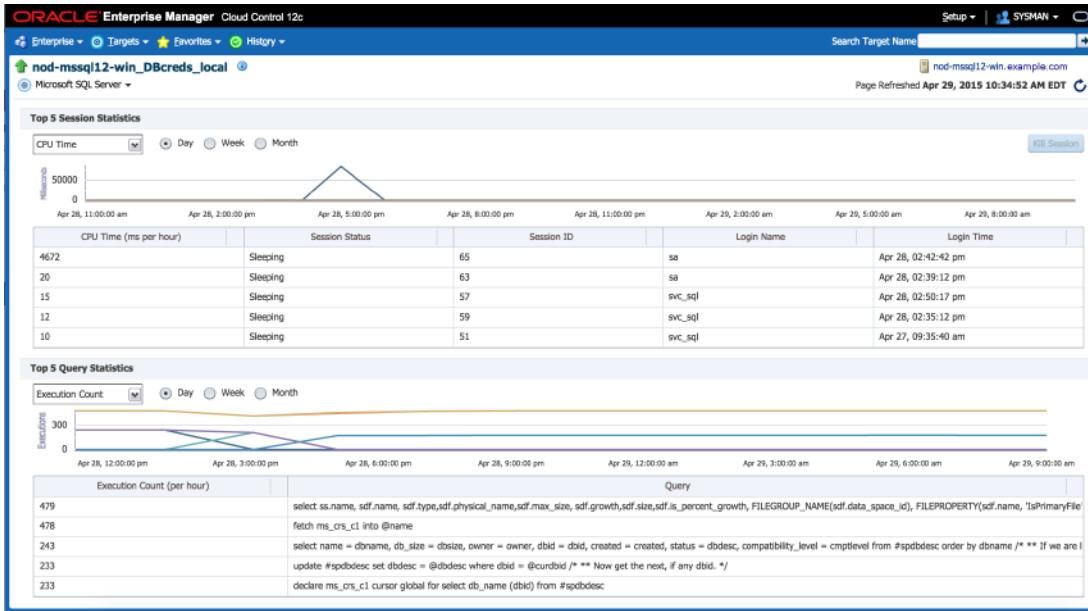
Figure 3–4   Microsoft SQL Server Database Page
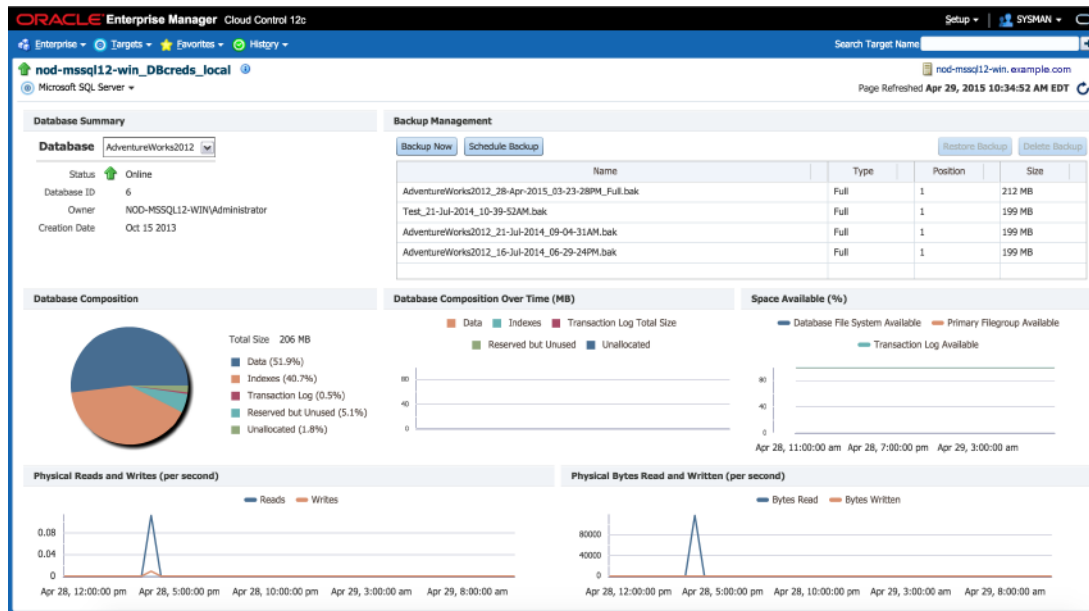
6. View the Performance Page by selecting the **Microsoft SQL Server** drop down under the target name and selecting **Performance**. The Performance page appears (Figure 3–5). The performance page contains convenient performance graphs built from collected metrics.

Figure 3–5   Microsoft SQL Server Performance Page

7. View the Analysis Page by selecting the **Microsoft SQL Server** drop down under the target name and selecting **Analysis**. The Analysis page appears (Figure 3–6). The analysis page displayed SQL query and session information, as well as the "Kill Session" job button to quickly end any problematic sessions.

Figure 3–6   Microsoft SQL Server Analysis Page

8. View the indexes page by selecting the Microsoft SQL Server drop down under the target name and selecting **Indexes**. The indexes page appears (Figure 3–7). The indexes page displays metric graphs and tables about the database indexes. It also includes a Missing Indexes table that recommends indexes to be created. Click **Create Index** to create an index.

Figure 3–7   Microsoft SQL Server Index Page

4
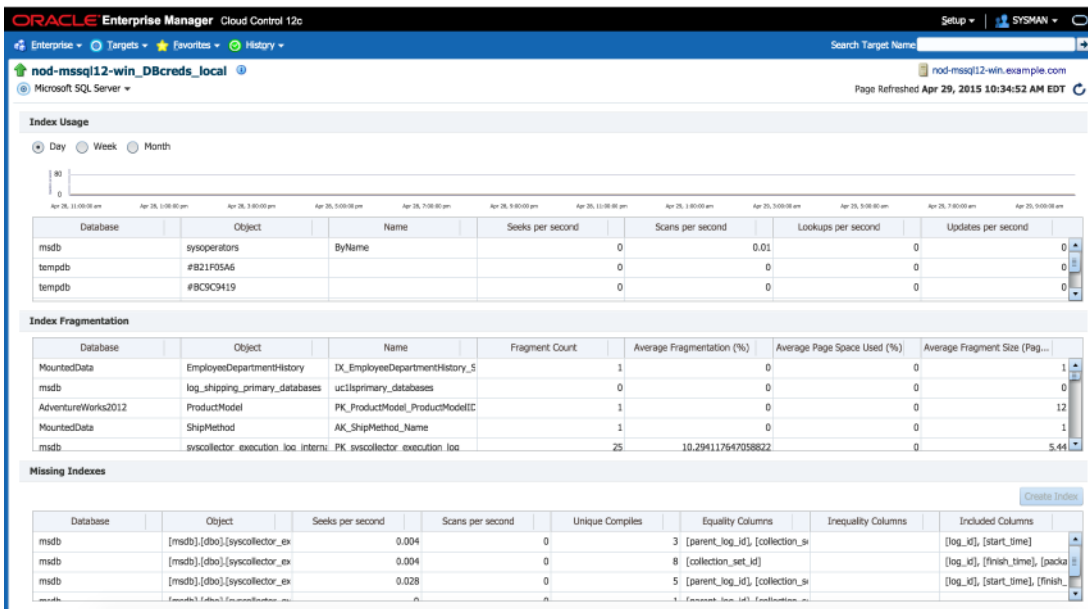
Configuring Connections

This chapter provides details about configuring connections for monitoring targets and executing jobs.

The following topics are provided:

- Configuring Remote Connections to Monitor Targets
- Configuring Connections to Execute Jobs

4.1 Configuring Remote Connections to Monitor Targets

If you want to monitor targets using remote Agents, then Oracle recommends that you do the following security configurations on every system where SQL Server target resides.

1. Set WMI namespace security.

2. Restrict access to the registry from a remote computer.

3. Set DCOM Security to allow user to access remotely.

4. Set privileges for System User to access Windows performance counters remotely as follows:

   a. Locally on the Microsoft Windows node hosting the Agent, open the **Local Security Settings** Windows Tool. Go to **Start**, select **Control Panel**, and then select **Administrative Tools**, select **Computer Management**, select **System Tools**, then **Local Users and Groups**, and select **Groups**.)

   b. Add System Username to **Performance Monitor Group** as shown in Figure 4–1:

Figure 4–1 Performance Group
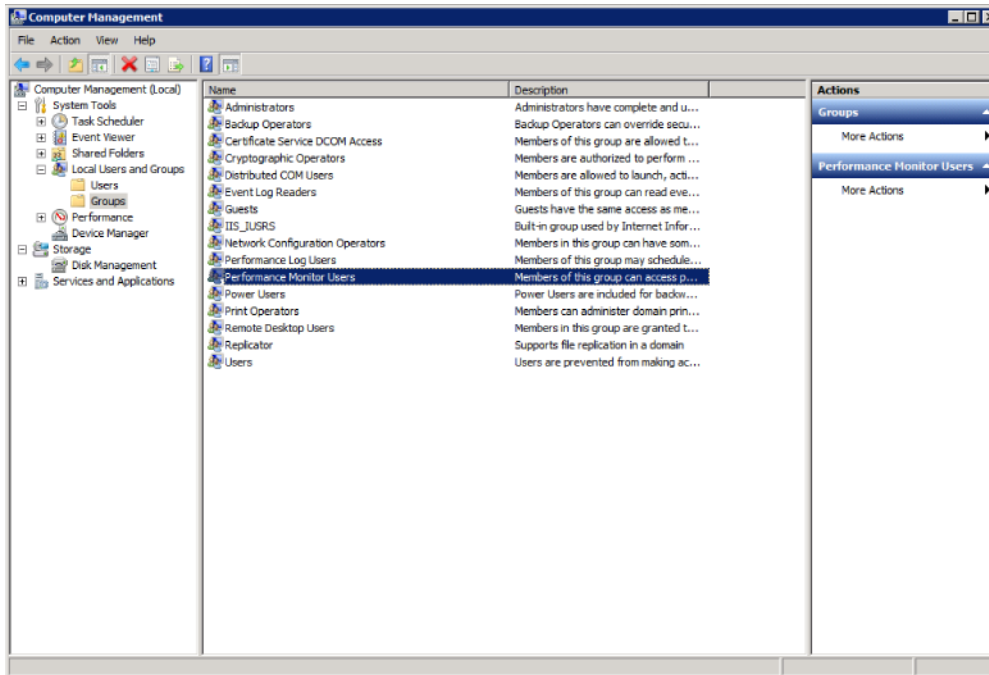
5. Set access privileges of SQL Server Services to allow user to access a computer remotely.

6. Set privileges for System User of target on Oracle Management Agent for Windows Integrated Authentication based monitoring.

   a. Locally on the Microsoft Windows node hosting the Agent, open the **Local Security Settings** Windows Tool. Go to **Start**, select **Control Panel**, and then select **Administrative Tools**, and select **Local Security Policy**.

   b. Click on **Local Policies** and then **User Rights Assignment**.

   c. Assign the following right to the System User of the target:

   ```
   Logon as batch job
   ```

7. Configure **Allow Remote Administration Exception in Windows Firewall** if Windows firewall is enabled on the SQL Server target system.

8. When using WIA remotely, the OMA host must be a member of the same Windows Domain.

4.2 Configuring Connections to Execute Jobs

If you want to execute jobs using local or remote Agents, then Oracle recommends that you do the following security configurations on every system where SQL Server target resides.

- Set WMI namespace security.

- Set DCOM Security to allow user to access a computer remotely.

For configuration details, refer to the following:

- Microsoft Help and Support Web site:

  http://support.microsoft.com

- *How To Troubleshoot Microsoft SQL Server Plug-In Issues* (Document 367797.1) on My Oracle Support:

  https://support.oracle.com/rs?type=doc&id=367797.1

5

Creating, Editing, and Using Jobs

This chapter describes how to create and edit jobs in Enterprise Manager Cloud Control for the Microsoft SQL Server.

The following topics are provided:

- Creating and Editing Jobs

- Using the Backup and Restore Jobs

5.1 Creating and Editing Jobs

To create and edit jobs, follow these steps:

1. In Enterprise Manager Cloud Control 12*c*, click **Enterprise**, then **Job**, then click **Activity**.

2. On the Job Activity page (Figure 5–1), select a job type from the **Create Job** menu and click **Go**.

   Select one of the following:

   - Microsoft SQL Server and/or SQL Agent Start

   - Microsoft SQL Server and/or SQL Agent Stop

   - Microsoft SQL Server Pause or Resume

   - Microsoft SQL Server Kill Session

   - Microsoft SQL Server Backup Database

   - Microsoft SQL Server Delete Backup Database

   - Microsoft SQL Server Restore Database

   - Microsoft SQL Server Create Index

Figure 5–1   Microsoft SQL Server Jobs Page
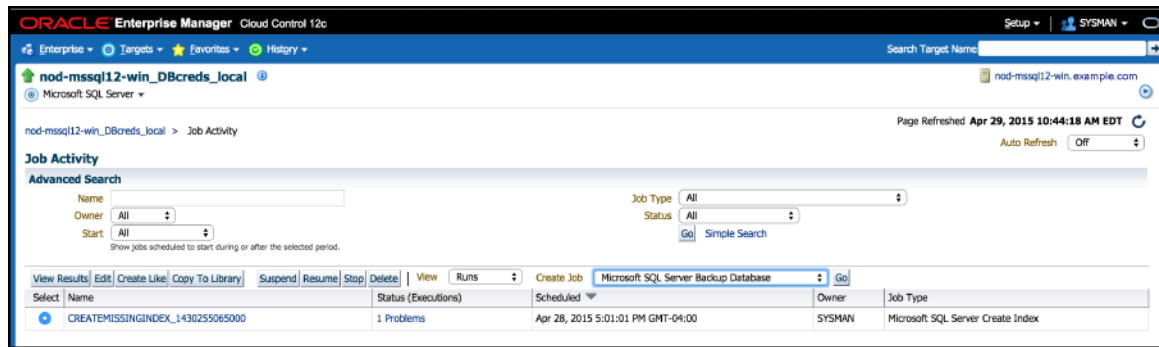
3. In the **General** tab of the Create *<Job Type>* Job page, provide a name for the job and add the individual targets or one composite target such as a Group.

> **Note:**   If you are editing a job, then modify the job name and the selected targets.

4. In the **Parameters** tab of the Create *<Job Type>* Job page, from the **Options** menu, select an appropriate option to make the job function accordingly when it starts.

    You can select one of these options as shown in Table 5–1:

Table 5–1   Job Parameters Options

Job Type	Available Options
Microsoft SQL Server and/or SQL Agent Start	■ Start SQL Server and SQL Server Agent services (You will select this option when both, SQL Server and SQL Server Agent, are stopped or when SQL Server is running but the SQL Server Agent is stopped) ■ Start SQL Server service (You will select this option when both, SQL Server and SQL Server Agent, are stopped and if you want to start only the SQL Sever)
Microsoft SQL Server and/or SQL Agent Stop	■ Stop SQL Server and SQL Server Agent services. You will select this option: - When both SQL Server and SQL Server Agent are running. - When SQL Server is paused but the SQL Server Agent is running. - When SQL Server is running/paused but the SQL Server Agent is stopped. ■ Stop SQL Server Agent service. (You will select this option when you want to stop a running SQL Server Agent)
Microsoft SQL Server Pause or Resume	■ Pause SQL Server service (You will select this option when you want to pause a running SQL Server) ■ Resume SQL Server service (You will select this option when you want to resume a paused SQL Server)
Microsoft SQL Server Kill Session	■ End a single active SQL Server user session. (You will select this option to end an active user session by specifying the session ID)

Table 5–1   (Cont.) Job Parameters Options

Job Type	Available Options
Microsoft SQL Server Backup Database	■ Creates a backup of the database specified by Database Name in the Parameters section of the job.
	■ Unless specified by editing the monitoring configuration of a deployed target in the Backup Path value, the database backup files will be saved to the default SQL Server backup location. The path specified must not end in a backslash.
	■ The Backup job is also available as a button on the Database page in the Backup Management section as **Backup Now**.
	(You will select this job when you want to take a backup of the specified database.)
	■ The Backup job comes with Full or Differential backup options.
	■ The Backup job also comes with the option to backup all databases on an instance. This option is available when creating the backup job from the Job Activity page (Figure 5–1).
	■ This option will back up all databases except master, model, msdb, and tempdb. This requires that all databases being backed up are set to the Simple Recovery Model, or the job will fail without backing up *any* databases.
Microsoft SQL Server Delete Backup Database	■ Removes the backup file from the SQL Server by specifying Media Set ID and full path to the backup file in the Job Parameters section.
	■ The Delete Backup job is also available as a button on the Database page in the Backup Management section as **Delete**.
	(You will select this job when you want to remove backup file that is no longer needed)
Microsoft SQL Server Restore Database	■ Restores a database from backup by specifying the full path to the backup file as well as the database name in the Job Parameters section.
	■ The Restore Database jobs is also available as a button on the Database page in the Backup Management section as **Restore**.
	(You will select this option when you want to restore a database from a backup taken using the Microsoft SQL Server Backup Database job.)
	■ The restore job may be run with a full backup file or a full backup file plus a differential backup file.

Cloud Control starts the SQL server and agent services according to the selection made.

5. In the **Credentials** tab of the Create *<Job Type>* Job page, select an appropriate option for credentials.

   You can choose to use the preferred credentials that are already set or override the preferred credentials with new credentials. In either case, you need to provide the credentials for agent host and database host.

   To set the preferred credentials, click **Preferences** at the top-right corner of the Cloud Control console. From the left-vertical navigation bar, click **Preferred Credentials**. Cloud Control displays the Preferred Credentials page. On this page, you can set the preferred credentials

6. In the **Schedule** tab of the Create *<Job Type>* Job page, schedule the job.

7. In the **Access tab** of the Create *<Job Type>* Job page, define or modify the access you want other users to have to this job.

8. Click **Submit** to create the job.

> **Notes:**
>
> - To enable use of the Job buttons found in the Summary section of the Target home page and the Backup Management buttons found in the Database page, be sure to set the Preferred Credentials with SQL Server Authentication for the Microsoft SQL Server target type.
>
> - Regardless of the authentication used for monitoring, the Kill Session, Backup, Delete Backup, and Restore jobs require SQL Server Authentication. To use these jobs be sure to specify credentials for SQL Server authentication.
>
> - The Microsoft SQL Server Pause or Resume job is only supported for stand-alone Microsoft SQL Server instances. Pause of Resume Jobs submitted for Microsoft SQL Server 2005, 2008, 2012, and 2014 cluster instances will fail with the appropriate error message.

5.2 Using the Backup and Restore Jobs

To use the backup and restore jobs:

1. From the Targets, select **All Targets**, then select the **Microsoft SQL Server** target.

2. From the Microsoft SQL Server menu, select **Database** as shown in Figure 5–2:

Figure 5–2   Microsoft SQL Server Database Menu
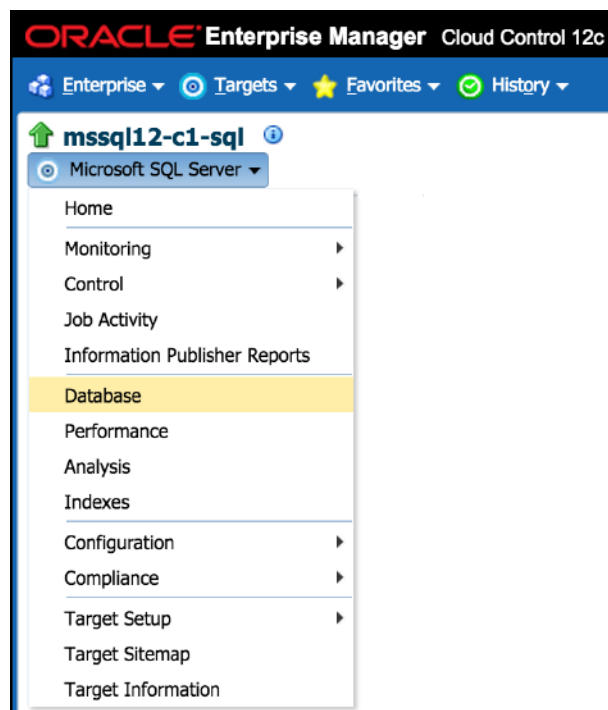
3. Use the drop down to select the database you wish to back up as shown in Figure 5–3.

Figure 5–3   Select a Database

Several options are available using the Backup Management Region.

4.   Click **Backup Now** to create a backup immediately (Figure 5–4).

Figure 5–4   Backup Microsoft SQL Database

If you want to give your backup a custom name, then use the **Backup Name** text box. Select either **Full** or **Differential** for the Backup Type (Figure 5–5). Click **Backup** to confirm.

Figure 5–5   Backup Type

When the backup is complete, it will appear in the list (Figure 5–6):

Figure 5–6   Completed Backup

5. You can also create a backup schedule by clicking **Schedule Backup**.

6. Click **Yes** to confirm that you would like to go to Enterprise Manager's job creation system where you can complete the scheduling process.

7. Give the Job a name (Figure 5–7):

Figure 5–7   Microsoft SQL Server Job Name

8. Click on **Parameters** and specify the name of the database you wish to backup.

9. Optionally, you can specify a custom backup name and use the Backup Type drop down to select **Full** or **Differential**. Users also have the option to back up all user databases on the instance by selecting **True** for Backup All User Databases. Otherwise, only the specified database is backed up.

10. Select or enter credentials as shown in Figure 5–8. If you've configured Preferred Credentials for the target, you can select **SYSADMIN Database Credentials**, **Target System Credentials**, and **Agent Host Credentials**.

Figure 5–8   Enter Credentials

11. Use Enterprise Manager's built-in scheduling options to define the time and recurrence of the schedule as shown in Figure 5–9:

Figure 5–9   Scheduling Options

12. Click **Submit**. The schedule will be shown in the Job Activity view (Figure 5–10).

Figure 5–10   Microsoft SQL Server Job Activity View

> **Note:**   You can only restore backups that meet the following criteria. The backup is:
>
> - File backup (not tape)
> - MS SQL Server knows this backup (that is, the backup is in the list of known backups, list comes from query, seen below)
> - Not password protected
> - Of the type 'SIMPLE'
> - Not damaged

6

Using Reports and Monitoring Templates

This chapter describes how to use the reports and monitoring templates that the system monitoring plug-in for Microsoft SQL Server provides. Use the available out-of-the-box reports to further aid administrators with critical tasks such as problem diagnosis, trend analysis, and capacity planning. Monitoring templates simplify the task of setting up monitoring for large numbers of targets by allowing you to specify the monitoring and metric and collection settings once and applying them to many groups of targets as often as needed
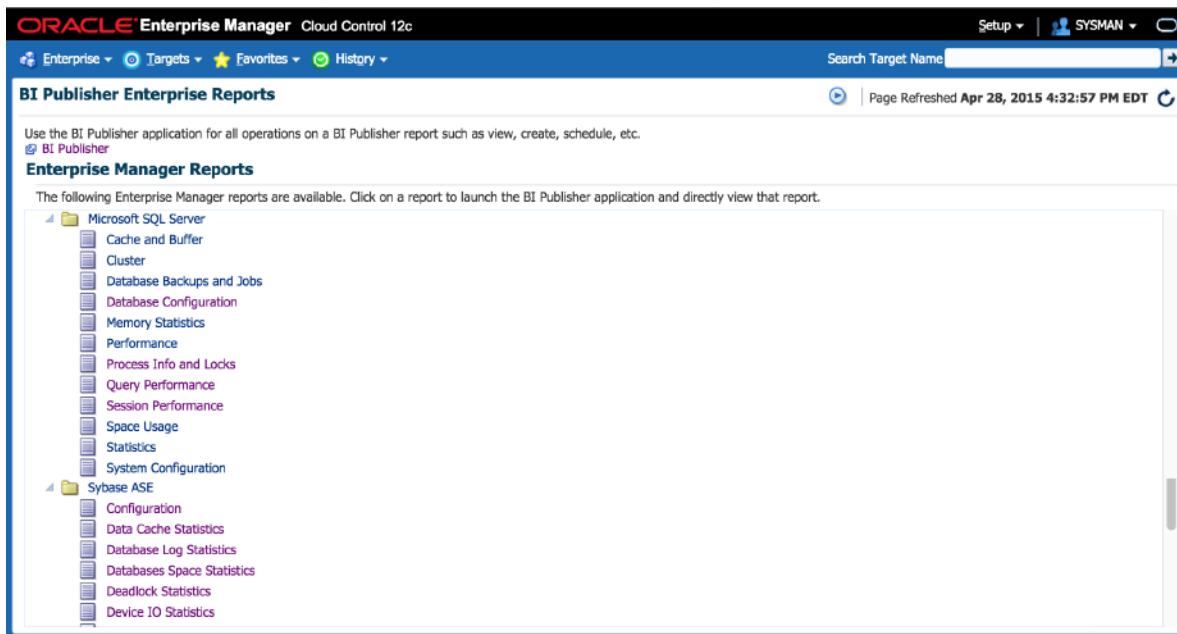
The following topics are provided:

- Using the Microsoft SQL Server Plug-in Reports
- Deploying Reports After BI Publisher is Configured
- Using the Microsoft SQL Server Plug-in Monitoring Templates

6.1 Using the Microsoft SQL Server Plug-in Reports

The Microsoft SQL Server plug-in includes 12 out-of-box reports (Figure 6–1):

Figure 6–1   Microsoft SQL Server Reports

To generate a new report from one of the out-of-the-box reports provided by Oracle, follow these steps:

1. From the Enterprise menu, select **Reports**, then **BI Publisher Enterprise Reports** as shown in Figure 6–2:

Figure 6–2   BI Publisher Enterprise Reports Menu

2. Scroll down to the Microsoft SQL Server section, find the desired report, and click the report title hyperlink.

3. After the reports have been sorted to Microsoft SQL Server reports only, find the desired report and click on the report title hyperlink.

   After clicking the report title hyperlink, the desired report will generate as shown in the example in Figure 6–3:

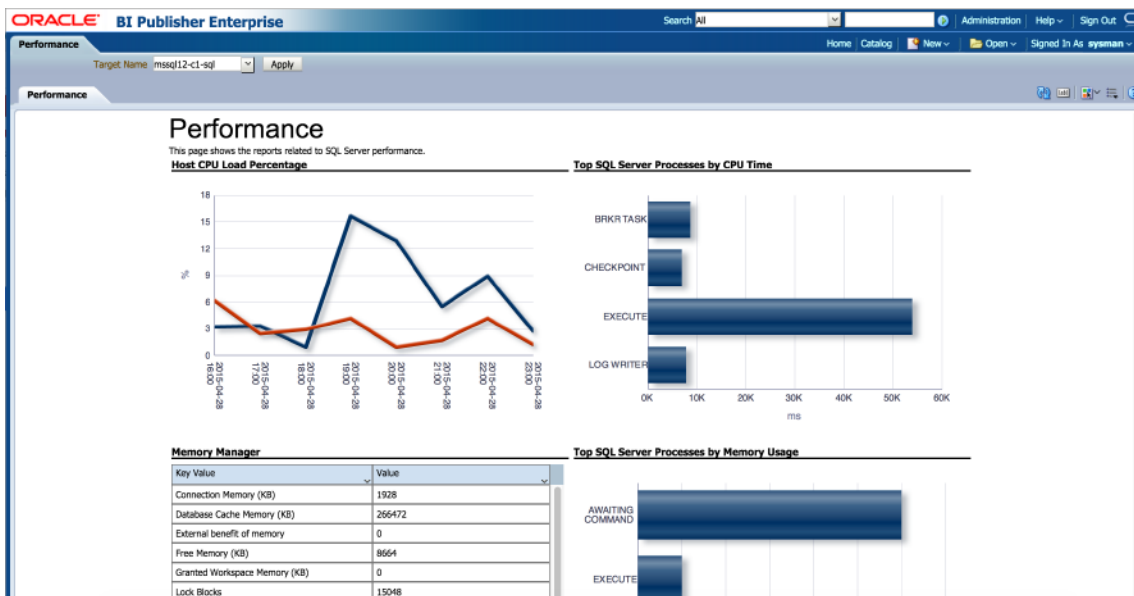*Figure 6–3   Microsoft SQL Server BI Publisher Report Example*

Table 6–1 shows the BI Publisher Reports that are provided by Oracle:

Table 6–1   Microsoft SQL Server Plug-in Reports

Report Name	Report Description
Microsoft SQL Server Database Configuration	Displays Configuration Information for the various Databases.
Microsoft SQL Server System Configuration	Displays Configuration Information for the SQL Server System.
Microsoft SQL Server Database Backups and Jobs	Displays Information about the Database Backups and Jobs.
Microsoft SQLServer Memory Statistics	Displays Information about the Memory in SQL Server.
Microsoft SQLServer Performance	Displays Information about the Performance of the SQL Server.
Microsoft SQL Server Query Performance	Displays information about the Performance of the Most Active Queries of the SQL Server.
Microsoft SQL Server Session Performance	Displays information about the Performance of the Most Active Sessions of the SQL Server.
Microsoft SQL Server Statistics	Displays Statistical Information for SQL Server.
Microsoft SQL Server Cluster	Displays Information about the SQL Server Cluster.
Microsoft SQL Server Space Usage	Displays Information about Space Usage in the Database.
Microsoft SQL Server System Process Info and Locks	Displays information about the System Processes and locks of the SQL Server.
Microsoft SQL Server System Cache and Buffer	Displays information about the System Cache and Buffer of the SQL Server.

6.2 Deploying Reports After BI Publisher is Configured

If the Microsoft SQL Server plug-in is deployed or upgraded after BI Publisher is already configured and the reports were not deployed automatically, then run the following command:

```
emcli deploy_bipublisher_reports -pluginid="oracle.em.smss"
-pluginversion="12.1.0.6.0" -force
```

6.3 Using the Microsoft SQL Server Plug-in Monitoring Templates

To view the out-of-box templates, from the **Enterprise** menu, select **Monitoring** and then **Monitoring Templates**. Using the Target Type drop down, select **Microsoft SQL Server** and press the arrow button.

A complete list of all out-of-box monitoring templates will be available for use as follows (also, see Figure 6–4):

- **Basic MS SQL Monitoring Template** - Recommended basic template for monitoring SQL Server.

- **Cluster Template** - Recommended template for monitoring errors in a clustered SQL Server environment.

- **High Availability Disaster Recovery Template** - Recommended template for monitoring errors in a HADR (Always On) SQL Server environment.

Figure 6–4   Microsoft SQL Server Monitoring Templates
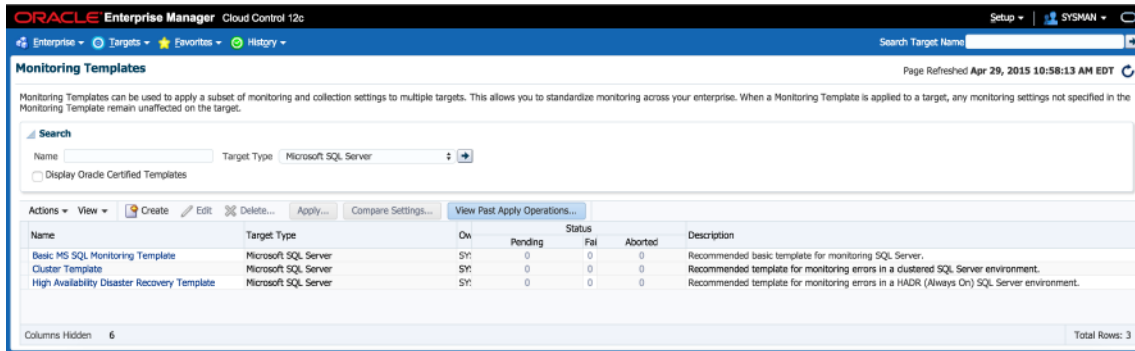
To apply a monitoring template to a SQL Server Target, perform the following actions:

1. Click the desired monitoring template to select it.

2. Click the **Actions** button and select **Apply**.

3. Choose to either *replace* or *override* existing thresholds with the **Apply Options** option.

4. Click **Add** to add the SQL Server Targets to apply the template to. Follow the prompts through the target Search and Select Targets screen.

5. Click **Ok** and a confirmation message will appear at the top of the page notifying of a successful application.

The **Actions** button found on the Monitoring Templates screen will also give access to setting a selected template as "Default" for all new SQL Server Target deployments, or Edit an existing template's threshold values.

Refer to "Using Monitoring Templates" section in the *Enterprise Manger Cloud Control Administrator's Guide* for more information on how to use Monitoring Templates in Enterprise Manager 12*c*:

https://docs.oracle.com/cd/E24628_01/doc.121/e24473/mon_temp.htm#EMADM12262

7

Chargeback Functionality

This chapter provides the instructions for configuring chargeback functionality for Microsoft SQL Server.

This chapter contains the following sections:

- About Chargeback
- Chargeback Plug-in Deployment
- Configuring Global Settings for Chargeback
- Configuring a Charge Plan
- Revising Extended Charge Plans
- Configuring a Cost Center
- Configuring an Entity
- Generating and Distributing Chargeback Reports
- Additional Information

7.1 About Chargeback

Chargeback, as the name implies, is a tool of accountability. The application's primary uses can generally be described as follows:

- Provide resource usage metering by aggregating and normalizing the enormous amount of metric data Enterprise Manager collects.
- Provide IT with a means to "charge" a currency amount to the consumers of resources.
- Provide consumers with reports detailing their consumption and associated charges.

7.2 Chargeback Plug-in Deployment

In order to use the Chargeback functionality, it is necessary to deploy the Chargeback plug-in (from the **Setup** menu, select **Extensibility**, and then select **Plug-ins**).

For information on how to deploy the Chargeback Plug-in for Oracle Enterprise Manager, see the *Enterprise Manager 12c Cloud Control Metering and Chargeback White Paper*:
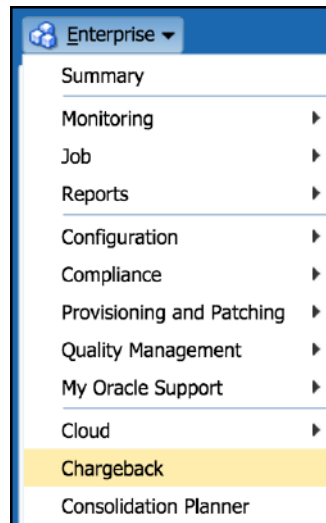
http://www.oracle.com/technetwork/oem/cloud-mgmt/wp-em12c-chargeback-final-1585483.pdf

7.3 Configuring Global Settings for Chargeback

To configure the global settings for chargeback:

1. From the **Enterprise** menu, select **Chargeback**, as shown in Figure 7–1:

Figure 7–1 Chargeback Menu Item

2. If you have not already configured global settings for currency symbol and uptime calculations, select the **Settings** subtab on the bottom of the **Home** tab.

   - Currency Symbol

     To change the default currency (USD), click in the currency symbol text box and enter the desired currency symbol. The new selection becomes the default currency across all charge plans; that is, the universal plan and all extended charge plans. All reports, including historical reports, reflect the new currency.

     Note: No rate conversion occurs when you change the currency; that is, the numbers stay the same. For example, a change from dollars to euros means that a one dollar charge becomes a one euro charge.

   - Uptime Calculations

     Select the appropriate radio button to ignore or include uptime in charge calculations. The default is to include uptime as a consideration. Including uptime has an impact on all fixed and configuration-based charge calculations for all entities.

     Chargeback prorates charges and discounts accordingly. So, for example, if an entity was available 22.5 hours in a 24-hour period, the daily charge would be adjusted 1.5 hours. A change in the uptime setting is effective from the beginning of the current report cycle, but does not impact previous report cycles; that is, charges in historical reports are not prorated based on a change made to the setting in the current cycle.

3. Click **Save** to update the settings.

7.4 Configuring a Charge Plan

A *charge plan* defines the resources to charge for and their associated rates. There are two types of charge plan: the *universal* charge plan and the *extended* charge plan.

The universal plan establishes rates for three basic metrics (CPU, memory, and storage). If you have not configured the universal charge plan, refer to the "Chargeback Administration" section of the *Oracle Enterprise Manager Cloud Administration Guide*:

http://docs.oracle.com/cd/E24628_01/doc.121/e28814/chargeback_cloud_admin.htm#EMCLO926

An extended charge plan enhances the universal plan to include entity-specific metrics. It allows you to implement charges that relate to specific characteristics of an entity. The entity type determines the items for which rates can be charged.

Following the steps below to create an extended charge plan for Microsoft SQL Server:

1. From the **Charge Plans** tab, select **Create**, and then select **Plan** as shown in Figure 7–2. This will bring you to the Create Plan page.

Figure 7–2   Create Chargeback Plan
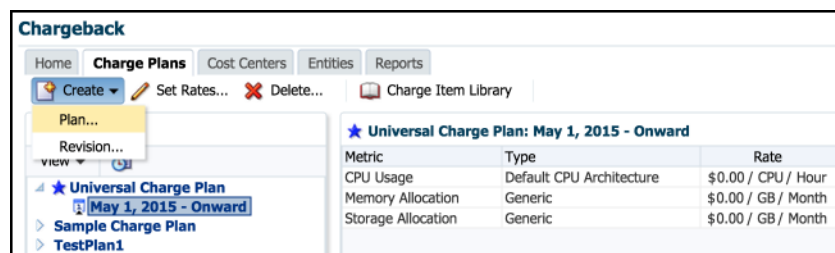
2. On the Create Plan page, you can name your plan at the top. In the left panel labeled "Entity Types" click **Add** and select **Microsoft SQL Server** as your Entity type.

3. Next, select **Add Item** in the center menu (Figure 7–3) to add the different items you can charge for. You can choose between the following four charge items or add them all:

    ■ Base Charge

    ■ Database Base Charge

    ■ Disk Space Usage

    ■ Memory Usage

Figure 7–3   Charge Items

4. Once you have selected the types you wish to include in your Charge Plan, set the rate and frequency. You can set the frequency for each item by hour, day, week, month, quarter or year. After you have set the charge items, click **Save** located at the top right of the screen. This will bring you back to the Charge Plans tab and give you confirmation at the top of your screen (Figure 7–4) that your plan was saved. You should now see it listed in the left hand panel.

At this point you will have created a Charge Plan.

Figure 7–4   Charge Plan Confirmation

7.5 Revising Extended Charge Plans

You can update an extended charge plan in the following ways:

- Make changes to the charge rates in effect for the current or a future cycle.
- Create a plan revision for the next or a later report cycle, based on an existing plan.

To make changes to the charge rates in effect for the current or a future cycle:

1. Select the plan revision in the navigation pane and click **Set Rates**.

2. Make adjustments to the charge items and rates in effect.

3. Click **Save** to update the plan revision.

Note: When changing charge rates for the current cycle, the changes are retroactive to the beginning of the cycle.

To create a plan revision for the next or a later report cycle, based on an existing plan revision:

1. Select a plan in the navigation pane, and then select **Revision** from the Create menu.

2. In the dialog that opens, select the effective date of the revision. The default date is the first month after the most recently added revision. For example, if the current cycle is for May and a June revision already exists, July 01 is the default effective date. Click **OK**.

3. In the familiar create-like model, the configurations, charge items, and rate adjustments for the plan you selected in the navigation pane appear in the plan details table on the right.

   Edit the plan details as desired:

   - Add and remove entity types.

   - Add and remove configurations.

   - Add, change, and delete charge items.

   - Make adjustments to metric rates.

4. When done, click **Save** to complete the plan revision.

7.6 Configuring a Cost Center

Cost centers can be an individual or department within an organization that spreads charges across an enterprise.

The next step to setting up chargeback functionality is to configure a cost center.

Follow the steps below to create a cost center:

1. From the Cost Centers tab, select **Add** as shown in Figure 7–5:

Figure 7–5   Add a Cost Center

2. In the box that appears, give your cost center a unique identifier and a display name. In the example shown below (Figure 7–6), **ACCT** was used as the identifier and the name was **Accounting Department**. For the Level value, select either **Top Level (Root)** or **Member of** depending on its position in the hierarchy.

Figure 7–6   New Cost Center Name and Display Name

3. Once you have selected the names, click **OK**. You should now see your cost center listed (Figure 7–7).

   You will now have successfully created a cost center.

Figure 7–7   Cost Center Confirmation

7.7 Configuring an Entity

For each chargeback *entity* (target), the administrator is able to assign a charge plan to a target and a target to a cost center.

The following steps are used to setup your entities:

1. From the Entities tab, select **Add Entities** (Figure 7–8). This will take you to the Add Entities page.

Figure 7–8   Add Entities

2. From the Add Entities page, click **Add**. In the box that appears (Figure 7–9), select **Microsoft SQL Server** for the target type and then select the target you would like to add. You can also search the target's name to find it, if it does not appear in the list.

Figure 7–9   Select an Entity Target

3. Once you have found the target you would like to add, click **Select**. It should now appear in the list of targets located at the center of the page (Figure 7–10). Click **Next**.

Figure 7–10   Added Target

4. Assign a plan to your entity. Select the target and click **Assign Plan**. In the Assign Plan pop-up (Figure 7–11), choose the charge plan you would like to assign to the entity and select **OK**.

Figure 7–11   Assign a Charge Plan

5. Assign a cost center to your entity. In the Assign Cost Center pop-up (Figure 7–12), choose the cost center that you would like to assign the entity to. After you have assigned both a charge plan and cost center, click **Next**.

Figure 7–12   Assign a Cost Center
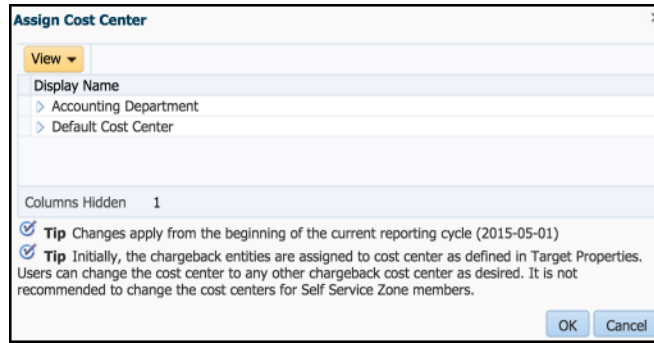
6. Review your selections. If everything appears correct, click **Submit**. At the top of the Chargeback page you should see confirmation that the entity was added correctly (Figure 7–13):

Figure 7–13   Entity Confirmation
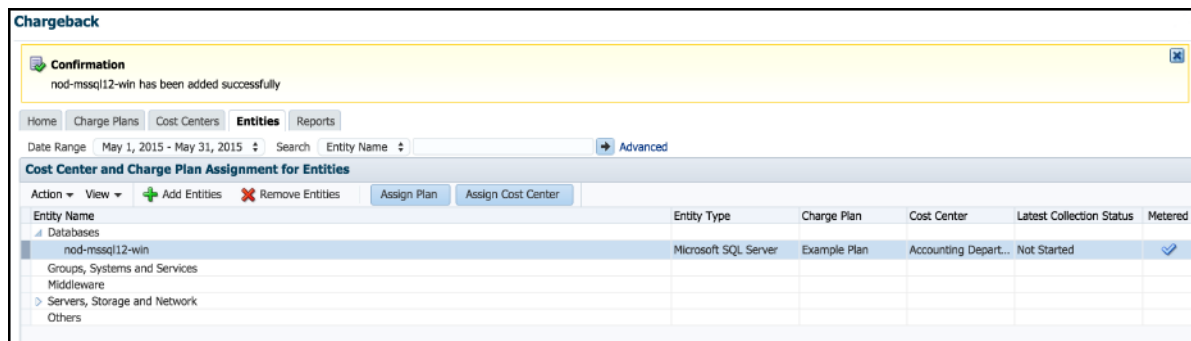
From the Entities tab, you can change the cost center or charge plan associated with a specific entity by selecting the entity and clicking either **Assign Plan** or **Assign Cost Center**, depending on which one you want to change. To delete the entity, click **Remove Entities**.

7.8 Generating and Distributing Chargeback Reports

Chargeback summary reports are a powerful analytical tool for tracking resource usage and charge distributions. These summary reports show information related to charge or resource utilization broken down by cost center, entity type, and resource. They enable you to quickly assess the entities or cost centers with the greatest charges or resource utilization. Summary reports are primarily useful for drill-down purposes.

Data collection occurs once a day. The daily data collection job for the current cycle is based on charge plan and cost center assignments. The reporting cycle defines the time period for which to calculate charges. The cycle is for the current month starting on the first day of the month.

To generate ad hoc reports:

1. From the Enterprise menu, select **Chargeback**.

2. Select the **Reports** tab.

3. Design your report from the following options:

   ■   Use the current report cycle or customize a date range to report on.

- Choose between summary and trend report types. A *summary* report presents a pie-chart breakdown, while a *trend* report uses a y-axis multiple bar chart to denote usage trends.

- Select specific cost centers or report on all users.

- Select specific entities or entity types or report on all entities within all entity types.

- Choose the metric to report on.

Click **View Report** to see the results.

The report displays color-coded graphs summarizing charges by cost center, entity type, and resource, with details displayed in the table at the bottom. Click a color box link in the respective graph to recalculate the report contents for the color-coded selection, for example memory in the resource graph.

Figure 7–14 shows and example of a summary report showing charges for the current reporting cycle for all cost centers and entity types, with a breakdown by resource.

Figure 7–14   Chargeback Summary Report
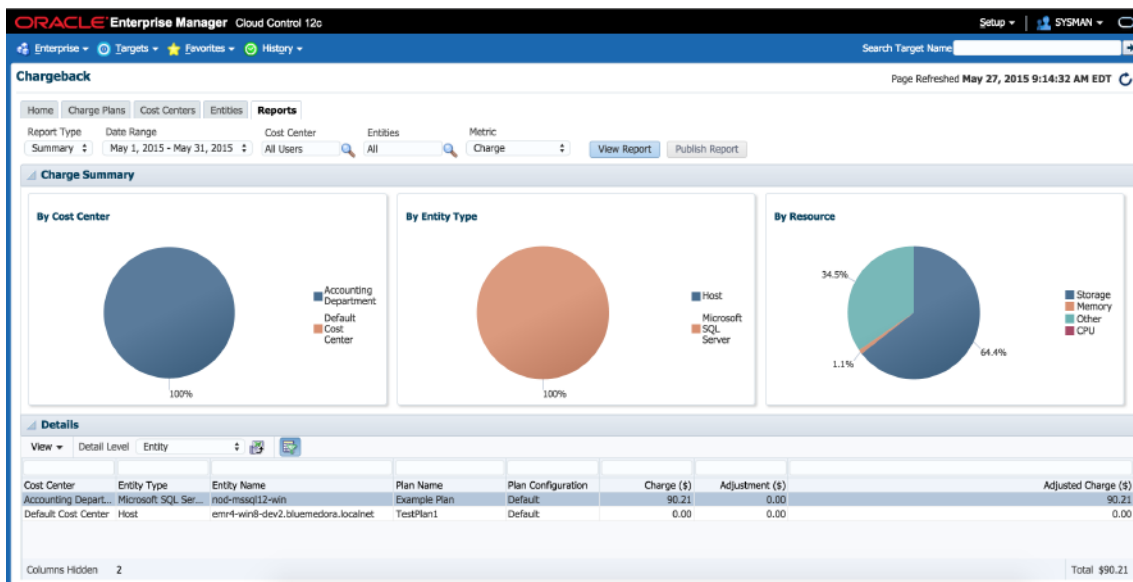
4. Filter the details by choosing from the drop-down list; the default is **All**. Use the query-by-example feature () to search report details. The icon acts as a toggle; clicking it alternately shows or hides text and selection boxes above the table columns. The feature is also available in the **View** menu. Enter search criteria in various combinations by selecting a date and by typing values in the respective columns. Click **Enter** to activate the search.

5. Click the Export icon () in the details region to export report contents to a file.

6. Click **Publish Report** to make report contents public. This action integrates with BI Publisher, where you can:

   - Save reports in a variety of formats (Excel, PowerPoint, HTML, PDF).

   - Distribute generated reports to e-mail lists (users who do not have access to Enterprise Manager, for example) on a defined schedule.

For information on BI Publisher setup, see the "Configuring BI Publisher on Enterprise Manager" chapter in the *Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*:

http://docs.oracle.com/cd/E24628_01/install.121/e24089/install_em_bip.htm#CEGBEJDJ

7.9 Additional Information

For further information regarding Chargeback, refer to the Chargeback Administration section of the *Oracle Enterprise Manager Cloud Administration Guide*.

http://docs.oracle.com/cd/E24628_01/doc.121/e28814/chargeback_cloud_
admin.htm#EMCLO926

8

Compliance Management

This chapter provides the instructions for configuring Compliance Management for Microsoft SQL Server.

This chapter contains the following sections:

- About Compliance Management
- Managing Compliance Framework
- Configuring the SQL Server Configuration Compliance Standard
- "Create Like" Compliance Standard
- Editing a Compliance Standard
- Evaluating Compliance
- Using Trend Overview
- Using Compliance Reports
- Managing Compliance Violations
- Additional Information

8.1 About Compliance Management

Compliance management allows the ability to evaluate the compliance of targets and systems. This is accomplished by defining, customizing, and managing compliance frameworks, compliance standards, and compliance standard rules.

A *compliance framework* is a hierarchical structure where any node can be mapped to one or more compliance standards, compliance standard rule folders, and compliance standard rules.

A *compliance standard* is a collection of checks or rules. It is a compliance control that must be tested against come set of IT infrastructure to determine if the control is being followed.

8.2 Managing Compliance Framework

To manage compliance frameworks, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, and then select **Library**.

2. Click the **Compliance Frameworks** tab.

3. Highlight the compliance framework you want to manage and choose the action you want to perform.

8.3 Configuring the SQL Server Configuration Compliance Standard

Follow the steps below to configure the Microsoft SQL Server configuration compliance standard:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.

2. Click the **Compliance Standards** tab.

3. Refine your search, by using the Search option (Figure 8–1). On the Compliance Standard line, enter **SQL Server Configuration Compliance Standard**, and click **Search**. This action will narrow the list down to the SQL Server Compliance Standard.

Figure 8–1 Refined Compliance Search
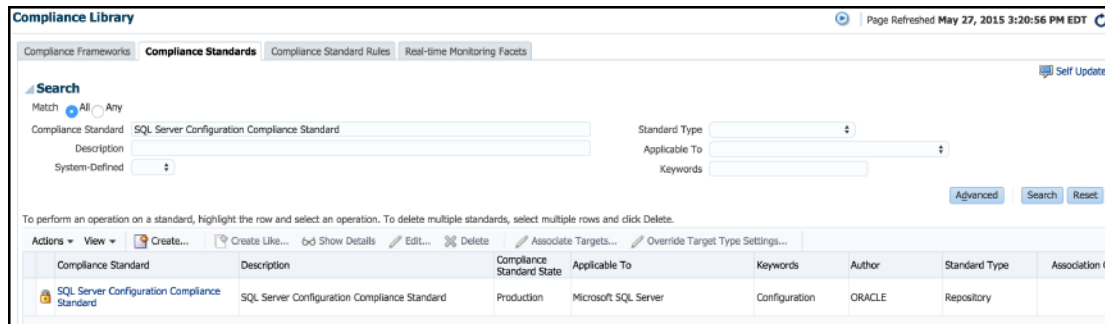
4. Highlight the compliance standard and select **Associate Targets**. This will take you to the Compliance Standard Target Association page, as shown in Figure 8–2:

Figure 8–2 Compliance Standard Target Association
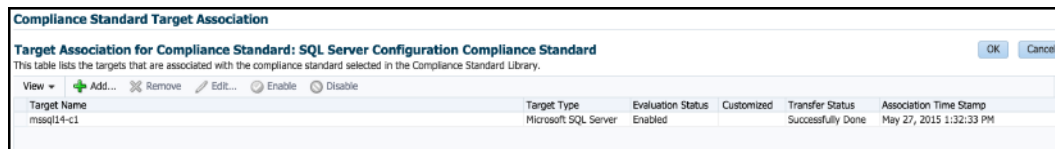
5. Click **Add**. The Select Targets menu will appear with a list of targets that you can select to associate with the SQL Server Compliance Standard (Figure 8–3). If you do not see the target you would like to select, use the Target Name search bar at the top. Once you have chosen the targets you would like to associate, click **Select**.

Figure 8–3 Select Targets
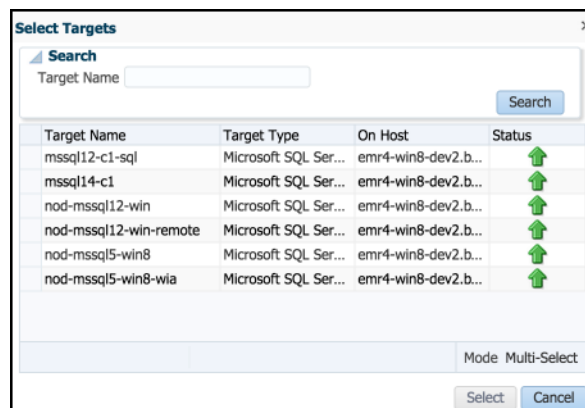
6. The targets that you selected will now appear in the Target Association table (Figure 8–4). Once targets are in the table you can edit the parameters, remove, enable, or disable them.

Figure 8–4 Added Targets

7. Once you are finished selecting targets, click **OK**. In the box that appears select **Yes** to save your changes. A box will appear advising that the compliance standard was submitted to the target for processing (Figure 8–5). Click **OK**.

Figure 8–5 Compliance Standard Confirmation
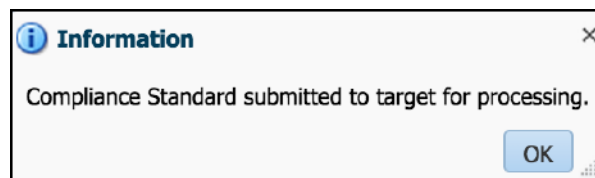
Your target will now be associated with the SQL Server Compliance Standard. It will begin evaluation based on metric collection from that target.

8.4 "Create Like" Compliance Standard

To create a compliance standard like another compliance standard, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.

2. Click the **Compliance Standards** tab.

3. Click **Create Like** (Create Like...).

4. Customize the fields as needed.

   The name of the compliance standard you are creating *must be different* than an existing compliance standard.

5. Click **Save**.

8.5 Editing a Compliance Standard

You can customize compliance standards by editing the existing compliance standard rule settings.

> **Note:** You cannot edit an Oracle-provided compliance standard; so, you should create a compliance standard like the compliance standard you wish to edit. See "Create Like" Compliance Standard.

Once you have created the like compliance standard you can make the customized changes.

To edit a compliance standard, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.

2. Click the **Compliance Standards** tab.

3. Highlight the standard you want to edit and click **Edit** (✎ Edit...).

4. Update the parameters as needed.

5. Click **Save**.

8.6 Evaluating Compliance

Compliance evaluation is the process of testing the compliance standard rules mapped to a compliance standard against a target and recording any violations in the Management Repository.

By evaluating a target against a compliance standard, you are determining whether a target complies with the checks of the standard. To ensure compliance you should regularly perform the following actions:

- Regularly monitor the compliance dashboard to find areas that may indicate your organization has a low compliance score or is at risk.

- Study Oracle-provided reports.

- View the results of an evaluation.

- Study the trend overview as a result of the evaluation.

8.7 Using Trend Overview

Use the graphs in the Trend Overview pages to visually determine whether the targets are adhering to or distancing themselves from the compliance best practices.

To access the Trend Overview pages for compliance standards:

1. From the **Enterprise** menu, select **Compliance**, and then select **Results**.

2. From the Compliance Standards tab, choose **Evaluation Results**.

3. On the Evaluation Results page, choose the compliance standard you want to investigate and click **Show Details**.

4. On the resulting details page, click the **Trend Overview** tab (Figure 8–6).

Figure 8–6   Compliance Trend Overview
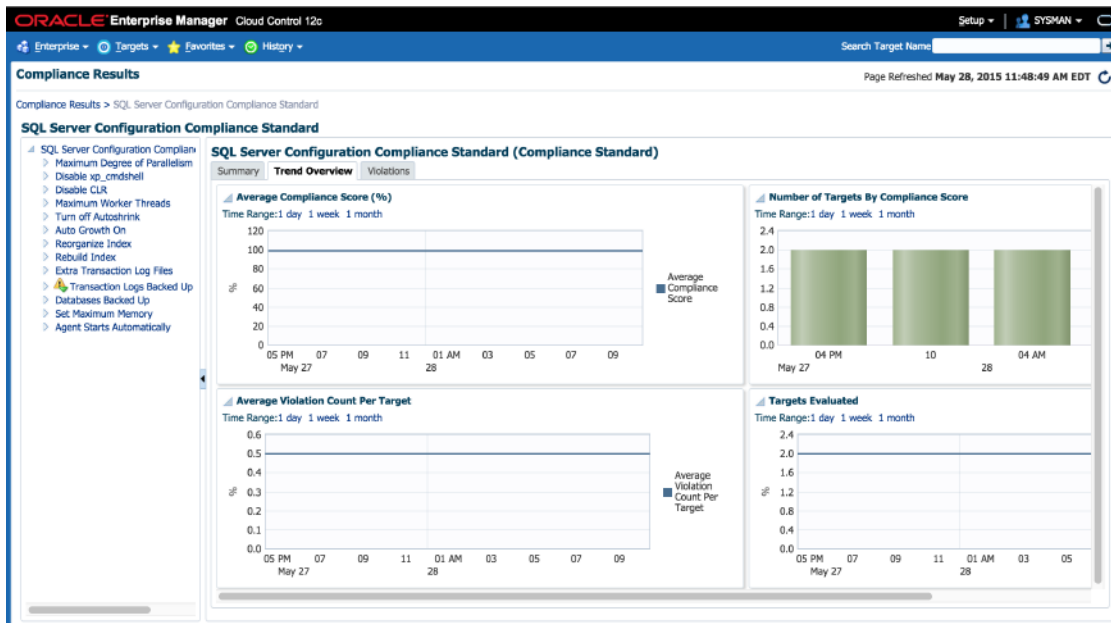

8.8 Using Compliance Reports

Enterprise Manager Cloud Control provides reports specific to compliance. To access these reports:

1.   From the **Enterprise** menu, select **Reports**, and then select **BI Publisher Enterprise Reports**.

2.   Scroll to the **Compliance Section**.

Here you will find a number of reports relating to evaluations against compliance standards and compliance frameworks, as shown in Figure 8–7:

Figure 8–7   Compliance Summary Report
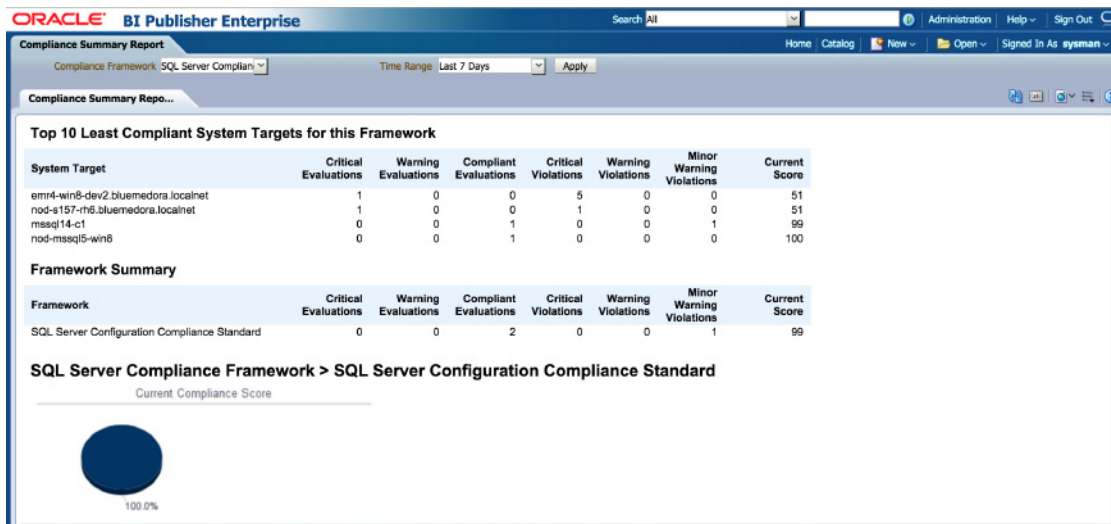
8.9 Managing Compliance Violations

You can use the Managing Violations feature to suppress, unsuppress, and clear manual violations:

- **Accessing the Managing Violations feature** (Figure 8–8)

    1. From the **Enterprise** menu, select **Compliance**, and then select **Results**.

    2. From the Compliance Standards tab, choose **Evaluation Results**.

    3. On the Evaluation Results page, choose the compliance standard you want to investigate and click **Manage Violations**.

Figure 8–8   Manage Violations
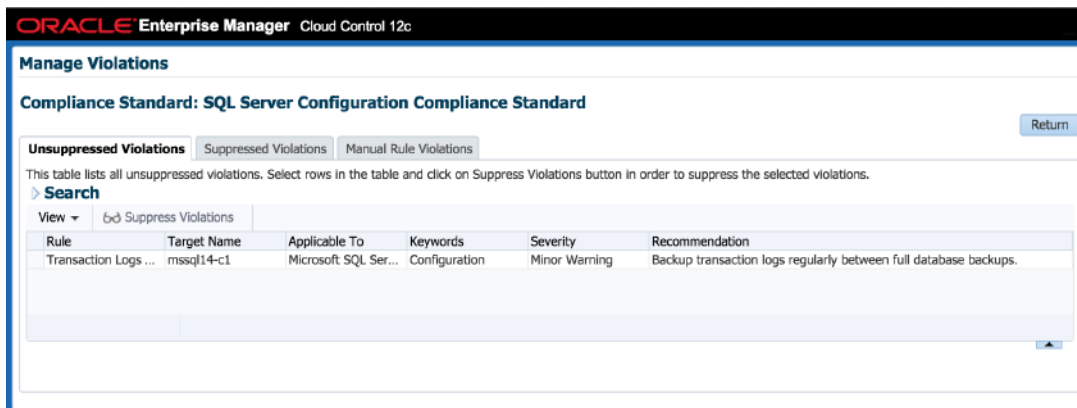
- **Unsuppressed Violations tab**

    Use this tab to suppress violations:

    1. Select one or more violations.

    2. Click **Suppress Violations**.

    3. On the Violation Suppressed Confirmation pop-up, you can suppress the violation indefinitely or provide a date by which the suppression will end. Optionally, you can provide an explanation for the suppression.

    4. Click **OK**.

    This submits a job to do the suppression asynchronously and returns you to the Result Library page. A suppression adds an annotation to the underlying event stating that the violation is suppressed along with the reason (if a reason was provided).

    Note: The job results are not instantaneous. It may take a few minutes for the results to be displayed.

- **Suppressed Violations tab**

    Use this tab to unsuppress violations:

    1. Select one or more violations.

    2. Click **Unsuppress Violations**.

    3. On the Violation Unsuppressed Confirmation pop-up, you can provide an explanation for the unsuppression.

4. Click **OK**.

   This submits a job to do the unsuppression asynchronously and returns you to the result library. An unsuppression adds an annotation to the underlying event that the violation is unsuppressed along with the reason (if a reason was provided).

   Note: The job results are not instantaneous. It may take a few minutes for the results to be displayed.

- **Manual Rule Violations tab**

  To clear a manual rule violation:

  1. Select one or more manual rule violations.

  2. Click **Clear Violations**.

  3. On the Clear Violations Confirmation pop-up, you can clear the violation indefinitely or provide a date by which the clear will end. Optionally, you can provide an explanation for the clear.

  4. Click **OK**.

     This submits a job to do the manual rule violations clearing asynchronously and returns you to the Result Library page. Clearing manual rule violations also clears the underlying violation event.

     Note: The job results are not instantaneous. It may take a few minutes for the results to be displayed.

## 8.10 Additional Information

For further information regarding Compliance Management refer to the "Managing Compliance" section of the *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*.

http://docs.oracle.com/cd/E24628_01/em.121/e27046/compliance_lcm.htm#EMLCM9378

Inventory and Usage Details

This chapter describes the features and how to access the Inventory and Usage Details page (Figure 9–1) for the Microsoft SQL Server.

Figure 9–1   Microsoft SQL Server Inventory and Usage Details Page
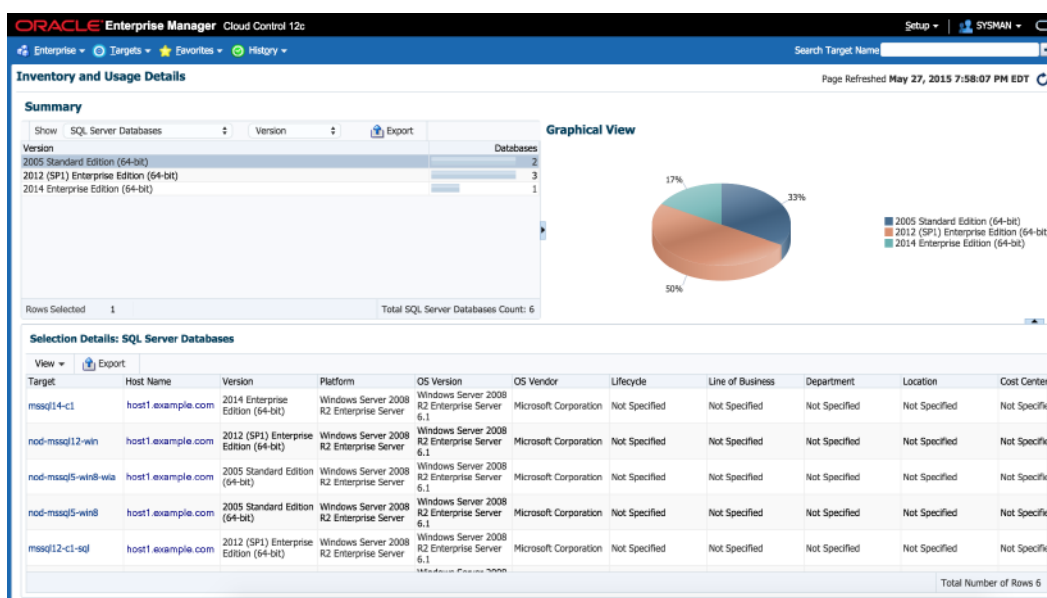
9.1 Inventory and Usage Details Page Feature Summary

With the Inventory and Usage Details page you can:

- View inventory summaries for your Microsoft SQL Server databases.

- View inventory summary information in the context of different dimensions such as version, platform, OS version and vendor, life cycle, department, location, and cost center.

- Drill down multiple levels of inventory details.

- View to a pie chart to break down the inventory data for the roll-up option by color-coded percentages.

- Repeatedly revise selections to refresh chart and details based on new selections.

- Export deployment and details tables as a `.csv` file.

9.2 Accessing the Inventory and Usage Details Page

To view inventory and usage details:

1. From the **Enterprise** menu, select **Configuration**, and then select **Inventory and Usage Details**.

   Alternatively, you can click **Details** in the Inventory and Usage region of the Enterprise Summary page.

2. Select the entity you want to examine and choose a roll-up option. For example, show all deployed hosts rolled up by platform. The page refreshes automatically upon selection.

3. In any given row in the top table, there is a count bar next to the count that represents a percentage of the maximum count. For example, if the maximum number of hosts by platform is four, the bar for hosts represented on two platforms would be half as long. Click the bar to refresh the details table and chart for the row.

9.3 Additional Information

For further information, refer to the "Inventory and Usage" section of the *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*:

http://docs.oracle.com/cd/E24628_01/em.121/e27046/config_mgmt.htm#EMLCM11629

Index