Oracle® Tuxedo System and Applications Monitor Plus

Configuration Guide

12*c* Release 2 (12.1.3)

June 2015

Oracle TSAM Plus Configuration Guide, 12*c* Release 2 (12.1.3)

Contents

CHAPTER 1

Configuring Oracle TSAM Plus Agent

This chapter contains the following topic:

Oracle TSAM Plus Agent Overview

The Oracle TSAM Plus Agent handles all Tuxedo-side back-end logic. It includes the following sub-components:

- Standalone TSAM Plus Agent components working in conjunction with the Oracle TSAM Plus Manager:
  - Oracle TSAM Plus Framework: The framework is the data collection engine. It is an independent layer working between Tuxedo infrastructure and other TSAM Plus components. This module is responsible for run time metrics collection, alert evaluation and monitoring policy enforcement.
  - Oracle TSAM Plus Plug-in: An extensible mechanism invoked by the Oracle TSAM Plus Framework. The Oracle TSAM Plus Agent provides default plug-ins to send data to the LMS (Local Monitor Server), and then to the Oracle TSAM Plus Manager. The plug-in allows custom plug-in to be hooked to intercept the metrics. The default plug-in

communicates with LMS with share memory. Application will not be blocked at metrics collection point.

You can develop your own plug-ins for additional data processing. A customized plug-in can be linked to an existing plug-in chain, or replace the default plug-in.

  - Local Monitor Server (LMS): The LMS is an Oracle Tuxedo system server. The Oracle TSAM Plus default plug-in sends data to the LMS. The LMS then passes the data to the Oracle TSAM Plus Manager in HTTP protocol. LMS is required on each Tuxedo machine if the node need to be monitored.
  - accrpt: An utility to analyze accounting and chargeback information generated by `-a` option in `servopts(5)`.

- JMX agent, which works in conjunction with the Enterprise Manager for Oracle Tuxedo to enable you to monitor and manage Oracle Tuxedo applications through the JMX interface and furthermore, through the Oracle Enterprise Manger cloud control 12c.
- Oracle Tuxedo Scripting tool, a command-line scripting environment that you can use to manage and monitor Tuxedo domains.
- BTM observer, which is used to monitor business transactions end-to-end spanning products, for example, Oracle WebLogic Server and Oracle Tuxedo.

Configuring Standalone TSAM Plus Agent

Prerequisites

To effectively and correctly use the Oracle TSAM Plus Agent, note the following prerequisites:

- The system clocks for all monitored Tuxedo machines and the Oracle TSAM Plus Manager are synchronized. A uniform time server is recommended.
- Set each Tuxedo domain to a unique DOMAINID in the UBBCONFIG file.

Adding LMS to UBBCONFIG

Local Monitor Server (LMS) performs the following tasks:

- Acts as a data proxy server between Oracle TSAM Plus agent framework and Oracle TSAM Plus Manager
- Accepts policy and alert configuration request from Oracle TSAM Plus Manager and apply to Tuxedo domain

- Sends Tuxedo domain configuration to Oracle TSAM Plus Manager
- Other help functionality

For more information, see LMS in the Oracle TSAM Plus Reference Guide.

To properly deploy the Oracle TSAM Plus Agent, you must add the LMS to each Oracle Tuxedo machine section in the UBBCONFIG file. Listing 1-1 shows an example.

Listing 1-1 LMS Added to UBBCONFIG File

```
...
*MACHINES
MACHINEA
...
*GROUPS
...
LMSGRP LMID=MACHINEA
...
*SERVERS
LMS SRVGRP=LMSGRP SRVID=1 CLOPT="-A -- -l tsamweb.abc.com:8080/tsam"
...
```

The "`-l`" option specifies the Oracle TSAM Plus Data Server address which is configured in the Oracle TSAM Plus Manager. For more information, see the Oracle TSAM Plus Reference Guide. The Oracle TSAM Plus Data Server uses the same port number as the Oracle TSAM Plus Manager Console.

Note: LMS can also be added to a running Oracle Tuxedo application using TMIB.

Turning Oracle TSAM Plus On and Off

You can use a `tmadmin` command to turn on or turn off Oracle TSAM Plus. The command format is:

```
changemonitor (chmo) [-m machine] on|off
```

The `-m` parameter specifies the logic machine name where the Oracle TSAM Plus collection is disabled. Without this option, monitoring on all machines is disabled. By default, monitoring is

turned on. If monitoring is turned off, all data collection is stopped even if there is a monitoring policy defined.

Configurations for Oracle Tuxedo ART for CICS and Batch Monitoring

To monitor Oracle Tuxedo Application Runtime for CICS, an additional configuration file (`Region-Group.mapping`)is required. You need to put the file in the directory specified by the `KIXCONFIG` environment variable. For more information, see Oracle Tuxedo Application Runtime for CICS Users Guide.

Note: The `KIXCONFIG environment` variable is required for all ART applications.

Listing 1-2 shows a `Region-Group.mapping` file format example.

Listing 1-2 Region-Group.mapping File Format Example

```
[region]
name= REG1
tuxgroups=APPGRP1,APPGRP2
resources_group=resgroup1,resgroup2

[region]
name= REG2
tuxgroups=APPGRP3,APPGRP4
resources_group=resgroup3,resgroup4
```

Each region has a section in this file. The CICS region is called "name". The `tuxgroups` parameter is followed by the Oracle Tuxedo group name. The `resources_group` parameter is the CICS resource group in this region.

For more information, see Oracle Tuxedo Application Runtime for CICS Reference Guide.

Note: For Oracle Tuxedo Application Runtime for CICS running on Linux, the ARTMON server must be configured in order to enable TSAM Plus monitoring.

If you need to monitor Oracle Tuxedo Application Runtime for Batch ARTJES component, set the `JESMONITOR` environment variable to `yes` before you start the LMS server.

Configuring JMX Agent

Starting the tlisten Process

Before you can use TSAM Plus to monitor the Tuxedo domain targets, you must start the `tlisten` process before starting the Tuxedo domain so that Tuxedo Domain MBeans can register with the JMX agent embedded in the `tlisten` process. For MP domains in particular, you should start `tlisten` for every machine.

Note: If Oracle TSAM Plus is used in conjunction with Oracle TSAM Plus 12c, either JRE 1.6 or one of the following JDK 1.6 versions is required to start the embedded JMX agent:

- 1.6.0 to 1.6.0_38 for both SUN JRE/JDK
- SR2 to SR9 for Linux on System z
- 1.6.0.00 to 1.6.0.17 for HP platform

It is also recommended you use the JRE shipped under TSAM Plus install directory.

Before starting `tlisten`, you must set the `tlisten` environment variable `SHLIB_PATH/LIBPATH/LD_LIBRARY_PATH` and include the `libjvm` library path. For windows platforms, you only need to set `JAVA_HOME`. For HP platforms, you need to set `LD_PRELOAD` to include the `libjvm.so` directory.

Listing 1-3 shows examples of environment variable settings on different platforms:

Listing 1-3 Environment Variable Setting on Different Platforms

For Linux 64-bit platforms:

```
LD_LIBRARY_PATH=$TUXDIR/lib:$JAVA_HOME/jre/lib/amd64/server:$LD_LIBRARY_PA
TH;

export LD_LIBRARY_PATH;
```

For AIX 64-bit platforms:

```
LIBPATH=$TUXDIR/lib:$JAVA_HOME/jre/lib/ppc64:${JAVA_HOME}/jre/lib/ppc64/de
fault:$LIBPATH;

export LIBPATH;
```

For HP 64-bit platforms:

```
LD_LIBRARY_PATH=$TUXDIR/lib:$JAVA_HOME/jre/lib/IA64W/server:$LD_LIBRARY_PA
TH;

export LD_LIBRARY_PATH;

LD_PRELOAD=$JAVA_HOME/jre/lib/IA64W/server/libjvm.so;

export LD_PRELOAD;
```

Note: `LD_PRELOAD` is only used for `tlisten` to start embedded JMX agent. It should not be set when building Tuxedo applications.

To start `tlisten`, use the following command:

```
tlisten -j rmi://<host>:<rmiport> -l //<host>:<tlistenport>
```

Note: Make sure that the host and port specified by the `-l` option are the same as the `NLSADDR` value specified inthe `UBBCONFIG` file.

When the `tlisten` process is started correctly, you can view the message "**RMI connector server successfully started** and **Started the embedded JMX agent successfully"** in ULOG.

The following functions are added to the `tlisten` process:

- A JMX agent is embedded, and creates a JMX domain for every Tuxedo Domain (SHM mode), or Tuxedo Machine (MP mode), connecting to it. Every MBean in the JMX domain corresponds to a Tuxedo target.
- `tlisten` acts as the Tuxedo-side monitoring and management agent . It receives monitoring and management requests from Enterprise Manager and dispatches these requests to corresponding Tuxedo services.
- `tlisten` creates a Tuxedo context for each JMX connection. If a monitored Tuxedo domain enables authentication and authorization, `tlisten` provides the credentials attained from Enterprise Repository when it attaches a Tuxedo domain.
- If the JMX fetchlet in EM agent sends a metrics request to `tlisten`, `tlisten`:
  - transforms the request message to an FML32 buffer and forwards the request to the MIB service of the corresponding Tuxedo domain,
  - receives the metrics conveyed in the response buffer and then returns metrics to Enterprise Repository agent. The connection between the JMX fetchlet and the `tlisten` agent are reused across multiple metrics requests for the same Enterprise Repository user.

- `tlisten` also forwards job requests from Enterprise Repository agent to MIB service. Enterprise Repository agent creates a new JMX connection for every job request, and releases the connection after the job finishes. Accordingly, `tlisten` creates a Tuxedo context for each job request.

For more information about additional `tlisten` options for JMX monitoring, see Oracle TSAM Plus Reference Guide.

Configuring the UBBCONFIG File

Adding the NETWORK Section

To monitor and manage the Tuxedo domain monitoring targets, you must register the targets in the `tlisten` process by adding the `*NETWORK` section and configuring the `NLSADDR` parameters inthe `UBBCONFIG` file for the Tuxedo domain in SHM mode.

Adding EXT_MON in the RESOUCES Section

Collection and calculation of certain metrics (such as Service Metrics and IPC Queue Metrics in MIB), consumes CPU time and potentially impacts Oracle Tuxedo performance. Oracle Tuxedo uses the `EXT_MON OPTIONS` parameter in the `UBBCONFIG` file `*RESOURCES` section to allow MIB performance sensitive metrics collection.

If the indicator is specified, all metrics listed in the Tuxedo Targets section are collected in MIB; otherwise, if the indicator is not specified, the following metrics are not collected by Oracle Tuxedo:

- Tuxedo Server Service metrics
- Tuxedo Server IPC Queue metrics
- Tuxedo Bridge IPC Queue metrics

The metrics collection policy changes immediately once you modify this parameter setting.

Listing 1-4 shows an SHM mode `UBBCONFIG` file example supporting Enterprise Manager monitoring.

Listing 1-4 An SHM UBBCONFIG Sample Supporting Enterprise Manager Monitoring

```
*RESOURCES
IPCKEY     65831
```

```
DOMAINID   shm
MASTER    L1
MODEL     SHM
MAXACCESSERS 100
MAXSERVERS  100
OPTIONS    EXT_MON
*MACHINES
"<hostname>" LMID     = L1
     APPDIR   = "/testarea/tux/test/jmx/servers"
    TUXCONFIG = "/testarea/tux/test/jmx/servers/tuxconfig"
     TUXDIR   = "/testarea/tux/oracle/tuxedo12c"
*GROUPS
ATMIGRP1   LMID     = L1
       GRPNO     = 10
*SERVERS
SvrUpdate  SRVGRP    = ATMIGRP1
       SRVID     = 100
*SERVICES

*NETWORK
"L1"
NLSADDR="<hostname>:16998"
```

Configuring BTM Observer

A new CLOPT option is introduced for `GWTDOMAIN`.

`-m`

The BTM monitor URL. The format is `http://<HOST>:<PORT>/btmmonitor/agent/agent/`.

Example:

```
GWTDOMAIN SRVGRP="gwgrp" SRVID=1003 CLOPT="-A -- -m
http://bej301493.cn.oracle.com:9001/btmmonitor/agent/agent/"
```

When this option is specified, `GWTDOMIAN` starts an embedded JVM and runs a BTM delegate observer to monitor bidirectional calls between WTC and itself.

CHAPTER 2

Configuring Oracle TSAM Plus Manager

This chapter describes configuration tasks made on Oracle TSAM Plus Manager after you have configured standalone TSAM Plus Agent as described in the first chapter.

This chapter contains the following topics:

Overview

The Oracle TSAM Plus Manager is the data manipulation and representation component of Oracle TSAM Plus. It is a J2EE application. The Oracle TSAM Plus Manager provides the following functionality:

- Communicates with the Oracle TSAM Plus Agent for performance metrics, configuration information and other utility messages.
- Provides a Web console for Oracle TSAM Plus administration, monitored data presentation and alerts management.

Configuring Oracle TSAM Plus Data Server

The Oracle TSAM Plus Data Server is the communication interface to Oracle TSAM Plus. It accepts requests from LMS and metrics query requests from web browser. For each LMS, the URL of the data server must be configured correctly. The format is as follows:

```
CLOPT="-A -- -l host:port/tsam"
```

- `host` is the box where the web application deployed.
- `port` is the port number of the java server.
- `tsam` is the Oracle TSAM Plus URL.

Note: From an HTTP perspective, the Oracle TSAM Plus Agent LMS is the HTTP client, and the Oracle TSAM Plus Manager is the HTTP server. If a firewall is deployed between the Oracle TSAM Plus Manager and Tuxedo applications, the firewall must allow the LMS to issue HTTP requests to the Oracle TSAM Plus Manager.

Configuring Oracle TSAM Plus Manager

Oracle TSAM Plus Manager provides some global parameters for tuning purpose. They are available at the Data Management/Global Parameters page. For more information, see Oracle TSAM Plus User Guide.

TSAM Plus LDAP Configuration File

The Oracle TSAM Plus LDAP configuration file is similar to the Oracle Tuxedo GAUTHSVR configuration file.

Although the default values for the LDAP configuration file are usually sufficient, you can choose to configure it with different names. Therefore, you should be aware of the following requirements for the LDAP configuration file:

- The LDAP configuration file is a plain text file.
- Keywords are case-sensitive, but their order does not matter. The keyword format is `keyword=value`.
- Blank lines or lines starting with a # sign are treated as comments, and are ignored.
- The upper limit of a line is 255 characters. If a line exceeds this upper limit, it is truncated.

- The Principal must have privileges to access the LDAP database (usually the LDAP administrator).

Table 2-1 lists the LDAP configuration file keywords.

Table 2-1 LDAP Configuration File Keywords

Configuration Keyword	Value Type	Description
`Host`	string	The host name or IP address of the LDAP server.The default value is `localhost`.
`Port`	numeric	The port number on which the LDAP server is listening.The default value is `389`.
`Principal`		The Distinguished Name (DN) of the LDAP user that is used to connect to the LDAP server.
`Credential`		The credential (generally a password) used to authenticate the LDAP user that is defined in the Principal attribute.
`UserObjectClass`	string	The LDAP object class that stores users. The default is `person`.
`UserBaseDN`	string	The base distinguished name (DN) of the tree in the LDAP directory that contains users. The default is `ou=people`, `o=example.com`
`UserFromNameFilter`	string	An LDAP search filter for finding a user given the name of the user. The default is `(&(cn=%u)(objectclass=person))`
`UserUIDAttrName`	string	The attribute name of an LDAP user object that specifies the UID of the user or the UID and GID of the user in a fixed format. The default value is `userid`.
`UserGroupAttrNames`	string	The attribute names of an LDAP user object that specify the groups the user belongs to. This attribute can contain three types of values: GID, group CN and group DN. One type of value for each configuration. More names are separated by comma. The default value is `usergroups`.
`RetrieveUIDAndGID`	boolean	It should always be "true"

Table 2-1 LDAP Configuration File Keywords

Configuration Keyword	Value Type	Description
`UIDAttrValueType`	string	It should always be "UIDAndGID"
`UseZOSRACF`	boolean	Specifies whether the LDAP server is z/OS RACF LDAP server. The default is `false`.
`SSLEnabled`	boolean	Specifies that SSL is used to connect to the LDAP server
`ConnectTimeout`	numeric	The maximum number of seconds to wait for the LDAP connection to be established. If set to `0`, there is no maximum time limit. The default value is `0`.

Weblogic Embedded LDAP Server LDAP Configuration File Example

Listing 2-1 shows a Weblogic embedded LDAP server LDAP configuration file example.

Listing 2-1 Weblogic Embedded LDAP Server LDAP Configuration File Example

```
Host = localhost
Port = 7001
Principal = cn=Admin
Credential = aaa
UserObjectClass = person
UserBaseDN = ou=people,ou=myrealm,dc=base_domain
UserFromNameFilter = (&(uid=%u)(objectclass=person))
UserUIDAttrName = description
UserGroupAttrNames=wlsMemberOf
RetrieveUIDAndGID = true
UIDAttrValueType = UIDAndGID
UseZOSRACF=false
SSLEnabled=false
ConnectTimeout=5
```

CHAPTER 3

Configuring Enterprise Manager for Oracle Tuxedo

This chapter describes subsequent configuration tasks made on Enterprise Manager for Oracle Tuxedo after you have configured JMX agent as described in the first chapter.

This chapter contains the following topics:

Discovering and Adding Oracle Tuxedo Targets

In order to manage and monitor Oracle Tuxedo applications, you must first discover the Tuxedo targets using Enterprise Manager Cloud Control.

Once discovered, the domain and the components within it can be promoted to "managed target" status and an automatic discovery job runs every 24-hours to update the targets. In this process, management agents are assigned to each target, enabling Enterprise Manager Cloud Control to collect the data needed to monitor the target.

This section covers the following topics:

Discovering Targets Manually

To discover all Tuxedo domains on a JMX agent, do the following steps:

1. Log in to Enterprise Manager Cloud Control.
2. From the home page, go to **Targets >Middleware**.
3. Click **Middleware Features** >**Tuxedo Summary**.
4. In the Tuxedo Summary page, click **Add** > **Tuxedo Domain Discovery**.
5. If only one domain exists in the JMX agent, specify the following options on the page that appears:
   - **Hostname**: Mandatory parameter. Specifies the host where the Tuxedo domain master machine is running.
   - **Port**: Mandatory parameter. The port number specified by `tlisten -j` option.
   - **Application Password**: Optional parameter. Specifies the Tuxedo application password Enterprise Manager agent uses to connect to the Tuxedo domain. You must input this parameter if the Tuxedo domain `SECURITY` value is one of following: `APP_PW`, `USER_AUTH`, `ACL`, or `MANDATORY_ACL`; otherwise, leave the field blank.
   - **User name**: Optional parameter. Specifies the Tuxedo user name Enterprise Manager agent uses to connect to the Tuxedo domain. You must input this parameter if the Tuxedo domain `SECURITY` value is one of following: `USER_AUTH`, `ACL`, or `MANDATORY_ACL`; otherwise, leave the field blank.
   - **User Password**: Optional parameter. Specifies the Tuxedo user password Enterprise Manager agent uses to connect to the Tuxedo domain. You need to input this parameter if the Tuxedo domain `SECURITY` value is one of following: `USER_AUTH`, `ACL`, or `MANDATORY_ACL`; otherwise, leave the field blank.
   - **Use SSL**: Optional. This option refers to SSL mechanism between Enterprise Manager and JMX agent in the `tlisten` process.
   - **Find Oracle Tuxedo Domains**: If this box is unchecked, Tuxedo security related information is ignored and only `tlisten` and the Tuxedo Home targets are discovered. Leave this box checked if you want to discover the Tuxedo domains monitored by the `tlisten` process.
   - **Monitoring Agent**: Mandatory option. It is recommended you select the one residing on the same physical machine with `tlisten`.

Note: The User name, Password, and Application password are used to generate Enterprise Manager Monitoring Credentialsfor all discovered targets. You can manage Monitoring Credentials by clicking **Setup -> Security** in the Enterprise Manager console.

6. Click **Discover Now**.

If only one domain is being monitored by `tlisten`, you will get a list of discovered targets; otherwise, select the domain on the page that appears and enter the parameters specific to the domain, then click **Discover Now** again.

Manually Adding a Standalone Target

To add a standalone Tuxedo target to Enterprise Manager Cloud Control, do the following steps:

1. Log in to Enterprise Manager Cloud Control as SYSMAN.
2. From the home page, navigate to **Setup >Add Targets**.
3. Click **Add Targets Manually >Add Non-Host Targets by Specifying Target Monitoring Properties**.

Enterprise Manager Cloud Control bypasses `tlisten` and directly adds the target into Enterprise Repository.

Configuring Security

Enterprise Manager for Oracle Tuxedo supports the following security mechanism:

Tuxedo Authentication and Authorization

If the `SECURITY` parameter of the Tuxedo domain is `APP_PW`, Enterprise Manager agents provide a Tuxedo application password for authentication. If the `SECURITY` parameter is `USR_AUTH`, `ACL` or `MANDATORY_ACL`, Enterprise Manager agents provide application password, user name, and user password for authentication; meanwhile, `AUTHSVR` must be configured in the `UBBCONFIG` file.

The client name of Tuxedo users used by Enterprise Manager must be "`tpsysadm`"; otherwise, some metrics and job requests will fail.

JOB

When any JOB (based on Tuxedo security configuration), is invoked, the following three cases may occur.

- `NONE`

  No "Credentials" page appears. Your job is executed immediately.

- `APP_PW`

"Credentials" page appears, requiring you to provide Tuxedo username, password, and application password. Enterprise Manager OMS takes such information together to talk with JMX agent. If authentication is passed, your job is executed ; otherwise, your job will be rejected.

Note: Even though Tuxedo does not use the value of Tuxedo Username and Tuxedo Password fields to authenticate or authorize, the two fields must be inputted as place holders.

- `ACL/ACL_MANDATORY`

  "Credentials" page appears requiring you to provide Tuxedo username, password, and application password. Enterprise Manager OMS uses this information to talk with JMX agent. If authentication is passed, the job is executed afterwards; by contrast, if either authentication or authorization is failed, your job will be rejected.

  Note: The startup of Tuxedo targets with Tuxedo Domain or Tuxedo Machine type:

  - does not need Authentication or Authorization;
  - can be invoked under any its target status.

Discovery

After discovery, all targets, which are required to update status/metric, are updated with username/password and application password into its target instance property.

For more information, see Discovering and Adding Oracle Tuxedo Targets.

Metric Fetchlet

Invoked by Enterprise Manager Agent, fetchlet utilizes username, password, and application password (which are stored as target instance properties), to connect with Tuxedo JMX Agent when Tuxedo security is enabled.

Standalone JMX Authentication

If you don't want to enable Oracle Tuxedo authentication, but require authentication at JMX interface, you can configure the standalone JMX authentication.

To enable the standalone JMX authentication, do the following steps:

1. Run the command line tool `jmxaaacfg` to generate the password file.

   The usage of `jmxaaacfg` is as follows:

   ```
   $ jmxaaacfg [action] [username] [password] [password file name]
   ```

The argument `action` specifies one of the actions in add/delete/modify.

- `add`: adds a new username/password pair.
- `delete`: deletes the username/password pair.
- `modify`: changes an existing username/password pair.

The parameters "`username`" and "`password`" are plaintext. `jmxaaacfg` will make it encrypted and save it in a password file the user creates. JMX AAA password file has its own format for RMI authentication, which is "`username password`". The parameter `[password file name]` should include a reasonable absolute path of the password file the user want to store.

For example:

```
a. jmxaaacfg add [username] [password] [path/filename]
b. jmxaaacfg modify [username] [new password] [path/filename]
c. jmxaaacfg delete [username] [path/filename]
```

2. Add the `-q` option to tlisten. The `-q` option specifies the location of the password file.

SSL Connection Between EM OMS/Agent and JMX Agent Embedded in "tlisten" Process

SSL connection has two types:

- Between EM OMS and JMX agent

  For example: Admin job action from every Tuxedo target home page, such as startup/shutdown, etc.

- Between EM Agent and JMX agent

  Both Metric fetchlet and Discovery (Manual / Automatic) are based on this connection.

Note: You must install Enterprise Manager Cloud Control using advanced configuration mode, otherwise the admin job (modify UBB/boot or shutdown one target) will fail.

For more information, see Starting the tlisten Process.

JMX Agent

To enable SSL, you should enable SSL at `tlisten` startup. For more information , see Starting the tlisten Process.

If JMX Agent enables SSL, Enterprise Manager OMS/Agent must enable SSL; otherwise, OMS fails to connect with JMX Agent.

Discovery

If JMX Agent enables SSL, the "Use SSL" checkbox must be checked onthe discover UI page; otherwise, discovery will be rejected.

At discovery UI, if the "Use SSL" checkbox is checked, the discovery process runs with SSL security. Before discovery with the enabled SSL, the SSL runtime environment should be ready in three areas: Tuxedo Application, Enterprise Manager OMS, and Enterprise Manager Agent.

- For Tuxedo Application

  Make sure SSL is enabled for JMX Agent. For more information, see Starting the tlisten Process.

- For Enterprise Manager OMS
  - Trust store should be configured well.
  - Each time auto discovery is invoked, "Use SSL" property on the domain target is checked. If "Use SSL" is `true`, the connection between OMS and JMX Agent is under SSL; otherwise, it is not.
  - Each time a job is invoked from Tuxedo target home page, "Use SSL" property on the domain target is checked. If "Use SSL" is true, the connection between OMS and JMX Agent is under SSL; otherwise, it is not.
- For Enterprise Manager agent
  - Trust store should be well configured.
  - Modify startup options for SSL.
  - If a metric collection is scheduled, "Use SSL" property on that target is checked. For the connection between Enterprise Manager agent and JMX agent, if "Use SSL" is `true`, SSL is enabled; otherwise, it is not.
  - If discovery is successful, Enterprise Manager OMS saves all targets discovered using target properties (of which "Use SSL" should be set to `true`).

WARNING: If you have already discovered all Tuxedo targets with SSL disabled and then started JMX agent with SSL enabled, Enterprise Manager OMS/Agent fails to connect with JMX agent; all relative targets status is unknown and all job actions from the Tuxedo home page are rejected.

Solution: you should run manual discovery again if this scenario occurs.

Keystore and Trust Store Configuration

JMX Agent

keystore

`tlisten` startup options provide keystore location/password to enable SSL.

Notes:

- You must keep or know the keystore password;
- Reboot `tlisten` after `keystore` change if `tlisten` is active.

Listing 3-1 Example - Generate keystore.jks

```
$ keytool -genkeypair -alias tuxedo -keyalg RSA  -validity 1825  -keystore
keystore.jks
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  Tuxedo
What is the name of your organizational unit?
  [Unknown]:  Oracle Tuxedo
What is the name of your organization?
  [Unknown]:  Oracle Corporation
What is the name of your City or Locality?
  [Unknown]:  Redwood Shores
What is the name of your State or Province?
  [Unknown]:  CA
What is the two-letter country code for this unit?
  [Unknown]:  US
```

```
Is CN=Tuxedo, OU=Oracle Tuxedo, O=Oracle Corporation, L=Redwood Shores,
ST=CA, C=US correct?
  [no]:  yes


Enter key password for <tuxedo>
        (RETURN if same as keystore password):
```

Note: You must press Enter to set key password the same as keystore password ; otherwise, your discovery will not succeed.

Enterprise Manager OMS

Trust Store

On the OMS side, SSL follows the standard Java Secure Socket Extension (JSSE). For more information , see the Java Secure Socket Extension (JSSE) Reference Guide.

To configure trust store, do the following steps:

1. Generate a JMXAgent trust certificate from JMXAgent keystore. (Suppose the certificate name is `tuxedo.cer`.)
2. Import JMXAgent trust certificate into one of the following trust stores:
   - The trust store given by `javax.net.ssl.trustStore`, if such option is set in the WLS startup script, `startWebLogic.sh`, or WLS startup system property.
   - `$MW_HOME/jdk16/jdk/jre/lib/security/jssecacerts`, if it exists.
   - `$MW_HOME/jdk16/jdk/jre/lib/security/cacerts`, if it exists.

     Where, `$MW_HOME` is the Oracle Enterprise Manager installation directory.

Listing 3-2 Example - Export Certificate

```
$ keytool -export -alias tuxedo  -keystore keystore.jks -rfc -file
tuxedo.cer
Enter keystore password:
Certificate stored in file <tuxedo.cer>
```

Listing 3-3 Example - Import tuxedo.cer

```
$ keytool -import -alias tuxedo -file tuxedo.cer -keystore
$MW_HOME/jdk16/jdk/jre/lib/security/jssecacerts

Enter keystore password:

Re-enter new password:

Owner: CN=Tuxedo, OU=Oracle Tuxedo, O=Oracle Corporation, L=Redwood Shores,
ST=CA, C=US

Issuer: CN=Tuxedo, OU=Oracle Tuxedo, O=Oracle Corporation, L=Redwood
Shores, ST=CA, C=US

Serial number: 4fab2940

Valid from: Thu May 10 10:34:40 CST 2012 until: Tue May 09 10:34:40 CST 2017

Certificate fingerprints:

         MD5:  63:E2:6E:93:AD:5A:7F:21:CB:3C:51:3F:8C:92:AA:0D

         SHA1: 77:D2:86:4F:74:A3:84:64:A0:5B:CA:50:7A:EF:66:DC:7F:92:83:0F

         Signature algorithm name: SHA1withRSA

         Version: 3

Trust this certificate? [no]:  yes

Certificate was added to keystore
```

Note: The default password for `$MW_HOME/jdk16/jdk/jre/lib/security/jssecacerts` and `$MW_HOME/jdk16/jdk/jre/lib/security/cacerts` is **changeit**.

Enterprise Manager Agent

Trust Store

Enterprise Manager Agent may have a trust store pre-installed , `$ORACLE_HOME/sysman/config/montrust/AgentTrust.jks`, where `$ORACLE_HOME` is the

installed Enterprise Manager agent directory (e.g.,`/testarea/em/installed_em/EM_110922/agent/agent_inst`).

If `AgentTrust.jks` exists, you should import your public key into `AgentTrust.jks`; otherwise, copy `TuxedoTrust.jks` to `$ORACLE_HOME /sysman/config/montrust/` and rename it to `AgentTrust.jks`.

Usually, on the Enterprise Manager Agent side, you need to import the CA certificate into `$EMAGENT_HOME/agent_inst/sysman/config/montrust/AgentTrust.jks`. For AIX 5.3 64-bit platforms, you must also import the CA certificate into `$EMAGENT_HOME/core/<agent_version>/jdk/jre/lib/security/cacerts`.

For example, type the following commands:

```
cd  $EMAGENT_HOME/core/<agent_version>/jdk/jre/lib/security
```

```
keytool -import -alias tuxedo -file tuxedo.cer -keystore
$EMAGENT_HOME/core/<agent_version>/jdk/jre/lib/security/cacerts -storepass
changeit
```

Where:

- `$EMAGENT_HOME` is the agent install home on the AIX host
- `tuxedo` is the CA certificate alias
- `tuxedo.cer` is the CA certificate file

Notes:

- The Trust store name is `AgentTrust.jks` and the password is "`welcome`"; both of them are unchangeable.
- Reboot Enterprise Manager Agent after `truststore` change if Enterprise Manager Agent is active.

Listing 3-4 Example - Import into AgentTrust.jks

```
$ keytool -import -alias tuxedo -file tuxedo.cer -keystore AgentTrust.jks

Enter keystore password:

Owner: CN=Tuxedo, OU=Oracle Tuxedo, O=Oracle Corporation, L=Redwood Shores,
ST=CA, C=US
```

```
Issuer: CN=Tuxedo, OU=Oracle Tuxedo, O=Oracle Corporation, L=Redwood
Shores, ST=CA, C=US
Serial number: 4fab2940
Valid from: Thu May 10 10:34:40 CST 2012 until: Tue May 09 10:34:40 CST 2017
Certificate fingerprints:
         MD5:  63:E2:6E:93:AD:5A:7F:21:CB:3C:51:3F:8C:92:AA:0D
         SHA1: 77:D2:86:4F:74:A3:84:64:A0:5B:CA:50:7A:EF:66:DC:7F:92:83:0F
         Signature algorithm name: SHA1withRSA
         Version: 3
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

Listing 3-5 Example - Verify AgentTrust.jks

```
$ keytool -list -v -keystore AgentTrust.jks
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 11 entries

...

Alias name: tuxedo
Creation date: May 10, 2012
Entry type: trustedCertEntry
```

```
Owner: CN=Tuxedo, OU=Oracle Tuxedo, O=Oracle Corporation, L=Redwood Shores,
ST=CA, C=US

Issuer: CN=Tuxedo, OU=Oracle Tuxedo, O=Oracle Corporation, L=Redwood
Shores, ST=CA, C=US

Serial number: 4fab2940

Valid from: Thu May 10 10:34:40 CST 2012 until: Tue May 09 10:34:40 CST 2017

Certificate fingerprints:

         MD5:  63:E2:6E:93:AD:5A:7F:21:CB:3C:51:3F:8C:92:AA:0D

         SHA1: 77:D2:86:4F:74:A3:84:64:A0:5B:CA:50:7A:EF:66:DC:7F:92:83:0F

         Signature algorithm name: SHA1withRSA

         Version: 3
```

Summary

Before enabling SSL, do the following steps:

1. Ensure that keystore at JMX agent is available and start `tlisten` with SSL enabled options correctly
2. Ensure Enterprise Manager agent trust store is available. Restart Enterprise Manager agent
3. Ensure Enterprise Manager OMS trust store is available
4. Reboot `tlisten`/EM Agent/OMS after `keystore`/`trustore` is changed
5. Ensure that SSL follows the rule of Maximum Key length (Bits) used in SSL (For example, RSA: 512 and larger; AES: 256/128).