

Tivoli Application Dependency Discovery  
Manager  
Version 7.3

*Installation Guide*



**Note**

Before using this information and the product it supports, read the information in [“Notices” on page 117.](#)

**Edition notice**

This edition applies to version 7, release 3 of IBM® Tivoli® Application Dependency Discovery Manager (product number 5724-N55) and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright International Business Machines Corporation 2006, 2020.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

<b>Figures.....</b>	<b>V</b>
<b>Tables.....</b>	<b>vii</b>
<b>About this information.....</b>	<b>xi</b>
Conventions used in this information center.....	xi
Terms and definitions.....	xi
<b>Chapter 1. Installing.....</b>	<b>1</b>
Three ways of deploying TADDM.....	1
Domain server deployment.....	2
Synchronization server deployment.....	3
Streaming server deployment.....	4
Planning for installation.....	6
Prerequisite checking.....	6
TADDM server requirements.....	10
Client requirements.....	38
Planning for monitoring of TADDM servers.....	40
Planning for security.....	40
Planning for single sign-on with IBM Tivoli CCMDB or IBM SmartCloud Control Desk.....	43
Planning worksheet for synchronization server deployment installation.....	43
Planning worksheet for streaming server deployment installation.....	46
Installing TADDM.....	50
Configuring the remote database server.....	50
Configuring for the Context Menu Service and Data Integration Service.....	52
Installing TADDM servers.....	55
Verifying the TADDM server installation.....	75
Installing TADDM with secure database.....	76
Post-installation configuration.....	76
Configuring Oracle RAC after installation.....	76
Checking the server status.....	77
Configuring clients for secure access.....	78
Clearing the Java Web Start cache.....	79
Clearing your browser cache.....	80
Configuring post-installation DB2 secure access.....	80
Configuring post-installation Oracle secure access.....	81
Enabling Software License Metric Tags.....	81
Installing SLM.....	82
Running SLM.....	82
SLM tag file.....	83
Configuring the IBM License Metric Tool log files.....	84
Upgrading TADDM.....	84
Migration tuning guidelines.....	85
Performing prerequisite tasks.....	86
Upgrading the TADDM server.....	89
Upgrading the database manually.....	94
Converting a 32-bit TADDM deployment to 64-bit.....	96
Rolling back the upgrade.....	97
Uninstalling TADDM.....	99

Uninstalling a TADDM server.....	99
Moving TADDM from one operating system to another.....	101
Troubleshooting installation problems.....	101
Troubleshooting upgrade problems.....	108
<b>Notices.....</b>	<b>117</b>
Trademarks.....	118

---

# Figures

- 1. Domain server deployment..... 2
- 2. Synchronization server deployment..... 3
- 3. Streaming server deployment..... 5
- 4. Streaming server deployment in more detail..... 6
- 5. The I/O traffic for the Windows computer system..... 26
- 6. The I/O traffic for the Linux computer system..... 26



---

# Tables

- 1. Servers and associated databases in each deployment type..... 1
- 2. Servers and associated user interfaces in each deployment type..... 2
- 3. Product codes.....10
- 4. TADDM server hardware requirements..... 13
- 5. TADDM server hardware requirements..... 14
- 6. Baseline processor types..... 15
- 7. Processor speed..... 16
- 8. Processor quantity..... 16
- 9. Memory.....16
- 10. Product codes..... 16
- 11. Processor speed.....17
- 12. Processor quantity..... 17
- 13. Memory.....17
- 14. Product codes..... 18
- 15. Processor speed.....18
- 16. Processor quantity..... 18
- 17. Memory.....19
- 18. Product codes..... 19
- 19. Processor speed.....19
- 20. Processor quantity..... 20
- 21. Memory.....20
- 22. Number of disk drives or disk arms..... 21
- 23. Product codes..... 22

24. Typical discovery rates.....	22
25. Typical discovery sensor rates.....	23
26. Sample data transfer during L2 discovery between the TADDM server and the anchor.....	24
27. Sample data transfer during L2 discovery between the TADDM server and the anchor by using lazy deployment.....	25
28. Bytes transferred between the TADDM server and the target during Level 1 discovery.....	26
29. Bytes transferred between the TADDM server and the target during Level 2 discovery.....	27
30. Example using one storage server.....	29
31. Example using two storage servers.....	29
32. Example for discovery servers.....	30
33. Results of scale tests which used a gateway with two, four, and six 2Ghz CPUs.....	30
34. Results of scale test which used various numbers of gateways.....	31
35. Comparison of the Cygwin and WinSSHD servers performance.....	32
36. Hardware requirements for anchors.....	33
37. Supported operating systems for TADDM servers.....	34
38. Supported software for TADDM database server.....	36
39. Supported browsers for the Discovery Management Console and the Data Management Portal.....	38
40. Security features and benefits for the discovery process.....	40
41. TADDM roles and permissions.....	41
42. Common installation settings.....	43
43. Settings for a Domain Server Installation.....	44
44. Synchronization server installation settings.....	45
45. Settings for Oracle database.....	45
46. Settings for DB2 database .....	46
47. Common installation settings.....	46
48. Discovery server port values.....	47



49. Port values for primary storage server.....	48
50. Port values for secondary storage server.....	48
51. Settings for DB2 database .....	48
52. Settings for Oracle database.....	49
53. Ports used by the PingSensor and PortSensor to make connections.....	49
54. TADDM deployment types and servers.....	55
55. Resulting deployment type after upgrade.....	85
56. Order in which to upgrade the TADDM servers.....	89



## About this information

---

The purpose of this PDF document version is to provide the related topics from the information center in a printable format.

## Conventions used in this information center

---

In the IBM Tivoli Application Dependency Discovery Manager (TADDM) documentation certain conventions are used. They are used to refer to the operating system-dependent variables and paths, the `COLLATION_HOME` directory, and the location of the `collation.properties` file, which is referenced throughout the TADDM documentation, including in the messages.

### Operating system-dependent variables and paths

In this information center, the UNIX conventions are used for specifying environment variables and for directory notation.

When using the Windows command line, replace `$variable` with `%variable%` for environment variables, and replace each forward slash (/) with a backslash (\) in directory paths.

If you are using the bash shell on a Windows system, you can use the UNIX conventions.

### COLLATION\_HOME directory

TADDM root directory is also referred to as the `COLLATION_HOME` directory.

On operating systems such as AIX® or Linux®, the default location for installing TADDM is the `/opt/IBM/taddm` directory. Therefore, in this case, the `$COLLATION_HOME` directory is `/opt/IBM/taddm/dist`.

On Windows operating systems, the default location for installing TADDM is the `c:\IBM\taddm` directory. Therefore, in this case, the `%COLLATION_HOME%` directory is `c:\IBM\taddm\dist`.

### Location of collation.properties file

The `collation.properties` file contains TADDM server properties and includes comments about each of the properties. It is located in the `$COLLATION_HOME/etc` directory.

## Terms and definitions

---

Refer to the following list of terms and definitions to learn about important concepts in the IBM Tivoli Application Dependency Discovery Manager (TADDM).

### access collection

A collection that is used to control the access to configuration items and permissions to modify configuration items. You can create access collections only when data-level security is enabled.

### asynchronous discovery

In TADDM, the running of a discovery script on a target system to discover systems that cannot be accessed directly by the TADDM server. Because this discovery is performed manually, and separately from a typical credentialed discovery, it is called "asynchronous".

### business application

A collection of components that provides a business functionality that you can use internally, externally, or with other business applications.

### CI

See *configuration item*.

### collection

In TADDM, a group of configuration items.

**configuration item (CI)**

A component of IT infrastructure that is under the control of configuration management and is therefore subject to formal change control. Each CI in the TADDM database has a persistent object and change history associated with it. Examples of a CI are an operating system, an L2 interface, and a database buffer pool size.

**credentialed discovery**

TADDM sensor scanning that discovers detailed information about the following items:

- Each operating system in the runtime environment. This scanning is also known as Level 2 discovery, and it requires operating system credentials.
- The application infrastructure, deployed software components, physical servers, network devices, virtual systems, and host data that are used in the runtime environment. This scanning is also known as Level 3 discovery, and it requires both operating system credentials and application credentials.

**credential-less discovery**

TADDM sensor scanning that discovers basic information about the active computer systems in the runtime environment. This scanning is also known as Level 1 discovery, and it requires no credentials.

**Data Management Portal**

The TADDM web-based user interface for viewing and manipulating the data in a TADDM database. This user interface is applicable to a domain server deployment, to a synchronization server deployment, and to each storage server in a streaming server deployment. The user interface is very similar in all deployments, although in a synchronization server deployment, it has a few additional functions for adding and synchronizing domains.

**discover worker thread**

In TADDM, a thread that runs sensors.

**Discovery Management Console**

The TADDM client user interface for managing discoveries. This console is also known as the Product Console. It is applicable to a domain server deployment and to discovery servers in a streaming server deployment. The function of the console is the same in both of these deployments.

**discovery server**

A TADDM server that runs sensors in a streaming server deployment but does not have its own database.

**domain**

In TADDM, a logical subset of the infrastructure of a company or other organization. Domains can delineate organizational, functional, or geographical boundaries.

**domain server**

A TADDM server that runs sensors in a domain server deployment and has its own database.

**domain server deployment**

A TADDM deployment with one domain server. A domain server deployment can be part of a synchronization server deployment.

In a domain server deployment, the following TADDM server property must be set to the following value:

```
com.collation.cmdbmode=domain
```

**launch in context**

The concept of moving seamlessly from one Tivoli product UI to another Tivoli product UI (either in a different console or in the same console or portal interface) with single sign-on and with the target UI in position at the proper point for users to continue with their task.

**Level 1 discovery**

TADDM sensor scanning that discovers basic information about the active computer systems in the runtime environment. This scanning is also known as credential-less discovery because it requires no credentials. It uses the Stack Scan sensor and the IBM® Tivoli® Monitoring Scope sensor. Level 1 discovery is very shallow. It collects only the host name, operating system name, IP address, fully

qualified domain name, and Media Access Control (MAC) address of each discovered interface. Also, the MAC address discovery is limited to Linux on System z® and Windows systems. Level 1 discovery does not discover subnets. For any discovered IP interfaces that do not belong to an existing subnet that is discovered during Level 2 or Level 3 discovery, new subnets are created based on the value of the `com.collation.IpNetworkAssignmentAgent.defaultNetmask` property in the `collation.properties` file.

### **Level 2 discovery**

TADDM sensor scanning that discovers detailed information about each operating system in the runtime environment. This scanning is also known as credentialed discovery, and it requires operating system credentials. Level 2 discovery collects application names and the operating system names and port numbers that are associated with each running application. If an application has established a TCP/IP connection to another application, this information is collected as a dependency.

### **Level 3 discovery**

TADDM sensor scanning that discovers detailed information about the application infrastructure, deployed software components, physical servers, network devices, virtual systems, and host data that are used in the runtime environment. This scanning is also known as credentialed discovery, and it requires both operating system credentials and application credentials.

### **multitenancy**

In TADDM, the use by a service provider or IT vendor of one TADDM installation to discover multiple customer environments. Also, the service provider or IT vendor can see the data from all customer environments, but within each customer environment, only the data that is specific to the respective customer can be displayed in the user interface or viewed in reports within that customer environment.

### **Product Console**

See *Discovery Management Console*.

### **script-based discovery**

In TADDM, the use, in a credentialed discovery, of the same sensor scripts that sensors provide in support of asynchronous discovery.

### **SE**

See *server equivalent*.

### **server equivalent (SE)**

A representative unit of IT infrastructure, defined as a computer system (with standard configurations, operating systems, network interfaces, and storage interfaces) with installed server software (such as a database, a web server, or an application server). The concept of a server equivalent also includes the network, storage, and other subsystems that provide services to the optimal functioning of the server. A server equivalent depends on the operating system:

<b>Operating system</b>	<b>Approximate number of CIs</b>
Windows	500
AIX	1000
Linux	1000
HP-UX	500
Network devices	1000

### **storage server**

A TADDM server that processes discovery data that is received from the discovery servers and stores it in the TADDM database. The primary storage server both coordinates the discovery servers and all other storage servers and serves as a storage server. All storage servers that are not the primary are called secondary storage servers.

### **streaming server deployment**

A TADDM deployment with a primary storage server and at least one discovery server. This type of deployment can also include one or more optional secondary storage servers. The primary storage server and secondary storage servers share a database. The discovery servers have no database.

In this type of deployment, discovery data flows in parallel from multiple discovery servers to the TADDM database.

In a streaming server deployment, the following TADDM server property must be set to one of the following values:

- `com.collation.taddm.mode=DiscoveryServer`
- `com.collation.taddm.mode=StorageServer`

For all servers except for the primary storage server, the following properties (for the host name and port number of the primary storage server) must also be set:

- `com.collation.PrimaryStorageServer.host`
- `com.collation.PrimaryStorageServer.port`

If the `com.collation.taddm.mode` property is set, the `com.collation.cmdbmode` property must not be set or must be commented out.

### **synchronization server**

A TADDM server that synchronizes discovery data from all domain servers in the enterprise and has its own database. This server does not discover data directly.

### **synchronization server deployment**

A TADDM deployment with a synchronization server and two or more domain server deployments, each of which has its own local database.

In this type of deployment, the synchronization server copies discovery data from multiple domain servers one domain at a time in a batched synchronization process.

In a synchronization server deployment, the following TADDM server property must be set to the following value:

```
com.collation.cmdbmode=enterprise
```

This type of deployment is obsolete. Therefore, in a new TADDM deployment where more than one server is needed, use the streaming server deployment. A synchronization server can be converted to become a primary storage server for a streaming server deployment.

### **TADDM database**

In TADDM, the database where configuration data, dependencies, and change history are stored.

Each TADDM server, except for discovery servers and secondary storage servers, has its own database. Discovery servers have no database. Storage servers share the database of the primary storage server.

### **TADDM server**

A generic term that can represent any of the following terms:

- domain server in a domain server deployment
- synchronization server in a synchronization server deployment
- discovery server in a streaming server deployment
- storage server (including the primary storage server) in a streaming server deployment

### **target system**

In the TADDM discovery process, the system to be discovered.

### **utilization discovery**

TADDM sensor scanning that discovers utilization information for the host system. A utilization discovery requires operating system credentials.

# Chapter 1. Installing

## Three ways of deploying TADDM

You can deploy IBM Tivoli Application Dependency Discovery Manager (TADDM) in a domain server deployment, a synchronization server deployment, or a streaming server deployment. The TADDM servers are different depending on the type of deployment you choose.

Table 1 on page 1 indicates the TADDM servers and associated databases that are present according to which deployment type you choose.

The synchronization server deployment is obsolete. Therefore, in a new TADDM deployment, use either a domain server deployment or a streaming server deployment. If more than one server is needed, use the streaming server deployment. A synchronization server can be converted to become a primary storage server for a streaming server deployment.

Table 2 on page 2 indicates the user interfaces that are associated with each TADDM server.

The following definitions describe the user interfaces in more detail:

### Data Management Portal

The TADDM web-based user interface for viewing and manipulating the data in a TADDM database. This user interface is applicable to a domain server deployment, to a synchronization server deployment, and to each storage server in a streaming server deployment. The user interface is very similar in all deployments, although in a synchronization server deployment, it has a few additional functions for adding and synchronizing domains.

### Discovery Management Console

The TADDM client user interface for managing discoveries. This console is also known as the Product Console. It is applicable to a domain server deployment and to discovery servers in a streaming server deployment. The function of the console is the same in both of these deployments.

Deployment type	Servers	Associated databases
domain server deployment	one domain server	The domain server has its own database.
synchronization server deployment	one synchronization server A synchronization server deployment also requires one or more domain server deployments, each of which has a domain server.	The synchronization server has its own database.
streaming server deployment	at least one discovery server	A discovery server does not have a database.
	primary storage server	The primary storage server has its own database.
	one or more optional secondary storage servers	The secondary storage servers share the database of the primary storage server.

<i>Table 2. Servers and associated user interfaces in each deployment type</i>		
<b>Deployment type</b>	<b>Servers</b>	<b>Associated user interfaces</b>
domain server deployment	one domain server	Data Management Portal
		Discovery Management Console
synchronization server deployment	one synchronization server A synchronization server deployment also requires one or more domain server deployments, each of which has a domain server.	Data Management Portal
streaming server deployment	at least one discovery server	Discovery Management Console
	primary storage server	Data Management Portal
	one or more optional secondary storage servers	Data Management Portal

## Domain server deployment

A domain is a logical subset of the infrastructure of a company or other organization. Domains can delineate organizational, functional, or geographical boundaries. The domain server runs sensors that discover data about only the respective domain.

### domain server

A TADDM server that runs sensors in a domain server deployment and has its own database.

### domain server deployment

A TADDM deployment with one domain server. A domain server deployment can be part of a synchronization server deployment.

In a domain server deployment, the following TADDM server property must be set to the following value:

```
com.collation.cmdbmode=domain
```

Figure 1 on page 2 illustrates the domain server deployment.

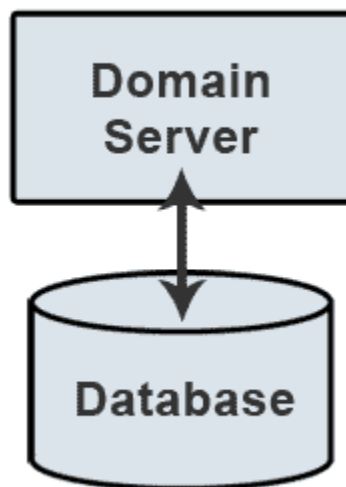


Figure 1. Domain server deployment



## Synchronization server deployment

The synchronization server is used in large enterprise environments, and it unifies the data from individual IBM Tivoli Application Dependency Discovery Manager (TADDM) domains.

### synchronization server

A TADDM server that synchronizes discovery data from all domain servers in the enterprise and has its own database. This server does not discover data directly.

### synchronization server deployment

A TADDM deployment with a synchronization server and two or more domain server deployments, each of which has its own local database.

In this type of deployment, the synchronization server copies discovery data from multiple domain servers one domain at a time in a batched synchronization process.

In a synchronization server deployment, the following TADDM server property must be set to the following value:

```
com.collation.cmdbmode=enterprise
```

This type of deployment is obsolete. Therefore, in a new TADDM deployment where more than one server is needed, use the streaming server deployment. A synchronization server can be converted to become a primary storage server for a streaming server deployment.

Figure 2 on page 3 illustrates the synchronization server deployment.

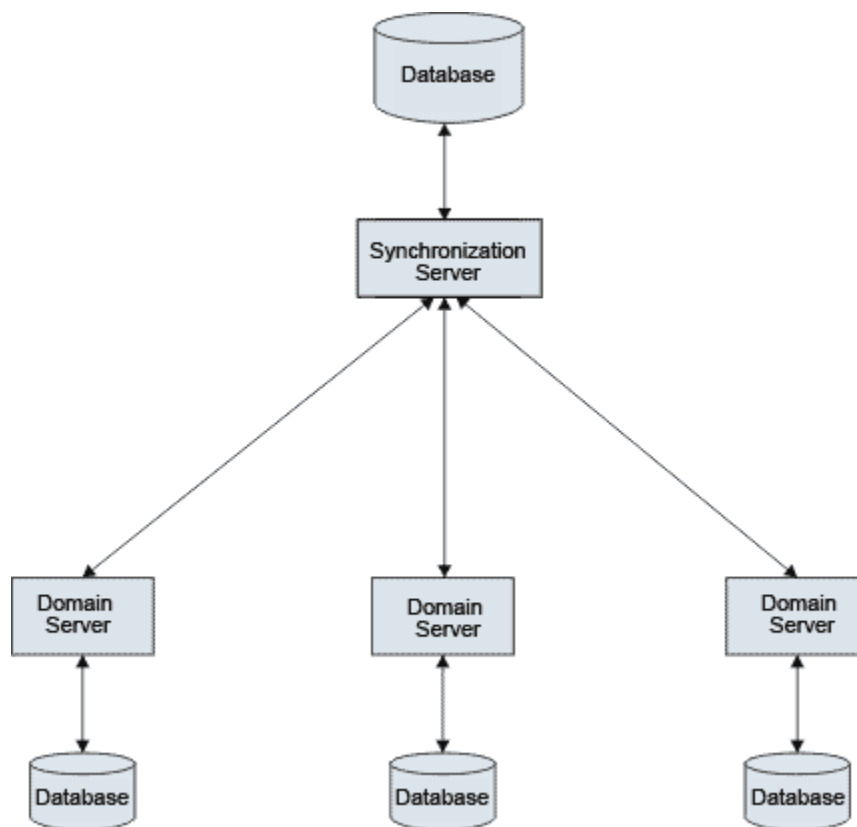


Figure 2. Synchronization server deployment

## Streaming server deployment

If your deployment requires more than one server, you realize the following benefits from using a streaming server deployment rather than a synchronization server deployment (which is obsolete): greater availability of data, cost savings, and elimination of merging problems when consolidating data.

During discovery, data flows in parallel (or streams) from multiple discovery servers to the primary storage server, where the data is processed and stored in the database. Only the primary storage server has a database. Discovery servers are used only for running sensors and therefore do not have a database.

This type of deployment therefore provides the following benefits:

### **Greater availability of data**

In a streaming server deployment, data is available as soon as it is discovered.

In contrast, in a synchronization server deployment, the data for a specific domain is unavailable until the synchronization occurs, and data is also unavailable during the synchronization.

### **Cost savings**

A streaming server deployment requires less hardware and resources.

### **Elimination of merging problems when consolidating data**

In a streaming server deployment, data streams directly to the primary storage server, which prevents the following issues that can occur in a synchronization server deployment:

- Complicated merging scenarios
- Problems that occur if domains overlap

The primary storage server is the coordinator of the storage server pool, which is a cluster of storage servers. Each secondary storage server registers with the primary storage server, and each discovery server is notified when a secondary storage server is added to, or removed from, the storage server pool.

If a discovery server has problems when trying to contact a specific secondary storage server, it tries to contact a different secondary storage server, and it continues this process until it succeeds. When a new storage server joins the storage server pool, the discovery server is notified by the primary storage server. The discovery server then contacts the new storage server.

In a streaming server deployment, you use the Data Management Portal (web-based user interface) to view discovery, topology, reporting, and analytical information. You use the Discovery Management Console (client user interface) to perform discovery-related activities, such as the following activities:

- Starting a discovery
- Showing the progress of a discovery
- Managing discovery scopes
- Managing discovery profiles
- Managing access list information

### **discovery server**

A TADDM server that runs sensors in a streaming server deployment but does not have its own database.

### **storage server**

A TADDM server that processes discovery data that is received from the discovery servers and stores it in the TADDM database. The primary storage server both coordinates the discovery servers and all other storage servers and serves as a storage server. All storage servers that are not the primary are called secondary storage servers.

### **streaming server deployment**

A TADDM deployment with a primary storage server and at least one discovery server. This type of deployment can also include one or more optional secondary storage servers. The primary storage server and secondary storage servers share a database. The discovery servers have no database.

In this type of deployment, discovery data flows in parallel from multiple discovery servers to the TADDM database.

In a streaming server deployment, the following TADDM server property must be set to one of the following values:

- `com.collation.taddm.mode=DiscoveryServer`
- `com.collation.taddm.mode=StorageServer`

For all servers except for the primary storage server, the following properties (for the host name and port number of the primary storage server) must also be set:

- `com.collation.PrimaryStorageServer.host`
- `com.collation.PrimaryStorageServer.port`

If the `com.collation.taddm.mode` property is set, the `com.collation.cmdbmode` property must not be set or must be commented out.

Figure 3 on page 5 is a simple illustration of a streaming server deployment that shows the information flow from the discovery servers to the storage server and its database. Figure 4 on page 6 provides more detail. It shows the information flow from the discovery servers, each with a Discovery Management Console, to the storage server pool, which includes multiple storage servers and one primary storage server. Each storage server has a Data Management Portal, and all storage servers share one database.

In the Data Management Portal, a storage server is shown as part of the **Storage Pool Member** list under either of the following conditions:

- The storage server is not building topologies
- The value of the TADDM server property `com.collation.AlwaysBusyStorageServer` in the `collation.properties` file is false.

If the value of the `com.collation.AlwaysBusyStorageServer` property is true, the storage server is not shown as part of the **Storage Pool Member** list because it is dedicated to graphical user interface and integration services.

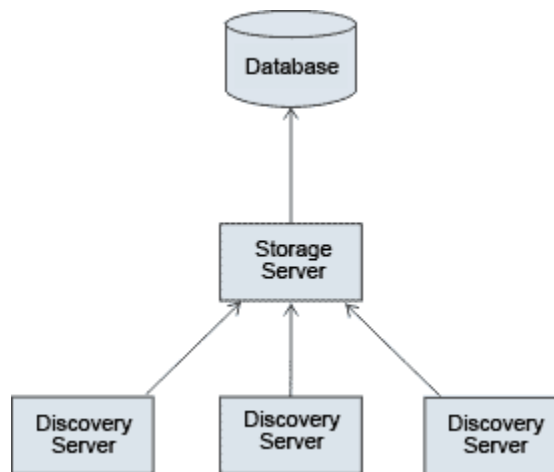


Figure 3. Streaming server deployment

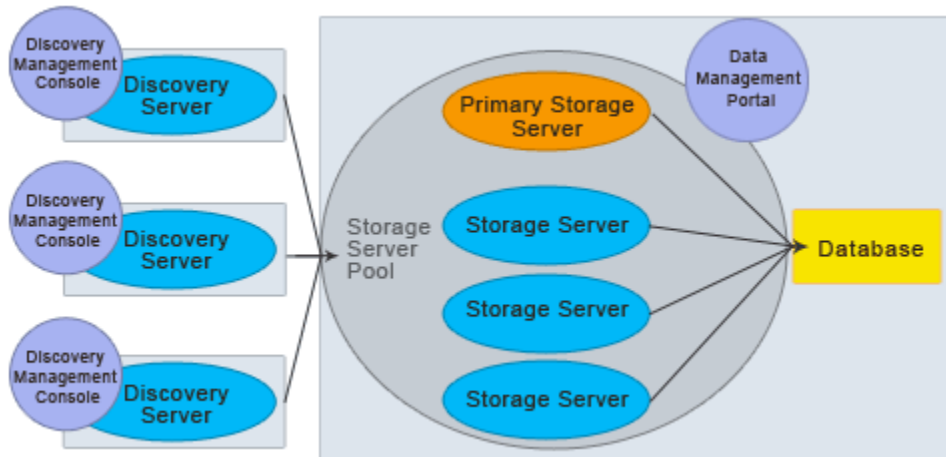


Figure 4. Streaming server deployment in more detail

## Planning for installation

Before installing TADDM, you must decide which type of TADDM deployment you want to use. Each type has different requirements and a different installation process. You must also plan for the number of servers, the types of server, and the type and location of the database.

If you plan to use TADDM with the IBM Tivoli Change and Configuration Management Database (CCMDB) or IBM SmartCloud Control Desk, refer to the planning and installing information for CCMDB or IBM SmartCloud Control Desk.

In Streaming server TADDM deployment, files are copied from the primary storage server to secondary storage server (if configured) using port 9430, hence port 9430 shall be open between primary or secondary storage servers for successful installation. In addition to this, since **http** is used by default, hence **ssl** shall not be enforced for successful installation.

## Prerequisite checking

You can perform basic prerequisite checking, before you carry out an installation, by using the prerequisite checker tool.

### Restriction:

- Prerequisite checking is not comprehensive. Some sensors or specific configurations might require additional prerequisites on the TADDM server. The prerequisite checker tool does not check for existence of such prerequisites.
- The prerequisite checker tool checks for safe average values of memory and disk space. Your installation might work with lower values.

You can find the prerequisite checker version 1.2.0.14 on the TADDM Disc 1 installation DVD in the /prereqchecker/ directory. The latest version can be downloaded from Fix Central at <http://www-933.ibm.com/support/fixcentral/swg/selectFixes?parent=ibm~Tivoli&product=ibm/Tivoli/Tivoli+Application+Dependency+Discovery+Manager&release=7.3.0&platform=All&function=all>. The name of the file is TADDM\_v730\_prerequisiteChecker.zip. If you downloaded TADDM in the zip format, zip files number 1 and 2 are the equivalent of Disc 1.

## Running the prerequisite checker

Complete the following steps to run the stand-alone prerequisite checker.

There are several TADDM configurations for which prerequisites can be checked. We categorize them by size, type of deployment, and server type. The size of a deployment is defined in terms of the number of server equivalents (SEs). The following deployment size groupings are used:

- Small deployment: Fewer than 2,000 SEs

- Large deployment: 2,000 - 10,000 SEs
- Enterprise deployment: More than 10,000 SEs

You can run the prerequisite scanner in the following two ways:

#### Quick run

In quick-run mode, you can use ready-to-run scripts that set all of the required parameters for the prerequisite checker.

#### Custom

In custom mode, you must provide all of the required (and optional) parameters for the prerequisite checker.

Run the prerequisite checker in either quick or custom mode. Complete one of the following sets of steps:

- To run the prerequisite checker in quick-run mode, complete the following steps:
  - (Optional) Copy the prerequisite checker for the appropriate operating system to the target computer.
  - Open a command-line interface:
    - On the Windows operating system, open a Command Prompt.
    - On Linux and UNIX operating systems, open a shell environment.
  - Change to the directory where the prerequisite checker is located and run the appropriate script for your environment.

For the Windows operating system, the following scripts are available:

Script	Product
taddm_domain_small.bat	IBM Tivoli Application Dependency Discovery Manager Domain Server - Small
taddm_domain_large.bat	IBM Tivoli Application Dependency Discovery Manager Domain Server - Large
taddm_domain_enterprise.bat	IBM Tivoli Application Dependency Discovery Manager Domain Server - Enterprise
taddm_domain_database_small.bat	Database Server for IBM Tivoli Application Dependency Discovery Manager Domain Server - Small
taddm_domain_database_large.bat	Database Server for IBM Tivoli Application Dependency Discovery Manager Domain Server - Large
taddm_domain_database_enterprise.bat	Database Server for IBM Tivoli Application Dependency Discovery Manager Domain Server - Enterprise
taddm_streaming_small.bat	IBM Tivoli Application Dependency Discovery Manager Discovery or Storage Server - Small
taddm_streaming_large.bat	IBM Tivoli Application Dependency Discovery Manager Discovery or Storage Server - Large
taddm_streaming_enterprise.bat	IBM Tivoli Application Dependency Discovery Manager Discovery or Storage Server - Enterprise
taddm_streaming_database_small.bat	Database Server for IBM Tivoli Application Dependency Discovery Manager Storage Server - Small

<b>Script</b>	<b>Product</b>
taddm_streaming_database_large.bat	Database Server for IBM Tivoli Application Dependency Discovery Manager Storage Server - Large
taddm_streaming_database_enterprise.bat	Database Server for IBM Tivoli Application Dependency Discovery Manager Storage Server - Enterprise

For Linux and UNIX operating systems, the following scripts are available:

<b>Script</b>	<b>Product</b>
taddm_domain_small.sh	IBM Tivoli Application Dependency Discovery Manager Domain Server - Small
taddm_domain_large.sh	IBM Tivoli Application Dependency Discovery Manager Domain Server - Large
taddm_domain_enterprise.sh	IBM Tivoli Application Dependency Discovery Manager Domain Server - Enterprise
taddm_domain_database_small.sh	Database Server for IBM Tivoli Application Dependency Discovery Manager Domain Server - Small
taddm_domain_database_large.sh	Database Server for IBM Tivoli Application Dependency Discovery Manager Domain Server - Large
taddm_domain_database_enterprise.sh	Database Server for IBM Tivoli Application Dependency Discovery Manager Domain Server - Enterprise
taddm_streaming_small.sh	IBM Tivoli Application Dependency Discovery Manager Discovery or Storage Server - Small
taddm_streaming_large.sh	IBM Tivoli Application Dependency Discovery Manager Discovery or Storage Server - Large
taddm_streaming_enterprise.sh	IBM Tivoli Application Dependency Discovery Manager Discovery or Storage Server - Enterprise
taddm_streaming_database_small.sh	Database Server for IBM Tivoli Application Dependency Discovery Manager Storage Server - Small
taddm_streaming_database_large.sh	Database Server for IBM Tivoli Application Dependency Discovery Manager Storage Server - Large
taddm_streaming_database_enterprise.sh	Database Server for IBM Tivoli Application Dependency Discovery Manager Storage Server - Enterprise

d. After the prerequisite scanner completes, detailed scan information is displayed. The results are also saved locally.

On the Windows operating system, the results are saved to %TMP%\taddm\prs.

On Linux and UNIX operating systems, the results are saved to /tmp/taddm/prs.

- To run the prerequisite checker in custom mode, complete the following steps:

- a. Copy the prerequisite checker for the appropriate operating system to the target computer.
- b. Open a command-line interface:
  - On the Windows operating system, open a Command Prompt.
  - On Linux and UNIX operating systems, open a shell environment.
- c. Change to the directory where the prerequisite checker is located and run the following command:
  - On the Windows operating system, run the **prereq\_checker.bat** command.
  - On Linux and UNIX operating systems, run the **prereq\_checker.sh** command.

The following input parameters are displayed:

```
Usage: ./prereq_checker.sh "<Product Code> [product version], <Product Code>
[product version]..." [PATH=<Product install path>] [detail]
[-p <Product Code>.SECTION.NAME=VALUE pairs] [outputDir="<PRS output dir
path>"]
[xmlResult] [-health<active|inactive>]
```

Examples:

- For the Windows operating system: `prereq_checker.bat "TS1" outputDir="c:\PRS"`
- For Linux and UNIX operating systems: `./prereq_checker.sh "TS1" outputDir="/tmp/prereq_check_output/"`

The following paragraphs provide a detailed description of the input parameters.

- `Product Code` and `product version` pairs.

At least one product code is required. For IBM TADDM, the code is a three-letter product code for the deployment type and size. For example, for a "small" domain deployment, you must enter TS1.

Enter the product codes in upper-case letters. Multiple product codes must be comma-separated.

Each component or agent has a `config` file with the naming convention `*.cfg`, for example `TS1_07220000.cfg`. If you specify a product code that does not have a corresponding `*.cfg` file, that product code is ignored.

The `product version` parameter is not applicable to TADDM.

- `[PATH=product_install_path]`

The `PATH` parameter is optional. An example of the `PATH` parameter with a set value is `PATH=D:\IBM\taddm`. If you do not specify the `PATH` parameter, the prerequisite checker checks the following default IBM TADDM installation paths:

- On the Windows operating system, the default path is `C:\IBM\taddm`.
- On Linux and UNIX operating systems, the default path is `/opt/IBM/taddm`.

- `[detail]`

The `detail` parameter is optional. This flag indicates that you want to see detailed results on the screen when you run the prerequisite checker.

Do not enclose the word `detail` in quotation marks.

If you do not specify the `detail` parameter, then only `PASS` or `FAIL` is displayed on the screen. Omitting this parameter is a simple way to see whether your system meets the prerequisites.

The detailed output is written to the `precheck.log` file, regardless of whether you specify the `detail` parameter or not. You can view this file to see the results of the prerequisite checker. You can also view the `result.txt` file to see the detailed steps that were taken by the prerequisite checker.

- `[outputDir=fully_qualified_path]`

When you run the prerequisite checker from a read-only media or from a directory without write permissions, you must set this parameter to the fully qualified path and place that value in quotation marks. The outputDir option is case-sensitive.

- [-health active|inactive]

This parameter is not applicable to TADDM.

The following specific product codes are available:

<i>Table 3. Product codes</i>	
<b>Code</b>	<b>Product</b>
TS1	IBM Tivoli Application Dependency Discovery Manager Domain Server - Small
TS2	IBM Tivoli Application Dependency Discovery Manager Domain Server - Large
TS3	IBM Tivoli Application Dependency Discovery Manager Domain Server - Enterprise
TS4	Database Server for IBM Tivoli Application Dependency Discovery Manager Domain Server - Small
TS5	Database Server for IBM Tivoli Application Dependency Discovery Manager Domain Server - Large
TS6	Database Server for IBM Tivoli Application Dependency Discovery Manager Domain Server - Enterprise
TS7	IBM Tivoli Application Dependency Discovery Manager Discovery or Storage Server - Small
TS8	IBM Tivoli Application Dependency Discovery Manager Discovery or Storage Server - Large
TS9	IBM Tivoli Application Dependency Discovery Manager Discovery or Storage Server - Enterprise
TSA	Database Server for IBM Tivoli Application Dependency Discovery Manager Storage Server - Small
TSB	Database Server for IBM Tivoli Application Dependency Discovery Manager Storage Server - Large
TSC	Database Server for IBM Tivoli Application Dependency Discovery Manager Storage Server - Enterprise

## TADDM server requirements

A TADDM deployment might require several types of servers, depending on the type of deployment you want to use.

### Number of servers

The number of servers that you need depends on the estimated number of items that must be discovered. You can base your estimate on either of the following two units:

#### configuration item (CI)

A component of IT infrastructure that is under the control of configuration management and is therefore subject to formal change control. Each CI in the TADDM database has a persistent object and change history associated with it. Examples of a CI are an operating system, an L2 interface, and a database buffer pool size.

#### server equivalent (SE)

A representative unit of IT infrastructure, defined as a computer system (with standard configurations, operating systems, network interfaces, and storage interfaces) with installed server software (such as a database, a web server, or an application server). The concept of a server equivalent also includes



the network, storage, and other subsystems that provide services to the optimal functioning of the server. A server equivalent depends on the operating system:

Operating system	Approximate number of CIs
Windows	500
AIX	1000
Linux	1000
HP-UX	500
Network devices	1000

For Level 3 discovery applications, 2000 CIs per SE must be assumed.

## Types of servers

### Domain servers

TADDM domain servers discover and track the configuration items (CIs) in your environment. A domain server is part of a stand-alone domain server deployment or a synchronization server deployment.

Each domain server, and its associated database, should be limited to approximately 10,000 SEs (or 10,000,000 CIs). If your environment is larger than this, use multiple servers. You can also improve performance by limiting each server to a few sources and types of discovered data. For example, you might want one server to discover a single type of managed software system regardless of location, rather than organizing the servers according to geography.

**Note:** The synchronization server deployment type is obsolete. If you need to install a new deployment with multiple servers, use a streaming server deployment.

### Discovery servers

Discovery servers discover and track the configuration items (CIs) in your environment. A discovery server is part of a streaming server deployment.

Each discovery server should be limited to approximately 10,000 SEs (or 10,000,000 CIs). If your environment is larger than this, use multiple discovery servers. You can also improve performance by limiting each server to a few sources and types of discovered data. For example, you might want one server to discover a single type of managed software system regardless of location, rather than organizing the servers according to geography.

### Storage servers

Storage servers process the discovery data from discovery servers. A storage server is part of a streaming server deployment.

A streaming server deployment has at least one storage server, called the primary storage server; there might also be additional storage servers, depending upon the size of the environment and the number of items that need to be discovered.

If you are not sure how many storage servers you need, you can deploy TADDM with only one storage server and then add more storage servers as needed to improve performance.

### Database servers

The TADDM database stores the discovered information about configuration items and their relationships, represented using the Tivoli Common Data Model. Each TADDM domain server or primary storage server has a corresponding database; in a synchronization server deployment, the synchronization server also has a database.

For testing or evaluation purposes, you can install the TADDM database on the same system as the domain server, synchronization server, or primary storage server. However, in production environments, a separate database server is recommended.

## **Anchors**

If any of the components you need to discover are separated from the TADDM domain server or discovery server by firewalls, you must configure one or more anchors.

To discover components, each TADDM server must communicate with other computer hosts and network devices. If a firewall prevents direct access to certain hosts or devices, you can configure an anchor. An anchor is a TADDM server running on a system that has direct access to the hosts or devices behind the firewall and acts as a proxy to assist in the discovery process.

You do not need to configure anchors during the installation process, but you must include anchors in your installation plan and verify the system requirements for candidate systems. After the installation, you can use the Discovery Management Console to configure hosts to serve as anchors on your network.

## **Windows gateways**

If your network contains Windows systems, you must specify a Windows system to serve as a gateway server to discover information about the Windows systems that are running in your environment. This gateway server should be in the same firewall zone as the discovered Windows hosts, and must have SSH access from the server.

You do not need to configure Windows gateways during the installation process, but you must include gateways in your installation plan and verify the system requirements for candidate systems. After the installation, you can use the Discovery Management Console to configure hosts to serve as Windows gateways on your network.

An anchor and a gateway can run on the same Windows system.

## **Hardware sizing for a synchronization or domain server deployment**

These guidelines can help you determine the quantity and specification of servers that you need to meet your discovery requirements in a synchronization or domain server deployment.

### ***TADDM server hardware requirements***

Use this information to estimate the processor, memory, and disk space requirements for the TADDM servers in a synchronization or domain server deployment.

These guidelines are the minimum specifications for hardware sizing. Several factors, including the number of users, can affect server use.

Use the following general guidelines:

- Use a fast multiprocessor system for the TADDM servers.
- Using a small number of faster processors is generally a better solution than using a large number of slower processors. For example, a 4-way 3.6 GHz Intel implementation is preferable to an 8-way 2.0 GHz Intel implementation.
- DB2<sup>®</sup> and Oracle databases that TADDM uses are configured to take advantage of multiple processors and parallel operations.

**Note:** When you run a TADDM server on virtualized hardware, use dedicated (static) resources. Shared (dynamic) resources might cause performance problems.

These guidelines assume that the TADDM server and the database server are on separate systems. You can install a TADDM server with a local database, but this is not recommended for production environments.

The following table indicates how to determine the server hardware requirements for your environment, based on the number of server equivalents (SEs) to be discovered.

Table 4. TADDM server hardware requirements

Server type	Processors	Processor speed	Memory	Prerequisite checker product code	Disk space
Domain server with < 2000 SEs	2	2 GHz minimum, 3 GHz advised	8 GB	TS1	<ul style="list-style-type: none"> <li>• 5 GB for product installation</li> <li>• 50 GB additional space (for DLA books, log and trace files, and other data)</li> </ul>
Domain server with 2000 – 10,000 SEs	4	2 GHz minimum, 3 GHz advised	<ul style="list-style-type: none"> <li>• TADDM 7.3.0.2, and earlier: 8 GB</li> <li>• <b>Fix Pack 3</b> TADDM 7.3.0.3, and later: 16 GB</li> </ul>	TS2	
Synchronization server with > 10,000 SEs	4	2 GHz minimum, 3 GHz advised	<ul style="list-style-type: none"> <li>• TADDM 7.3.0.2, and earlier: 8 GB</li> <li>• <b>Fix Pack 3</b> TADDM 7.3.0.3, and later: 16 GB, or more</li> </ul>	TS3	
Anchor	2	2 GHz minimum, 3 GHz advised	<ul style="list-style-type: none"> <li>• TADDM 7.3.0.2, and earlier: 6 GB</li> <li>• <b>Fix Pack 3</b> TADDM 7.3.0.3, and later: 8 GB</li> </ul>	n/a	5 GB
Windows gateway	2	2 GHz minimum, 3 GHz advised	<ul style="list-style-type: none"> <li>• TADDM 7.3.0.2, and earlier: 6 GB</li> <li>• <b>Fix Pack 3</b> TADDM 7.3.0.3, and later: 8 GB</li> </ul>	n/a	2 GB

**Note:** For an anchor server, when exchanging data you must use Secure Shell (SSH) version 2 protocol.

### ***Database server hardware requirements***

The processor, memory, and disk space requirements for TADDM database servers are based on the size of your deployment (small, medium, or large).

These guidelines assume that the TADDM database is installed on a separate system. You can install TADDM with a local database, but this is not recommended for production environments. Database performance is also affected by the speed of input/output operations.

Table 5. TADDM server hardware requirements

Deployment type	Processors	Processor speed	Memory	Prerequisite checker product code	Disk space
Small (< 2000 SEs)	1	2 GHz minimum, 3 GHz advised	<ul style="list-style-type: none"> <li>TADDM 7.3.0.2, and earlier: 4 GB</li> <li><b>Fix Pack 3</b> TADDM 7.3.0.3, and later: 6 GB</li> </ul>	TS4	<ul style="list-style-type: none"> <li>At least 2 physical drives (3 or more recommended).</li> <li>Initial disk space of 5 GB (required for creating the TADDM schema).</li> <li>Disk space for discovery data. Use either of these formulas to estimate disk space requirement (assuming Level 3 discovery):                             <ul style="list-style-type: none"> <li>– <math>CI_s \times 7000</math> bytes</li> <li>– <math>SE_s \times 7,000,000</math> bytes</li> </ul>                             where <math>CI_s</math> is the number of configuration items, and <math>SE_s</math> is the number of server equivalents.                         </li> <li>Additional disk space for ongoing growth. Plan for 10% growth weekly.</li> </ul>
Large (2000 – 10,000 SEs)	2	2 GHz minimum, 3 GHz advised	<ul style="list-style-type: none"> <li>TADDM 7.3.0.2, and earlier: 4 GB</li> <li><b>Fix Pack 3</b> TADDM 7.3.0.3, and later: 6 GB</li> </ul>	TS5	<ul style="list-style-type: none"> <li>Disk space for discovery data. Use either of these formulas to estimate disk space requirement (assuming Level 3 discovery):                             <ul style="list-style-type: none"> <li>– <math>CI_s \times 7000</math> bytes</li> <li>– <math>SE_s \times 7,000,000</math> bytes</li> </ul>                             where <math>CI_s</math> is the number of configuration items, and <math>SE_s</math> is the number of server equivalents.                         </li> <li>Additional disk space for ongoing growth. Plan for 10% growth weekly.</li> </ul>
Enterprise (> 10,000 SEs)	4	2 GHz minimum, 3 GHz advised	<ul style="list-style-type: none"> <li>TADDM 7.3.0.2, and earlier: 6 GB</li> <li><b>Fix Pack 3</b> TADDM 7.3.0.3, and later: 8 GB</li> </ul>	TS6	<ul style="list-style-type: none"> <li>Disk space for discovery data. Use either of these formulas to estimate disk space requirement (assuming Level 3 discovery):                             <ul style="list-style-type: none"> <li>– <math>CI_s \times 7000</math> bytes</li> <li>– <math>SE_s \times 7,000,000</math> bytes</li> </ul>                             where <math>CI_s</math> is the number of configuration items, and <math>SE_s</math> is the number of server equivalents.                         </li> <li>Additional disk space for ongoing growth. Plan for 10% growth weekly.</li> </ul>

## Hardware sizing for a streaming server deployment

These guidelines can help you determine the quantity and specification of servers that you need to meet your discovery requirements in a streaming server deployment. These guidelines do not apply to an environment where TADDM is running on the Linux for System z® operating system.

These guidelines are the minimum specifications for hardware sizing. Several factors, including the number of users, can affect server use.

The size of a deployment is defined in terms of the number of server equivalents (SEs).

- Small deployment: Less than 2,000 SEs
- Large deployment: 2,000 - 10,000 SEs
- Enterprise deployment: More than 10,000 SEs

**Note:** When you run a TADDM server on virtualized hardware, use dedicated (static) resources. Shared (dynamic) resources might cause performance problems.

Use the following general guidelines:

- Use a fast multiprocessor system for the TADDM servers.

- Using a small number of faster processors is generally a better solution than using a large number of slower processors. For example, a 4-way 3.6 GHz Intel implementation is preferable to an 8-way 2.0 GHz Intel implementation.
- DB2 and Oracle databases that TADDM uses are configured to take advantage of multiple processors and parallel operations.
- For a streaming server deployment, which is a single database system, run the database on a dedicated database server.

These guidelines assume that the TADDM server and the database server are on separate systems.

The following options are examples of how you can scale your TADDM environment as needed:

- Horizontally, by increasing the size, capacity, or both, of an individual component. For example, to run more discovery worker threads on a single discovery server, you might want to increase the number of processors from two to four.
- Vertically, by adding additional components to your deployment. For example, if you have a data center in the USA, Europe, and Japan, you might want to place a discovery server at each location.

## Disk space

To ensure that sufficient space is available for the TADDM installation and logging information, disk space requirements are provided. Alternatively, you can use the supplied formulas to estimate disk space requirements, paying particular attention to considerations such as growth, TADDM logging, and database logging.

## Memory size

A discover worker thread is a thread that runs sensors. For a streaming server deployment, 64-bit hardware is required for all storage servers and discovery servers that use more than 24 concurrent discover worker threads. This also implies a 64-bit operating system and Java™ virtual machine. For large and enterprise deployments, a 64-bit version of the database software is required also.

## Processor speed

The following table outlines the baseline processor types by platform.

<i>Table 6. Baseline processor types</i>	
<b>Platform</b>	<b>Baseline processor type</b>
Intel	Xeon
pSeries	Power6
Sun (Oracle)	Sparc

You can compare other processor types by using industry standard benchmark data that is available from The Standard Performance Evaluation Corporation (SPEC) at <http://www.spec.org/>.

## Primary storage server

The hardware specifications for the primary storage server depend on the platform and deployment size.

The primary storage server handles topology builds, data presentation requests, and manages the storage server pool. You must have one primary storage server for each TADDM deployment. You can add additional capacity by deploying secondary storage servers.

## Processor speed

The following table lists the minimum processor speed that is required for a primary storage server, depending on platform and deployment size. Faster processors improve performance.

Platform	Minimum processor speed for small deployments	Minimum processor speed for large and enterprise deployments
Intel	2.5 GHz	3 GHz
pSeries	2.3 GHz	3 GHz

## Processor quantity

The following table lists the minimum processor quantity that is required for a primary storage server, depending on deployment size.

Deployment size	Number of processors
Small	2
Large	4
Enterprise	4

## Memory size

The following table lists the minimum memory amount that is required for a primary storage server, depending on deployment size.

Deployment size	Minimum memory
Small	<ul style="list-style-type: none"> <li>TADDM 7.3.0.2, and earlier: 6 GB</li> <li><a href="#">Fix Pack 3</a> TADDM 7.3.0.3, and later: 8 GB</li> </ul>
Large	<ul style="list-style-type: none"> <li>TADDM 7.3.0.2, and earlier: 8 GB</li> <li><a href="#">Fix Pack 3</a> TADDM 7.3.0.3, and later: 12 GB</li> </ul>
Enterprise	<ul style="list-style-type: none"> <li>TADDM 7.3.0.2, and earlier: 8 GB, or more</li> <li><a href="#">Fix Pack 3</a> TADDM 7.3.0.3, and later: 12 GB, or more</li> </ul>

## Disk space

A minimum of 50 GB is needed in addition to what is required for the TADDM product installation. This additional disk space is used to store items such as DLA books, additional logging, and tracing information.

## Prerequisite checker product codes

The following table lists product codes that are used with the prerequisite checking tool.

Deployment size	Product code
Small	TS7
Large	TS8

<i>Table 10. Product codes (continued)</i>	
<b>Deployment size</b>	<b>Product code</b>
Enterprise	TS9

### **Secondary storage server**

The hardware specifications for the secondary storage server depend on the platform and deployment size.

You can add additional secondary storage servers at any time without reconfiguring the discovery servers.

Typically, secondary storage servers are used only in streaming server deployments, but you can, in certain situations, configure secondary storage servers for use in a synchronization server deployment. For example, you can start up and use multiple secondary storage servers to run several bulk loads at an off-peak time to meet elapsed load time requirements. These additional secondary storage servers are used only for this purpose and shut down when not in use.

### **Processor speed**

The following table lists the minimum processor speed that is required for a secondary storage server, depending on the platform and deployment size.

<i>Table 11. Processor speed</i>		
<b>Platform</b>	<b>Minimum processor speed for small deployments</b>	<b>Minimum processor speed for large and enterprise deployments</b>
Intel	2.5 GHz	3 GHz
pSeries	2.3 GHz	3 GHz


### **Processor quantity**

The following table lists the minimum processor quantity that is required for a secondary storage server, depending on deployment size.

<i>Table 12. Processor quantity</i>	
<b>Deployment size</b>	<b>Number of processors</b>
Small	2
Large	4
Enterprise	4

### **Memory size**

The following table lists the minimum memory that is required for a secondary storage server, depending on deployment size.

<i>Table 13. Memory</i>	
<b>Deployment size</b>	<b>Minimum memory</b>
Small	<ul style="list-style-type: none"> <li>TADDM 7.3.0.2, and earlier: 6 GB</li> <li> TADDM 7.3.0.3, and later: 8 GB</li> </ul>

<i>Table 13. Memory (continued)</i>	
<b>Deployment size</b>	<b>Minimum memory</b>
Large	<ul style="list-style-type: none"> <li>TADDM 7.3.0.2, and earlier: 8 GB</li> <li><b>Fix Pack 3</b> TADDM 7.3.0.3, and later: 12 GB</li> </ul>
Enterprise	<ul style="list-style-type: none"> <li>TADDM 7.3.0.2, and earlier: 8 GB</li> <li><b>Fix Pack 3</b> TADDM 7.3.0.3, and later: 12 GB, or more</li> </ul>

## Disk space

A minimum of 50 GB is needed in addition to what is required for the TADDM product installation. This additional disk space is used to store items such as DLA books, additional logging, and tracing information.

## Prerequisite checker product codes

The following table lists product codes that are used with the prerequisite checking tool.

<i>Table 14. Product codes</i>	
<b>Deployment size</b>	<b>Product code</b>
Small	TS7
Large	TS8
Enterprise	TS9

## Discovery server

The hardware specifications for the discovery server depend on the platform and deployment size.

## Processor speed

The following table lists the minimum processor speed that is required for a discovery server, depending on the platform and deployment size.

<i>Table 15. Processor speed</i>		
<b>Platform</b>	<b>Minimum processor speed for small deployments</b>	<b>Minimum processor speed for large and enterprise deployments</b>
Intel	2.5 GHz	3 GHz
pSeries	2.3 GHz	3 GHz

## Processor quantity

The following table lists the minimum processor quantity that is required for a discovery server, depending on deployment size.

<i>Table 16. Processor quantity</i>	
<b>Deployment size</b>	<b>Number of processors</b>
Small	2
Large	4



<i>Table 16. Processor quantity (continued)</i>	
Deployment size	Number of processors
Enterprise	4

## Memory size

The following table lists the minimum memory that is required for a discovery server, depending on deployment size.

<i>Table 17. Memory</i>	
Deployment size	Minimum memory
Small	<ul style="list-style-type: none"> <li>TADDM 7.3.0.2, and earlier: 6 GB</li> <li><b>Fix Pack 3</b> TADDM 7.3.0.3, and later: 8 GB</li> </ul>
Large	<ul style="list-style-type: none"> <li>TADDM 7.3.0.2, and earlier: 8 GB</li> <li><b>Fix Pack 3</b> TADDM 7.3.0.3, and later: 12 GB</li> </ul>
Enterprise	<ul style="list-style-type: none"> <li>TADDM 7.3.0.2, and earlier: 8 GB</li> <li><b>Fix Pack 3</b> TADDM 7.3.0.3, and later: 12 GB, or more</li> </ul>

## Disk space

A minimum of 50 GB is needed in addition to what is required for the TADDM product installation. This additional disk space is used to store items such as DLA books, additional logging, and tracing information.

## Prerequisite checker product codes

The following table lists product codes that are used with the prerequisite checking tool.

<i>Table 18. Product codes</i>	
Deployment size	Product code
Small	TS7
Large	TS8
Enterprise	TS9

## Database server

The hardware specifications for the database server depend on the platform and deployment size.

## Processor speed

The following table lists the minimum processor speed that is required for a database server, depending on the platform and deployment size.

<i>Table 19. Processor speed</i>		
Platform	Minimum processor speed for small deployments	Minimum processor speed for large and enterprise deployments
Intel	2.5 GHz	3 GHz

Table 19. Processor speed (continued)

Platform	Minimum processor speed for small deployments	Minimum processor speed for large and enterprise deployments
pSeries	2.3 GHz	3 GHz

## Processor quantity

The following table lists the minimum processor quantity that is required for a database server, depending on deployment size.

Table 20. Processor quantity

Deployment size	Number of processors
Small	2
Large	4
Enterprise	4 Add a processor for each additional 10,000 SEs over 10,000, up to a total of 12.

## Memory size

The following table lists the minimum memory that is required for a database server, depending on deployment size.

Table 21. Memory

Deployment size	Minimum memory
Small	<ul style="list-style-type: none"> <li>TADDM 7.3.0.2, and earlier: 4 GB</li> <li><b>Fix Pack 3</b> TADDM 7.3.0.3, and later: 8 GB</li> </ul>
Large	<ul style="list-style-type: none"> <li>TADDM 7.3.0.2, and earlier: 8 GB</li> <li><b>Fix Pack 3</b> TADDM 7.3.0.3, and later: 12 GB</li> </ul>
Enterprise	<ul style="list-style-type: none"> <li>TADDM 7.3.0.2, and earlier: 8 GB, or more. Add 2 GB of memory for each additional 20,000 SEs over 20,000.</li> <li><b>Fix Pack 3</b> TADDM 7.3.0.3, and later: 12 GB, or more. Add 2 GB of memory for each additional 20,000 SEs over 20,000.</li> </ul>

## Disk space

The following components require database disk space:

- System catalog
- Tables
- Indexes
- Logs
- Temporary space, for sorts and joins, for example
- Backup space

Disk space and disk drive requirements for a database server are not a function of only disk capacity. The following table lists some general guidance about disk drive layout on the database server.

<i>Table 22. Number of disk drives or disk arms</i>		
Deployment size	Number of disk drives (RAID) or disk arms (SAN) required for the TADDM database tables	
	Minimum	Recommended
Small	2	3 or more
Large	6	7 or more
Enterprise	8	9 or more

Place database logs on separate disk drives (RAID) or disk arms (SAN) from the TADDM database tables. Database logs are required for large and enterprise deployments.

### Initial amount of disk space required for TADDM database

To estimate the initial amount disk space that is required for your TADDM database implementation, complete the following steps. These estimates are based on Level 3 discovery data. Depending on the breadth and depth of data in your environment, the disk space requirements can change.

1. Use the *ci\_no* variable to represent the number of CIs.
2. Use the *se\_no* variable to represent the number of SEs.
3. Use the *ci\_rds* variable to represent the amount of raw disk space for CIs without any additional disk space for growth. Allow 4000 bytes per CI.

$$ci\_rds = ci\_no \times 4000$$

4. Use the *se\_rds* variable to represent the amount of raw disk space for SEs without any additional disk space for growth. An SE consists of approximately 1000 CIs. Allow 4,000,000 bytes per SE.

$$se\_rds = se\_no \times 4,000,000$$

5. Use the *tds* variable to represent the total disk space, including some additional disk space for growth. Use one of the following formulas:

- $tds = ci\_rds \times 1.75$
- $tds = se\_rds \times 1.75$

This calculation includes additional disk space for temporary space and more.

6. Use the *chs* variable to represent the change history disk space. The change history disk space is the amount of space by which the database grows weekly, over and above the initial disk allocation, depending on the frequency of discovery.

$$chs = tds \times 1.1$$

This calculation allows for an increase of 10%.

The space requirements increase if additional data is discovered or loaded or if you use the TADDM version management feature.

The following example of a disk space calculation, based on CIs, is for a large deployment:

1.  $ci\_no = 10,000,000$
2.  $ci\_rds = ci\_no \times 4,000 = 40,000,000,000$
3.  $tds = ci\_rds \times 1.75 = 70,000,000,000$
4.  $chs = tds \times 1.1 = 77,000,000,000$

The following example of a disk space calculation, based on SEs, is for a large deployment:

1.  $se\_no = 10,000$

2.  $se\_rds = se\_no \times 4,000,000 = 40,000,000,000$
3.  $tds = se\_rds \times 1.75 = 70,000,000,000$
4.  $chs = tds \times 1.1 = 77,000,000,000$

## Prerequisite checker product codes

The following table lists product codes that are used with the prerequisite checking tool.

Deployment size	Product code
Small	TSA
Large	TSB
Enterprise	TSC

## Hardware scaling guidelines

You can use the sample configurations as a guideline for selecting the components for your TADDM implementation.

The guidelines assume that you are running Level 3 discoveries. To optimize discovery throughput, the storage servers should be 100% in use. If they are not, additional discovery servers can be added or the `dwcount` value can be increased on the existing discovery servers, if they have spare capacity. If a storage server has spare capacity, you can increase the `topopumpcount` value. When the storage servers are 100% in use, to increase throughput, increase the number of storage servers.

If UI performance becomes poor when running data load operations (for example, sensor discovery or bulk load), you can dedicate storage servers to UI, API, or report operations. If you want discovery servers to use other storage servers, instead of a particular storage server when persisting results, you can set the following property value to `true` on that storage server:

```
com.collation.AlwaysBusyStorageServer=true
```

Typically, you set this property value to `true` on the primary storage server or any other storage server dedicated to UI, API, or report operations.

### Discovery storage rates

You can use the discovery storage rates that are listed to help you determine the number of components that are required to meet your objectives for discovery.

In a synchronization server deployment, storage to the database is typically the main bottleneck. In a streaming server deployment, any bottleneck in discovery throughput has moved to the sensors that are waiting for the data to be stored.

The following table lists typical discovery storage rates.

Number of storage servers	Number of imports (discovery servers)	CI rate per second	Percent improvement	Number of threads used for persisting discovery results in the database (topopumpcount)
1	2	144		16
2	2	246	101.83	16
3	2	280	33.91	16

The number of imports that is listed is the number of discovery servers that are able to send enough data to the storage servers so that they are not waiting on sensor results, which means that they are storing at their maximum rate. As the number of storage servers increases, there is an increase in the CI storage rate.

*Discovery sensor rates*

You can use the discovery sensor rates that are listed to help estimate your discovery server configuration, based on your discovery requirements.

The information in this topic was gathered when discovery testing with 96 discovery worker threads (dwcount) running on the discovery servers. This value is three times higher than the default of 32. Higher dwcount values can be used, increasing the number of sensors that are running concurrently and the amount of data being stored.

The information uses the average sensor time per server, which can vary widely depending on which sensors run, and the breadth and depth of the objects being discovered.

The total sensor elapsed time is calculated in the following way: (Number of servers/dwcount) x average sensor time per server

The following table lists typical discovery sensor rates.

Number of servers	Average sensor time per server (in minutes)	Number of discovery worker threads (dwcount)	Total sensor elapsed time (in minutes)	Total sensor elapsed time (in hours)
5,000	30	32	4,688	78
5,000	30	64	2,344	39
5,000	30	96	1,563	26
10,000	30	32	9,375	156
10,000	30	64	4,688	78
10,000	30	96	3,125	52

*Discovered target resources utilization footprint*

The TADDM discovery process uses minimal system and network resources. Based on lab-based benchmarks, TADDM typically uses less than 10% of CPU utilization, and less than 1% of operating system memory (on discovered hosts) during Level 3 discovery.

**Note:** Discovered target resource utilization footprint (on discovered hosts) might vary depending on the application type, or its configuration, or both.

*Data transfer between TADDM server and anchor*

You can use the data transfer totals that are listed in the following tables as a guideline for selecting the components for your TADDM implementation.

The following table shows the data that is transferred between the TADDM server and the anchor during Level 2 discovery:

Table 26. Sample data transfer during L2 discovery between the TADDM server and the anchor

<b>Discovery - Discovered Computer System</b>	<b>Port</b>	<b>Bytes</b>	<b>Transmitted Bytes</b>	<b>Received Bytes</b>
First discovery - Linux and anchor deployment	epmap	1870	900	970
	ssh	610691279	8118553	602572726
	telnet	1496	720	776
	ncube-lm	748	360	388
	ldap	748	360	388
	domain	748	360	388
	microsoft-ds	748	360	388
	cisco-net-mgmt	748	360	388
	<b>Total</b>	<b>610698385</b>	<b>8121973</b>	<b>602576412</b>
Next - Linux	ssh	2331201	1077409	1253792
	epmap	1870	900	970
	telnet	1496	720	776
	ncube-lm	748	360	388
	ldap	748	360	388
	domain	748	360	388
	microsoft-ds	748	360	388
	cisco-net-mgmt	748	360	388
	<b>Total</b>	<b>2338307</b>	<b>1080829</b>	<b>1257478</b>
Next - Windows	epmap	1870	900	970
	ssh	2393622	1560238	833384
	telnet	1496	720	776
	ncube-lm	748	360	388
	ldap	748	360	388
	domain	748	360	388
	microsoft-ds	748	360	388
	cisco-net-mgmt	748	360	388
	<b>Total</b>	<b>2400728</b>	<b>1563658</b>	<b>837070</b>

The following table shows the data that is transferred between the TADDM server and the anchor during Level 2 discovery by using lazy deployment:

Table 27. Sample data transfer during L2 discovery between the TADDM server and the anchor by using lazy deployment

<b>Discovery - Discovered Computer System</b>	<b>Port</b>	<b>Bytes</b>	<b>Transmitted Bytes</b>	<b>Received Bytes</b>
First discovery - Linux and lazy mode anchor deployment	epmap	1870	900	970
	ssh	273079491	4203717	268875774
	telnet	1496	720	776
	ncube-lm	748	360	388
	ldap	748	360	388
	domain	748	360	388
	microsoft-ds	748	360	388
	cisco-net-mgmt	748	360	388
	<b>Total</b>	<b>273086597</b>	<b>4207137</b>	<b>268879460</b>
Next - Linux	telnet	1496	720	776
	ssh	2062061	1446161	615900
	epmap	1744	840	904
	ncube-lm	748	360	388
	ldap	748	360	388
	domain	748	360	388
	microsoft-ds	748	360	388
	cisco-net-mgmt	748	360	388
	<b>Total</b>	<b>2069041</b>	<b>1449521</b>	<b>619520</b>
Next - Windows	epmap	1744	840	904
	telnet	1370	660	710
	ssh	2312829	1455331	857498
	ncube-lm	748	360	388
	ldap	748	360	388
	domain	748	360	388
	microsoft-ds	748	360	388
	cisco-net-mgmt	748	360	388
	<b>Total</b>	<b>2319683</b>	<b>1458631</b>	<b>861052</b>

**Note:** The extension of the number of the discovery targets shows no significant change in the transferred bytes per target.

#### Data transfer during Level 1 discovery

You can use the data transfer totals that are listed in the following table as a guideline for selecting the components for your TADDM implementation.

The following table shows the data that is transferred between the TADDM server and the target during Level 1 discovery:

Discovered computer system	Bytes	Received bytes	Transferred bytes
Windows	56355	24654	31701
Linux	51724	22208	29516

The following charts show the I/O traffic for the Windows and Linux computer systems. The x-axis shows the time, which is specified in seconds, and the y-axis shows the number of bytes per second.

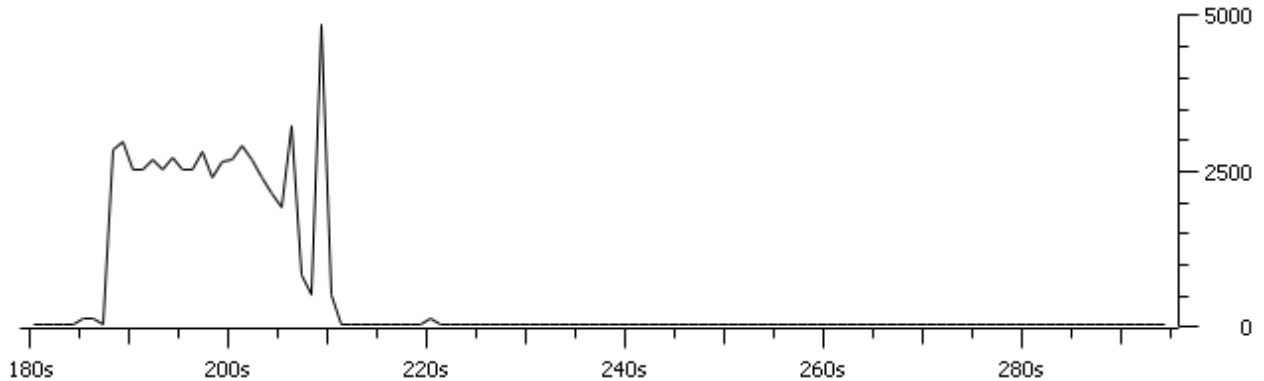


Figure 5. The I/O traffic for the Windows computer system.

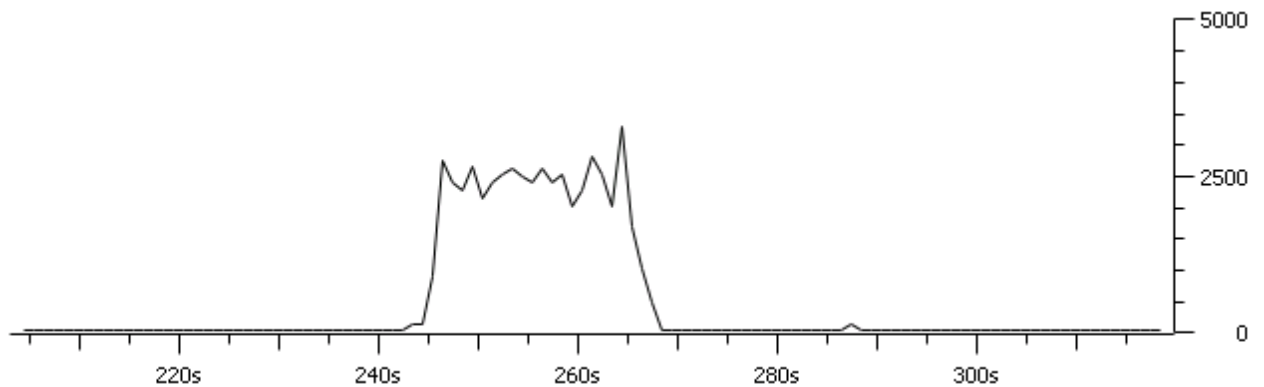


Figure 6. The I/O traffic for the Linux computer system.

#### Data transfer during Level 2 discovery

You can use the data transfer totals that are listed in the following table as a guideline for selecting the components for your TADDM implementation.

The following table shows the data that is transferred between the TADDM server and the target during Level 2 discovery:



Table 29. Bytes transferred between the TADDM server and the target during Level 2 discovery

Discovered computer system	Port	Bytes	Transmitted bytes	Received bytes
Windows	56997	9272239	371876	8900363
	62640	767991	286377	481614
	ssh	821444	766930	54514
	epmap	708	186	522
	ncube-im	472	124	348
	ldap	748	360	388
	domain	748	360	388
	telnet	748	360	388
	microsoft-ds	472	124	348
	cisco-net-mgmt	748	360	388
	<b>Total</b>	<b>10866318</b>	<b>1427057</b>	<b>9439261</b>
SunSparc	ssh	399092	334420	64672
	epmap	1122	540	582
	ncube-im	748	360	388
	ldap	748	360	388
	domain	748	360	388
	telnet	540	192	348
	microsoft-ds	748	360	388
	cisco-net-mgmt	748	360	388
	<b>Total</b>	<b>11270812</b>	<b>1764009</b>	<b>9506803</b>
Linux	ssh	343395	297075	46320
	epmap	1122	540	582
	ncube-im	748	360	388
	ldap	748	360	388
	domain	748	360	388
	telnet	748	360	388
	microsoft-ds	480	132	348
	cisco-net-mgmt	748	360	388
	<b>Total</b>	<b>11619549</b>	<b>2063556</b>	<b>9555993</b>

Table 29. Bytes transferred between the TADDM server and the target during Level 2 discovery (continued)

Discovered computer system	Port	Bytes	Transmitted bytes	Received bytes
HP-UX	ssh	182742	139592	43150
	epmap	720	198	522
	ncube-im	778	390	388
	ldap	778	390	388
	domain	778	390	388
	telnet	480	132	348
	microsoft-ds	778	390	388
	cisco-net-mgmt	778	390	388
	<b>Total</b>	<b>11807381</b>	<b>2205428</b>	<b>9601953</b>

### Server configurations

You can use the server configuration guidelines to help estimate the number of storage and discovery servers that you need, depending on the size of your deployment.

Based on your discovery requirements, the number of servers you that you need might differ from the numbers that are listed.

#### Small deployment

- One primary storage server
- One discovery storage server

#### Large deployment

- One primary storage server
- One secondary storage server
- Two discovery servers

Depending on the geographic location of target computers (one per data center), discovery elapsed time requirements, and so on, more or fewer discovery servers might be required.

#### Enterprise deployment

- One primary storage server
- Two secondary storage servers
- Three discovery servers

Depending on the geographic location of target computers (one per data center), discovery elapsed time requirements, and so on, more or fewer discovery servers might be required.

### Sample scenarios

You can use the typical discovery sensor rates to help determine how many discovery servers that you need to meet your discovery requirements.

Increase the thread count value, `dwcourt`, until you get memory, processor usage, or both, constrained on your discovery server. Then, scale your discovery servers as appropriate.

Estimating the number of discovery servers that are required is difficult for the following reasons:

- It is not always known in advance how many sensors will run on each server.
- The time taken for a sensor to complete can vary widely based on the configuration of the target server.

When monitoring discovery through the UI, consider the following general rules:

- If the number of sensors that are running is much greater than the dwcount value, TADDM is waiting to store data. TADDM waiting to store data is an indication that you might need to increase the capacity of your storage servers, that is, add another secondary storage server.
- If the number of sensors running is about the same as the dwcount value, TADDM is waiting for sensors to run. TADDM waiting for sensors to run is an indication that you might need to increase the capacity of your discovery servers, that is, add another discovery server, increase the dwcount value, and so on.

When using a streaming server deployment, you can easily add or remove secondary storage servers, discovery servers, or both, as your needs change or your environment grows.

## Sizing example

The discovery storage rates are theoretical maximum rates. While the maximum rate might be reached for some time during a long discovery, in most cases the storage rate is less. For this scenario, a 50% rate is assumed.

The number of SEs to be discovered is 60,000 and there is a requirement for the discovery to complete within five days.

Using one storage server, it would take 9.6 days to discover and store the results of 60,000 SEs, not meeting the requirement. The following table displays the calculations for the example using one storage server.

*Table 30. Example using one storage server*

	<b>CI</b> s	<b>SE</b> s	<b>Time (days)</b>
<b>Week</b>	43,545,600	43,545.6	
<b>Day</b>	6,220,800	6,220.8	9.645061728
<b>Hour</b>	259,200	259.2	
<b>Minute</b>	4,320	4.32	
<b>Second</b>	72	0.072	

Using one primary storage server and two secondary servers, it would take 4.96 days to discover and store the results of 60,000 SEs, meeting the requirement. The following table displays the calculations for the example using two storage servers.

*Table 31. Example using two storage servers*

	<b>CI</b> s	<b>SE</b> s	<b>Time (days)</b>
<b>Week</b>	84,672,000	84,672	
<b>Day</b>	12,096,000	12,096	4.96031746
<b>Hour</b>	504,000	504	
<b>Minute</b>	8,400	8.4	
<b>Second</b>	140	0.14	

Using the discovery sensor rates from the previous example, the following table shows the number or discovery servers that are required for sensor processing to meet the one day requirement.

Table 32. Example for discovery servers

Number of servers	Average sensor time per server (in minutes)	dwcount	Total sensor elapsed time (in minutes)	Total sensor elapsed time (in hours)	Number of discovery servers needed per hour
60,000	30	32	56,250	938	39.06
60,000	30	64	28,125	469	19.53
60,000	30	96	18,750	313	13.02

The total sensor elapsed time is calculated in the following way: (Number of servers/dwcount) x average sensor time per server

This example is for illustrative purposes and assumes Level 3 discovery. The actual number of discovery servers can vary based on the actual average time per sensor.

## Windows gateways

You can configure the Windows gateways in your TADDM environment.

Sufficient capacity for any Windows gateway server is an important component in the overall configuration of your TADDM discovery environment. Windows gateway processing is processor-intensive and can become a bottleneck to overall discovery throughput when sufficient capacity is not available. The following guidelines can be used to configure your Windows gateways:

- Gateways can be configured as a shared pool for multiple discovery servers. This method ensures that all of the gateway servers can be used while discovery is running on any of the discovery servers.
- For optimum performance, do not deploy the gateway on Microsoft Windows Server 2008.
- Monitor the processor usage on the Windows gateway servers to determine whether sufficient capacity is available. You can use Windows Task Manager or any other tool available that monitors processor usage. If the processor usage on any of the Windows gateway servers runs at 100% for long periods of time, there is insufficient processor capacity on that gateway. Running at 100% use indicates that some of the TADDM sensors running through this gateway are waiting for available processor resources to do their work. This delay negatively affects the total elapsed time for the sensor to complete.
- Different guidelines apply for queue lengths on multiprocessor systems. For busy systems (those having processor use in the range 80 - 90%) that use thread scheduling, the queue length acceptable range is 1 - 3 threads per processor. For example, on a four-processor system, the expected range of processor queue length on a system with high processor activity is 4 - 12. On systems with lower processor use, the processor queue length is typically 0 or 1.
- Processor queue length, can be an indication that there is insufficient capacity on that gateway. Address this situation by completing one or more of the following actions:
  - Add additional processors to the gateway server.

Large and enterprise deployments must have a minimum of four processors.

The following table contains results of scale tests for which gateways with two, four, and six 2Ghz CPUs were used. Tests environment: VMware guest with dedicated resources, Windows Server 2012, Cygwin SSH server, dwcount property set to 96.

Table 33. Results of scale tests which used a gateway with two, four, and six 2Ghz CPUs.

Number of gateways	Number of 2Ghz CPUs	Performance improvement (%)	CPU max usage (%)	CPU max usage length reduction (%)
1	2	-	100	-
1	4	17	100	50

*Table 33. Results of scale tests which used a gateway with two, four, and six 2Ghz CPUs. (continued)*

Number of gateways	Number of 2Ghz CPUs	Performance improvement (%)	CPU max usage (%)	CPU max usage length reduction (%)
1	6	20	60	80

The results show that the more processors you use, the better performance you achieve.

- Use gateway servers with faster processors, for example processors with a speed of 2.0 - 3.0 GHz. For large and enterprise deployments, use the highest speed processors available.
- Add additional gateway servers to the pool.

The following table contains results of scale tests for which various numbers of gateways were used. Tests environment: VMware guest with dedicated resources, Windows Server 2012, Cygwin SSH server, dwcount property set to 96.

*Table 34. Results of scale test which used various numbers of gateways.*

Number of gateways	Number of 2Ghz CPUs	Performance improvement (%)	CPU max usage (%)	CPU max usage length reduction (%)
1	2	-	100	-
2	2	7	100	60
3	2	8	80	80

The results show that with the same number of processors, the more gateways you use, the better performance you achieve. However, the preceding tests show that it is best to use more processors than more gateways.

Typically, users have 70 - 80% of their total distributed servers running the Windows operating system. Using this information, you can determine the number of Windows gateways needed, depending on the deployment size.

- For small deployments: Two Windows gateways
- For large deployments: Four Windows gateways
- For enterprise deployments: Four Windows gateways

These categories are based on the total number of Windows servers being discovered, not the total number of servers in the environment.

You might have to add more gateways if you are not meeting your discovery throughput requirements.

## Required software

Operating system requirements for gateway servers are the same as Windows operating system requirements for TADDM servers. For details, see [“TADDM server software requirements”](#) on page 33.

All Windows gateways must be running a supported version of Bitvise WinSSHD, Cygwin SSH daemon, Tectia SSH Server, or Remotely Anywhere. OpenSSH server, available as an installable feature in Windows Server 2019, is also supported.

**Note:** If you use anchors on the Windows operating system, the requirements are the same as for the Windows gateways.

The following is the list of supported versions of the software:

- Bitvise: WinSSHD 4.06, and later.
- For Cygwin, you must install the following packages:

- From the **admin** category: **cygrunsrv** (version 1.17 - 1 or later).
- From the **net** category: **opensshd** (version 4.6p 1 - 1 or later).
- Tectia SSH Server: 6.4.4 or later.
- Remotely Anywhere: 9.x, 11.x.
- OpenSSH Server 7.7 (on Windows Server 2019)

**Restrictions:**

- For Windows Server 2012, only Bitvise 5.59 or later, Tectia 6.4.4 or later, Remotely Anywhere 11.x and Cygwin are supported.
- Anchors and gateways are supported on Cygwin 64-bit edition on Windows Server 2012 x64. However, the discovery user and the user that starts the service must be the same. The discovery user must be a member of the Administrators group. These requirements must be fulfilled for successful discovery with the use of Cygwin SSH.
- For Windows Server 2016, Bitvise 6.51 or later, Tectia 6.4.13 or later, Remotely Anywhere 12.x and Cygwin are supported.
- For Windows Server 2019, Bitvise 8.22 or later, Tectia 6.4.13 or later, Remotely Anywhere 12.x, Cygwin are supported. OpenSSH Server, available as an installable feature in Windows Server 2019, is also supported.

For more information about availability, installation and configuration of the preceding software, see the *Configuring for discovery of Windows systems* topic in the *TADDM Administrator's Guide*.

The following table compares the performance of the Cygwin and WinSSHD servers. Tests environment: VMware guest with dedicated resources, Windows Server 2012, dwcount property set to 96.

*Table 35. Comparison of the Cygwin and WinSSHD servers performance.*

SSH server	Number of gateways	Number of CPUs	Performance improvement (%)	CPU max usage (%)	CPU max usage length reduction (%)
Cygwin	1	2	-	100	-
WinSSHD	1	2	11	100	50

The results show that in the test environment, in comparison to the Cygwin server, the WinSSHD server achieves better performance because of the lower CPU usage.

**Running Windows gateways on virtual machines**

You can run Windows gateways on virtual machines (VMs). The guidelines in the previous section are based on dedicated physical resources. For example, an enterprise-sized deployment requiring four gateways can use one of the following configurations:

- An eight-way physical server into four 2-way VMs, with each VM used as one of the four gateways. This configuration is acceptable.
- An eight-way physical server into eight 2-way VMs, with four of the VMs being used by TADDM as gateways, and the other four VMs used for other, non-TADDM usage.

This server is over allocated, that is, eight physical processors and 16 virtual processors. This configuration might be acceptable if the four TADDM VMs are the only VMs running when a TADDM discovery is running.

This configuration is probably not acceptable if all eight VMs are running while a TADDM discovery is running. Because the physical processor resources are over allocated, the processor resources that are required by TADDM are not available.

When using VMs for Windows gateways, any monitoring of the gateways for capacity must be done on the physical server. Performance information you see on the VM is not reliable or accurate.

## Anchors

You can configure anchors in your TADDM environment.

## Hardware requirements

The following table specifies anchor hardware requirements in the TADDM environment:

Processors	Processor speed	Memory	Disk space
2	2 GHz minimum, 3 GHz advised	8 GB	5 GB

## Software requirements

Anchors support the same operating systems as the TADDM servers. For details, see [“TADDM server software requirements”](#) on page 33.

## TADDM server software requirements

Each TADDM server must be running a supported operating system and Java runtime environment (JRE). These servers might include domain servers, discovery servers, storage servers, synchronization servers, anchors, and Windows gateways.

**Important:** Be sure to read the following important information before installing the TADDM server:

- You must install the latest patches and updates from the operating system vendor before installing the TADDM server.
- The server hosts file must include the IP address and host name of the local system. The hosts file is in one of the following locations:
  - Windows systems: `c:\Windows\system32\drivers\etc\hosts`
  - Linux and UNIX systems: `/etc/hosts`

Specify both the fully qualified host name and the short name of the server. The format of a hosts file entry is as follows:

```
ip_address hostname [hostname_2 ... hostname_n] [#comment]
```

The fully qualified host name must occur before the short name in the hosts file.

Alternatively, you can configure the host name resolution order for your system to use DNS resolution before checking the hosts file. For more information about how to configure the host name resolution order, see the documentation for your operating system.

- The TADDM server supports only the IBM Java runtime environment (JRE).
- The user ID under which the TADDM server runs must have read, write, and execute permissions for its installation directory and contents, and for the temporary directory of the system. By default, the installation directory is `/opt/IBM/taddm` on Linux and UNIX systems, or `c:\ibm\taddm` on Windows systems. Typically, the temp directory is `%TEMP%` on a Windows system and `/tmp` on Linux and UNIX systems.
- On UNIX systems, the user ID under which the TADDM server runs must have an open file limit of at least 8192 files. You can set the open file limit using the **ulimit** command.
- On UNIX systems, the user ID under which the TADDM server runs must have a limit of at least 4096 processes for the maximum number of processes running per user. You can set the limit of the number of running processes using the **ulimit** command.
- On Linux and UNIX systems, the TADDM server user ID must also have root execution permission for the **nmap** command. For detailed information about Nmap and the Stack Scan sensor, see the *Stack Scan sensor* topic in the *TADDM Sensor Reference*.

- On supported AIX operating systems, you must have the unzip extraction utility available in the /usr/bin or /usr/local/bin directory. If not installed, you must install the extraction utility into one of those directories before beginning the TADDM server installation.
- lsof is required on AIX operating systems. Download it from the AIX Web Download Pack Programs website.
- AIX requires GNU **tar** version 1.14 or later.
- Discovered systems might be running operating systems and applications that are no longer supported by their vendors. While every effort is made to fix issues encountered on these targets of a discovery, you might have to reproduce the problem on a vendor-supported operating system or application, and use the vendors support.

The following table provides details about operating systems that are supported for TADDM servers. Operating system requirements for anchor servers are the same as the requirements for TADDM servers. Operating system requirements for gateway servers are the same as Windows operating system requirements for TADDM servers.

**Note:** For the most current information about supported operating systems, refer to the IBM software product compatibility reports at <http://www-969.ibm.com/software/reports/compatibility/clarity/index.html>.

<i>Table 37. Supported operating systems for TADDM servers</i>	
<b>Operating system and supported release</b>	<b>Support details</b>
AIX 6.1	Technology Level 5 is required.
AIX 7.1	Technology Level 1, Service Pack 2, or later is required.
AIX 7.2	Technology Level 0, Service Pack 1, or later is required.
Red Hat Enterprise Linux 6 x86_64	Update 1 is required.
Red Hat Enterprise Linux 6 for SystemZ	<p>You must install the libgcc package in version 4.1.2 or later. You must also install ld-linux.so.2 library if it is not installed.</p> <p><b>Note:</b> <b>Fix Pack 5</b> TADDM versions 7301 and above require both 64 bit as well as 32 bit packages for libgcc.</p> <p>You must install the libXft.so.2 library, because it is not installed by default on Linux systems.</p> <p>The Security-Enhanced Linux (SELinux) security system must be disabled. To disable SELinux specify SELINUX=disabled in the /etc/sysconfig/selinux configuration file. Restart your system after you modify the file.</p>



Table 37. Supported operating systems for TADDM servers (continued)

Operating system and supported release	Support details	
Red Hat Enterprise Linux 7 x86_64	<p>You must install the <code>libgcc</code> package in version 4.1.2 or later. You must also install <code>ld-linux.so.2</code> library if it is not installed.</p> <p><b>Note:</b> <b>Fix Pack 5</b> TADDM versions 7301 and above require both 64 bit as well as 32 bit packages for <code>libgcc</code>.</p> <p>You must install the <code>libXft.so.2</code> library, because it is not installed by default on Linux systems.</p> <p>The Security-Enhanced Linux (SELinux) security system must be disabled. To disable SELinux specify <code>SELINUX=disabled</code> in the <code>/etc/sysconfig/selinux</code> configuration file. Restart your system after you modify the file.</p>	
Red Hat Enterprise Linux 7 for SystemZ		
<b>Fix Pack 7</b> Red Hat Enterprise Linux 8 x86_64	<p>You must install the <code>libgcc</code> package in version 4.1.2 or later. You must also install <code>ld-linux.so.2</code> library if it is not installed.</p> <p><b>Note:</b> <b>Fix Pack 5</b> TADDM versions 7301 and above require both 64 bit as well as 32 bit packages for <code>libgcc</code>.</p> <p>The <code>libnsl</code> package for <code>x86_64</code> architecture must be installed during installation, uninstallation and upgrade process of TADDM. When you are upgrading to TADDM 7.3.0.8, <code>libnsl</code> is not necessary.</p> <p>You must install the <code>libXft.so.2</code> library, because it is not installed by default on Linux systems.</p> <p>The Security-Enhanced Linux (SELinux) security system must be disabled. To disable SELinux specify <code>SELINUX=disabled</code> in the <code>/etc/sysconfig/selinux</code> configuration file. Restart your system after you modify the file.</p>	
SUSE Linux Enterprise Server 11 x86_64	Service Pack 1 is required.	
SUSE Linux Enterprise Server 11 for SystemZ		
SUSE Linux Enterprise Server 12 x86_64		
SUSE Linux Enterprises Server 15 x86_64		
Microsoft Windows Server 2008 R2 Standard x86-64 Edition, Enterprise x86-64 Edition	Service Pack 1 is required.	
Microsoft Windows Server 2012	<p>.NET Framework 3.5 is required.</p> <p><b>Note:</b> <b>Fix Pack 2</b> If you use TADDM 7.3.0.2, or later, you can install .NET Framework 4, and 4.5.</p>	
Microsoft Windows Server 2012 R2	<p>.NET Framework 3.5 is required.</p> <p><b>Note:</b> <b>Fix Pack 2</b> If you use TADDM 7.3.0.2, or later, you can install .NET Framework 4, and 4.5.</p>	

Table 37. Supported operating systems for TADDM servers (continued)

Operating system and supported release	Support details
<b>Fix Pack 5</b> Microsoft Windows Server 2016	
<b>Fix Pack 6</b> Microsoft Windows Server 2019	

## Database server software requirements

Each TADDM domain database server must be running a supported relational database.

For testing or demonstration purposes, you can install the TADDM database on the same system as the domain server, synchronization server, or primary storage server. For a streaming server deployment, you must install the database before installing the TADDM server. For a domain server deployment or synchronization server deployment, the installer can optionally install a local DB2 database as part of the TADDM installation process or can create the required tables using an existing local DB2 installation. (To use a local Oracle database, you must install the database before installing the TADDM server.)

In a production environment, you must install a supported database on a separate system before installing the TADDM server. Any of the following database software can support a TADDM database:

Table 38. Supported software for TADDM database server

Supported database	Support details
IBM DB2 Version 9.7	Fix Pack 7 or later required. If possible, use the latest Fix Pack level available.
IBM DB2 Version 9.8	Fix Pack 4 or later required.
IBM DB2 Version 10.1	Fix Pack 4 or later required.
IBM DB2 Version 10.5	Fix Pack 1 or later required.
IBM DB2 Version 11.1	<ul style="list-style-type: none"> <li>• Fix Pack 3</li> <li>• <b>Fix Pack 8</b> Fix Pack 4</li> <li>• <b>Fix Pack 8</b> Fix Pack 5</li> </ul>
<b>Fix Pack 8</b> IBM DB2 Version 11.5	<b>Fix Pack 8</b> GA is supported

Table 38. Supported software for TADDM database server (continued)

Supported database	Support details
<p>Oracle 11g Release 2 (11.2) Oracle 12c Release 1 (12.1)</p>	<p><b>Important:</b> Before you install or upgrade the TADDM server, you must have at least the following Oracle components installed in your environment:</p> <ul style="list-style-type: none"> <li>• XDK</li> <li>• XML</li> <li>• RUL</li> </ul> <p><b>Fix Pack 4</b> Oracle 12.1.0.2 is now supported with the application of Oracle bug fix 22256560. <a href="https://support.oracle.com/epmos/faces/BugDisplay?id=22256560">https://support.oracle.com/epmos/faces/BugDisplay?id=22256560</a></p> <p>For Oracle 11g Release 2 (11.2) Patch Set 3 (11.2.0.3) or later is required. However, because of the bug 14496772 that was fixed in Oracle JDBC Drivers 11.2.0.4, additional JDBC libraries must be at least in 11.2.0.4 version. You must copy these libraries to the <code>dist/lib/jdbc</code> directory on your TADDM server.</p> <p>Required JDBC libraries:</p> <ul style="list-style-type: none"> <li>• The JDBC driver file <code>ojdbc6.jar</code>, which is in the <code>../app/oracle/product/Oracle_version/dbhome/jdbc/lib</code> directory.</li> <li>• Libraries for XML support: <ul style="list-style-type: none"> <li>– <code>xdb6.jar</code>, which is in the <code>../app/oracle/product/Oracle_version/dbhome/rdbms/jlib</code> directory.</li> <li>– <code>xmlparserv2.jar</code>, which is in the <code>../app/oracle/product/Oracle_version/dbhome/xdk/lib</code> directory on Oracle 11g, and in the <code>../app/oracle/product/Oracle_version/dbhome/lib</code> on Oracle 12c.</li> </ul> </li> </ul> <p><b>Oracle 12c Release 1 (12.1) note:</b> The Oracle Multitenant option is not supported.</p>
<p><b>Fix Pack 8</b> Oracle 18c and Oracle 19c</p>	<p>Required JDBC libraries:</p> <ul style="list-style-type: none"> <li>• The JDBC driver file <code>ojdbc8.jar</code>, which is in the <code>{ORACLE_HOME}/jdbc/lib</code> directory.</li> <li>• Libraries for XML support: <ul style="list-style-type: none"> <li>– <code>xdb6.jar</code>, which is in the <code>{ORACLE_HOME}/rdbms/jlib</code> directory.</li> <li>– <code>xmlparserv2.jar</code>, which is in the <code>{ORACLE_HOME}/lib</code> directory.</li> </ul> </li> </ul> <p><b>Note:</b></p> <ol style="list-style-type: none"> <li>1. The Oracle Multitenant option is not supported.</li> <li>2. Oracle 18c and 19c RAC on AIX platform are not currently covered/ tested.</li> </ol>

To determine your database level, use the following DB2 SQL command:

```
db2 connect to <taddm db name>
db2 "select * from sysibm.sysversions"
```

**Note:**

1. TADDM no longer supports DB2 Database hosted on z/OS operating system.
2. In case TADDM DB2 database instance needs to be run on System Z, then IBM recommends using the **supported** DB2 version, running on a **supported** version of “Linux for System Z”.
3. For the most current information about supported operating systems, refer to the IBM software product compatibility reports at <http://www-969.ibm.com/software/reports/compatibility/clarity/index.html>.

For optimal performance, install the following database components on separate physical devices or disk arms:

- Database tables and indexes (use four or more physical devices or disk arms)
- Database logs
- Database temporary space

If you are using DB2 on a Linux system, and you plan to create the TADDM database and tables during the installation process, make sure the SHMMAX and SHMALL shared memory kernel parameters meet the required minimum values before you install TADDM. For more information, refer to the DB2 documentation at [http://www-01.ibm.com/support/knowledgecenter/SSEPGG\\_9.5.0/com.ibm.db2.luw.kc.doc/welcome.html](http://www-01.ibm.com/support/knowledgecenter/SSEPGG_9.5.0/com.ibm.db2.luw.kc.doc/welcome.html).

## Client requirements

Client computers accessing TADDM servers must meet minimum hardware and software requirements.

### Client hardware requirements

To run the Discovery Management Console, a client system must meet the following hardware requirements.

- Processor: 2.0 GHz or faster
- Memory: 512 MB – 1 GB of RAM available to TADDM, depending on the number of discovered configuration items

For more information about configuring the minimum and maximum memory settings, refer to the TADDM *Administrator's Guide*.

### Client software requirements

To access the Discovery Management Console and the Data Management Portal, a client must be running a compatible web browser. In addition, the Discovery Management Console requires a compatible Java runtime environment.

### Browser requirements

The following browsers are supported for the Discovery Management Console and the Data Management Portal:

Operating system	Supported browsers
Windows	<ul style="list-style-type: none"> <li>• Microsoft Internet Explorer 11</li> <li>• Mozilla Firefox 24</li> <li>• Mozilla Firefox 31</li> <li>• <b>Fix Pack 5</b> MS Edge 40</li> </ul>
Linux and UNIX systems	<ul style="list-style-type: none"> <li>• Mozilla Firefox 24</li> <li>• Mozilla Firefox 31</li> </ul>

**Note:** The default system fonts and font sizes can be required to ensure correct layout and function.

## Java requirements

In addition to a supported web browser, the Discovery Management Console also requires either the IBM or Oracle Java runtime environment (JRE), version 7.0 or 8.0 on each client system.

**Note:** **Fix Pack 1** Oracle Java runtime environment version 8.0 is available from TADDM 7.3.0.1.

To determine whether you have the correct version of the Java runtime environment, run the following command at a DOS command prompt or a UNIX or Linux console window:

```
java -version
```

If the output indicates that you are running either the IBM or Oracle Java runtime environment, version 7.0 or 8.0, then all prerequisites are met.

## Installing the IBM Java SDK

If a client computer does not have a compatible Java runtime environment, you can install the IBM Java SDK provided on the TADDM product DVD. The Discovery Management Console supports both IBM and Oracle JREs.

### ***Installing the IBM Java SDK on a Linux or UNIX client***

Follow these steps to install the IBM Java SDK on a client computer running Linux or AIX.

1. On the product DVD, go to the /collation directory and locate the .zip file for your operating system:
  - Linux: /collation/linux.zip
  - Linux on System z: /collation/linuxS390.zip
  - AIX: aix.zip
2. Extract the contents of the .zip file to a temporary location.
3. Go to the dist/external/jdk directory of the location where you extracted the .zip file, and locate the .zip file containing the IBM Java SDK.  
The file name varies depending upon your operating system:
  - Linux: jdk-Linux-i686.zip
  - Linux on System z: jdk-Linux-s390.zip
  - AIX: jdk-AIX-powerpc.zip
4. Extract the Java SDK .zip file to the appropriate location on the client computer.  
Refer to your browser documentation to determine the correct location; your browser might require a specific directory location in order to associate the Java runtime environment with the browser (typically /usr/lib/javaxxx on Linux and UNIX systems).
5. Close all browser windows and then reopen the TADDM launch page.

### ***Installing the IBM Java SDK on a Windows client***

Follow these steps to install the IBM Java SDK on a client computer running Windows.

1. On the product DVD, go to the ibm-java/windows directory.
2. Run the ibm-java2-jre-version-win-i386.exe file.
3. Close all browser windows and then reopen the TADDM launch page.

## Planning for monitoring of TADDM servers

If you have multiple TADDM servers in your deployment, you might want to use the IBM Tivoli Monitoring Agent for TADDM Serviceability and Manageability to monitor the performance and availability of the TADDM servers.

This agent supports monitoring in both a streaming server deployment and a synchronization server deployment.

The Tivoli Monitoring Agent for TADDM Serviceability and Manageability is delivered on the second DVD ISO file for 7.3.0 version.

**Fix Pack 1** If you use TADDM 7.3.0.1, or later, you must download the agent from <http://www-933.ibm.com/support/fixcentral/swg/selectFixes?parent=ibm%7ETivoli&product=ibm/Tivoli/Tivoli+Application+Dependency+Discovery+Manager&release=7.3.0.1&platform=All&function=all>.

You can download the documentation for Tivoli Monitoring Agent for TADDM Serviceability and Manageability from <http://www.ibm.com/software/brandcatalog/ismlibrary/details?catalog.label=1TW10TA29>.

## Planning for security

Before installing, decide which user registry configuration you want to use for TADDM security. During the installation process, you must specify which user registry is used to authenticate TADDM users.

TADDM uses many forms of security, including user authentication and user authorization. User authentication ensures that a TADDM user is who the user claims to be. User authorization ensures that a TADDM user can manipulate TADDM objects and perform TADDM operations that the user is permitted to access.

The following table identifies the ways TADDM ensures that data that is collected during the discovery process is secure:

<b>Feature</b>	<b>Benefit</b>
Credentials required for user of API access	Eliminates unauthorized access to information or control
Logging of user activity	Enables security audits
Utilize SSH for host access	Authenticates and secures discovery activity

### Authentication

TADDM supports three types of user repositories that can be used to authenticate TADDM users: a TADDM file-based repository, LDAP repositories, and the federated repositories functions of IBM WebSphere® Application Server. You can select the type of user registry that you want to use during the installation process. These types of registries are mutually exclusive.

### TADDM file-based repository

The TADDM file-based repository is used for small proof-of-concept installations or environments where TADDM product integration that uses a single sign-on (SSO) is not required. The TADDM file-based repository requires that all users and groups (including passwords) are created, managed, and maintained within TADDM. To configure TADDM to use the file-based repository, select this repository during the TADDM installation.

### LDAP registry

If your environment has a central LDAP registry, you can use this repository to authenticate TADDM users. TADDM supports LDAP authentication by using the following products:

- IBM Tivoli Directory Server V6.0, V6.2 or later
- Microsoft Active Directory 2008 R2
- OpenLDAP V2.4.26 and V2.3.43
- Apache Directory Server V1.5.3

**Note:** However, If single sign-on is required, you must configure TADDM to use WebSphere federated repositories as the user registry.

## WebSphere federated repositories

The WebSphere federated repositories feature is a flexible meta-repository within WebSphere that supports multiple types of repositories, including Microsoft Active Directory. If you use other Tivoli products in your environment, including IBM Tivoli Change and Configuration Management Database (IBM SmartCloud Control Desk (SCCD)) or Tivoli Business Service Manager (TBSM) you can configure TADDM to use WebSphere federated repositories.

To see supported versions of the products, go to the *Supported versions* topic in the TADDM *Administrator's Guide*.

This configuration enables single sign-on (SSO) between Tivoli applications by using WebSphere Lightweight Third-Party Authentication (LTPA) tokens. For example, configuring TADDM for the same WebSphere federated repositories used by IBM Tivoli CCMDB or IBM SmartCloud Control Desk supports SSO for launch in context between IBM Tivoli CCMDB or IBM SmartCloud Control Desk and TADDM.

## Planning for the future

If you cannot use the federated repositories functionality of IBM WebSphere Application Server, but you plan to install IBM Tivoli CCMDB or IBM SmartCloud Control Desk in the future, it is easier for you to move to federated repositories if you choose the LDAP user registry instead of the file-based user registry. If you use an LDAP user registry, you do not have to re-create your users when moving to federated repositories.

## Authorization

TADDM supports two types of authorization: run time and data-level. These types of authorization are based on TADDM roles which are groups of permissions. The Data Management Portal manages the assignment of roles to users. This feature is not available through the Discovery Management Console. The following table shows the three core TADDM roles (administrator, operator, and supervisor) and their permissions.

<i>Table 41. TADDM roles and permissions</i>	
<b>Roles</b>	<b>Permissions</b>
Administrator	Read, Update, Admin, Discover
Operator	Read
Supervisor	Read, Update, Discover

## Runtime authorization

When using TADDM runtime authorization, the user interface (UI) and application programming interface (API) check specific TADDM permissions to prevent or authorize access to TADDM capabilities. The following list shows examples of runtime authorization:

- The Admin permission is checked before a user administering users, groups, and roles through the Data Management Portal.
- The Discover permission is checked before a user initiating TADDM discoveries or manually creating TADDM components in the Discovery Management Console.

Runtime authorization is always in effect and cannot be disabled.

## Data-level authorization

When using TADDM data-level security, named groups of TADDM objects (access collections) are created to define groups of objects that are managed by particular users. Users are assigned a role and access collections of objects with which to interact. One virtual access collection, `DefaultAccessCollection`, represents access to all objects. The TADDM-specific permissions (Read, Update) are used with access collections so that a user can view and modify objects (contained by the access collections) that the user can access. You can set up access collections, roles, and users in the Discovery Management Console after you complete the installation process.

Data-level authorization is disabled by default and can be enabled by setting `com.collation.security.enabledatalevelsecurity` to `true` in the `$COLLATION_HOME/etc/collation.properties` file.

## Multitenancy

TADDM can host multiple organizations or customers, allowing users to access the data that belongs to their organizations. Large companies and service providers might prefer multitenancy capabilities. TADDM supports multitenancy through the creation of access collections along organizational or customer lines.

For example, organization A's objects are grouped into access collections (A, B, and C). Organization B's objects are also grouped into access collections (D, E, and F). User #1 has administrator access (Read, Update, Admin, and Discover) for access collections (A, B, and C). User #2 has administrator access (Read, Update, Admin, and Discover) for access collections (D, E, and F). Therefore, each user can view the details of and modify the objects to which the user can access.

The TADDM user interface supports data-level security. If data-level security is enabled, a user can view details only about objects that are in access collections to which the user has access.

When planning for TADDM security, there are limitations:

- Because all TADDM administrators have Admin permission, each administrator is able to administer all TADDM users, including users that are associated with a particular organization. TADDM does not have a hierarchy of administrators.
- Data-level security does not apply to scopes. Therefore, any user with the Discovery permission can see all scope sets and scope groups, including those associated with other organizations or customers.
- Some TADDM reports might show objects to which users do not have access. TADDM reports generated by using the Business Intelligence and Reporting Tools (BIRT) system, access the TADDM database directly and do not support data-level security.

## Secure DB access

TADDM can use the SSL connection to the underlying database. Now only DB2 is supported in the SSL mode. You must configure all DB related SSL settings manually after installation for every installed server which has access to the database. Those servers are the domain server, primary storage server, secondary storage server, and enterprise server.

### Related tasks

[“Configuring post-installation DB2 secure access” on page 80](#)



After you install the TADDM server, you can configure secure DB2 access.

## Planning for single sign-on with IBM Tivoli CCMDB or IBM SmartCloud Control Desk

You can install TADDM to use the federated repositories function of IBM WebSphere Application Server to authenticate TADDM users. Use federated repositories to take advantage of the user and group management capabilities that it provides and to enable single sign-on (SSO) between Tivoli applications.

To see supported versions of the products, go to the *Supported versions* topic in the TADDM *Administrator's Guide*.

To use single sign-on, the IBM Tivoli Change and Configuration Management Database (IBM Tivoli CCMDB) or IBM SmartCloud Control Desk (IBM SCCD) and TADDM systems must be members of the same DNS domain that is configured in the WebSphere Application Server for single sign-on. Furthermore, the Authentication Service application (authnsvc\_ctges enterprise application) must be running on the CCMDB/SCCD or WebSphere Application Server in order to log in to TADDM, if TADDM is configured to use federated repositories. These functions are installed and configured as part of the IBM Tivoli CCMDB or IBM SCCD installation. For more information, see the guides on planning and installation of IBM Tivoli CCMDB and IBM SmartCloud Control Desk.

If you have WebSphere Application Server configured to use a stand-alone LDAP user registry, change the configuration to use federated repositories. To make this change, set up a subtree of the LDAP repository that combines all of the existing LDAP parameters into a single federated repository realm.

### Configuration of single sign-on between TADDM and IBM Tivoli CCMDB or IBM SCCD

When configuring TADDM to use WebSphere federated repositories, there are some configuration considerations:

- When specifying the WebSphere port, use the bootstrap port of the WebSphere instance. The bootstrap port is used for incoming EJB communications with the WebSphere Application Server.

For WebSphere Application Server and bundled version of WebSphere Application Server, this port is 2809.

For WebSphere Application Server Network Deployment, which IBM Tivoli CCMDB or IBM SCCD uses, this port is 9809.

- To implement single sign-on between IBM Tivoli CCMDB or IBM SCCD and TADDM, the two systems must be members of the same DNS single sign-on domain configured in WebSphere.

The instructions to configure the WebSphere single sign-on domain are found in the WebSphere 6.1 online documentation, in the section titled *Implementing single sign-on to minimize Web user authentications*.

## Planning worksheet for synchronization server deployment installation

You must make a number of settings to TADDM for a synchronization server deployment

Do not use port 10339 or 9436 as TADDM server port values during the installation. In a domain server deployment, do not use these ports for the Enterprise server port values.

Setting	Default	Your value
Installation directory for TADDM	<ul style="list-style-type: none"><li>• Linux, AIX, and Linux on System z Operating Systems: /opt/IBM/taddm</li><li>• Windows:c:\ibm\taddm</li></ul>	

<i>Table 42. Common installation settings (continued)</i>		
<b>Setting</b>	<b>Default</b>	<b>Your value</b>
Non-root user ID	<ul style="list-style-type: none"> <li>Linux, AIX, and Linux on System z Operating Systems:<i>taddmusr</i></li> <li>Windows: <i>user name for the person running the TADDM installation process</i></li> </ul>	
Global listening interface to bind TADDM installation to the specified IP interface	0.0.0.0	
Inter-server listening interface	0.0.0.0	
Public service registry port for obtaining access to TADDM public services (for example, API Service)	9433	
Inter-server service registry port for interactions between TADDM services	1100	
Local service registry port for TADDM internal use	1099	
Web Server port - main TADDM http server's port	9430	
Web Server SSL port - main TADDM secure HTTP server's port	9431	
API Server port - port of public TADDM service that provides access to TADDM Java API	9530	
Secure API Server port - secure port of public TADDM service that provides access to TADDM Java API	9531	
Start TADDM server at system boot (check box)	Not Selected	
Start TADDM server after installation (check box)	Selected	
IBM® Tivoli® CCMDB or IBM SmartCloud Control Desk server host name, for launch-in-context function		
IBM® Tivoli® CCMDB or IBM SmartCloud Control Desk server port, for launch-in-context function		

<i>Table 43. Settings for a Domain Server Installation</i>		
<b>Setting</b>	<b>Default</b>	<b>Your value</b>
Security Manager port for TADDM internal use	9540	

*Table 43. Settings for a Domain Server Installation (continued)*

<b>Setting</b>	<b>Default</b>	<b>Your value</b>
Topology Manager port for TADDM internal use	9550	
Registries URL Provider port	9560	
GUI-Server communication port for communication with Java Product Console	9435	
GUI-Server SSL port for secure communication with Java Product Console	9434	

*Table 44. Synchronization server installation settings*

<b>Setting</b>	<b>Default</b>	<b>Your value</b>
Enterprise Security Manager Service port for TADDM internal use	9570	
Registries URL Provider port	9560	

*Table 45. Settings for Oracle database*

<b>Setting</b>	<b>Default</b>	<b>Your value</b>
Oracle database system ID	orcl	
Oracle host name		
Oracle database port	1521	
Oracle user ID	taddmuser	
Oracle password		
Oracle additional (archive) user ID	archuser	
Oracle additional (archive) password		
Oracle system user ID (required only if the installer is creating the Oracle database users)	sys	
Oracle system password (required only if the installer is creating the Oracle database users)		
Oracle connect as role (required only if the installer is creating the Oracle database users)	sysdba	
Oracle home directory (required only if the installer is creating the Oracle database users)		

<i>Table 46. Settings for DB2 database</i>		
<b>Setting</b>	<b>Default</b>	<b>Your Value</b>
Database type	DB2	
Database server host name		
Database server port	50000	
Database name	taddm	
Node name for DB2 client		
Create database during installation (check box)	Yes	
DB2 instance user ID	<ul style="list-style-type: none"> <li>Linux, AIX, and Linux on System z Operating Systems: <i>db2inst1</i></li> <li>Windows: <i>db2admin</i></li> </ul>	
DB2 instance password		
DB2 database server port	50000	
Archive DB2 user ID	<i>archuser</i>	
Archive DB2 user ID password		

## Planning worksheet for streaming server deployment installation

You must make a number of settings to TADDM for a streaming server deployment

Do not use port 10339 or 9436 as TADDM server port values during the installation.

<i>Table 47. Common installation settings</i>		
<b>Setting</b>	<b>Default</b>	<b>Your value</b>
Installation directory for TADDM	<ul style="list-style-type: none"> <li>Linux, AIX, and Linux on System z Operating Systems: <i>/opt/IBM/taddm</i></li> <li>Windows: <i>c:\ibm\taddm</i></li> </ul>	
Non-root user ID	<ul style="list-style-type: none"> <li>Linux, AIX, and Linux on System z Operating Systems: <i>taddmusr</i></li> <li>Windows: <i>user name for the person running the TADDM installation process</i></li> </ul>	
Global listening interface to bind TADDM installation to the specified IP interface	0.0.0.0	
Inter-server listening interface	0.0.0.0	
Public service registry port for obtaining access to TADDM public services (for example, API Service)	9433	

Table 47. Common installation settings (continued)

Setting	Default	Your value
Inter-server service registry port for interactions between TADDM services	1100	
Local service registry port for TADDM internal use	1099	
Web Server port - main TADDM http server's port	9430	
Web Server SSL port - main TADDM secure HTTP server's port	9431	
API Server port - port of public TADDM service that provides access to TADDM Java API	9530	
Secure API Server port - secure port of public TADDM service that provides access to TADDM Java API	9531	
Start TADDM server at system boot (check box)	Not Selected	
Start TADDM server after installation (check box)	Selected	
IBM® Tivoli® CCMDB or IBM SmartCloud Control Desk server host name, for launch-in-context function		
IBM® Tivoli® CCMDB or IBM SmartCloud Control Desk server port, for launch-in-context function		

Table 48. Discovery server port values

Setting	Default	Your value
Primary storage server host name		
Primary storage server web server port	9430	
Primary storage server administrator user ID	administrator	
Primary storage server administrator password		
GUI-Server communication port for communication with Java Product Console	9435	
GUI-Server SSL port for secure communication with Java Product Console	9434	

Table 49. Port values for primary storage server

Setting	Default	Your value
Security Manager port for TADDM internal use	9540	
Topology Manager port for TADDM internal use	9550	
Registries URL Provider port	9560	
IBM® Tivoli® CCMDB or IBM SmartCloud Control Desk server host name (for launch-in-context function)		
IBM Tivoli CCMDB or IBM SmartCloud Control Desk server port (for launch-in-context function)		

Table 50. Port values for secondary storage server

Setting	Default	Your value
Topology Manager port for TADDM internal use	9550	
Registries URL Provider port	9560	
Primary storage server host name		
Primary storage server web server port	9430	
Primary storage server administrator user ID	administrator	
Primary storage server administrator password		

Table 51. Settings for DB2 database

Setting	Default	Your Value
Database type	DB2	
Database server host name		
Database server port	50000	
Database name	taddm	
Node name for DB2 client		
Create database during installation (check box)	Yes	
DB2 instance user ID	<ul style="list-style-type: none"> <li>• Linux, AIX, and Linux on System z Operating Systems: <i>db2inst1</i></li> <li>• Windows: <i>db2admin</i></li> </ul>	
DB2 instance password		


Table 51. Settings for DB2 database (continued)

Setting	Default	Your Value
DB2 database server port	50000	
Archive DB2 user ID	archuser	
Archive DB2 user ID password		

Table 52. Settings for Oracle database

Setting	Default	Your value
Oracle database system ID	orcl	
Oracle host name		
Oracle database port	1521	
Oracle user ID	taddmuser	
Oracle password		
Oracle additional (archive) user ID	archuser	
Oracle additional (archive) password		
Oracle system user ID (required only if the installer is creating the Oracle database users)	sys	
Oracle system password (required only if the installer is creating the Oracle database users)		
Oracle connect as role (required only if the installer is creating the Oracle database users)	sysdba	
Oracle home directory (required only if the installer is creating the Oracle database users)		

Table 53. Ports used by the PingSensor and PortSensor to make connections. These ports must be open for discovery to work.

Port name	Port number
CiscoWorks	1741
DNS	53
LDAP	389
 PowerShell	5985, 5986
SSH	22
WBEM	5988
WMI	135

# Installing TADDM

---

Follow these steps to install TADDM.

You can access the product software from DVD or from IBM Passport Advantage®.

**Note:** If the TADDM user upgrades the DB2 version in a TADDM installation, then compatible version of the driver should also be updated. You can ask your DBA for `db2jcc.jar` from the TADDM DB2 server, or you can download the one appropriate for your version of DB2 here: <http://www-01.ibm.com/support/docview.wss?uid=swg21363866> Once you have it, stop TADDM, copy it to `dist/lib/jdbc/`, confirm permissions are correct so that the TADDM user can read the file and then start TADDM. Repeat this step on all TADDM servers in your environment.

## Configuring the remote database server

Before installing the TADDM server for a production environment, configure the database server on a remote system.

### Preparing a DB2 database

Before you install TADDM with a remote DB2 database, you must prepare the database.

You must install the DB2 database software on the database server.

Make sure that your database server meets all of the hardware and software requirements for a TADDM database server. For more information, see [“Planning for installation” on page 6](#).

To prepare a DB2 database, complete the following steps:

1. Optional: If you want to use a new DB2 instance for the TADDM database, use the **db2icrt** command to create the DB2 instance.

Typically, the primary DB2 database user ID is the instance owner (`db2inst1` on Linux and UNIX systems, or `db2admin` on Windows systems). This database user ID is created during the DB2 installation. If you want to use the existing DB2 instance for the TADDM database, skip this step.

For more information about the **db2icrt** command, see the [DB2 documentation](#).

2. Use the user-account management facilities of your operating system to create the secondary database user ID (the archiver user, typically `archuser1`). Add it to the DB2 group of the DB2 instance owner.

To have permission to access the database, the secondary database user ID must be in the same DB2 group as the DB2 instance owner. Add the secondary database user ID to one of the following groups:

- Windows systems: `DB2ADMNS`
- Linux and UNIX systems: `db2grp1`, `db2iadm1`

3. Configure the DB2 by setting the following parameters:

#### All versions of DB2

```
db2 update dbm cfg using UTIL_IMPACT_LIM 95
```

#### DB2 10.1, and later

```
db2 update dbm cfg using SHEAPTHRES 0
```

For more information about the parameters, see the [DB2 documentation](#).

4. From the product DVD, copy the following file to the system where the DB2 database is installed:

- For Linux, and UNIX systems: `support/bin/make_db2_db.sh`
- For Windows systems: `support\bin\make_db2_db.bat`

5. Use one of the following procedures to run the `make_db2_db` script on the system where the DB2 database is installed:

- For Linux and UNIX operating systems:
  - a. Log in as the DB2 database instance owner. Use the `db2inst1` ID.



- b. Run the following command: **make\_db2\_db.sh taddm**
- For Windows operating systems:
  - a. Open the **DB2CMD** command line.
  - b. Run the following command: **make\_db2\_db.bat taddm**

## Preparing an Oracle database

Before installing TADDM with a remote Oracle database, you must first prepare the database by creating the Oracle user IDs required by the TADDM server.

You must first install the Oracle software on the database server.

- When creating the Oracle database, select the Unicode character set (AL32UTF8) in the **Database Character Set** field. Otherwise, data that is in languages other than English might not display correctly. If you see the Oracle message `OALL8 is in inconsistent state`, TADDM cannot access some of the national language-specific text in your database. Re-create your database with the correct character set.
- For Oracle RAC, complete the following steps for one of its nodes. Select the locally running SID as script parameter.

To prepare an Oracle database, complete the following steps:

1. From the product DVD, copy the following file to the system where the Oracle database is installed:
  - Linux and UNIX systems: `support/bin/make_ora_user.sh`
  - Windows systems: `support\bin\make_ora_user.bat`
2. Complete one of the following procedures to run the `make_ora_user` script on the system where the Oracle database is installed:
  - Linux and UNIX systems:
    - a. Log in as the Oracle user or the user that was used to install the Oracle database (typically `oracle`).

### Note:

When performing new 7.3 TADDM installation with Oracle 18C or 19C, the TADDM installers allow only `ojdbc6.jar` during installation. To proceed, add following in the `sqlnet.ora` file located at `${ORACLE_HOME}/network/admin` and then proceed with the creation of users as steps given below.

```
SQLNET.ALLOWED_LOGON_VERSION_SERVER=11
```

- b. Run the following command:

```
make_ora_user.sh sid cmdb_usr cmdb_pwd archive_usr archive_pwd
```

### **sid**

Oracle System Identification Database

### **cmdb\_usr**

Primary Oracle user ID

### **cmdb\_pwd**

Primary Oracle user password

### **archive\_usr**

Secondary (archive) user ID

### **archive\_pwd**

Secondary (archive) user password

- Windows systems:
  - a. At a command prompt, run the following command:

```
make_ora_user.bat sid cmdb_usr cmdb_pwd archive_usr archive_pwd
```

**sid**

Oracle System Identification Database

**cmdb\_usr**

Primary Oracle user ID

**cmdb\_pwd**

Primary Oracle user password

**archive\_usr**

Secondary (archive) user ID

**archive\_pwd**

Secondary (archive) user password

## Configuring for the Context Menu Service and Data Integration Service

If you want to use the Context Menu Service (CMS) and Data Integration Service (DIS) to enable cross-product launch points, you can connect to an existing DIS database used by other Tivoli or IBM products, or if one does not already exist, configure the TADDM database for CMS and DIS.

CMS and DIS support flexible cross-product launch points by storing information about available launch points in a database. By using this approach, a product can provide a launch capability for any other product that has registered launch points in the database, without having to implement product-specific launch functions. TADDM can use CMS and DIS to register TADDM launch points for use by other products such as CCMDB or IBM SmartCloud Control Desk.

You can configure CMS and DIS in either one of the following two ways:

- Configure TADDM to connect to an existing CMS/DIS database already used by other Tivoli or IBM products.
- Configure the TADDM database for CMS and DIS. In this situation, other Tivoli or IBM products in the enterprise using CMS and DIS can connect to this CMS/DIS database.

You must not set up more than one CMS/DIS database within a Tivoli enterprise.

You can optionally specify that the CMS/DIS configuration be completed automatically during the TADDM installation process. Follow these steps if you need to manually configure the CMS/DIS database after installation.

**Note:** To avoid delays in registering configuration items in the database, install the CMS/DIS database on a server that is geographically close to the TADDM database server.

## Preparing a DB2 database for the Context Menu Service and Data Integration Service

Follow these steps to manually configure a DB2 database for the Context Menu Service (CMS) and Data Integration Service (DIS).

You must install the DB2 database software on the database server.

You can optionally specify that the CMS and DIS configuration be completed automatically during the TADDM installation process. Follow these steps if you did not use this option and need to manually configure the database after installation.

To prepare a DB2 database for CMS and DIS:

1. Optional: If you want to use a new DB2 instance for the TADDM database, use the **db2icrt** command to create the DB2 instance.

Typically, the primary DB2 database user ID is the instance owner (db2inst1 on Linux and UNIX systems, or db2admin on Windows systems). This database user ID is created during the DB2 installation. If you want to use the existing DB2 instance for the TADDM database, skip this step.

Refer to the DB2 documentation for more information about the **db2icrt** command.

2. From the product DVD, copy the `support/cmsdis/cmsdis.zip` file to the system where the DB2 database is installed.
3. Use one of the following procedures to run the **make\_db2\_cms\_dis** script on the system where the DB2 database is installed:

- For Linux and UNIX systems:

- a. Log in as the DB2 database instance owner. Use the `db2inst1` ID.
- b. Extract the contents of the `cmsdis.zip` file.
- c. Navigate to the `cmsdis` directory.
- d. At a command prompt, run the following command:

```
make_db2_cms_dis.sh -d db_name db_user db_password
```

where:

**db\_name**

The database name. The database name for CMS and DIS must be different from the TADDM database name.

**db\_user**

The database instance user ID.

**db\_password**

The password for the database instance user ID.

- For Windows systems:

- a. Open the DB2CMD command prompt.
- b. Extract the contents of the `cmsdis.zip` file.
- c. Navigate to the `cmsdis` directory.
- d. At a command prompt, run the following command:

```
make_db2_cms_dis.bat -d db_name db_user db_password
```

where:

**db\_name**

The database name. The database name for CMS and DIS must be different from the TADDM database name.

**db\_user**

The database instance user ID.

**db\_password**

The password for the database instance user ID.

Check the standard output for any errors resulting from the **make\_db2\_cms\_dis** script.

4. Set the following configuration parameters in the `$COLLATION_HOME/etc/collation.properties` file:

```
com.ibm.cdb.DisCmsIntegration.enabled=true
com.ibm.cdb.DisCmsIntegration.dbUser=db2_instance_userid
com.ibm.cdb.DisCmsIntegration.dbPassword=db2_instance_password
com.ibm.cdb.DisCmsIntegration.dbUrl=jdbc:db2://db2_hostname:db2_port/db2_name
com.ibm.cdb.DisCmsIntegration.dbDriver=com.ibm.db2.jcc.DB2Driver
```

where:

**db2\_instance\_userid**

The user ID of the DB2 instance owner.

**db2\_instance\_password**

The password for the DB2 instance owner user ID.

**db2\_hostname**

The host name of the DB2 server.

**db2\_port**

The DB2 port on the server.

**db2\_name**

The DB2 instance name.

## Preparing an Oracle database for the Context Menu Service and Data Integration Service

Follow these steps to manually configure an Oracle database for the Context Menu Service (CMS) and Data Integration Service (DIS).

You must install the Oracle database software on the database server, and the **sqlplus** command must be available.

**Note:** When creating the Oracle database, select the Unicode character set (AL32UTF8) in the **Database Character Set** field. Otherwise, data that is in languages other than English might not display correctly. If you see the Oracle message `OALL8 is in inconsistent state`, TADDM cannot access some of the national language-specific text in your database. Re-create your database with the correct character set.

You can optionally specify that the CMS and DIS configuration automatically complete during the TADDM installation process. Follow these steps if you did not use this option and have to manually configure the database after installation.

To prepare an Oracle database for CMS and DIS:

1. From the product DVD, copy the `support/cmsdis/cmsdis.zip` file to the system where the Oracle database is installed.
2. Use one of the following procedures to run the **make\_oracle\_cms\_dis** script on the system where the Oracle database is installed:
  - For Linux and UNIX systems:
    - a. Log in as the Oracle user, or the user that was used to install the Oracle database (typically `oracle`).
    - b. Extract the contents of the `cmsdis.zip` file.
    - c. Go to the `cmsdis` directory.
    - d. At a command prompt, run the following command:

```
make_oracle_cms_dis.sh -d sid cmsdis_usr cmsdis_pwd
```

where:

**sid**

The Oracle system ID.

**cmsdis\_usr**

The Oracle user ID. This user ID must be different from the Oracle user ID used for TADDM.

**cmsdis\_pwd**

The password for the Oracle user ID.

- For Windows systems:
  - a. Extract the contents of the `cmsdis.zip` file.
  - b. Go to the `cmsdis` directory.
  - c. At a command prompt, run the following command:

```
make_oracle_cms_dis.bat -d sid cmsdis_usr cmsdis_pwd
```

where:

**sid**

The Oracle system ID.

**cmsdis\_usr**

The Oracle user ID. This user ID must be different from the Oracle user ID used for TADDM.

**cmsdis\_pwd**

The password for the Oracle user ID.

Check the standard output for any errors resulting from the **make\_oracle\_cms\_dis** script.

3. Set the following configuration parameters in the `$COLLATION_HOME/etc/collation.properties` file:

```
com.ibm.cdb.DisCmsIntegration.enabled=true
com.ibm.cdb.DisCmsIntegration.dbUser=oracle_cmsdis_user
com.ibm.cdb.DisCmsIntegration.dbPassword=oracle_cmsdis_password
com.ibm.cdb.DisCmsIntegration.dbUrl=
  jdbc:oracle:thin:@oracle_hostname:oracle_port:oracle_sid
com.ibm.cdb.DisCmsIntegration.dbDriver=oracle.jdbc.driver.OracleDriver
```

where:

**oracle\_cmsdis\_user**

The Oracle user ID for CMS and DIS.

**oracle\_cmsdis\_password**

The password for the Oracle user ID.

**oracle\_hostname**

The host name of the Oracle server.

**oracle\_port**

The Oracle port on the server.

**oracle\_sid**

The Oracle system ID.

## Installing TADDM servers

You can use any one of several methods to install TADDM servers.

There are several different TADDM servers you might need to install, depending on the type of deployment you want to use:

<i>Table 54. TADDM deployment types and servers</i>	
<b>Deployment type</b>	<b>Servers</b>
Domain server deployment	<ul style="list-style-type: none"> <li>• 1 domain server</li> </ul>
Synchronization server deployment (obsolete)	<ul style="list-style-type: none"> <li>• 2 or more domain servers</li> <li>• 1 synchronization server</li> </ul>
Streaming server deployment	<ul style="list-style-type: none"> <li>• 1 primary storage server</li> <li>• 1 or more discovery servers</li> <li>• 1 or more optional secondary storage servers</li> </ul>

You can use any of several methods to install TADDM servers.

## Installing TADDM servers using the installation wizard

Use the installation wizard to install a TADDM server by specifying options in a graphical user interface that guides you through the installation process step by step.

### *Installing a domain server using the installation wizard*

Follow these steps to install a domain server using the installation wizard. You can use a domain server in a stand-alone domain server deployment, or as part of a synchronization server deployment.

**Note:** The synchronization server deployment type is obsolete. In a new TADDM deployment where more than one server is needed, use the streaming server deployment.

You must be logged in to an account with administrator privileges to install the TADDM server. Complete all prerequisite steps, including any required database configuration, before starting the installation process.

If you are installing the TADDM server on a supported Microsoft Windows Server, you must temporarily turn off User Account Control (UAC) before starting the installation process. You must restart the system each time you modify this option. For more information on Windows Server 2012 see <http://social.technet.microsoft.com/wiki/contents/articles/13953.windows-server-2012-deactivating-uac.aspx>.

There are two basic types of domain server installation:

- **Simple installation** installs the domain server with default options, using a local DB2 database (which you can optionally install during the server installation). This type of installation is suitable for testing but is not intended for production environments.
- **Advanced installation** installs the domain server using a remote DB2 or Oracle database, and with installation options that you can customize for your environment. Use advanced installation for production environments.

The installation wizard prompts you to select either simple or advanced installation. If you select simple installation, some steps in the installation procedure do not apply.

### Notes

- If you are installing on a dual-stack system that supports both the IPv4 and IPv6 protocols, make sure any numeric IP addresses you specify during the installation process are IPv4 addresses.
- For Oracle RAC database, you can only select Advanced installation. TADDM installer does not support RAC configuration directly. You can only install TADDM with one RAC node configuration, and then update JDBC connection string in the `collation.properties` file after the installation. See “[Configuring Oracle RAC after installation](#)” on page 76.

To install the domain server using the installation wizard:

1. Insert the TADDM Disc 1 installation DVD for your supported operating system into the DVD drive. If you downloaded TADDM in the zip format, the zip files number 1 and 2 are the equivalent of Disc 1.
2. At a command prompt, go to the DVD drive, or to the directory where you saved the zip files, and run the appropriate command for your operating system:
  - For AIX operating systems, **setupAix.bin**
  - For Linux operating systems, **setupLinux.bin**
  - For Linux on System z operating systems, **setupZLinux.bin**
  - For Windows operating systems, **setupWin.bat**

**Restriction:** When you run the TADDM installation wizard `setupWin.bat` on Windows operating systems, select the **Run as administrator** option. Otherwise, the installation will fail.

**Note:** If an error message is displayed that there is insufficient disk space in the temp directory, run the installation again and specify a different temp directory. Use the option `-t temp` (for example, `setupLinux.bin -t /mytempdir`).

3. Select the language to use for your installation. Click **OK**.
4. On the Introduction page, click **Next**.

5. Read and accept the terms of the software license agreement and click **Next**.

6. Specify the location where you want to install the server.

Make sure that the path you specify contains only ASCII characters, and does not contain any spaces. Non-ASCII characters or spaces in the path can cause installation problems and problems starting the server.

After you specify the server location, click **Next**.

7. Specify the user ID you want to use to run the server.

- On Windows operating systems, the user must belong to the Administrators group. If the user does not exist or is not part of the Administrators group, select the check box to create the user or add the user to the Administrators group. The user ID must be a local user account.
- On Linux and UNIX operating systems, the user ID you specify must be non-root.

After you have specified the user ID, click **Next**.

**Note:** If the user ID you are using to run the installer is not an administrator or root, this page is not displayed.

8. On the IBM Tivoli Application Dependency Discovery Manager Deployment Option page, select **Domain server deployment**.

Click **Next**.

9. Select the installation type (**Simple** or **Advanced**):

- To install the server with default options and a local DB2 database, select **Simple**. This type of installation is suitable for testing but is not intended for production environments.

If the DB2 database software is not already installed on your system, you can optionally select **Install DB2 database on the system** to include the DB2 software as part of a simple installation.

**Note:** Make sure that the password that you choose for the DB2 user complies with the DB2 and operating system requirements. TADDM installer does not verify the password and if the password does not comply with the requirements, DB2 installation fails.

On Linux and UNIX operating systems, DB2 is installed in `/opt/ibm/db2/10.1` and the DB2 instance is installed in `/home/db2inst1`.

On Windows operating systems, DB2 and the DB2 instance are installed in `Program_files\IBM\SQLLIB`

Ensure that there is enough disk space available at these locations. The disk space used by the instance will increase with use. For more information about the amount of disk space required for a typical installation, see [“Database server hardware requirements”](#) on page 13.

The default installation locations cannot be changed when installing DB2 as part of a simple installation. If sufficient disk space is not available, you must either install DB2 manually on the local server, or use a remote DB2 instance installed on another computer.

- To install the server for a production environment with a remote DB2 or Oracle database, select **Advanced**. With advanced installation, you can customize the installation options.

After you select the installation type, click **Next**.

**Note:** If you chose a simple installation, configure Registry Services connection as described in [10. e.](#) and skip to step [“11”](#) on page 59.

10. Specify advanced server options and the database type:

- a) On the General network connection settings page, specify the required settings. Click **Next**.
- b) On the Public ports on server page, specify the required port information. Click **Next**.
- c) On the Inter-server communication ports page, specify the required port information. Click **Next**.
- d) On the Additional Server Information page, specify the following options:

- The platform binaries to install. If you configure the binaries later, the binaries are pushed to the remote gateway or anchor. If you are not sure which platform binaries you want to install, select **All**.
- Server startup options.

Click **Next**.

- e) On the Registry Services connection information page, specify the Registry Services **Connection URL** and the user information. You can also choose data providers. Click **Next**. If you do not want to configure Registry Services connection, clear the **Configure Registry Services connection** check box.
- f) Select the database type (**DB2** or **Oracle**). Click **Next**.
- g) If you are using an Oracle database, specify the path to a directory that contains the Oracle JDBC driver and two other Oracle jars that support XML operations, `ojdbc6.jar`, `xdb6.jar`, and `xmlparserv2.jar`. Click **Next**.

Verify that the version of all the files that you are using is the same as the version of the Oracle server.

**Important:** If you use Oracle 11.2.0.3, or 11.2.0.4, the jars must be in version 11.2.0.4. If you use Oracle 12, the jars must be in version 12. You must place the jar files in the `dist/lib/jdbc` directory on your TADDM server. You can download them from the Oracle website, or copy them from the Oracle server, not Oracle client, from the following locations:

- `../app/oracle/product/Oracle_version/dbhome/jdbc/lib/ojdbc6.jar`
- `../app/oracle/product/Oracle_version/dbhome/rdbms/jlib/xdb6.jar`
- `../app/oracle/product/Oracle_version/dbhome/xdk/lib/xmlparserv2.jar` on Oracle 11g, or `../app/oracle/product/Oracle_version/dbhome/lib/xmlparserv2.jar` on Oracle 12c

Oracle provides various copies of the `xmlparserv2.jar` file, therefore, you must copy it from the preceding location, not from another one. For more information, contact your database administrator.

**Note:** **Fix Pack 4** If you use Oracle 12 (version 12.2.0.1), after completion of TADDM installation, the jars- `ojdbc6.jar`, `xdb6.jar`, and `xmlparserv2.jar` at the path `dist/lib/jdbc` must be replaced with jars `ojdbc7.jar`, `xdb6.jar`, and `xmlparserv2.jar`. These jars can be copied from the path : `../app/oracle/product/Oracle_version/dbhome/sqldeveloper/sqlcl/lib`.

**Note:** **Fix Pack 8** If you use Oracle 18c or 19c, after completion of TADDM installation, the jars - `ojdbc6.jar`, `xdb6.jar`, and `xmlparserv2.jar` at the path `dist/lib/jdbc` must be replaced with jars `ojdbc8.jar`, `xdb6.jar`, and `xmlparserv2.jar`. You can download these jars from the Oracle website, or copy from the Oracle server (not from Oracle client), from the following locations:

- `${ORACLE_HOME}/jdbc/lib/ojdbc8.jar`
- `${ORACLE_HOME}/rdbms/jlib/xdb6.jar`
- `${ORACLE_HOME}/lib/xmlparserv2.jar`

Besides `dist/lib/jdbc`, check if `ojdbc6.jar` or `ojdbc7.jar` is present at any of the following location on TADDM. If yes, remove it and then add `ojdbc8.jar` used above at the following locations on TADDM:

- `ist/apps/dap/WEB-INF/lib`
- `dist/apps/birt-viewer/WEB-INF/platform/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.1.r22x_v20070919/drivers`

Post installation, you may revert the `SQLNET.ALLOWED_LOGON_VERSION_SERVER=11` entry, if set during user creation for fresh TADDM installation, with Oracle 18c or 19c.



11. On the Database Information page, specify the TCP/IP host name or numeric IP address, listening port, database name, and user information for the database.

If you are using the simple installation process with an existing local installation of DB2, select **Create the database during install** unless the required TADDM database and tables already exist.

Click **Next**.

**Note:** If you are using the simple installation process, skip to step [“17” on page 60](#) after you complete this step.

See [“Configuring the remote database server” on page 50](#) for information about user account requirements.

12. Optional: If you want to configure the Context Menu Service and Data Integration Service during the installation process, select the **Configure Context Menu Service (CMS) / Data Integration Service (DIS)** check box.

(If you do not select this option during the installation process, you can manually configure the Context Menu Service and Data Integration Service after installing. For more information, see [“Configuring for the Context Menu Service and Data Integration Service” on page 52.](#))

If you are not configuring the Context Menu Service and Data Integration Service, skip to [“14” on page 59.](#)

13. Optional: If you are configuring the Context Menu Service and Data Integration Service, specify the required database information.

**Note:** To avoid delays in registering configuration items in the database, install the CMS/DIS database on a server that is geographically close to the TADDM database server.

If you are using a DB2 database, follow these steps:

- a) Specify the database server, port, database name, and user information for the database.  
The database name must be different from the TADDM database name.
- b) Select **Create the database during install** unless the required database and tables already exist.  
(If you select **Create the database during install** and the database already exists, the installer deletes the existing database and creates the new one.)

**Note:** The **Create the database during install** check box is available only if the DB2 database is on the local system and the user ID running the installation process has root or administrator privileges.

Click **Next**.

If you are using an Oracle database, follow these steps:

- a) Specify the database server, port, system ID, and Oracle user information for the database.  
The Oracle user for the Context Menu Service and Data Integration Service must be different from the Oracle user for the domain server.
- b) Select **Create the user during install** unless the required user already exists.  
(If you select **Create the user during install** and the user already exists, the installer deletes the existing user and creates the new one.)

**Note:** The **Create the user during install** check box is available only if the user ID running the installation process has root or administrator privileges.

Click **Next**.

- c) If you selected the **Create the user** check box, specify the Oracle database administrator information and the Oracle home directory.

This information is used to create the Context Menu Service and Data Integration Service Oracle user during the installation process.

Click **Next**.

14. Select the user registry option:

- To use a file-based registry, select **File-based user registry**. No additional configuration information is required for this option.
- To use a Lightweight Directory Access Protocol (LDAP) user registry, select **LDAP user registry**.
- To use a WebSphere Federated Repositories registry, select **WebSphere Federated Repositories**.

Click **Next**.

15. If you selected an LDAP user registry, additional pages prompt you for LDAP server and configuration information:

- a) Specify the LDAP server and user information. Click **Next**.
- b) Specify the LDAP configuration parameters (or accept the defaults values). Click **Next**.

16. If you selected a WebSphere Federated Repositories registry, specify the WebSphere Federated Repositories server and user information.

**Note:** User IDs and passwords are case sensitive. Make sure you use the correct case.

Click **Next**.

17. Review the pre-installation summary. After you verify that the information is correct, click **Next** to start the installation process.

18. If you are installing the DB2 software as part of a simple installation, follow the instructions to install DB2:

**Important:** If you are installing a Linux, or AIX system, make sure you navigate to the root directory and unmount the optical drive before changing disks.

- a) Insert TADDM Disc 2, or specify the DB2 installation image directory. If you downloaded TADDM in the zip format, the zip files number 3 and 4 are the equivalent of Disc 2. Click **Next**.
- b) Insert TADDM Disc 1 (zip files number 1 and 2), or specify image directory. Click **Next**.

19. When prompted, insert TADDM Disc 3 into the DVD drive. Specify the image directory. If you downloaded the zip files, specify the path to the zip file number 5. Click **Next**.

**Note:** **Fix Pack 6** TADDM Disc 3 is the unzipped path to TADDM 7.3.0.1 which is available on fix central, see <https://www-945.ibm.com/support/fixcentral>.

20. After the installation finishes, click **Done** to close the installation wizard.

This installation can be a lengthy process, depending on the number and type of components you are installing. While the installation process is running, you can monitor progress by viewing changes to the installation log. The log also contains information that can help you troubleshoot problems that occur during installation. Log files can be found in the `installLogs` subdirectory of the installation directory.

On a supported Microsoft Windows Server, remember to turn User Account Control (UAC) on after you have finished the installation, and to restart your system. For more information on Windows Server 2012 see <http://social.technet.microsoft.com/wiki/contents/articles/13953.windows-server-2012-deactivating-uac.aspx>.

### ***Installing a synchronization server using the installation wizard***

Follow these steps to install a synchronization server for a TADDM synchronization server deployment.

**Note:** The synchronization server deployment type is obsolete. In a new TADDM deployment where more than one server is needed, use the streaming server deployment.

You must be logged in to an account with administrator privileges to install the TADDM server. Complete all prerequisite steps, including any required database configuration, before starting the installation process.

If you are installing the TADDM server on a supported Microsoft Windows Server, you must temporarily turn off User Account Control (UAC) before starting the installation process. You must restart the system each time you modify this option. For more information on Windows Server 2012 see <http://social.technet.microsoft.com/wiki/contents/articles/13953.windows-server-2012-deactivating-uac.aspx>.

The installation wizard guides you through the installation process. Depending on the selections you make in the wizard, some steps in the installation procedure might not apply.

**Note:** If you are installing on a dual-stack system that supports both the IPv4 and IPv6 protocols, make sure any numeric IP addresses you specify during the installation process are IPv4 addresses.

To install the synchronization server using the installation wizard:

1. Insert the TADDM Disc 1 installation DVD for your supported operating system into the DVD drive. If you downloaded TADDM in the zip format, the zip files number 1 and 2 are the equivalent of Disc 1.
2. At a command prompt, go to the DVD drive, or to the directory where you saved the zip files, and run the appropriate command for your operating system:
  - For AIX operating systems, **setupAix.bin**
  - For Linux operating systems, **setupLinux.bin**
  - For Linux on System z operating systems, **setupZLinux.bin**
  - For Windows operating systems, **setupWin.bat**

**Restriction:** When you run the TADDM installation wizard `setupWin.bat` on Windows operating systems, select the **Run as administrator** option. Otherwise, the installation will fail.

**Note:** If an error message is displayed that there is insufficient disk space in the temp directory, run the installation again and specify a different temp directory. Use the option `-t temp` (for example, `setupLinux.bin -t /mytempdir`).

3. Select the language to use for your installation. Click **OK**.
4. On the Introduction page, click **Next**.
5. Read and accept the terms of the software license agreement and click **Next**.
6. Specify the location where you want to install the server.

Make sure the path you specify contains only ASCII characters, and does not contain any spaces. Non-ASCII characters or spaces in the path can cause installation problems and problems starting the server.

After you specify the server location, click **Next**.

7. Specify the user ID you want to use to run the server.
  - On Windows operating systems, the user must belong to the Administrators group. If the user does not exist or is not part of the Administrators group, select the check box to create the user or add the user to the Administrators group. The user ID must be a local user account.
  - On Linux and UNIX operating systems, the user ID you specify must be non-root.

After you have specified the user ID, click **Next**.

**Note:** If the user ID you are using to run the installer is not an administrator or root, this page is not displayed.

8. On the IBM Tivoli Application Dependency Discovery Manager Deployment Option page, select **Synchronization server deployment**.

Click **Next**.

9. On the General network connection settings page, specify the required settings. Click **Next**.
10. On the Public ports on server page, specify the required port information. Click **Next**.
11. On the Inter-server communication ports page, specify the required port information. Click **Next**.
12. On the Additional Server Information page, specify the following options:
  - The RMI server host name. If the server resides on the same system as IBM Tivoli CCMDB or IBM SmartCloud Control Desk, accept the default value. If the server resides on a different system, type the numeric IP address (not the host name) of the server.
  - The platform binaries to install. If you configure the binaries later, the binaries are pushed to the remote gateway or anchor. If you are not sure which platform binaries you want to install, select **All**.
  - Server startup options.

Click **Next**.

13. On the Registry Services connection information page, specify the Registry Services **Connection URL** and the user information. You can also choose data providers. Click **Next**. If you do not want to configure Registry Services connection, clear the **Configure Registry Services connection** check box.
14. Select the database type (**DB2** or **Oracle**). Click **Next**.
15. If you are using an Oracle database, specify the path to a directory that contains the Oracle JDBC driver and two other Oracle jars that support XML operations, `ojdbc6.jar`, `xdb6.jar`, and `xmlparserv2.jar`. Click **Next**.

Verify that the version of all the files that you are using is the same as the version of the Oracle server.

**Important:** If you use Oracle 11.2.0.3, or 11.2.0.4, the jars must be in version 11.2.0.4. If you use Oracle 12, the jars must be in version 12. You must place the jar files in the `dist/lib/jdbc` directory on your TADDM server. You can download them from the Oracle website, or copy them from the Oracle server, not Oracle client, from the following locations:

- `../app/oracle/product/Oracle_version/dbhome/jdbc/lib/ojdbc6.jar`
- `../app/oracle/product/Oracle_version/dbhome/rdbms/jlib/xdb6.jar`
- `../app/oracle/product/Oracle_version/dbhome/xdk/lib/xmlparserv2.jar` on Oracle 11g, or `../app/oracle/product/Oracle_version/dbhome/lib/xmlparserv2.jar` on Oracle 12c

Oracle provides various copies of the `xmlparserv2.jar` file, therefore, you must copy it from the preceding location, not from another one. For more information, contact your database administrator.

**Note:** **Fix Pack 4** If you use Oracle 12 (version 12.2.0.1), after completion of TADDM installation, the jars- `ojdbc6.jar`, `xdb6.jar`, and `xmlparserv2.jar` at the path `dist/lib/jdbc` must be replaced with jars `ojdbc7.jar`, `xdb6.jar`, and `xmlparserv2.jar`. These jars can be copied from the path: `../app/oracle/product/Oracle_version/dbhome/sqldeveloper/sqlcl/lib`.

**Note:** **Fix Pack 8** If you use Oracle 18c or 19c, after completion of TADDM installation, the jars - `ojdbc6.jar`, `xdb6.jar`, and `xmlparserv2.jar` at the path `dist/lib/jdbc` must be replaced with jars `ojdbc8.jar`, `xdb6.jar`, and `xmlparserv2.jar`. You can download these jars from the Oracle website, or copy from the Oracle server (not from Oracle client), from the following locations:

- `${ORACLE_HOME}/jdbc/lib/ojdbc8.jar`
- `${ORACLE_HOME}/rdbms/jlib/xdb6.jar`
- `${ORACLE_HOME}/lib/xmlparserv2.jar`

Besides `dist/lib/jdbc`, check if `ojdbc6.jar` or `ojdbc7.jar` is present at any of the following location on TADDM. If yes, remove it and then add `ojdbc8.jar` used above at the following locations on TADDM:

- `ist/apps/dap/WEB-INF/lib`
- `dist/apps/birt-viewer/WEB-INF/platform/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.1.r22x_v20070919/drivers`

Post installation, you may revert the `SQLNET.ALLOWED_LOGON_VERSION_SERVER=11` entry, if set during user creation for fresh TADDM installation, with Oracle 18c or 19c.

16. On the Database Information page, specify the TCP/IP host name or numeric IP address, listening port, database name, and user information for the database.

If you are using the simple installation process with an existing local installation of DB2, select **Create the database during install** unless the required TADDM database and tables already exist.

Click **Next**.

See “[Configuring the remote database server](#)” on page 50 for information about user account requirements.

17. Optional: If you want to configure the Context Menu Service and Data Integration Service during the installation process, select the **Configure Context Menu Service (CMS) / Data Integration Service (DIS)** check box.

(If you do not select this option during the installation process, you can manually configure the Context Menu Service and Data Integration Service after installing. For more information, see [“Configuring for the Context Menu Service and Data Integration Service”](#) on page 52.)

If you are not configuring the Context Menu Service and Data Integration Service, skip to [“19”](#) on page 63.

18. Optional: If you are configuring the Context Menu Service and Data Integration Service, specify the required database information.

**Note:** To avoid delays in registering configuration items in the database, install the CMS/DIS database on a server that is geographically close to the TADDM database server.

If you are using a DB2 database, follow these steps:

- a) Specify the database server, port, database name, and user information for the database.  
The database name must be different from the TADDM database name.
- b) Select **Create the database during install** unless the required database and tables already exist.  
(If you select **Create the database during install** and the database already exists, the installer deletes the existing database and creates the new one.)

**Note:** The **Create the database during install** check box is available only if the DB2 database is on the local system and the user ID running the installation process has root or administrator privileges.

Click **Next**.

If you are using an Oracle database, follow these steps:

- a) Specify the database server, port, system ID, and Oracle user information for the database.  
The Oracle user for the Context Menu Service and Data Integration Service must be different from the Oracle user for the domain server.
- b) Select **Create the user during install** unless the required user already exists.  
(If you select **Create the user during install** and the user already exists, the installer deletes the existing user and creates the new one.)

**Note:** The **Create the user during install** check box is available only if the user ID running the installation process has root or administrator privileges.

Click **Next**.

- c) If you selected the **Create the user** check box, specify the Oracle database administrator information and the Oracle home directory.  
This information is used to create the Context Menu Service and Data Integration Service Oracle user during the installation process.

Click **Next**.

19. Select the user registry option:

- To use a file-based registry, select **File-based user registry**. No additional configuration information is required for this option.
- To use a Lightweight Directory Access Protocol (LDAP) user registry, select **LDAP user registry**.
- To use a WebSphere Federated Repositories registry, select **WebSphere Federated Repositories**.

Click **Next**.

20. If you selected an LDAP user registry, additional pages prompt you for LDAP server and configuration information:

- a) Specify the LDAP server and user information. Click **Next**.
- b) Specify the LDAP configuration parameters (or accept the defaults values). Click **Next**.

21. If you selected a WebSphere Federated Repositories registry, specify the WebSphere Federated Repositories server and user information.

**Note:** User IDs and passwords are case sensitive. Make sure you use the correct case.

Click **Next**.

22. Review the pre-installation summary. After you verify that the information is correct, click **Next** to start the installation process.
23. If you are installing the DB2 software as part of a simple installation, follow the instructions to install DB2:

**Important:** If you are installing a Linux, or AIX system, make sure you navigate to the root directory and unmount the optical drive before changing disks.

- a) Insert TADDM Disc 2 or specify the DB2 installation image directory. If you downloaded TADDM in the zip format, the zip files number 3 and 4 are the equivalent of Disc 2. Click **Next**.
  - b) Insert TADDM Disc 1 (zip files number 1 and 2), or specify image directory. Click **Next**.
24. When prompted, insert TADDM Disc 3 into the DVD drive. Specify the image directory. If you downloaded the zip files, specify the path to the zip file number 5. Click **Next**.
  25. After the installation finishes, click **Done** to close the installation wizard.

This installation can be a lengthy process, depending on the number and type of components you are installing. While the installation process is running, you can monitor progress by viewing changes to the installation log. The log also contains information that can help you troubleshoot problems that occur during installation. Log files can be found in the `installLogs` subdirectory of the installation directory.

On a supported Microsoft Windows Server, remember to turn User Account Control (UAC) on after you have finished the installation, and to restart your system. For more information on Windows Server 2012 see <http://social.technet.microsoft.com/wiki/contents/articles/13953.windows-server-2012-deactivating-uac.aspx>.

### ***Installing the primary storage server using the installation wizard***

Follow these steps to install the primary storage server using the installation wizard. The primary storage server is required for a streaming server deployment.

You must be logged in to an account with administrator privileges to install TADDM. Complete all prerequisite steps, including any required database configuration, before starting the installation process.

If you are installing the TADDM server on a supported Microsoft Windows Server, you must temporarily turn off User Account Control (UAC) before starting the installation process. You must restart the system each time you modify this option. For more information on Windows Server 2012 see <http://social.technet.microsoft.com/wiki/contents/articles/13953.windows-server-2012-deactivating-uac.aspx>.

A storage server processes discovery data and stores it in a local or remote DB2 or Oracle database. A streaming server deployment requires at least one storage server (the primary storage server). Install the primary storage server before installing any discovery servers.

**Note:** For Oracle RAC database, you can only select Advanced installation. TADDM installer does not support RAC configuration directly. You can only install TADDM with one RAC node configuration, and then update JDBC connection string in the `collation.properties` file after the installation. See [“Configuring Oracle RAC after installation”](#) on page 76.

To install the primary storage server using the installation wizard:

1. Insert the TADDM Disc 1 installation DVD for your supported operating system into the DVD drive. If you downloaded TADDM in the zip format, the zip files number 1 and 2 are the equivalent of Disc 1.
2. At a command prompt, go to the DVD drive, or to the directory where you saved the zip files, and run the appropriate command for your operating system:
  - For AIX operating systems, **setupAix.bin**
  - For Linux operating systems, **setupLinux.bin**
  - For Linux on System z operating systems, **setupZLinux.bin**

- For Windows operating systems, **setupWin.bat**

**Restriction:** When you run the TADDM installation wizard `setupWin.bat` on Windows operating systems, select the **Run as administrator** option. Otherwise, the installation will fail.

**Note:** If an error message is displayed that there is insufficient disk space in the temp directory, run the installation again and specify a different temp directory. Use the option `-t temp` (for example, `setupLinux.bin -t /mytempdir`).

3. Select the language to use for your installation. Click **OK**.

4. On the Introduction page, click **Next**.

5. Read and accept the terms of the software license agreement and click **Next**.

6. Specify the location where you want to install the server.

Make sure the path you specify contains only ASCII characters, and does not contain any spaces. Non-ASCII characters or spaces in the path can cause installation problems and problems starting the server.

After you specify the server location, click **Next**.

7. Specify the user ID you want to use to run the server.

- On Windows operating systems, the user must belong to the Administrators group. If the user does not exist or is not part of the Administrators group, select the check box to create the user or add the user to the Administrators group. The user ID must be a local user account.
- On Linux and UNIX operating systems, the user ID you specify must be non-root.

After you specify the server location, click **Next**.

8. On the IBM Tivoli Application Dependency Discovery Manager Deployment Option page, select **Streaming server deployment**.

Click **Next**.

9. When prompted for the type of server you want to install, select **Primary Storage Server**.

10. On the General network connection settings page, specify the required settings. Click **Next**.

11. On the Public ports on server page, specify the required port information. Click **Next**.

12. On the Inter-server communication ports page, specify the required port information. Click **Next**.

13. On the Additional Server Information page, specify the following options:

- Server startup options.

Click **Next**.

14. On the Registry Services connection information page, specify the Registry Services **Connection URL** and the user information. You can also choose data providers. Click **Next**. If you do not want to configure Registry Services connection, clear the **Configure Registry Services connection** check box.

15. Select the database type (**DB2** or **Oracle**). Click **Next**.

16. If you are using an Oracle database, specify the path to a directory that contains the Oracle JDBC driver and two other Oracle jars that support XML operations, `ojdbc6.jar`, `xdb6.jar`, and `xmlparserv2.jar`. Click **Next**.

Verify that the version of all the files that you are using is the same as the version of the Oracle server.

**Important:** If you use Oracle 11.2.0.3, or 11.2.0.4, the jars must be in version 11.2.0.4. If you use Oracle 12, the jars must be in version 12. You must place the jar files in the `dist/lib/jdbc` directory on your TADDM server. You can download them from the Oracle website, or copy them from the Oracle server, not Oracle client, from the following locations:

- `../app/oracle/product/Oracle_version/dbhome/jdbc/lib/ojdbc6.jar`
- `../app/oracle/product/Oracle_version/dbhome/rdbms/jlib/xdb6.jar`
- `../app/oracle/product/Oracle_version/dbhome/xdk/lib/xmlparserv2.jar` on Oracle 11g, or `../app/oracle/product/Oracle_version/dbhome/lib/xmlparserv2.jar` on Oracle 12c



Oracle provides various copies of the `xmlparserv2.jar` file, therefore, you must copy it from the preceding location, not from another one. For more information, contact your database administrator.

**Note:** **Fix Pack 4** If you use Oracle 12 (version 12.2.0.1), after completion of TADDM installation, the `jars-ojdbc6.jar`, `xdb6.jar`, and `xmlparserv2.jar` at the path `dist/lib/jdbc` must be replaced with `jars ojdbc7.jar`, `xdb6.jar`, and `xmlparserv2.jar`. These jars can be copied from the path: `./app/oracle/product/Oracle_version/dbhome/sqldeveloper/sqlc1/lib`.

**Note:** **Fix Pack 8** If you use Oracle 18c or 19c, after completion of TADDM installation, the `jars -ojdbc6.jar`, `xdb6.jar`, and `xmlparserv2.jar` at the path `dist/lib/jdbc` must be replaced with `jars ojdbc8.jar`, `xdb6.jar`, and `xmlparserv2.jar`. You can download these jars from the Oracle website, or copy from the Oracle server (not from Oracle client), from the following locations:

- `${ORACLE_HOME}/jdbc/lib/ojdbc8.jar`
- `${ORACLE_HOME}/rdbms/jlib/xdb6.jar`
- `${ORACLE_HOME}/lib/xmlparserv2.jar`

Besides `dist/lib/jdbc`, check if `ojdbc6.jar` or `ojdbc7.jar` is present at any of the following location on TADDM. If yes, remove it and then add `ojdbc8.jar` used above at the following locations on TADDM:

- `ist/apps/dap/WEB-INF/lib`
- `dist/apps/birt-viewer/WEB-INF/platform/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.1.r22x_v20070919/drivers`

Post installation, you may revert the `SQLNET.ALLOWED_LOGON_VERSION_SERVER=11` entry, if set during user creation for fresh TADDM installation, with Oracle 18c or 19c.

17. On the Database Information page, specify the TCP/IP host name or numeric IP address, listening port, database name or DB2 location name, and user information for the database.

To use an existing local installation of DB2, select **Create the database during install** unless the required TADDM database and tables already exist.

Click **Next**.

See [“Configuring the remote database server”](#) on page 50 for information about user account requirements.

18. If you want to configure the Context Menu Service and Data Integration Service during the installation process, select the **Configure Context Menu Service (CMS) / Data Integration Service (DIS)** check box.

(If you do not select this option during the installation process, you can manually configure the Context Menu Service and Data Integration Service after installing. For more information, see [“Configuring for the Context Menu Service and Data Integration Service”](#) on page 52.)

19. Optional: If you are configuring the Context Menu Service and Data Integration Service, specify the required database information.

**Note:** To avoid delays in registering configuration items in the database, install the CMS/DIS database on a server that is geographically close to the TADDM database server.

If you are using a DB2 database, follow these steps:

- a) Specify the database server, port, database name, and user information for the database.  
The database name must be different from the TADDM database name.
- b) Select **Create the database during install** unless the required database and tables already exist.  
(If you select **Create the database during install** and the database already exists, the installer deletes the existing database and creates the new one.)



**Note:** The **Create the database during install** check box is available only if the DB2 database is on the local system and the user ID running the installation process has root or administrator privileges.

Click **Next**.

If you are using an Oracle database, follow these steps:

- a) Specify the database server, port, system ID, and Oracle user information for the database.  
The Oracle user for the Context Menu Service and Data Integration Service must be different from the Oracle user for the domain server.
- b) Select **Create the user during install** unless the required user already exists.  
(If you select **Create the user during install** and the user already exists, the installer deletes the existing user and creates the new one.)

**Note:** The **Create the user during install** check box is available only if the user ID running the installation process has root or administrator privileges.

Click **Next**.

- c) If you selected the **Create the user** check box, specify the Oracle database administrator information and the Oracle home directory.  
This information is used to create the Context Menu Service and Data Integration Service Oracle user during the installation process.

Click **Next**.

20. Select the user registry option:

- To use a file-based registry, select **File-based user registry**. No additional configuration information is required for this option.
- To use a Lightweight Directory Access Protocol (LDAP) user registry, select **LDAP user registry**.
- To use a WebSphere Federated Repositories registry, select **WebSphere Federated Repositories**.

Click **Next**.

21. If you selected an LDAP user registry, additional pages prompt you for LDAP server and configuration information:

- a) Specify the LDAP server and user information. Click **Next**.
- b) Specify the LDAP configuration parameters (or accept the defaults values). Click **Next**.

22. If you selected a WebSphere Federated Repositories registry, specify the WebSphere Federated Repositories server and user information.

**Note:** User IDs and passwords are case sensitive. Make sure you use the correct case.

Click **Next**.

23. Review the pre-installation summary. After you verify that the information is correct, click **Next** to start the installation process.

24. When prompted, insert TADDM Disc 3 into the DVD drive. Specify the image directory. If you downloaded the zip files, specify the path to the zip file number 5. Click **Next**.

25. After the installation finishes, click **Done** to close the installation wizard.

This installation can be a lengthy process, depending on the number and type of components you are installing. While the installation process is running, you can monitor the progress by viewing changes to the installation log. The log also contains information that can help you troubleshoot problems that occur during installation. Log files can be found in the `installLogs` subdirectory of the installation directory..

On a supported Microsoft Windows Server, remember to turn User Account Control (UAC) on after you have finished the installation, and to restart your system. For more information on Windows Server 2012 see <http://social.technet.microsoft.com/wiki/contents/articles/13953.windows-server-2012-deactivating-uac.aspx>.

## ***Installing a secondary storage server using the installation wizard***

Follow these steps to install a secondary storage server using the installation wizard. A secondary storage server is an optional part of a streaming server deployment.

You must be logged in to an account with administrator privileges to install TADDM. Complete all prerequisite steps, including any required database configuration, before starting the installation process.

If you are installing the TADDM server on a supported Microsoft Windows Server, you must temporarily turn off User Account Control (UAC) before starting the installation process. You must restart the system each time you modify this option. For more information on Windows Server 2012 see <http://social.technet.microsoft.com/wiki/contents/articles/13953.windows-server-2012-deactivating-uac.aspx>.

The primary storage server must be installed before you can install a secondary storage server. Do not start the secondary storage server unless the server is the same version as the primary storage server. All TADDM servers in a streaming server deployment must have the same version and release.

The primary storage server must resolve the fully qualified domain name (FQDN) for each secondary storage server and discovery server. You can configure the host name resolution order for your system to use DNS resolution. Alternatively, you can edit the `/etc/hosts` file in the primary storage server. Include the IP address and host name for each discovered secondary storage server and discovery server to this file.

A storage server processes discovery data and stores it in a local or remote DB2 or Oracle database. A streaming server deployment requires at least one storage server (the primary storage server). Depending on your environment, you might also need one or more secondary storage servers. A secondary storage server automatically uses the database information specified for the primary storage server.

To install a secondary storage server using the installation wizard:

1. Insert the TADDM Disc 1 installation DVD for your supported operating system into the DVD drive. If you downloaded TADDM in the zip format, the zip files number 1 and 2 are the equivalent of Disc 1.
2. At a command prompt, go to the DVD drive, or to the directory where you saved the zip files, and run the appropriate command for your operating system:
  - For AIX operating systems, **setupAix.bin**
  - For Linux operating systems, **setupLinux.bin**
  - For Linux on System z operating systems, **setupZLinux.bin**
  - For Windows operating systems, **setupWin.bat**

**Restriction:** When you run the TADDM installation wizard `setupWin.bat` on Windows operating systems, select the **Run as administrator** option. Otherwise, the installation will fail.

**Note:** If an error message is displayed that there is insufficient disk space in the temp directory, run the installation again and specify a different temp directory. Use the option `-t temp` (for example, `setupLinux.bin -t /mytempdir`).

3. Select the language to use for your installation. Click **OK**.
4. On the Introduction page, click **Next**.
5. Read and accept the terms of the software license agreement and click **Next**.
6. Specify the location where you want to install the server.

Make sure that the path you specify contains only ASCII characters, and does not contain any spaces. Non-ASCII characters or spaces in the path can cause installation problems and problems starting the server.

After you specify the server location, click **Next**.
7. Specify the user ID you want to use to run the server.
  - On Windows operating systems, the user must belong to the Administrators group. If the user does not exist or is not part of the Administrators group, select the check box to create the user or add the user to the Administrators group. The user ID must be a local user account.
  - On Linux and UNIX operating systems, the user ID you specify must be non-root.

After you specify the server location, click **Next**.

8. On the IBM Tivoli Application Dependency Discovery Manager Deployment Option page, select **Streaming server deployment**.

Click **Next**.

9. When prompted for the type of server you want to install, select **Secondary Storage Server**.

10. On the General network connection settings page, specify the required settings. Click **Next**.

11. On the Public ports on server page, specify the required port information. Click **Next**.

12. On the Inter-server communication ports page, specify the required port information. Click **Next**.

13. On the Additional Server Information page, specify the following options:

- Server startup options.

**Note:** If the version you are installing is not the same version as the primary storage server, clear the **Start the server after installation** check box.

Click **Next**.

14. Specify the host name and port information for the primary storage server.

Also specify the primary storage server user ID and password (specify the user account you use to log in to the Discovery Management Console). The default user ID is `administrator`, and the default password is `collation`.

**Note:** The primary storage server must be already installed and running.

15. Review the pre-installation summary. After you verify that the information is correct, click **Next** to start the installation process.

16. When prompted, insert TADDM Disc 3 into the DVD drive. Specify the image directory. If you downloaded the zip files, specify the path to the zip file number 5. Click **Next**.

17. After the installation finishes, click **Done** to close the installation wizard.

This installation can be a lengthy process, depending on the number and type of components you are installing. While the installation process is running, you can monitor the progress by viewing changes to the installation log. The log also contains information that can help you troubleshoot problems that occur during installation. Log files can be found in the `installLogs` subdirectory of the installation directory.

On a supported Microsoft Windows Server, remember to turn User Account Control (UAC) on after you have finished the installation, and to restart your system. For more information on Windows Server 2012 see <http://social.technet.microsoft.com/wiki/contents/articles/13953.windows-server-2012-deactivating-uac.aspx>.

### ***Installing a discovery server using the installation wizard***

Follow these steps to install a discovery server using the installation wizard. At least one discovery server is required for a streaming server deployment.

You must be logged in to an account with administrator privileges to install TADDM. Complete all prerequisite steps, including any required database configuration, before starting the installation process.

If you are installing the TADDM server on a supported Microsoft Windows Server, you must temporarily turn off User Account Control (UAC) before starting the installation process. You must restart the system each time you modify this option. For more information on Windows Server 2012 see <http://social.technet.microsoft.com/wiki/contents/articles/13953.windows-server-2012-deactivating-uac.aspx>.

Before installing a discovery server, you must install the primary storage server. Do not start the discovery server unless the server is the same version as the primary storage server. All TADDM servers in a streaming server deployment must have the same version and release.

The primary storage server must resolve the fully qualified domain name (FQDN) for each secondary storage server and discovery server. You can configure the host name resolution order for your system to use DNS resolution. Alternatively, you can edit the `/etc/hosts` file in the primary storage server. Include the IP address and host name for each discovered secondary storage server and discovery server to this file.

A discovery runs sensors in a streaming server deployment. The number of discovery servers you need depends upon the number of items that need to be discovered. A discovery server does not have its own database; discovered data flows from the discovery server to a storage server.

To install a discovery server using the installation wizard, complete the following steps:

1. Insert the TADDM Disc 1 installation DVD for your supported operating system into the DVD drive. If you downloaded TADDM in the zip format, the zip files number 1 and 2 are the equivalent of Disc 1.
2. At a command prompt, go to the DVD drive, or to the directory where you saved the zip files, and run the appropriate command for your operating system:
  - For AIX operating systems, **setupAix.bin**
  - For Linux operating systems, **setupLinux.bin**
  - For Linux on System z operating systems, **setupZLinux.bin**
  - For Windows operating systems, **setupWin.bat**

**Restriction:** When you run the TADDM installation wizard `setupWin.bat` on Windows operating systems, select the **Run as administrator** option. Otherwise, the installation will fail.

**Note:** If an error message is displayed that there is insufficient disk space in the temp directory, run the installation again and specify a different temp directory. Use the option `-t temp` (for example, `setupLinux.bin -t /mytempdir`).

3. Select the language to use for your installation. Click **OK**.
4. On the Introduction page, click **Next**.
5. Read and accept the terms of the software license agreement and click **Next**.
6. Specify the location where you want to install the server.

Make sure the path you specify contains only ASCII characters, and does not contain any spaces. Non-ASCII characters or spaces in the path can cause installation problems and problems starting the server.

After you specify the server location, click **Next**.
7. Specify the user ID you want to use to run the server.
  - On Windows operating systems, the user must belong to the Administrators group. If the user does not exist or is not part of the Administrators group, select the check box to create the user or add the user to the Administrators group. The user ID must be a local user account.
  - On Linux and UNIX operating systems, the user ID you specify must be non-root.

After you have specified the user ID, click **Next**.

8. On the IBM Tivoli Application Dependency Discovery Manager Deployment Option page, select **Streaming server deployment**.

Click **Next**.
9. When prompted for the type of server you want to install, select **Discovery Server**.
10. On the General network connection settings page, specify the required settings. Click **Next**.
11. On the Public ports on server page, specify the required port information. Click **Next**.
12. Specify the host name and port information for the primary storage server.

Also specify the primary storage server user ID and password (specify the user account you use to log in to the Discovery Management Console). The default user ID is `administrator`, and the default password is `collation`.

**Note:** The primary storage server must be already installed and running.
13. On the Additional Server Information page, specify the following options:
  - Server startup options.

**Note:** If the version you are installing is not the same version as the primary storage server, clear the **Start the server after installation** check box.

Click **Next**.

14. Review the pre-installation summary. After you verify that the information is correct, click **Next** to start the installation process.
15. When prompted, insert TADDM Disc 3 into the DVD drive. Specify the image directory. If you downloaded the zip files, specify the path to the zip file number 5. Click **Next**.
16. After the installation finishes, click **Done** to close the installation wizard.

This installation can be a lengthy process, depending on the number and type of components you are installing. While the installation process is running, you can monitor the progress by viewing changes to the installation log. The log also contains information that can help you troubleshoot problems that occur during installation.

On Linux and UNIX systems, message log files can be found in the following directory: `install_dir/installLogs`.

On Windows systems, message log files can be found in the following directory: `install_dir\installLogs`.

On a supported Microsoft Windows Server, remember to turn User Account Control (UAC) on after you have finished the installation, and to restart your system. For more information on Windows Server 2012 see <http://social.technet.microsoft.com/wiki/contents/articles/13953.windows-server-2012-deactivating-uac.aspx>.

## Installing the TADDM server at a console

You can run the installer in console mode to install a TADDM server using an interactive text-mode interface.

To run a console mode installation of the server, complete the following steps:

1. Insert the TADDM installation DVD for your supported operating system into the CD drive.
2. Open a command prompt, navigate to the CD drive, and enter one of the following commands:
  - For AIX operating systems, **setupAix.bin -i console**
  - For Linux operating systems, **setupLinux.bin -i console**
  - For Linux on System z operating systems, **setupZLinux.bin -i console**
  - For Windows operating systems, **setupWin.bat -i console**

**Restriction:** When you run the TADDM installation wizard `setupWin.bat` on Windows operating systems, select the **Run as administrator** option. Otherwise, the installation will fail.

You might have to wait a few minutes for files to decompress before the installation process begins.

**Note:** If an error message is displayed that there is insufficient disk space in the temp directory, run the installation again and specify a different temp directory. Use the option `-t temp`, for example, `setupLinux.bin -i console -t /mytempdir`.

3. Follow the prompts in the console window to complete the installation.

The console installation process follows the same steps as the wizard installation process. For more information about the information you must specify during installation, refer to the wizard installation instructions for the server type you are installing (see [“Installing TADDM servers using the installation wizard”](#) on page 56).

This installation can be a lengthy process, depending on the number and type of components that you are installing. While the installation process is running, you can monitor the progress by viewing changes to the installation log. The log also contains information that can help you troubleshoot problems that occur during installation. Log files can be found in the `installLogs` subdirectory of the installation directory.

## Silently installing the TADDM server

You can run the installer in silent mode to install a TADDM server with no user interaction.

**Restriction:** Silent installation is not supported if firewall exists between IBM Tivoli CCMDB or IBM SmartCloud Control Desk and TADDM resources.

**Restriction:** When you run the TADDM installation wizard `setupWin.bat` on Windows operating systems, select the **Run as administrator** option. Otherwise, the installation will fail.

To run a silent installation of the server, complete the following steps:

1. Go to the server and use one of the following procedures:
  - For Linux, AIX, and Linux on System z operating systems, use either root or non-root user ID to log in.
  - For the Windows operating systems, use a Windows logon ID with Administrator authority.
2. To generate a response file, complete one of the following options.

**Important:** The response file must be saved in the UTF-8 encoding without the BOM so that the installer reads it properly. If the response file is in the UTF-8 encoding with the BOM or uses Unicode or Unicode Big Endian encoding, the installer is unable to read the file properly.

**Important:** If you are installing on a dual-stack system that supports both the IPv4 and IPv6 protocols, make sure that any numeric IP addresses you specify in the response file are IPv4 addresses.

- Run the installation wizard with the record option, ensuring that the folder that is to contain the response file already exists. As you proceed through the pages of the installation wizard, your answers are captured and the response file is generated.

When you complete the installation, the response file (for example, `install.rsp`) is available in the `tmp` directory.

When recording the response file, password information is not saved. Before installing TADDM in silent mode, you must manually edit the response file and ensure the appropriate database passwords are included.

- For Linux operating systems:

```
setupLinux.bin -r /tmp/install.rsp
```

- For AIX operating systems:

```
setupAix.bin -r /tmp/install.rsp
```

- For Linux on System z operating systems:

```
setupZLinux.bin -r /tmp/install.rsp
```

- For Windows operating systems:

```
setupWin.bat -r c:\temp\install.rsp
```

- If you do not want to generate a response file by recording input values to a response file, you can create a response file to use for the silent installation. To create a response file, run the following command for your operating system, ensuring that the folder that is to contain the response file already exists:

- For Linux operating systems:

```
setupLinux.bin -g /tmp/install.rsp
```

- For AIX operating systems:

```
setupAix.bin -g /tmp/install.rsp
```

- For Linux on System z operating systems:

```
setupZLinux.bin -g /tmp/install.rsp
```

- For Windows operating systems:

```
setupWin.bat -g c:\temp\install.rsp
```

You must edit the template response file, `install.rsp`, with the appropriate values before you can use it. The template response file includes instructions for each value.

Sample response files are provided in the `support/samples` directory.

You can use any text editor to edit the response file.

3. Run the silent installation using the response file:

- For Linux operating systems:

```
setupLinux.bin -i silent -f /tmp/install.rsp
```

- For AIX operating systems:

```
setupAix.bin -i silent -f /tmp/install.rsp
```

- For Linux on System z operating systems:

```
setupZLinux.bin -i silent -f /tmp/install.rsp
```

- For Windows operating systems:

```
setupWin.bat -i silent -f c:\temp\install.rsp
```

**Note:** If an error message is displayed that there is insufficient disk space in the temp directory, run the installation again and specify a different temp directory. Use the option `-t temp`, for example, `setupLinux.bin -i silent -f /tmp/install.rsp -t /mytempdir`.

This installation can be a lengthy process, depending on the number and type of components that you are installing. While the installation process is running, you can monitor the progress by viewing changes to the installation log. The log also contains information that can help you troubleshoot problems that occur during installation. Log files can be found in the `installLogs` subdirectory of the installation directory.

## Guidelines for installing multiple TADDM servers

Use the following guidelines to install multiple TADDM server instances on one workstation. Only the latest server is recognized as a system service.

- Specify either different listening interfaces for each instance or at least different ports for each service.
- On UNIX systems, install each instance as a different user.
- Only the latest TADDM instance can be automatically configured as a service. Configure other instances as system services manually by completing the following steps:

For UNIX:

1. As root, copy the `/etc/init.d/collation` file and rename it. The name of the file reflects the service name.
2. As root, edit the file and set the following values to match the instance that you want to configure as a system service:
  - USER
  - COLLATION\_HOME

For Windows:

1. Go to the `dist\support\jbservice` directory of a TADDM instance that you want to install as a system service.
2. Edit the `CDTService.cfg` file and set the following values to match the new service:
  - `serviceDisplayName`
  - `serviceName`
  - `description`

3. Run the following command to install the service:

```
jservice.exe -i CDTService.cfg
```

## Reinstalling primary storage server only

In some cases, for example when hardware crashes, you can reinstall the primary storage server without its discovery workers and secondary storage servers.

Several server files and properties must be the same across all servers in deployment because of the streaming deployment nature. During normal installation, the primary storage server is installed before other servers. In this case, files and properties synchronization is performed by the installer. When you reinstall the primary storage server, you must synchronize the files and properties. You can do it manually or use a method that includes conversion of servers.

**Important:** Several configuration options are present on the primary storage server only. After you reinstall the primary storage server, restore them from backup or reconfigure them.

### ***Synchronizing files and properties by converting servers***

You can reinstall the primary storage server without synchronizing files and properties manually.

To synchronize the required files and properties, complete the following steps:

1. Convert any of your secondary storage servers (server1) to the primary storage server:
  - a) Remove the following properties:

```
com.collation.PrimaryStorageServer.host  
com.collation.PrimaryStorageServer.portun
```

- b) Add the following properties:

```
com.ibm.cdb.service.SecurityManager.port  
com.ibm.cdb.service.ClientProxyServer.port  
com.ibm.cdb.service.SecureClientProxyServer.secure.portrestart server
```

2. Install a new server that you want to be the primary storage server as a secondary storage server (server2).
3. Convert the newly installed secondary storage server (server2) to the primary storage server. Use the same procedure as described in point 1.
4. Bring back original secondary storage server (server1) function by restoring the previously backed up `collation.properties` file.
5. Restart all servers in the correct order: the primary storage server before other servers.

### ***Synchronizing files and properties manually***

You can reinstall the primary storage server by synchronizing required files and properties manually.

Synchronize all necessary properties in the `collation.properties` file. You can use any of your secondary storage servers as a source and the newly installed primary storage server as a target. Otherwise, you must synchronize the files and properties from the primary storage server to all other servers in the deployment.

- Copy the following files from the source system to the target system. They overwrite any existing files on the target system.
  - `dist/etc/TADDMSec.properties`
  - `dist/etc/userdata.xml`
  - `dist/etc/ibmessclientauthncfg.properties`
  - `dist/etc/sas.client.props`
  - `dist/etc/serverkeys`
- Copy the following properties from the source system to the target system. They overwrite any existing properties on the target system.



```
com.collation.sslpassphrase
com.collation.db.password
com.collation.db.archive.password
com.ibm.cdb.DisCmsIntegration.dbPassword
com.collation.security.internal
com.collation.security.auth.VMMAdminPassword
com.collation.security.auth.ESSClientTrustPwd
```

## Verifying the TADDM server installation

After you finish installing the TADDM server, you can use the **checkinstall** script to verify the results of the installation.

This script verifies the required TADDM user IDs and passwords, as well as the connection to the domain database.

1. Go to the `$COLLATION_HOME/support/install` directory.
2. Run the **checkinstall** script for your operating system:
  - Windows systems: **checkinstall.bat**
  - Linux and UNIX systems: **checkinstall.sh**
3. Review the resulting messages to identify any problems with the installation.

The following examples show the results for a successful installation:

- TADDM 7.3.0:

```
Run-as user:taddmuser
DB User:db2admin
Archive DB User:archuser
DB type:db2
DB url:jdbc:db2://localhost:50000/cmdb

CHECKED AND PASSED:
/opt/IBM/taddm1234/dist/external/jdk [ok]
/opt/IBM/taddm1234/dist/lib [ok]
/opt/IBM/taddm1234/dist/deploy-tomcat [ok]
/opt/IBM/taddm1234/dist/etc/collation.properties [ok]
db2admin jdbc:db2://localhost:50000/cmdb [ok]
archuser jdbc:db2://localhost:50000/cmdb [ok]
taddmuser [ok]

EXCEPTIONS RAISED:

ERROR LIST:

Basic TADDM installation check: Passed
```

- TADDM 7.3.0.1, and later:

```
Run-as user:taddmuser
DB User:db2admin
Archive DB User:archuser
DB type:db2
DB url:jdbc:db2://localhost:50000/cmdb

CHECKED AND PASSED:
/opt/IBM/taddm1234/dist/external/jdk [ok]
/opt/IBM/taddm1234/dist/lib [ok]
/opt/IBM/taddm1234/dist/apps [ok]
/opt/IBM/taddm1234/dist/etc/collation.properties [ok]
db2admin jdbc:db2://localhost:50000/cmdb [ok]
archuser jdbc:db2://localhost:50000/cmdb [ok]
taddmuser [ok]

EXCEPTIONS RAISED:

ERROR LIST:

Basic TADDM installation check: Passed
```

If your installation does not pass the installation check, review the EXCEPTIONS RAISED and ERROR LIST sections to identify the problems that need to be corrected.

## Installing TADDM with secure database

Currently, TADDM does not support secure (SSL) database connections. You can install the TADDM server with configured, secure database.

1. Install the server by using a regular method, but disable the **Start server after installation** option.

**Note:** If your database is remote and already works in the SSL mode, ignore the errors that are displayed during the database connection validation.

2. Configure the secure DB2 access after installation.

**Note:** If your database is already in the SSL mode, the silent mode installation is not possible.

### Related tasks

[“Installing TADDM servers” on page 55](#)

You can use any one of several methods to install TADDM servers.

[“Configuring post-installation DB2 secure access” on page 80](#)

After you install the TADDM server, you can configure secure DB2 access.

## Post-installation configuration

---

After you complete the installation process, you must complete some configuration tasks before using TADDM.

### Configuring Oracle RAC after installation

If you use Oracle RAC as TADDM primary storage server or TADDM domain database, these steps are required to complete the database setup. TADDM installer does not directly support Oracle RAC configuration.

Complete the following steps before you install TADDM secondary storage server so that RAC configuration is automatically loaded to TADDM secondary storage server. If TADDM secondary storage server is already installed, you must configure the server the way you configure Oracle RAC in the `collation.properties` file.

1. Stop TADDM primary storage server or TADDM domain database.
2. Go to the `$COLLATION_HOME/etc/` directory and edit the `collation.properties` file. Replace the RAC node configuration, which is used for installation purpose and contains all available nodes with the new configuration as shown in the examples.

Examples:

- RAC node configuration, which is used for installation purpose.

```
#com.collation.db.url=jdbc:oracle:thin:@<node1_ip>:<node1_port>:<node1_sid>  
com.collation.db.url=jdbc:oracle:thin:@10.10.10.1:1521:RAC1
```

```
#com.collation.db.archive.url=jdbc:oracle:thin:@<node1_ip>:<node1_port>:  
<node1_sid>  
com.collation.db.archive.url=jdbc:oracle:thin:@10.10.10.1:1521:RAC1
```

- Oracle RAC configuration. In this example, two nodes are used, but the number of nodes can be increased if needed.

```
jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)  
(ADDRESS=(PROTOCOL=TCP)(HOST=node1)(PORT=1521))  
(ADDRESS=(PROTOCOL=TCP)(HOST=node2)(PORT=1521))  
(CONNECT_DATA=(SERVICE_NAME=service)))
```

The jdbc url must be formatted inline and included for both `com.collation.db.url` and `com.collation.db.archive.url`.

```
#com.collation.db.url=jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)
(ASS= (PROTOCOL=TCP) (HOST=node1_ip) (PORT=node1_port)) (ADDRESS=(PROTOCOL=TCP)
(HOST=node2_ip) (PORT=node2_port)) (CONNECT_DATA=(SERVICE_NAME=rac_service)))
com.collation.db.url=jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)
(ASS= (PROTOCOL=TCP) (HOST=10.10.10.1) (PORT=1521)) (ADDRESS=(PROTOCOL=TCP)
(HOST=10.10.10.2) (PORT=1521)) (CONNECT_DATA=(SERVICE_NAME=rac.localdomain)))
```

```
#com.collation.db.archive.url=jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)
(ASS= (PROTOCOL=TCP) (HOST=node1_ip) (PORT=node1_port)) (ADDRESS=(PROTOCOL=TCP)
(HOST=node2_ip) (PORT=node2_port)) (CONNECT_DATA=(SERVICE_NAME=rac_service)))
com.collation.db.archive.url=jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)
(ASS= (PROTOCOL=TCP) (HOST=10.10.10.1) (PORT=1521)) (ADDRESS=(PROTOCOL=TCP)
(HOST=10.10.10.2) (PORT=1521)) (CONNECT_DATA=(SERVICE_NAME=rac.localdomain)))
```

## Checking the server status

After installing TADDM, you can check the status of the server.

To verify that all services are started, complete the following steps:

1. Go to the installation directory of the TADDM server:
  - For Linux, and UNIX systems: `$COLLATION_HOME/bin`
  - For Windows systems: `%COLLATION_HOME%\bin`
2. Enter one of the following commands:
  - For Linux and UNIX systems: `./control status`
  - For Windows systems: `control status`

If TADDM is running on a domain server, the following output is displayed:

- TADDM 7.3.0:

```
Discover: Started
DbInit: Started
Tomcat: Started
Topology: Started
DiscoverAdmin: Started
Proxy: Started
EventsCore: Started

TADDM: Running
```

- TADDM 7.3.0.1, and later:

```
Discover: Started
DbInit: Started
Liberty: Started
Topology: Started
DiscoverAdmin: Started
Proxy: Started
EventsCore: Started

TADDM: Running
```

If TADDM is running on a synchronization server, the following output is displayed:

- TADDM 7.3.0:

```
DbInit: Started
Tomcat: Started
EcmdbCore: Started

TADDM: Running
```

- TADDM 7.3.0.1, and later:

```
DbInit: Started
Liberty: Started
EcmdbCore: Started

TADDM: Running
```

If TADDM is running on a storage server, the following output is displayed:

- TADDM 7.3.0:

```
DbInit: Started
Tomcat: Started
StorageService: Started

TADDM: Running
```

- TADDM 7.3.0.1, and later:

```
DbInit: Started
Liberty: Started
StorageService: Started

TADDM: Running
```

If TADDM is running on a discovery server, the following output is displayed:

- TADDM 7.3.0:

```
Discover: Started
Tomcat: Started
DiscoveryService: Started

TADDM: Running
```

- TADDM 7.3.0.1, and later:

```
Discover: Started
Liberty: Started
DiscoveryService: Started

TADDM: Running
```

## Configuring clients for secure access

You can configure TADDM client systems to use Secure Sockets Layer (SSL) connections for accessing the Discovery Management Console and the Administrator Console.

**Note:** If you have a TADDM enterprise environment which spans multiple domains requiring SSL, you cannot launch a domain Discovery Management Console that requires SSL from the Data Management Portal running on the synchronization server. To avoid this problem, do not configure SSL for domains that are leaf nodes of a synchronization server.

### Configuring secure access to the Discovery Management Console

To configure secure access to the Discovery Management Console using SSL security, you must download and record the location of the truststore on the client system.

To configure secure access to the Discovery Management Console, complete the following steps:

1. In a web browser on the client system, open the TADDM launch page by entering the hostname and port of the TADDM server.

The default URL is as follows:

```
http://hostname:9430
```

where *hostname* is the TCP/IP hostname or numeric IP address of the system where the TADDM server is installed.

2. On the TADDM launch page, click **Show SSL Options**.

3. Click **Download Trust Store**.

4. Click **Save**.

Make sure you record the location where you save the file.

5. In the text field next to **Download Trust Store**, type the path to the directory where you saved the truststore file.

Do not include the file name.

After you download the truststore, client systems can establish secure connections to the Discovery Management Console. To establish a secure session, click **Establish a secure (SSL) session** on the login window.

## Configuring secure access to the Administrator Console

You can establish a secure session with the Administrator Console by specifying an HTTPS connection.

No special configuration is required for secure access to the Administrator Console.

However, client systems should be configured to specify the HTTPS protocol and secure port when connecting to the TADDM console. The default URL for HTTPS access is as follows:

```
https://hostname:9431
```

where *hostname* is the TCP/IP hostname or numeric IP address of the system where the TADDM server is installed. Make sure any bookmarks on the client system are configured to specify HTTPS.

**Note:** On client systems, the web browser might report security warnings. These warnings can sometimes be prevented by specifying the host name as a fully qualified domain name (for example, `host.example.com`).

You can ignore warnings about the following issues when attempting to access the Administrator Console:

- The certificate issuer (localhost) is not recognized as being trusted.
- The **Issued to** field of the security certificate does not match the URL entered in the browser.

In addition, the client browser must be configured to use Transport Layer Security (TLS) 1.0. You must also follow the steps required for accepting the TADDM server security certificate. For more information, refer to the documentation for your browser.

## Clearing the Java Web Start cache

After you install the server, you might have to clear the Java Web Start cache on each client system where you log in to the Discovery Management Console.

Depending on the Java runtime environment version that you use, and the operating system from where you previously deployed the TADDM Discovery Management Console, the procedure of clearing the Java Web Start cache is different. Refer to your operating system documentation for appropriate instructions.

The following procedure is an example task that you can complete if you use IBM Java runtime environment 7.0 on Windows 2007.

1. Go to the directory where the Java runtime environment is installed.
2. Change to the `\jre\bin` directory.
3. Run the following command:

```
javaws.exe -viewer
```

4. In the **Java Cache Viewer** window, right-click the entry for IBM Tivoli Application Dependency Discovery Manager.
5. Select **Delete**.
6. Close the **Java Cache Viewer** window.

## Clearing your browser cache

After you upgrade a TADDM synchronization server from one TADDM release to another, you might have to clear your browser cache for the Data Management Portal to display correctly.

Depending on which browser you use, refer to the appropriate online help for the detailed method of clearing your browser cache.

## Configuring post-installation DB2 secure access

After you install the TADDM server, you can configure secure DB2 access.

You must complete the following steps for each server in installation, which has access to the database. Those servers are the domain server, primary storage server, secondary storage server, and enterprise server.

1. Stop the TADDM server.
2. Configure your DB2 instance to work in a secure mode. For the detailed instruction, refer to the section Configuring Secure Sockets Layer (SSL) support for a DB2 instance at [http://www-01.ibm.com/support/knowledgecenter/SSEPGG\\_10.1.0/com.ibm.db2.luw.admin.sec.doc/doc/t0025241.html](http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.1.0/com.ibm.db2.luw.admin.sec.doc/doc/t0025241.html) in DB2 documentation.
3. If the database access data that was provided during the installation is not valid, correct it in the `collation.properties` file.
  - `com.collation.db.url` - a JDBC url for the primary database.
  - `com.collation.db.user` - a user name that is used to access the primary database.
  - `com.collation.db.password` - a password that is used to access the primary database.
  - `com.collation.db.archive.url` - a JDBC url for the archive database. It is usually the same as for the primary database.
  - `com.collation.db.archive.user` - a user name that is used to access the archive database.
  - `com.collation.db.archive.password` - a password that is used to access the archive database.
4. Import DB2 certificate as trusted certificate.
  - a) Run the following command:

```
keytool -import -file db2certificate.arm -keystore taddm_db2.truststore
```

where:

**certificate.arm**

is the DB2 instance SSL certificate. You might need to provide the full path.

**taddm\_db2.truststore**

is a truststore file where the certificate is to be stored.

- b) Copy the `taddm_db2.truststore` file into the `$COLLATION_HOME/dist/etc` directory.

**Note:** The `keytool` program is available in the TADDM installation directory `$COLLATION_HOME/dist/external/jdk-Linux-x86_64/bin`. The `jdk` directory name varies depending on the operating system or architecture.

5. Set the DB connection to a secure mode for both primary and archive databases by adding the following properties in the `collation.properties` file:

```
com.ibm.cdb.db.connection.ssl.enable=true  
com.ibm.cdb.db.archive.connection.ssl.enable=true
```

6. Set the truststore file location for the DB connection for both primary and archive databases by adding the following properties in the `collation.properties` file:

```
com.ibm.cdb.db.connection.ssl.truststore.file=taddm_db2.truststore  
com.ibm.cdb.db.archive.connection.ssl.truststore.file=taddm_db2.truststore
```

**Note:** The file name is the same as in the `$COLLATION_HOME/dist/etc` directory.

7. Set the password for the truststore file for both primary and archive databases by adding the following properties in the `collation.properties` file

```
com.ibm.cdb.db.connection.ssl.truststore.password=password  
com.ibm.cdb.db.archive.connection.ssl.truststore.password=password
```

8. Run either the `encryptprops.sh` file or the `encryptprops.bat` file. The file is in the `$COLLATION_HOME/bin` directory. This script encrypts the passwords.
9. Restart the TADDM server.

## Configuring post-installation Oracle secure access

To securely access the Oracle database, you must configure each server in installation, which has access to the database. These servers are the domain server, primary storage server, secondary storage server, and synchronization server.

**Important:** In the following configuration, SSL certificates and Oracle Wallet are not allowed. Also, the configuration is enabled only for communication from the database server to a client.

Complete the following steps for the domain server, primary storage server, secondary storage server, and synchronization server.

1. Stop the TADDM server.
2. Configure your Oracle instance to work in the secure mode. For the detailed instructions, see the [Configuring Network Data Encryption](#).
3. If the database access data that you provided during the installation is invalid, correct it in the `collation.properties` file. Modify the following properties:
  - `com.collation.db.url` - a JDBC URL for the primary database.
  - `com.collation.db.user` - a user name that is used to access the primary database.
  - `com.collation.db.password` - a password that is used to access the primary database.
  - `com.collation.db.archive.url` - a JDBC URL for the archive database. It is usually the same as for the primary database.
  - `com.collation.db.archive.user` - a user name that is used to access the archive database.
  - `com.collation.db.archive.password` - a password that is used to access the archive database.
4. Start the TADDM server.

## Enabling Software License Metric Tags

---

In TADDM 7.3.0.6 and onwards, you can generate Software License Metric (SLM) tags for license usage. The following information explains the TADDM and IBM License Metric Tool integration.

### Integrating with the IBM license metric tool

IBM License Metric Tool (ILMT) is a product that identifies which software assets you have installed and their license usage. IBM License Metric Tool provides a simple way to track IBM software that you are using.

When you install TADDM, the installation enables you to generate IBM software license metric tag (`slmtag`) files. You can use versions of the SLM tool that support IBM `slmtag` format to generate license consumption reports. This topic provides you information that allows you to interpret these reports, and to configure the generation of `slmtag` files.

## SLM tags

SLM tags provide a standardized capability to report the consumption of the product license metrics (resources related to the use of a software asset). In short – it's an XML file generated by a product in runtime to self-report its license usage. An SLM tag file has a `.slmtag` file name extension.

## Understanding the TADDM Metrics

The Software License Metric helps you monitor the license usage of IBM® Tivoli Application Dependency Discovery Manager (TADDM).

It helps calculate the number of RVUs available to installed TADDM software.

Each TADDM installation instance generates or appends to an `.slmtag` file, and captures below monitored metrics:

- `APPLIANCE_INSTALL` with subtype of `NUMBER_OF_TADDM_INSTANCES`
  - This metric represents unique TADDM installation. Its value will always be 1
- `RESOURCE_VALUE_UNIT` with subtype of `NUMBER_OF_CS_SERVERS`
  - This metric represents number of "licensable" servers discovered by TADDM, i.e. count of machines which excludes virtual machines and includes AWS EC2 instances

### Fix Pack 6 Installing SLM

The software license metric tracking tool is automatically installed inside the `bin` sub-directory under TADDM root directory, (also referred to as `$COLLATION_HOME`), when TADDM software is installed or upgraded to the 7.3.0.6 FixPack release.

## Running SLM

After you install TADDM, you can execute the SLM scripts using TADDM user, `taddmusr`.

`slmTag.sh` for UNIX and UNIX-like systems or `slmTag.bat` for Windows machines present in the directory `/opt/IBM/taddm/dist/bin` is used to generate license metric tag files.

Default paths will look something like below:

```
/opt/IBM/taddm/dist/bin/slmTag.sh - on Linux  
C:\IBM\taddm\dist\bin\slmTag.bat - on Windows
```

The SLM tracking tool records and writes the license metrics to tag file (`.slmtag`). SLM tag file is located in the "slmTag" sub-directory under TADDM root directory (`$COLLATION_HOME`, e.g. `/opt/IBM/taddm/dist/`).

For using the SLM tool, some key SLM commands are:

```
[COLLATION_HOME/bin directory] ./slmTag.sh  
[taddmusr@pnc162201 bin]$ ./slmTag.sh  
Starting...  
Status: SUCCESS  
[taddmusr@pnc162201 bin]$
```

Above command generates the `.slmTag` file:

```
[COLLATION_HOME/slmTag directory]  
[taddmusr@pnc162201 slmTag]$ pwd  
/opt/IBM/taddm/dist/slmTag  
[taddmusr@pnc162201 slmTag]$  
[taddmusr@pnc162201 slmTag]$ ll  
total 4  
-rw-rw-r--. 1 taddmusr taddmusr 1052 Feb 12 10:14 d00729ab42cc5b773ff119dca5e1b247.slmtag  
[taddmusr@pnc162201 slmTag]$
```



You can check the slm logs under slmTag directory in COLLATION\_HOME/log directory

```
[COLLATION_HOME/log/slmTag/ directory]
[taddmusr@pnc162201 slmTag]$ pwd
/opt/IBM/taddm/dist/log/slmTag
[taddmusr@pnc162201 slmTag]$
[taddmusr@pnc162201 slmTag]$ ll
total 8
drwxrwxr-x. 2 taddmusr taddmusr 4096 Feb 12 10:02 20190212100206
drwxrwxr-x. 2 taddmusr taddmusr 4096 Feb 12 10:14 20190212101423
[taddmusr@pnc162201 slmTag]$
```

**Note:**

SLM tag generation scripts MUST be executed, only on the Primary Storage Server.

SLM tag file will also be generated on the PSS only.

## SLM tag file

SLM tag files provide a standardized capability for a product to report its consumption of license metrics.

Here is a sample of .slmTag file:

```
<SchemaVersion>2.1.1</SchemaVersion>
<SoftwareIdentity>
  <PersistentId>a0367022df88464680e9ad0195f95249</PersistentId>
  <Name>IBM Tivoli Application Dependency Discovery Manager</Name>
  <InstanceId>/opt/IBM/taddm</InstanceId>
</SoftwareIdentity>
<Metric logTime="2019-02-12T10:14:24+01:00">
  <Type>APPLIANCE_INSTALL</Type>
  <SubType>NUMBER_OF_TADDM_INSTANCES</SubType>
  <Value>1</Value>
  <Period>
    <StartTime>2019-02-12T10:14:24+01:00</StartTime>
    <EndTime>2019-02-12T10:14:24+01:00</EndTime>
  </Period>
</Metric>
<Metric logTime="2019-02-12T10:14:25+01:00">
  <Type>RESOURCE_VALUE_UNIT</Type>
  <SubType>NUMBER_OF_CS_SERVERS</SubType>
  <Value>10</Value>
  <Period>
    <StartTime>2019-02-12T10:14:24+01:00</StartTime>
    <EndTime>2019-02-12T10:14:25+01:00</EndTime>
  </Period>
</Metric>
```

The Value element for NUMBER\_OF\_TADDM\_INSTANCES displays the number of TADDM installation instances deployed and its value will always be one.

The Value element for NUMBER\_OF\_CS\_SERVERS displays the number of TADDM servers discovered that can be considered for licensing purposes.

The .slmTag file is located in the \$COLLATION\_HOME/slmTag directory.

A new slmTag file will always be generated on slmTag tool invocation, whenever different "persistenceId" is present in the SWID tag file.

This will usually occur, post upgrade of TADDM software to a new fix pack or release.

**Note:** Persistence Id parameter is present in the SWID tag file, which is located at below location:

```
$COLLATION_HOME/./iso-swid/ (e.g. /opt/IBM/taddm/iso-swid/)
```

## Configuring the IBM License Metric Tool log files

By default, the SLM files are stored in the directory `/opt/IBM/taddm/dist/slmTag` on UNIX and UNIX-like systems and in directory `C:\IBM\taddm\dist\slmTag` on Windows. You can configure the properties of these files.

The configuration settings are located at:

```
/opt/IBM/taddm/dist/bin/log4j_slmTag.xml
```

You can configure the following properties:

- `<param name="maxFileSize" value="{filesize}" />`  
Maximum size of a SLM tag file, before a rotation is performed. The default size is 20 MB.
- `<param name="maxBackupIndex" value="{backupIndex}" />`  
Maximum number of SLM tag archive files to keep in rotation. The default number is 5.
- `<priority value="{logLevel}" />`  
Change the logging level of `slmTag.log` files. The default log level is Debug. SLM tag log files are stored in directory `$COLLATION_HOME/log/slmTag/`.

## Upgrading TADDM

Before upgrading the IBM Tivoli Application Dependency Discovery Manager (TADDM), ensure that your environment meets the requirements for each TADDM component, including the hardware, operating system, and software prerequisites.

For more information about hardware, operating system, and software prerequisites, see [“Planning for installation”](#) on page 6.

### Note:

1. If the TADDM user upgrades the DB2 version in a TADDM installation, then compatible version of the driver should also be updated. You can ask your DBA for `db2jcc.jar` from the TADDM DB2 server, or you can download the one appropriate for your version of DB2 here: <http://www-01.ibm.com/support/docview.wss?uid=swg21363866> Once you have it, stop TADDM, copy it to the following paths, and confirm permissions are correct so that the TADDM user can read the file and then start TADDM. Repeat this step on all TADDM servers in your environment.
2. **Fix Pack 8** If the TADDM user upgrades the Oracle DB version in a TADDM installation, then compatible version of the driver must also be updated. Obtain the supported `ojdbc` jar and the related jars (as mentioned in the 'Upgrading the TADDM server' topic in the *Installing Guide*) from Oracle website or the oracle server and once you have it, stop TADDM, remove old jars and copy the obtained jars to the `dist/lib/jdbc/` and other locations where older jars are present as mentioned in above link, confirm permissions are correct so that the TADDM user can read the file and then start TADDM. Repeat this step on all TADDM servers in your environment.
  1. `/dist/lib/jdbc/db2jcc`
  2. `/dist/apps/dap/WEB-INF/lib/`
  3. `/dist/apps/birt-viewer/WEB-INF/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.1.r22x_v20070919/drivers/`
  4. `/dist/apps/birt-viewer/WEB-INF/platform/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.1.r22x_v20070919/drivers/`

**Note:** If you do not update the `db2jcc.jar` at above path, then the SSL function `gsk_secure_soc_init` might fail with the return code 402 in `sqlccSSLSocketSetup`.

**Important:** When you want to upgrade to TADDM 7.3.0, you must have TADDM 7.2.2 installed. You cannot upgrade from TADDM 7.2.1, or earlier, to TADDM 7.3.0.

During the upgrade new objects are created that results in the creation of new database tables. The size of the database can slightly increase, typically by up to 10%. The increase varies depending on the number and type of objects in the database. So, you might need to increase the size of database table spaces to ensure that there is enough free space available for a successful upgrade. Work with your database administrator to make any necessary changes during the upgrade.

Table 55 on page 85 indicates the type of deployment that you have after you upgrade, depending on your original TADDM installation.

<i>Table 55. Resulting deployment type after upgrade</i>	
<b>TADDM installation before upgrade</b>	<b>TADDM deployment type after upgrade</b>
one domain server	domain server deployment
Enterprise Domain Server and two or more domain servers	synchronization server deployment
<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. After the upgrade, any Enterprise Domain Server is a synchronization server, and domain servers are still domain servers.</li> <li>2. After the upgrade, if you have a synchronization server deployment but you want to use a streaming server deployment, you can manually convert the servers. For information about how to do this, see <i>Converting from a synchronization server deployment to a streaming server deployment</i> in the TADDM Wiki at <a href="https://github.com/TADDM/taddm-wiki/wiki">https://github.com/TADDM/taddm-wiki/wiki</a>.</li> </ol>	

## Migration tuning guidelines

Before you upgrade to a new version of TADDM, you can complete the following guidelines for better performance.

1. Do not limit the number of physical disk drives available to your database based on storage capacity alone.
2. Place the following components on separate disk drives:
  - Application data
  - Database logs
  - Database temporary space for sort and join operations

For the optimal number of disk drives, see [Table 22 on page 21](#).

3. Use the fastest disks available for your database operations and log files.
4. Enable write caching on disk volumes with the database and log files.

Enable write caching only if the cache is nonvolatile and can stand unexpected power outages and other failures. It is useful to gauge performance of a database volume by measuring the IOPS (I/Os per second) rate. Measuring the IOPS rate works best with only one database volume allocated per a physical volume. A typical Fibre Channel attached disk manages roughly 150 IOPS before it starts queuing. When a physical disk approaches the mark of 150 IOPS, you can add additional disk and database volumes to the database configuration. Operating system tools, such as `iostat` or `filemon`, can measure the IOPS rate for physical volumes. Advanced storage adapters or subsystems that use solid-state drive (SSD) technologies can improve TADDM server database performance.

The SSD devices are suited for random IOPS workloads. Some subsystems can dynamically manage the IOPS workload for better performance of the SSD devices and the physical disk drives. It is better to have many small capacity physical disks than few large capacity ones with the same rotation speed.

5. Enable asynchronous I/O at the operating system level.
6. The following DB2 settings provide good results in the lab environment for enterprise size database that consists of 10,000,000 CIs:

## DB2 9.7, and 9.8

```
db2 update dbm config using UTIL_IMPACT_LIM 95
```

```
db2 update db config using SORTHEAP 8000
db2 update db config using DBHEAP 8000
db2 update db config using APPLHEAPSZ 2000
db2 update db config using UTIL_HEAP_SZ 8000
```

Additionally, you can change the buffer pools to the following values:

```
db2 alter bufferpool IBMDEFAULTBP size 240000
db2 alter bufferpool BUF8K size 40000
db2 alter bufferpool BUF32K size 8000
```

## DB2 10.1, and later:

```
db2 update dbm cfg using UTIL_IMPACT_LIM 95
db2 update dbm cfg using SHEAPTHRES 0
```

```
db2 update db config using SORTHEAP AUTOMATIC
db2 update db config using SHEAPTHRES_SHR AUTOMATIC
db2 update db config using DBHEAP AUTOMATIC
db2 update db config using APPLHEAPSZ AUTOMATIC
db2 update db config using UTIL_HEAP_SZ AUTOMATIC
```

Additionally, you can change the buffer pools to the following values:

```
db2 alter bufferpool IBMDEFAULTBP size AUTOMATIC
db2 alter bufferpool BUF8K size AUTOMATIC
db2 alter bufferpool BUF32K size AUTOMATIC
```

## Performing prerequisite tasks

Before upgrading the TADDM server, you must complete these prerequisite tasks.

1. Ensure that the names of any existing business applications, business services, or collections (now called *groups*) do not contain single or double quotation marks.
2. Ensure that the primary and secondary database users have the authority to run the **LOAD** command in DB2. The **LOAD** command enhances the performance of DB2. The primary and secondary database users must have the following authority:
  - For DB2 LUW: DATAACCESS authority, LOAD or DBADM authority.

To grant the DBADM and LOAD authorities for the user, complete the following steps:

- a) Connect to the TADDM database with instance owner.
- b) Run the following command:

```
db2 grant dbadm, load on database to user user
```

Replace *user* with the name of your user.

3. If you use an Oracle database, ensure that the TADDM primary user and archive user have access to DBMS\_STATS and DBMS\_UTILITY. To grant the execute privilege to the TADDM primary user and archive user, run the following commands:

```
grant execute on dbms_utility to taddm user
grant execute on dbms_utility to taddm archive user
grant execute on dbms_stats to taddm user
grant execute on dbms_stats to taddm archive user
```

4. Create a backup of the database. To create a backup of a DB2 database, complete the following steps:

- a) Stop the TADDM server.
- b) Use one of the following procedures:
  - For Linux, AIX, and Linux on System z operating systems, log in as the DB2 database instance owner. For example, you could use the **db2inst1** ID.
  - For Windows operating systems, open the **DB2CMD** command prompt.
- c) Run the following command:

```
db2 backup database taddm
```

Replace *taddm* with the name of your database.

If you use an Oracle database, refer to the database software documentation for instructions about how to back up the database.

5. If you created any custom database views or triggers, drop them.  
Any views that you do not drop are automatically dropped during the migration process. If you do not drop the triggers, the upgrade process cannot complete successfully.
6. Create a backup of the \$COLLATION\_HOME directory (which includes databases).
7. On Linux operating systems, run the following command to verify that the libstdc++ compatibility package is installed:

```
rpm -a -q |grep compat-libstdc++-33
```

If this package is not installed, run the following command to install the package:

```
yum install compat-libstdc++-33
```

#### 8. **Fix Pack 6**

On Linux operating systems, ensure that the 32-bit version of the library "**libstdc++.so.6**" is present on the TADDM server.

9. If the TADDM server is running, stop the server.

Use one of the following procedures to ensure that all TADDM server Java processes are stopped:

- For Linux, AIX, and Linux on System z operating systems, complete the following steps:
  - a. Go to the \$COLLATION\_HOME/bin directory.
  - b. Enter the following command:

```
./control stop
```

- c. If all of the Java processes do not stop after entering the **./control stop** command and waiting for an appropriate amount of time for the processes to shut down, use the process ID information provided by the **ps** command to identify and stop the running Java processes that are related to TADDM:

```
ps -ef | grep java
```

- For Windows operating systems, use the Windows Task Manager to ensure that all TADDM server Java processes are stopped.
10. If you are using a DB2 database, make sure intrapartition parallelism is not enabled on the database server.

You can verify this by checking the status of the **intra\_parallel** configuration parameter at a DB2 command prompt:

```
db2 get dbm cfg | grep INTRA_PARALLEL
```

**Note:** On Linux and UNIX systems, you must be logged in as the DB2 database instance owner.

If the **intra\_parallel** parameter is set to YES, run the following command:

```
db2 update dbm cfg using INTRA_PARALLEL NO
```

If you modify the **intra\_parallel** parameter, you must then restart the DB2 server before continuing with the upgrade process.

11. The minimum values for the database log configuration parameters are as follows:

- Log file size (4KB) (LOGFILSIZ) = 4096
- Number of primary log files (LOGPRIMARY) = 12
- Number of secondary log files (LOGSECOND) = 40

Use the following commands to access the configuration parameters:

```
db2 connect to cmdb
db2 get db cfg |grep LOG
```

To set the parameters to the required values, if they are incorrect, use the following commands:

```
db2 update db cfg using LOGFILSIZ 4096
db2 update db cfg using LOGPRIMARY 12
db2 update db cfg using LOGSECOND 40
```

12. Create a complete backup of the server files.

Depending on the operating system, compress the entire directory. For Linux, AIX, and Linux on System z operating systems, you want to compress the /opt/IBM/taddm directory. For Windows operating systems, you want to compress the C:\ibm\taddm directory.

13. Optional: Save copies of any configuration files you have customized.

These files might include the following:

- \$COLLATION\_HOME/deploy-tomcat/ROOT/WEB-INF/cmdb-context.xml (for domain server)
- **Fix Pack 1** \$COLLATION\_HOME/apps/ROOT/WEB-INF/cmdb-context.xml (for domain server)
- \$COLLATION\_HOME/deploy-tomcat/ROOT/WEB-INF/ecmdb-context.xml (for synchronization server)
- **Fix Pack 1** \$COLLATION\_HOME/apps/ROOT/WEB-INF/ecmdb-context.xml (for synchronization server)
- \$COLLATION\_HOME/deploy-tomcat/ROOT/WEB-INF/storage-server-context.xml (for storage server)
- **Fix Pack 1** \$COLLATION\_HOME/apps/ROOT/WEB-INF/storage-server-context.xml (for storage server)
- \$COLLATION\_HOME/deploy-tomcat/ROOT/WEB-INF/discovery-server-context.xml (for discovery server)
- **Fix Pack 1** \$COLLATION\_HOME/apps/ROOT/WEB-INF/discovery-server-context.xml (for discovery server)
- \$COLLATION\_HOME/external/apache-tomcat\*/conf/server.xml
- **Fix Pack 1** \$COLLATION\_HOME/external/wlp/usr/servers/TADDM/server.xml
- \$COLLATION\_HOME/external/apache-tomcat\*/conf/web.xml **Fix Pack 1** In TADDM 7.3.0.1, and later, this file does not exist.
- \$COLLATION\_HOME/etc/sync/\*
- \$COLLATION\_HOME/etc/detail/screenscontent.xml
- \$COLLATION\_HOME/etc/detail/screenlayout.xml
- \$COLLATION\_HOME/etc/templates
- \$COLLATION\_HOME/osgi

- Custom BIRT reports
14. If you are using an Oracle database, make sure that the **UNDO\_RETENTION** parameter is set to an appropriate value based on the size of the database.
- Refer to the Oracle documentation for information about how to calculate the appropriate value. Also, use the following commands to adjust the **open cursors** parameter:

- Use the following command to set the **open cursors** parameter to a minimum value of 1000:

```
SQL> ALTER SYSTEM SET OPEN_CURSORS=1000 SCOPE=BOTH;
```

- Use the following command to see the current value of the parameter:

```
SQL> SHOW PARAMETER OPEN_CURSORS;
```

## Upgrading the TADDM server

Before beginning the upgrade, verify that your system is running a supported operating system and that all hardware and software requirements are met.

Depending on the type of TADDM deployment that you are using, upgrade the associated TADDM servers in the order that is described in [Table 56 on page 89](#).

Deployment type	Order in which to upgrade the associated TADDM servers
Synchronization server deployment	<ol style="list-style-type: none"> <li>1. Upgrade the synchronization server.</li> <li>2. Upgrade the domain servers. You must upgrade a domain server and all leaf nodes at the same time.</li> </ol>
Streaming server deployment	<ol style="list-style-type: none"> <li>1. Upgrade the primary storage server.</li> <li>2. After the successful upgrade of the primary storage server, upgrade the remaining TADDM servers in this order:               <ol style="list-style-type: none"> <li>a. Upgrade any secondary storage servers.</li> <li>b. Upgrade the discovery servers.</li> <li>c. Start secondary storage servers and discovery servers. By default, they are not started after the upgrade.</li> </ol> </li> </ol> <p>All TADDM servers in a streaming server deployment must be upgraded together so that they have the same version and release. Do not start the secondary storage server or the discovery server unless the server is the same version as the primary storage server.</p>

If you are installing on a dual-stack system that supports both the IPv4 and IPv6 protocols, ensure that any numeric IP addresses that you specify during the installation process are IPv4 addresses.

Upgrading the data model requires significant data processing. Depending on the size of the discovered data and your system configuration, the upgrade process might take several hours.

To upgrade a TADDM server, complete the following steps:

1. For each TADDM server that you plan to upgrade, complete the prerequisite tasks, which include stopping all TADDM servers.
2. Insert the TADDM Disc 1 installation DVD and change to the TADDM directory. If you downloaded TADDM in the zip format, the zip files number 1 and 2 are the equivalent of Disc 1.
3. Use one of the following commands to run the upgrade process:
  - For AIX operating systems, **setupAIX.bin**
  - For Linux operating systems, **setupLinux.bin**

- For Linux for System z operating systems, **setupZLinux.bin**
- For Windows operating systems, **setupWin.bat**

**Restriction:** When you run the TADDM installation wizard setupWin.bat on Windows operating systems, select the **Run as administrator** option.

In addition, you can run the upgrade process in console mode, by using the **-i console** parameter.

4. Click the **I accept both the IBM and the non-IBM terms.** check box and click **Next**.
5. When prompted to do so, type the name of the TADDM installation directory.  
The existing installation is checked to ensure that it is eligible to be upgraded.
6. Click **Next**.
7. On Windows systems, specify the user ID and password for the user account you want to use to run the TADDM server Windows service.  
The specified user must belong to the Administrators group.

Click **Next**.

8. For primary storage server and domain server, if you are using an Oracle database server, specify the path to a directory that contains the Oracle JDBC driver and two other Oracle jars that support XML operations, ojdbc6.jar, xdb6.jar, and xmlparserv2.jar. Click **Next**.

Verify that the version of all the files that you are using is the same as the version of the Oracle server.

**Important:** If you use Oracle 11.2.0.3, or 11.2.0.4, the jars must be in version 11.2.0.4. If you use Oracle 12, the jars must be in version 12. You must place the jar files in the dist/lib/jdbc directory on your TADDM server. You can download them from the Oracle website, or copy them from the Oracle server, not Oracle client, from the following locations:

- ../app/oracle/product/Oracle\_version/dbhome/jdbc/lib/ojdbc6.jar
- ../app/oracle/product/Oracle\_version/dbhome/rdbms/jlib/xdb6.jar
- ../app/oracle/product/Oracle\_version/dbhome/xdk/lib/xmlparserv2.jar on Oracle 11g, or ../app/oracle/product/Oracle\_version/dbhome/lib/xmlparserv2.jar on Oracle 12c

Oracle provides various copies of the xmlparserv2.jar file, therefore, you must copy it from the preceding location, not from another one. For more information, contact your database administrator.

**Note:** **Fix Pack 4** If you use Oracle 12 (version 12.2.0.1), after completion of TADDM installation, the jars- ojdbc6.jar, xdb6.jar, and xmlparserv2.jar at the path dist/lib/jdbc must be replaced with jars ojdbc7.jar, xdb6.jar, and xmlparserv2.jar. These jars can be copied from the path : ../app/oracle/product/Oracle\_version/dbhome/sqldeveloper/sqlc1/lib.

**Note:** **Fix Pack 8** If you use Oracle 18c or 19c, after completion of TADDM installation, the jars - ojdbc6.jar, xdb6.jar, and xmlparserv2.jar at the path dist/lib/jdbc must be replaced with jars ojdbc8.jar, xdb6.jar, and xmlparserv2.jar. You can download these jars from the Oracle website, or copy from the Oracle server (not from Oracle client), from the following locations:

- \${ORACLE\_HOME}/jdbc/lib/ojdbc8.jar
- \${ORACLE\_HOME}/rdbms/jlib/xdb6.jar
- \${ORACLE\_HOME}/lib/xmlparserv2.jar

Besides dist/lib/jdbc, check if ojdbc6.jar or ojdbc7.jar is present at any of the following location on TADDM. If yes, remove it and then add ojdbc8.jar used above at the following locations on TADDM:

- ist/apps/dap/WEB-INF/lib
- dist/apps/birt-viewer/WEB-INF/platform/plugins/org.eclipse.birt.report.data.oda.jdbc\_2.2.1.r22x\_v20070919/drivers



**Post installation, you may revert the `SQLNET.ALLOWED_LOGON_VERSION_SERVER=11` entry, if set during user creation for fresh TADDM installation, with Oracle 18c or 19c.**

9. Review the summary information and click **Install**.
10. After the upgrade process is complete, a page, indicating the status of the upgrade, is displayed. Click **Finish** to close the upgrade program.

**Important:** During installation, the TADDM server is automatically started to perform several database migration steps. If the existing database contains a large number of configuration items, this startup process can take several hours, which can cause the installer to exit with one of the following messages:

- CTJTI0203E (The GUID migration fails because the Tivoli Application Dependency Discovery Manager Server did not start within a specified time.).
- CTJTI0191E (The GUID migration fails. See the following log file: `log_file. .\n\n` After correcting the problem, run the installation process to resume the upgrade process. Contact Support if unable to resolve the error, a database restore may be required in the event a code fix is necessary.).

If you are monitoring the system, you might see that the Proxy service remains in startup mode for several hours as the view information is reprocessed.

If this happens, wait for the server startup to complete, and then restart the installer process to complete migration; the installer automatically resumes at the point where the failure occurred.

11. If the TADDM database is an Oracle database running in an enterprise environment, for all domains that were upgraded, run the **purge recyclebin** command using SQL\*Plus.
12. If you have saved backup copies of any configuration files before upgrading, merge the contents of the backup copies with the contents of the new files installed as part of the upgrade.

See "Performing prerequisite tasks" on page 86, optional step: "Save copies of any configuration files you have customized" for details about files that can have backup copies.

If an error occurs during the upgrade, correct the problem and restart the TADDM installation process. The installation process resumes the upgrade process. It is not necessary to repeat any steps that were successfully completed.

Log files are created and stored in the `installLogs` directory during the upgrade. The file names of the main log files include the number of the product version, to which you are upgrading, for example "7.2.2", or "7.3.0".

The DB upgrade log file can be found in `$COLLATION_HOME/log/migration.log` directory.

13. On each client that uses the Discovery Management Console, clear the Java Web Start cache.

To clear the Java Web Start cache, complete the following steps:

- a. Go to the `\jre\bin` subdirectory of the IBM Java SDK directory.
- b. Double-click the `javaws.exe`.
  - 1) In the **Java Application Cache Viewer** window, select **Edit > Preferences**
  - 2) In the **Java Control Panel** window, from the Temporary Internet Files section, click **Delete Files**. Select all **Delete the temporary files** check boxes and click **OK**.
  - 3) Click **OK** to exit the **Java Control Panel** window.

If experiencing problem when accessing the Data Management Portal, for example, the screen appears blank clear the browser cache.

14. If integrating TADDM with Tivoli Business Service Manager, IBM Tivoli CCMDB or IBM SmartCloud Control Desk, or any software products copy the necessary client jar files to those installations.
15. Optional: If you automatically configured the Context Menu Service and Data Integration Service as part of the installation, and you have previously made any changes to the configuration files for these services, you might need to manually apply these changes to the upgraded configuration files.

Check the previous configuration files for customized values:

- `$COLLATION_HOME/solutions/disintegration/etc/cmsdis/classtype-detailsPanel.list`
- `$COLLATION_HOME/solutions/disintegration/etc/ cmsdis/classtype-changehistory.list`

Any changes you made in these files must now be applied to the new configuration files:

- `$COLLATION_HOME/etc/cmsdis/classtype-detailsPanel.list`
- `$COLLATION_HOME/etc/cmsdis/classtype-changehistory.list`

16. Restart the server.

- If you have customized discovery profiles, compare them to the new profiles to determine whether any new sensors must be added. The upgrade process does not modify customized profiles.
- After completing and verifying the upgrade, check the TADDM support web site and install any available maintenance fixes.
- TADDM uses file-based authentication for the administrator account, even when using VMM (Virtual Member Manager) or LDAP (Lightweight Directory Access Protocol) User Registry. As part of the upgrade process, the password for the default administrator account is set to `collation`. You can change this password after restarting TADDM. If you do not change this password, you must update the configuration of any products that integrate with TADDM, such as IBM Tivoli Business Service Manager, to reflect the new password for the administrator account.
- After the upgrade completes, the user must run database statistics. For information about how to run database statistics, see the *Database maintenance* topic in the *TADDM Administrator's Guide*.
- If TADDM and IBM Tivoli Monitoring environment integration is installed on the TADDM server, you must uninstall and reinstall the IBM Tivoli Monitoring workspaces and situations for TADDM.
- If you discover Oracle database servers, you must copy necessary `.jar` files again as described in the configuring Oracle sensor section in the *Sensor Guide*.
- If you are using database views for extended attributes, recreate them by following the procedure that is described in the *Running the extended attributes view tool* topic in the *TADDM SDK Developer's Guide*.
- If you are using TADDM Cognos model, to enable capabilities of the new TADDM Cognos model, follow the procedure that is described in the *Generating the TADDM model* topic in the *TADDM Administrator's Guide*, including the "What to do next" section.
- If you are running discoveries in the asynchronous mode, configure the discovery by following procedure described in the *Configuring for asynchronous discovery* topic in the *TADDM Administrator's Guide*.

## Silently upgrading the TADDM server

If a firewall does not exist between the IBM Tivoli Change and Configuration Management Database (IBM Tivoli CCMDB) or IBM SmartCloud Control Desk and TADDM resources, you can use a response file to silently upgrade the TADDM server.

To run a silent upgrade of the server, complete the following steps:

1. Create an upgrade response file or edit the sample files, `upgrade_unix.jsp` or `upgrade_windows.jsp`, that are in the `support/samples` directory of the TADDM distribution media.

Each of them includes a list of keys and their descriptions. You can use any text editor to create and edit the response file.

2. Use one of the following commands to run the silent upgrade using the response file:

- Linux systems (not including Linux on System z):

```
setupLinux.bin -i silent -f /tmp/upgrade.jsp
```

- Linux on System z systems:

```
setupZLinux.bin -i silent -f /tmp/upgrade.rsp
```

- AIX systems:

```
setupAix.bin -i silent -f /tmp/upgrade.rsp
```

- Windows systems:

```
setupWin.bat -i silent -f c:\temp\upgrade.rsp
```

**Restriction:** When you run the TADDM installation wizard `setupWin.bat` on Windows systems, select the **Run as administrator** option.

A silent upgrade can be a lengthy process, depending on the number and type of components that you are upgrading. During the upgrade process, you can monitor the progress by viewing changes to the upgrade log.

3. To go to the directory that contains the log files, use one of the following procedures:

- For Linux, AIX, and Linux on System z Operating Systems, in a terminal window, change to the log file directory: `cd install_dir/installLogs`
- For Windows operating systems, at a command prompt, change to the log file directory: `cd install_dir\installLogs`

4. Use the **tail** command to watch messages as they are written to the logs. Use this format:

```
tail -f taddm_taddm_version_install_msg.log
```

To exit the **tail** program, press Ctrl+C.

**Important:** During installation, the TADDM server is automatically started to perform several database migration steps. If the existing database contains many configuration items, this startup process can take several hours, which can cause the installer to exit with one of the following messages:

- CTJTI0203E (The GUID migration fails because the Tivoli Application Dependency Discovery Manager Server did not start within a specified time.).
- CTJTI0191E (The GUID migration fails. See the following log file: `log_file`. `.\n\n` After correcting the problem, run the installation process to resume the upgrade process. Contact Support if unable to resolve the error, a database restore may be required in the event a code fix is necessary.).

If you are monitoring the system, you might see that the Proxy service remains in startup mode for several hours as the view information is reprocessed.

If this happens, wait for the server startup to complete, and then restart the installer process to complete migration; the installer automatically resumes at the point where the failure occurred.

5. If the TADDM database is an Oracle database that runs in an enterprise environment, for all domains that were upgraded, run the **purge recyclebin** command using SQL\*Plus.
6. Choose the appropriate method to ensure that new database schema changes take effect and are saved:
  - If the file exists, delete it. Perform a full synchronization to synchronize the new database schema changes.
  - If the file does not exist, a pop-up message is displayed when performing a full synchronization. Click **OK** to ensure that implicit relationships are not deleted.
7. If you saved backup copies of any configuration files before upgrading, merge the contents of the backup copies with the contents of the new files installed as part of the upgrade. Complete this step before starting the server.
8. Restart the server.

## Upgrading the database manually

You can upgrade the database manually if the TADDM server is at the current version, but the database is still at the previous version.

Typically, the database is automatically upgraded during the TADDM upgrade process. However, in some situations you might need to upgrade the database manually, for example, if a problem during the upgrade process caused the database upgrade to fail.

**Note:** If the TADDM user upgrades the DB2 version in a TADDM installation, then compatible version of the driver should also be updated. You can ask your DBA for `db2jcc.jar` from the TADDM DB2 server, or you can download the one appropriate for your version of DB2 here: <http://www-01.ibm.com/support/docview.wss?uid=swg21363866> Once you have it, stop TADDM, copy it to `dist/lib/jdbc/`, confirm permissions are correct so that the TADDM user can read the file and then start TADDM. Repeat this step on all TADDM servers in your environment.

**Note:** Use the following procedure only when you upgrade to TADDM 7.3 GA version. If you upgrade to a fix pack version, see the instructions in the readme file that is included in the fix pack.

To manually upgrade the database, complete the following steps:

1. If the TADDM server is running, stop the TADDM server.
2. Reorganize the database.

For a DB2 database, follow these steps:

- a) Log in as the DB2 database instance owner.
- b) Run the following command:

```
db2 reorgchk update statistics on table all > reorg.out
```

- c) In the `reorg.out` file, look in the **reorg** column for entries that are marked with a wildcard character.

The wildcard character is an asterisk (\*). For each line with a wildcard character, run the following command:

```
db2 reorg table tablename  
db2 terminate
```

If you use an Oracle database, refer to the database software documentation for instructions about how to update database statistics.

3. If you are using a DB2 database, make sure intrapartition parallelism is not enabled on the database server.

You can verify this by checking the status of the **intra\_parallel** configuration parameter at a DB2 command prompt:

```
db2 get dbm cfg | grep INTRA_PARALLEL
```

**Note:** On Linux and UNIX systems, you must be logged in as the DB2 database instance owner.

If the **intra\_parallel** parameter is set to YES, run the following command:

```
db2 update dbm cfg using INTRA_PARALLEL NO
```

If you modify the **intra\_parallel** parameter, you must then restart the DB2 server before continuing with the upgrade process.

4. If you are using a DB2 database, change the **applheapsz** configuration parameter to at least 1536. Log in as the DB2 database instance owner on the DB2 server and run the following command:

```
db2 update db cfg for cmdb using applheapsz 1536
```

5. Go to the `$COLLATION_HOME/bin` directory.
6. Run one of the following commands according to the operating system to upgrade the database:

- For Linux and UNIX systems:

```
migration.sh -s -bv 7.2.2
```

- For Windows systems:

```
migration.bat -s -bv 7.2.2
```

7. Verify that no errors occurred by checking the `$COLLATION_HOME/log/migration.log` file.

If an error occurred, fix the problem and run the appropriate migration script again.

8. Start the TADDM server.

Wait for the server to start. The server status must be running before you complete the next step.

9. Run one of the following commands according to the operating system to migrate GUID by class:

- For Linux and UNIX systems:

```
migration.sh -gc -bv 7.2.2
```

- For Windows systems:

```
migration.bat -gc -bv 7.2.2
```

10. Run one of the following commands according to the operating system to migrate GUID by ID:

- For Linux and UNIX systems:

```
migration.sh -gi
```

- For Windows systems:

```
migration.bat -gi
```

11. Verify that no errors occurred by checking the `$COLLATION_HOME/log/migration.log` file.

If an error occurred, fix the problem and run the appropriate script again.

12. For a domain server database upgrade, run one of the following commands according to the operating system to migrate templates:

- For Linux and UNIX systems:

```
migration.sh -t -bv 7.2.2
```

- For Windows systems:

```
migration.bat -t -bv 7.2.2
```

**Note:** This step is not required for synchronization server database upgrades.

13. Verify that no errors occurred by checking the `$COLLATION_HOME/log/migration.log` file.

If an error occurred, fix the problem and run the appropriate script again.

14. Upgrade the sensor configurations by completing the following steps:

a) Run one of the following commands, according to the operating system:

- For Linux and UNIX systems:

```
migration.sh -sc
```

- For Windows systems:

```
migration.bat -sc
```

b) Verify that no errors occurred by checking the `$COLLATION_HOME/log/migration.log` file. If an error occurred, fix the problem and run the appropriate script again.

15. Go to the `$COLLATION_HOME/sdk/bin` directory.

16. Run one of the following commands twice, according to the operating system, to migrate business entities:

- For Linux and UNIX systems:

```
./bizappscli.sh runPattern -mwe default
```

- For Windows systems:

```
./bizappscli.bat runPattern -mwe default
```

17. Verify that no errors occurred by checking the `$COLLATION_HOME/log/error.log` file. If an error occurred, fix the problem and run the appropriate command again.

18. Go to the `$COLLATION_HOME/bin` directory.

19. Run one of the following commands, according to the operating system, to migrate authorization configuration:

- For Linux and UNIX systems:

```
migration.sh -ac
```

- For Windows systems:

```
migration.bat -ac
```

20. Verify that no errors occurred by checking the `$COLLATION_HOME/log/migration.log` file. If an error occurred, fix the problem and run the appropriate command again.

21. Run one of the following commands, according to the operating system, to change the upgrade status to `COMPLETED`, which enables the TADDM processes to operate:

- For Linux and UNIX systems:

```
migration.sh -e
```

- For Windows systems:

```
migration.bat -e
```

## Converting a 32-bit TADDM deployment to 64-bit

Follow these steps if you want to upgrade the operating system of your TADDM server from a 32-bit edition to a 64-bit edition while preserving your existing TADDM data.

Upgrading an operating system from a 32-bit edition to a 64-bit edition typically requires a "clean" installation and reinstallation of all applications. However, if you reinstall TADDM from the product DVD, the new installation is unable to access the TADDM database from a previous installation.

To avoid this problem, you can preserve your existing TADDM directory structure and then convert it to a 64-bit deployment after upgrading your operating system.

1. Make a backup copy of the 32-bit TADDM installation directory and all of its subdirectories.

The default installation directory is as follows:

- Linux and UNIX systems: `/opt/IBM/taddm`
- Windows systems: `c:\IBM\taddm`

This directory structure includes your entire TADDM server installation.

2. Upgrade the operating system to the 64-bit edition.

If possible, preserve the existing file system during the installation.

3. If necessary, restore the 32-bit TADDM directory structure from the backup copy.

If you were able to preserve the file system during the operating system upgrade, this step is not necessary.

**Note:** On AIX, and Linux for System z systems, no further conversion is necessary. For Windows and Linux systems, continue with the next step.

4. On Linux and UNIX systems, log on as a non-root user (such as the TADDM user you specified during TADDM installation).
5. Navigate to the `$COLLATION_HOME/external/jdk` directory.
6. Extract the files in the appropriate archive to the `$COLLATION_HOME/external` directory:

- Linux and UNIX systems: `jdk-Linux-x86_64.zip`
- Windows systems: `jdk-Windows-i386-64.zip`

This step creates a new 64-bit JDK subdirectory:

- Linux and UNIX systems: `$COLLATION_HOME/external/jdk-Linux-x86_64`
- Windows systems: `%COLLATION_HOME%\external\jdk-Windows-i386-64`

7. Copy the following files to the appropriate locations:

File	Location
<code>\$COLLATION_HOME/lib/websphere/6.1/orb.properties</code>	<code>\$COLLATION_HOME/external/64bit_jdk_dir/jre/lib</code>
<code>\$COLLATION_HOME/lib/websphere/6.1/iwsorbutil.jar</code>	<code>\$COLLATION_HOME/external/64bit_jdk_dir/jre/lib/ext</code>

where `64bit_jdk_dir` is the new 64-bit JDK subdirectory created in the previous step.

## Rolling back the upgrade

The procedure for rolling back an upgrade differs depending on the operating system of the TADDM server.

### Rolling back the upgrade on a Windows system

Follow these steps to roll back a server upgrade on a Windows system.

**Note:** These instructions assume the default installation location. If you used a different location when installing and upgrading your server, substitute that path for the paths specified in this task.

To roll back a server upgrade on a Windows system, complete the following steps:

1. Stop the server.

To stop the server, make sure you are logged in with the user ID that was specified as the owner of the installation when the software was installed. Go to the `%COLLATION_HOME%\bin` directory. Enter the following command:

```
stopserver.bat
```

2. Use the Windows Task Manager to ensure that all TADDM server Java processes are stopped.
3. Restore the server files, using the backup copies you created before the upgrade:
  - a) Go to the `c:\ibm\` directory.
  - b) Rename the current installation directory to `cmdb.bak`.
  - c) Extract the backup files.

For example, use the following command: **unzip cmdb.zip**

4. Restore the database.

To restore a DB2 database, follow these steps:

- a) Log in as the DB2 database instance owner (for example, `db2inst1`).
- b) Run the following command:

```
db2 restore database cmdb
```

where *cmdb* is the name of your database.

To restore an Oracle database, refer to the database software documentation for instructions.

#### 5. Start the TADDM server.

After the rollback process is complete, you might have one or more directories with the following prefix: `_uninst`. When the directories are empty, you can delete the directories with the `_uninst` prefix. If you have more than one directory with the `_uninst` prefix, the directory with the largest number is the directory that is used for the rollback process.

## Rolling back the upgrade on a Linux or UNIX system

Follow these steps to roll back a server upgrade on a Linux or UNIX system.

**Note:** These instructions assume the default installation location. If you used a different location when installing and upgrading your server, substitute that path for the paths specified in this task.

To roll back a server upgrade on a Linux or UNIX system, complete the following steps:

#### 1. Stop the server.

To stop the server, log in with the user ID that was specified as the owner of the installation when the software was installed. Go to the `$COLLATION_HOME/bin` directory. Enter the following command:

```
./control stop
```

#### 2. If all of the Java processes do not stop after you enter the `./control stop` command and wait an appropriate amount of time for the processes to shut down, use the process ID information that is provided by the `ps` command to identify and stop the running Java processes related to TADDM:

```
ps -ef | grep java
```

#### 3. Delete the TADDM installation directory.

The default location is `/opt/IBM/taddm`.

#### 4. Restore the server files, using the backup you created before the upgrade.

- a) Go to the `/opt/IBM` directory.
- b) Rename the current installation directory to `cmdb.bak`.
- c) Extract the backup files.

For example, use the following command:

```
tar -xvf cmdb.tar
```

#### 5. Use the following command to change file ownership to non-root (run as user):

```
chown non-root_user_ID: non-root_user_group collation_home
```

For example, `chown taddmusr:taddmusr /opt/ibm/taddm/dist`

#### 6. Restore the database.

To restore a DB2 database, follow these steps:

- a) Log in as the DB2 database instance owner (for example, `db2inst1`).
- b) Run the following command:

```
db2 restore database cmdb
```

where *cmdb* is the name of your database.

To restore an Oracle database, refer to the database software documentation for instructions.

#### 7. Start the TADDM server.



# Uninstalling TADDM

---

Follow these instructions to uninstall a TADDM server or other components.

## Uninstalling a TADDM server

The uninstallation process is the same for all types of TADDM server. You can uninstall the server using the uninstallation wizard, console uninstallation, or silent uninstallation.

### Uninstalling a TADDM server in wizard or console mode

You can uninstall the TADDM server interactively using the uninstallation wizard or console mode.

**Important:** The TADDM installation program generates a unique server key for each installation. If you uninstall and reinstall TADDM, you cannot reconnect to a preexisting domain database that was encrypted for a previous TADDM installation. To ensure that you can recover from file system failures or other problems that necessitate restoring the TADDM file system, regularly back up your TADDM installation.

Before you start the uninstallation processes, back up the server.

When you run the uninstallation process from a Windows computer, use a Windows logon ID with Administrator authority.

When you run the uninstallation process from a Linux, AIX, or Linux for System z operating system, use the same type of ID, either root or non-root user ID, that you used to complete the installation process.

If you do not know what ID was used to complete the installation process, look at the owner of the `taddm` directory. This ID was used for the installation process. Use this type of ID to complete the uninstallation process.

To uninstall the server, complete the following steps:

1. Optional: If you are uninstalling a synchronization server, you must first delete the domain from the synchronization server:
  - a) Log in to the Data Management Portal running on the synchronization server using the Administrator account.
  - b) In the **Domain Summary** pane, select the domain to delete.
  - c) Click **Delete**.
  - d) When prompted, click **Yes** to confirm that you want to delete the selected domain.

**Note:** Deleting a domain can take a long time to complete.

The domain is deleted from your enterprise and removed from the Domain Summary table.

2. Close all browser windows.

3. Use one of the following procedures to stop the server:

- For Linux, AIX, and Linux on System z operating systems, run the following command:

```
$COLLATION_HOME/bin/control stop
```

- For Windows operating systems, run the following command:

```
%COLLATION_HOME%\bin\stopserver.bat
```

Before continuing, verify that all TADDM processes have stopped. You can do this by using the **ps** command on Linux and UNIX systems, or Task Manager on Windows systems.

4. Complete one of the following procedures:

- To uninstall TADDM by using uninstallation wizard on Windows operating systems, run the `uninstall.exe` file. This file is in `TADDM_install_dir\_uninstall` directory, where `TADDM_install_dir` is the directory where you installed TADDM (the default installation directory on Windows systems is `c:\ibm\taddm`).

After the uninstallation process is complete, a summary window is displayed. A message also states that the uninstallation process is complete.

- To uninstall TADDM by using console mode:
  - For Linux, AIX, and Linux on System z operating systems, run the following command:

```
TADDM_install_dir/_uninstall/uninstall -i console
```

where *TADDM\_install\_dir* is the directory where you installed TADDM (the default installation directory on Linux and UNIX systems is /opt/IBM/taddm).

- For Windows operating systems, run the following command:

```
TADDM_install_dir\_uninstall\uninstall.exe -i console
```

where *TADDM\_install\_dir* is the directory where you installed TADDM (the default installation directory on Windows systems is c:\ibm\taddm).

After the uninstallation process is complete, log files and a few additional files remain in the directory. For Windows operating systems, you might have one or more directories with the following prefix: *\_uninstall*. When the directories are empty, you can delete the directories with the *\_uninstall* prefix. If you have more than one directory with the *\_uninstall* prefix, the directory with the largest number is the directory used for the uninstallation process.

## Silently uninstalling a TADDM server

To silently uninstall a TADDM server, you must first create an uninstallation response file.

**Note:** Silent uninstallation is not supported if a firewall exists between IBM Tivoli CCMDB or IBM SmartCloud Control Desk and TADDM resources.

To run a silent uninstall of the server using a response file, complete the following steps:

1. Create an uninstall response file containing the following values, with a text editor:

**REMOVE\_ALL\_FILES=true**

Valid values are *true* or *false*.

**DROP\_DB2\_DB=true**

Valid values are *true* or *false*

**UNINSTALL\_DB2=true**

Valid values are *true* or *false*

A sample uninstall response file is provided in the *sample* folder.

- For Linux, AIX, and Linux on System z operating systems: *support/samples/*
- For Windows operating systems: *support\samples\*

2. Run one of the following uninstall commands:

- For Linux, AIX, and Linux on System z operating systems:

```
TADDM_installDir/_uninstall/uninstall -i silent -f /tmp/uninstall.rsp
```

- For Windows operating systems:

```
TADDM_installDir\_uninstall\uninstall.exe -i silent -f \tmp\uninstall.rsp
```

In the preceding examples, the uninstall response file created is named *uninstall.rsp*.

You can also run the uninstall from the command line:

- For Linux, AIX, and Linux on System z operating systems:

```
TADDM_installDir/_uninstall/uninstall -i silent DREMOVE_ALL_FILES=true  
-DDRÖP_DB2_DB=true -DUNSTALL_DB2=true
```

- For Windows operating systems:

```
TADDM_installDir\uninstall\uninstall.exe -i silent DREMOVE_ALL_FILES=true  
-DDRÖP_DB2_DB=true -DUNINSTALL_DB2=true
```

## Moving TADDM from one operating system to another

---

To move TADDM from one operating system to another, complete the following steps.

1. Make an offline backup of your current production database.
2. Restore the backup to the new database server.
3. Stop TADDM.
4. Copy the taddm directories recursively from your current primary storage server to a new primary storage server. Change all `com.collation.db.*` properties in the `collation.properties` file to match the new database (primary and secondary schema).

When you copy the taddm directories, the following limitations apply:

- TADDM is not started automatically, unless you set it up.
- BIRT reports might still point to the production database. You can find the database server name hardcoded in the `dist/deploy-tomcat/birt-viewer/WEB-INF/report` files (TADDM 7.3.0) or in the `dist/apps/birt-viewer/WEB-INF/report` (TADDM 7.3.0.1, and later). Delete the `*rptdesigncompiled` files so that TADDM recompiles them correctly with the new `collation.properties` file settings.
- The SSL certificate has the old server name, which might generate warnings if you use SSL on the UI.

### Notes:

- After you copy the taddm directories, before you start TADDM, update the `collation.properties` file to point to the new database. Search for any IP addresses or FQDNs from your TADDM server environment, by default they are not added to the `collation.properties` file, but it is possible that a customization was made.
  - When you copy TADDM from the Windows operating system to the UNIX operating systems, run the **dos2unix** command for all `*properties` files.
5. If you have any additional servers (discovery servers and secondary storage servers), copy their taddm directories to the new servers, which are a part of the same setup as the primary storage server that you copied in step 3. Change the database `com.collation.db.*` parameters in the `collation.properties` file to point to the new database. Also, change the `com.collation.PrimaryStorageServer.host` property to point to the new primary storage server.  
**Note:** When you copy TADDM from the Windows operating system to the UNIX operating systems, run the **dos2unix** command for all `*properties` files.
  6. Go to the `external/` directory, and extract the `jdk` archive that corresponds to your operating system.
  7. Start TADDM and make sure that all user interfaces are displayed correctly, that you can run discoveries, and that any other function that is critical works.

## Troubleshooting installation problems

---

This information covers common problems that occur with installing or uninstalling IBM Tivoli Application Dependency Discovery Manager (TADDM).

### TADDM simple installation fails because the database cannot be created

#### Problem

The installation of the TADDM server with the local DB2 database fails, because the database cannot be created.

## Solution

Starting with DB2 version 10, there is a limitation regarding the passwords of the DB2 users. The installer cannot connect to the newly created database if password of any of the users includes the exclamation point (!).

Ensure that none of the passwords for the DB2, which were provided during the installation, contain the exclamation point (!).

## In a test environment, you can use the TADDM installer to create a remote TADDM DB2 database using DB2 client

### Problem

If you do not have the DB2 client installed on the TADDM server when creating a remote TADDM DB2 database, you receive an error message that states that the `db2cmd.exe` file is not found.

You receive the following error message after the DB2 installation panel:

```
"db2cmd.exe" was not found.
```

### Solution

In a production environment, do not install the TADDM server and the DB2 database on the same system. Install TADDM and the DB2 database on separate systems. On the system used for the DB2 database, manually run the scripts to create the database.

In a test environment, if you use the DB2 client to create the remote TADDM DB2 database, complete the following steps:

1. Install the DB2 client. See the DB2 documentation for instructions.
2. Install the appropriate DB2 fix pack. See the DB2 documentation for instructions.
3. Catalog the database node. See the DB2 documentation for instructions.
4. Create the local DB2 instance ID. The user ID must be the same as the user ID on the DB2 server. See the DB2 documentation for instructions.
5. Create the *archuser* user ID. The user ID must be the same as the user ID on the DB2 server. See the DB2 documentation for instructions.

Alternately, in test and production environments, you can create a remote TADDM DB2 database by using a script, `make_db2_db`, provided with the TADDM installation program. It is not required that you use the script that is provided with the TADDM installation program. This script is an example of a script that can be used. If used, the script creates a properly configured database for TADDM. You can use a different script that conforms to standards for your environment.

If you use the `make_db2_db` script, the existing database or users in your DB2 database are deleted when the `make_db2_db` script runs.

1. From the product DVD, copy the following file to the system where the DB2 database is installed:
  - For Linux, AIX, and Linux on System z operating systems, `support/bin/make_db2_db.sh`
  - For Windows operating systems, `support\bin\make_db2_db.bat`
2. Use one of the following procedures to run the `make_db2_db` script on the system where the DB2 database is installed:
  - For Linux, AIX, and Linux on System z operating systems, complete these steps:
    - a. Log in as the DB2 instance owner. For example, you can use the `db2inst1` ID.
    - b. Run the following command: **`make_db2_db.sh cmdb`**
  - For Windows operating systems, complete these steps:
    - a. Open the **DB2CMD** command prompt.
    - b. Run the following command: **`make_db2_db.bat cmdb`**

The DB2 client is used only for database creation during installation. After installation, the TADDM server does not use the DB2 client.

## SUSE Linux for System z operating system has memory problem

### Problem

When uninstalling TADDM on a computer with SUSE Linux for the IBM System z operating system, SUSE Linux runs out of memory.

The computer where TADDM is installed with SUSE Linux for the System z operating system must have 4 - 8 GB of memory. This problem occurs if the computer has less than 4 GB of memory.

### Solution

Before you uninstall the TADDM server, stop the server. If you do not stop the server, the system might run out of memory during the uninstall process, which means the uninstall process never completes in an orderly way. In this case, complete the following steps:

1. Stop the uninstall process.
2. Run the following command to stop all Java processes:

```
ps -ef | grep java
```

3. Run the following command, where *pid* is the process ID that is displayed as a result of running the preceding command:

```
kill pid
```

4. Uninstall the TADDM server.

## TADDM installed on system with an Internet connection that is incorrectly configured

### Problem

The TADDM installation process was successful, but the installation process was performed on a system where the Internet connection is incorrectly configured. The discovery process does not find any configuration items.

The Internet connection is fixed and a new IP address is assigned. During this process, all users of the system must redefine their user ID and password. TADDM fails with a DBInit Fails error.

### Solution

The password for both database users (the primary and archive users) must be reset and manually tested before TADDM restarts successfully.

## TADDM installation fails on a computer that is using a remote mounted CD/DVD on System z operating system

### Problem

When you attempt to install TADDM on a computer that is using a remote mounted CD/DVD on System z operating system, the installer GUI does not appear and the installation does not start.

### Solution

1. Copy the entire TADDM install image contents of the installer DVD on System z to the local drive of the computer on which you are trying to install TADDM.
2. From the local directory where you copied the files, run the following script: `setupZLinux.bin`

## Password verification fails on the Windows system even when the user ID and password are correct

### Problem

When you attempt to install TADDM on the Windows system, the installer is unable to successfully verify your password on the Runtime User Information page of the installation wizard, even if the user ID and password are correct.

### Solution

This problem can occur on the Windows system if the name of the %temp% directory includes non-ASCII characters. Because the default %temp% directory is based on the user that is currently logged on, this can happen if your user ID includes non-ASCII characters (for example, Russian characters).

To avoid the problem, use either of the following workarounds:

- Reset the temp environment variable so that it refers to a directory whose name includes only ASCII characters. For example, use this command to use the c:\temp directory:

```
set TEMP=c:\temp
```

**Note:** Make sure that the directory you specify exists.

- Set the FORCE\_OEM\_CHARSET environment variable to specify the active code page. For example, if the active code page is 852, run the following command:

```
set FORCE_OEM_CHARSET=852
```

You can determine the active code page by running the **chcp** command.

After using either of these workarounds, run the TADDM installation wizard (**setupWin.bat**) from the same command-line session.

**Restriction:** When you run the TADDM installation wizard **setupWin.bat** on Windows operating systems, select the **Run as administrator** option. Otherwise, the installation will fail.

## TADDM installation fails on the Windows system because of missing files

### Problem

When you attempt to install TADDM on the Windows system, the installation fails, and error messages in the logs indicate that required installation files could not be found (for example, **install.vbs**).

### Solution

This problem can occur on the Windows system if the name of the %temp% directory includes non-ASCII characters. For more information, see [“Password verification fails on the Windows system even when the user ID and password are correct”](#) on page 104.

## You cannot see part of the installation wizard window

### Problem

If you are using a low screen resolution such as 640x480 pixels, you might not see part of the installation wizard window, including some of the control buttons.

### Solution

If possible, change the screen resolution to a minimum of 1024x768, and then run the installation wizard again.

If you cannot change the screen resolution, run the TADDM installation in console mode by using the **-i console** option. For more information, see [“Installing the TADDM server at a console”](#) on page 71.

## The Tivoli Netcool Performance Flow Analyzer installer fails to start

### Problem

If you run the wrong Tivoli Netcool® Performance Flow Analyzer installer binary file for your operating system, you might see a misleading message that indicates success even though the installer does

not start. For example, if you try to run the AIX binary file on a Linux system, the following message is displayed:

```
Launching installer...
./setupTNPFAAix.bin: line 2432: /tmp/install.dir.17107/Aix/resource/
jre/jre/bin/java: cannot execute binary file
./setupTNPFAAix.bin: line 2432: /tmp/install.dir.17107/Aix/resource/
jre/jre/bin/java: Success
```

### Solution

Make sure that you are running the correct installer binary file for your operating system.

## Installation fails on a Windows system because of incorrect .vbs file association

### Problem

If you try to run the TADDM installer on a Windows system where the file type association for the extension .vbs has been changed from the default value, the installation fails, and the following message is displayed in the `taddm_7.2.1_install_msg.log` file:

```
Input Error: There is no script engine for file extension ".vbs"
```

### Solution

Make sure the Windows file type association for the extension .vbs is set to Microsoft Console Based Script Host. For more information about how to set file associations, see the Microsoft Windows documentation.

## Installation fails because of an error extracting from common.zip

### Problem

Under some circumstances, the installation process on a Windows system fails, and a message in the logs indicates an error extracting files from the `common.zip` file. This message usually indicates that the file has been locked by another process.

### Solution

Restart the Windows system and run the installation process again.

## Error when running `make_ora_cms_dis` script

### Problem

Under some circumstances, the `make_ora_cms_dis` script fails while attempting to configure the database for the Context Menu Service and Data Integration Service. The following error is displayed in the log file:

```
ERROR at line 1:
ORA-01119: error in creating database file 'DISTS00.dbf'
ORA-27038: created file already exists
OSD-04010: <create> option specified, file already exists
```

### Solution

Search the database server for the following files (typically found in the `$ORACLE_HOME/database` directory):

- `DISTS00.dbf`
- `DISTS01.dbf`

Rename these files (for example, `DISTS00.dbf.old`) and then run the `make_ora_cms_dis` script again.

## Installation fails on AIX system with no "/usr/bin -> /bin" directory link

### Problem

When running the installer on an AIX system, the installation fails with the following error message:

```
-bash: ./setupAix.bin: /bin/sh: bad interpreter: No such file or directory
```

### Solution

This error occurs when the AIX system does not have a symbolic link established between files in the /bin directory and the /usr/bin directory that contains the AIX shell.

To correct the problem:

1. Navigate to the root directory.
2. Run the following command:

```
ln -s /usr/bin/ /bin
```

3. Verify the link by running the following command:

```
ls -ld /bin
```

If you see the files in the /usr/bin directory, the link is established correctly.

4. Run the installer again.

## Installation fails on remote system

### Problem

If you start the installer on a remote system by using telnet or SSH, but do not specify the -i console option. The installer attempts to use console mode installation but fails.

### Solution

When starting the installation that uses telnet or SSH, make sure that you explicitly specify console mode installation, as in the following example:

```
setupAix.bin -i console
```

## Installation cannot proceed when using a custom temporary directory in a Linux environment

### Problem

If you use a custom temporary directory to install TADDM for example, `setupLinux.bin -t /path/to/custom/tmp`, the installation might not proceed on a Linux system. An error stating that there is not insufficient space (0 bytes free) can be displayed. The installation log has additional information as shown in the following example:

```
4/8/11 3:16:58 PM : SEVERE : com.ibm.cdb.install.ia.utils.Utils  
(from runCommand(content, envs, filetype)) - null  
Caused by: java.lang.NullPointerException  
at: com.ibm.cdb.install.ia.utils.Utils.setFileExecutable(Utils.java:2472)
```

### Solution

Check the option that was used to mount the temporary directory. You cannot use the `noexec` option. This option prevents direct execution of any binary files found in the custom temporary folder. Use the `exec` option to mount the temporary directory before carrying out the installation.

## Installation cannot proceed when the default configuration cannot be applied

### Problem

There is a port conflict when installing a domain server using the installation wizard. The following error message is displayed:



```
CTJT10057E The following port is being used by another application:
port_number
```

### Solution

For a simple installation, you can return and select the advanced installation option and specify port numbers that are free. Alternatively, you can change the system configuration to ensure that the defaults ports are free and start the simple installation again.

## Installation fails because of the missing files

### Problem

When you install TADDM on Windows operating systems, the following errors occur:

- The following message is displayed on the first installation panel:

```
CTJTI0017E The following file is not found: \collation\common.zip.
```

- A message about missing files in log files is displayed shortly after running the installation.

### Solution

When you create administrator account manually on Windows operating systems, run the TADDM installation wizard `setupWin.bat` as administrator. Select the **Run as administrator** option.

## DbInit fails to start after simple installation with DB2 database

### Problem

The following error can occur usually on a system where the DB2 database was installed and then uninstalled, and later the TADDM server was installed together with the DB2 database. The `error.log` contains the following message:

```
[InitServletThread] ERROR jdo.JdoDbInit - [JdoDbInit.E.8] An error occurred,
could not
connect to the jdbc:db2://100.101.102.103:50000/TADDM:deferPrepares=false;
database.
```

### Solution

Verify the DB2 server TCP/IP communications. For instructions, see the information about configuring DB2 server communications (TCP/IP) in the DB2 information center. You must also ensure that the JDBC connection URL in the `collation.properties` file is valid. Complete the following steps:

1. Find the port number in the JDBC connection URL. Go to the `$COLLATION_HOME/etc` directory, open the `collation.properties` file and locate the `com.collation.db.url=jdbc:db2://host:port/database` property.
2. Run the following commands to see whether the port is active. The port is usually not active. Run all commands on `host`.
  - For the Linux or UNIX operating systems: `netstat -an | grep port`
  - For the Windows operating system: `netstat -an | find "port"`
3. Depending on the operating system, complete the following step:
  - a. For the Linux or UNIX operating systems, log in as the DB2 database instance owner.
  - b. For the Windows operating system, open the DB2CMD command prompt.
4. Run `db2 GET DATABASE MANAGER CONFIGURATION` command.

The `SVCENAME` entry contains service name. The same entry is placed in the services file, but when this error occurs, there is no such entry. To fix the problem, complete either of the following steps:

- In the services file, update service name for the appropriate entry.
- Update DB2 configuration by following the instructions that are located in the DB2 information center.

You can find the services file in the following directories:

- For the Linux or UNIX operating systems: `/etc/services`
- For the Windows operating system: `%SystemRoot%\system32\drivers\etc\services`

5. Run the following commands:

```
db2set DB2COMM=tcPIP
db2stop
db2start
```

6. If the last command is successful, update `com.collation.db.url` with the service port number if necessary.

7. Restart the TADDM server.

See also the *Connectivity problems* topic in the *TADDM Troubleshooting Guide*.

## Simple installation fails on a Windows system

### Problem

A TADDM installation fails when it is installed with a DB2 10 system. The following message is displayed in the `cdb_cr_db2_stdout.log` file:

```
ATTACH TO DB2 USER db2admin USING SQL1042C
An unexpected system error occurred.
SQLSTATE=58004
```

### Solution

Exit the installer and start the installation procedure again. For more information about the problem, see the following technote: <http://www.ibm.com/support/docview.wss?uid=swg21502619>.

## Troubleshooting upgrade problems

---

This information covers common problems that occur when upgrading the TADDM database.

### Schema verification failed during the upgrade

#### Problem

During a database upgrade, multiple checks are performed to verify the database. For example, the structure of each table, index, and primary key are verified. If problems are identified that cannot be automatically solved, you must manually fix the problem. Check the `$COLLATION_HOME/log/migration/TADDM-version/date-time-PrimarySchema.log` and `$COLLATION_HOME/log/migration/TADDM-version/date-time-SecondarySchema.log` files.

#### Solution

Identify the cause of the problem, check the list of messages before the Schema verification failed error occurred in the `$COLLATION_HOME/log/migration/TADDM-version/date-time-DbMessages.log` file. You must have access to the TADDM database Data Definition Language (DDL) statements. Create and run the DDL statements to correct the problem. After correcting the problem, restart the upgrade. The database is verified again before continuing with the upgrade.

The following sections describe specific problems and solutions that are identified during the upgrade verification process.

### Schema verification failed because the index is missing

#### Problem

For example, a problem of a missing index occurs when upgrading a DB2 database and TADDM on a Linux system. Check the `$COLLATION_HOME/log/migration/TADDM-version/date-time-`

DbMessages.log. Use the grep command to search the log file: `grep verify_migration date-time-DbMessages.log`. The following sample shows a missing index problem in the log file:

```
mig_verify_migration: Missing index CHANGE_HISTORY_TABLE.CH_WHEN_INDEX on columns:
+WHEN_CHANGED+HANDLED_BY_STATE_MANAGER+TYPE_OF_EVENT+ACTUAL_CHANGE_TYPE+OBJECT_ID
```

### Solution

To solve the problem, complete the following steps:

1. Enter the following commands to extract the TADDM DDL statements:

```
mkdir /tmp/TADDM_DDL
cp $COLLATION_HOME/sdk/lib/oal-topomgr.jar /tmp/TADDM_DDL/
cd /tmp/TADDM_DDL/
$COLLATION_HOME/external/jdk-Linux-i686/bin/jar xf oal-topomgr.jar db2/ oracle/
```

2. Find the DDL statement required to create the missing index:

```
grep CH_WHEN_INDEX db2/*
```

3. Connect to the database by using the correct user ID, the correct user ID is dependent on which schema verification step fails:

```
db2 connect to TADDM USER archuser USING password
```

4. Run the DDL statement found in step 2 and create the missing index:

```
db2 "CREATE INDEX CH_WHEN_INDEX ON CHANGE_HISTORY_TABLE
(WHEN_CHANGED ASC, HANDLED_BY_STATE_MANAGER ASC, TYPE_OF_EVENT ASC,
ACTUAL_CHANGE_TYPE ASC, OBJECT_ID ASC)"
```

5. Optional: If the verification process failed as a result of a problem with the primary schema, then the same problem exists in the secondary schema. You can check and correct the problem using the same approach in the secondary schema before starting the upgrade. You can also correct the problem later after a verification step fails on the secondary schema.
6. Restart the upgrade. The database is verified again before continuing with the upgrade.

## Schema verification failed because the index definition is wrong

### Problem

For example, a problem of a wrong index definition occurs when upgrading a DB2 database and TADDM on a Linux system. Check the `$COLLATION_HOME/log/migration/TADDM-version/date-time-DbMessages.log`. Use the grep command to search the log file: `grep verify_migration date-time-DbMessages.log`. The following sample shows a wrong index definition in the log file:

```
mig_verify_migration: Wrong index definition for
FCPORTJD0_ROLES_X.I_FCPORTJD1EF26330
existing: +PK__JD0IDX+PK__ROLES_X+JD0ORDERX expected: +PK__JD0IDX+JD0ORDERX
+PK__ROLES_X
```

### Solution

To solve the problem, complete the following steps:

1. Enter the following commands to extract the TADDM DDL statements:

```
mkdir /tmp/TADDM_DDL
cp $COLLATION_HOME/sdk/lib/oal-topomgr.jar /tmp/TADDM_DDL/
cd /tmp/TADDM_DDL/
$COLLATION_HOME/external/jdk-Linux-i686/bin/jar xf oal-topomgr.jar db2/ oracle/
```

2. Find the DDL statement required to create the index which contains the wrong definition:

```
grep I_FCPORTJD1EF26330 db2/*
```

3. Connect to the database by using the correct user ID, the correct user ID is dependent on which schema verification step fails:

```
db2 connect to TADDM USER archuser USING password
```

4. Drop the existing index:

```
db2 "DROP INDEX I_FCPORTJD1EF26330"
```

5. Run the DDL statement found in step 2 and create the index:

```
db2 "CREATE INDEX I_FCPORTJD1EF26330 ON FCPORTJDO_ROLES_X  
(PK__JDOIDX, JDOORDERX ASC, PK__ROLES_X ASC)"
```

6. Optional: If the verification process failed as a result of a problem with the primary schema, then the same problem exists in the secondary schema. You can check and correct the problem using the same approach in the secondary schema before starting the upgrade. You can also correct the problem later after a verification step fails on the secondary schema.
7. Restart the upgrade. The database is verified again before continuing with the upgrade.

## Schema verification failed because the index definition is wrong (mixed)

### Problem

For example, a problem of a wrong index definition (mixed) occurs when upgrading a DB2 database and TADDM on a Linux system. Check the `$COLLATION_HOME/log/migration/TADDM-version/date-time-DbMessages.log`. Use the `grep` command to search the log file: `grep verify_migration date-time-DbMessages.log`. The following sample shows a wrong index definition in the log file:

```
mig_verify_migration: Wrong index definition for HIRDBUNIT.HIRDBUNITPEA483236  
existing: +PK__DICTIONARYSERVER_X expected: +PK__PARENTHIRDBUNIT_X  
mig_verify_migration: Wrong index definition for HIRDBUNIT.HIRDBUNITDF7FAE72C  
existing: +PK__PARENTHIRDBUNIT_X expected: +PK__DICTIONARYSERVER_X
```

### Solution

To solve the problem, complete the following steps:

1. Connect to the database by using the correct user ID, the correct user ID is dependent on which schema verification step fails:

```
db2 connect to TADDM USER archuser USING password
```

2. The `PK__PARENTHIRDBUNIT_X` and `PK__DICTIONARYSERVER_X` entries are indexed but you must rename the indexes. Create and run statements to rename the indexes:

```
db2 "RENAME INDEX HIRDBUNITPEA483236 TO TEMPINDEXNAME"  
db2 "RENAME INDEX HIRDBUNITDF7FAE72C TO HIRDBUNITPEA483236"  
db2 "RENAME INDEX TEMPINDEXNAME TO HIRDBUNITDF7FAE72C"
```

3. Optional: If the verification process failed as a result of a problem with the primary schema, then the same problem exists in the secondary schema. You can check and correct the problem using the same approach in the secondary schema before starting the upgrade. You can also correct the problem later after a verification step fails on the secondary schema.
4. Restart the upgrade. The database is verified again before continuing with the upgrade.

## Schema verification failed because the primary key definition is missing or wrong

### Problem

For example, a problem with a missing or wrong primary key occurs when upgrading a DB2 database and TADDM on a Linux system. Check the `$COLLATION_HOME/log/migration/TADDM-version/date-time-DbMessages.log`. Use the `grep` command to search the log file: `grep`

verify\_migration *date-time*-DbMessages.log. The following sample shows a missing primary key in the log file:

```
mig_verify_migration: Missing primary key DISCRUN.DISCRUN_PK
mig_verify_migration: Missing column PK_X in primary key DISCRUN.DISCRUN_PK
```

## Solution

To solve the problem, complete the following steps:

1. Enter the following commands to extract the TADDM DDL statements:

```
mkdir /tmp/TADDM_DDL
cp $COLLATION_HOME/sdk/lib/oal-topomgr.jar /tmp/TADDM_DDL/
cd /tmp/TADDM_DDL/
$COLLATION_HOME/external/jdk-Linux-i686/bin/jar xf oal-topomgr.jar db2/ oracle/
```

2. Find the DDL statement required to create the primary key which contains the missing or wrong definition:

```
grep DISCRUN_PK db2/*
```

3. Connect to the database by using the correct user ID, the correct user ID is dependent on which schema verification step fails:

```
db2 connect to TADDM USER archuser USING password
```

4. Drop the existing primary key:

```
db2 "ALTER TABLE DISCRUN DROP PRIMARY KEY"
```

5. Run the DDL statement found in step 2 and create the primary key:

```
db2 "ALTER TABLE DISCRUN ADD CONSTRAINT DISCRUN_PK PRIMARY KEY (PK_X)"
```

6. Optional: If the verification process failed as a result of a problem with the primary schema, then the same problem exists in the secondary schema. You can check and correct the problem using the same approach in the secondary schema before starting the upgrade. You can also correct the problem later after a verification step fails on the secondary schema.
7. Restart the upgrade. The database is verified again before continuing with the upgrade.

## Schema verification failed because a check constraint is missing

### Problem

For example, a problem with a missing check constraint occurs when upgrading a DB2 database and TADDM on a Linux system. Check the `$COLLATION_HOME/log/migration/TADDM_version/date-time-DbMessages.log` file. Use the following **grep** command to search the log file: `grep verify_migration date-time-DbMessages.log`. The following sample shows a missing check constraint in the log file:

```
mig_verify_migration: The check constraint DELETED_X IN (1,0) does not exist on the table DOMAINS
```

### Solution

To solve the problem complete the following steps:

1. Connect to the database by using the correct user ID. The correct ID is dependent on which schema verification step fails:

```
db2 connect to TADDM USER archuser USING password
```

2. Create and run an **ALTER** statement to add the missing check constraint. The table name and check constraint definition are defined in the verification message:

```
db2 "ALTER TABLE DOMAINS ADD CHECK (DELETED_X IN (1,0))"
```

3. Restart the upgrade. The database is verified before continuing with the upgrade.

## Upgrade fails with a communication error when an sql query cannot run

### Problem

When upgrading a DB2 Version 9.7 Fix Pack 3 database and TADDM, a communication error is generated. Check the `$COLLATION_HOME/log/migration.log` file. The following message is generated:

```
CTJOT0059E The SQL procedure cannot be run: CALL "MIG_MARK_OPERATION_COMPLETED"(?, ?, ?).  
Exception: [jcc][t4][2030][11211][3.62.56] A communication error occurred  
during operations on the connection's underlying socket, socket input stream, or  
socket output stream. Error location: Reply.fill() - insufficient data (-1).  
Message: Insufficient data. ERRORCODE=-4499, SQLSTATE=08001.
```

### Solution

Upgrade the DB2 database to Version 9.7 Fix Pack 4 or later and restart the upgrade.

## Batch Element Error

### Problem

During a database schema migration from TADDM 7.2.0.x to TADDM 7.2.1 the large number of primary key violations on ALIASES table are logged to `dist/log/migration/7.2.1/<timestamp>-PrimarySchema.log`. These violations can cause batch element errors.

### Example

```
DB2 SQL Error: SQLCODE=-803, SQLSTATE=23505, SQLERRMC=1;user.ALIASES,  
DRIVER=3.62.56
```

### Solution

This error can be ignored. The error indicates that an object cannot have aliases updated nor inserted for the class. These objects are typically orphans and get deleted automatically with cleanup agents or by running `verify-data.sh` on UNIX, or `verify-data.bat` on Windows, when the migration completes

## DB2 SQL error: SQLCODE: -964, SQLSTATE: 57011, SQLERRMC: null

### Problem

During a database migration, the following error occurs:

```
DB2 SQL error: SQLCODE: -964, SQLSTATE: 57011, SQLERRMC: null
```

### Solution

This error means that the transaction log size is too small. The size of **LOGPRIMARY** must be increased.

Use the following steps to increase the size of **LOGPRIMARY**:

- Run `db2 get db cfg for dbname | grep LOGP`
- Multiply the result by at least 3.
- Run `db2 update db cfg for dbname using LOGPRIMARYnewvalue`.
- Rerun the upgrade.

## Some HyperV servers cannot be processed because of failed merges or corrupted aliases

### Problem

The GuidById migration log contains, for example, the following message:

```
-----  
Migration statistics  
-----  
34 HyperV servers were affected.  
29 Computer systems were successfully processed out of 32 total.  
1 duplicates were removed.  
1 successful merges recorded.  
1 failed merges were recorded.
```

```

2 failed naming operations were recorded.

2013-01-17 11:37:17,675 guid.HyperVGuidMigration -
-----
The migration did not merge some HyperV servers.
See documentation: Troubleshooting upgrade problems.
-----
Durable: E9A6C057CA0C32A8B34A9432D8E68481 with transient:
65CFF267CBCF39D5950868C2BAF43AAF. Reason: ERROR_INVALID_TRANSIENT_GUID.

2013-01-17 11:37:17,676 guid.HyperVGuidMigration -
-----
The migration did not process some HyperV servers with corrupted aliases.
See documentation: Troubleshooting upgrade problems.
-----
7C102E065C973808AE31E03626490FF0. Reason:
class com.ibm.tivoli.nameconciliation.common.NrsNameException.
Error code: 1004.
....

```

## Solution

### Failed merges

The HyperV server migration first detects duplicated HyperV servers that must be merged before they can be further processed. If the operation is not possible, the failed merges list is populated. Each failed merge attempt is logged and the log contains the durable object GUID, the transient object GUID, and the failure reason. If the reason is `ERROR_INVALID_DURABLE_GUID` or `ERROR_INVALID_TRANSIENT_GUID`, it means that at least one of the objects has missing or corrupted aliases.

Such objects are deleted automatically by periodic Cleanup agents, when the migration completes. After the migration, check and repair data integrity by running the `verify-data.sh` command on UNIX, or the `verify-data.bat` command on Windows. If necessary, delete the remaining objects from that list manually.

### Corrupted aliases

When the merge is successful, or not needed, the HyperV server is updated with a naming rule and a corresponding new alias. If the operation is not possible, the corrupted aliases list is populated. Each case is logged, and the log contains the HyperV server GUID and the failure reason. If the reason is `class com.ibm.tivoli.nameconciliation.common.NrsNameException`. Error code: `1002` or `1004`, the object has missing or corrupted aliases.

Such objects are deleted automatically by periodic Cleanup agents, when the upgrade completes. After the upgrade, check and repair data integrity by running the `verify-data.sh` command on UNIX, or the `verify-data.bat` command on Windows. If necessary, delete the remaining objects from that list manually.

### Identifying the successful cases

After the migration, rediscover the HyperV servers. Each successfully discovered HyperV server is updated with a new type `com.collation.platform.model.topology.app.HyperV`. The remaining HyperV servers still have the type set to `com.collation.platform.model.topology.app.AppServer`.

## Some FCPorts cannot be processed because of failed merges or corrupted aliases

### Problem

The `GuidById` migration log contains, for example, the following message:

```

-----
Migration statistics
-----
10 FCPorts were affected.
8 FCPorts were successfully processed.
1 successful merges recorded.
1 failed merges were recorded.

```

```

1 failed naming operations were recorded.

2013-11-21 09:02:47,470 guid.WwnMigration -
-----
The migration did not merge some FCPorts.
See documentation: Troubleshooting upgrade problems.
-----
Durable: 03084B4FF7493AFE9EC84C1B7E66F617 with transient:
3F6091837A233C8A8E83313D4E8D89A4. Reason: ERROR_INVALID_TRANSIENT_GUID.

2013-11-21 09:02:47,470 guid.WwnMigration -
-----
The migration did not process some FCPorts with corrupted aliases.
See documentation: Troubleshooting upgrade problems.
-----
09B1BDFCAAC23D61900433F0900EE73A. Reason:
class com.ibm.tivoli.namereconciliation.common.NrsNameException.
Error code: 1004.
....

```

## Solution

### Failed merges

Based on the worldwide name (WWN), duplicated FCPorts are detected during the FCPorts migration. To be further processed, they must be merged. If the operation is not possible, the failed merges list is populated. Each failed merge attempt is logged and the log contains the durable object GUID, the transient object GUID, and the failure reason. If the reason is `ERROR_INVALID_DURABLE_GUID` or `ERROR_INVALID_TRANSIENT_GUID`, it means that at least one of the objects has missing or corrupted aliases.

Such objects are deleted automatically by periodic Cleanup agents, when the migration completes. After the migration, check and repair data integrity by running the `verify-data.sh` command on UNIX, or the `verify-data.bat` command on Windows. If necessary, delete the remaining objects from that list manually.

### Corrupted aliases

When the merge is not needed, but an FCPort has invalid WWN, the FCPort is updated with a naming rule and a corresponding new alias. If the operation is not possible, the corrupted aliases list is populated. Each case is logged, and the log contains the FCPort GUID and the failure reason. If the reason is class `com.ibm.tivoli.namereconciliation.common.NrsNameException`. Error code: `1002` or `1004`, the object has missing or corrupted aliases.

Such objects are deleted automatically by periodic Cleanup agents, when the upgrade completes. After the upgrade, check and repair data integrity by running the `verify-data.sh` command on UNIX, or the `verify-data.bat` command on Windows. If necessary, delete the remaining objects from that list manually.

### Identifying the successful cases

After the migration, each FCPort has correctly formatted WWN. The WWN of each FCPort is uppercase and separated by a colon from one another.

## Not able to open Data Management Portal after an upgrade to version 7.3.0

### Problem

When you upgrade from previous TADDM releases to version 7.3.0, Data Management Portal does not open in the Internet Explorer or Mozilla Firefox web browsers. The "Loading" message is displayed.

### Solution

Clear the cache and restart the web browser. For detailed instructions, see ["Clearing your browser cache" on page 80](#).



## **After you upgrade to 7.3, out of memory errors occur when you run the Microsoft IIS Web server sensor**

### **Problem**

When you run the discovery by using the Microsoft IIS Web server sensor after you upgraded to TADDM 7.3, out of memory errors occur.

### **Solution**

If in TADDM 7.2.2 you set the `com.collation.discover.agent.IIsWebServiceAgent.discoverIISParameters` property to `false` in the `collation.properties` file, this is the cause of the problem. In TADDM 7.3, this property is no longer in the `collation.properties` file. Therefore, after the upgrade, its value is set to `true`.

To modify its value, open the sensor configuration in Discovery Management Portal, and search for the `discoverIISParameters`. Set the value to `false`.



## Notices

---

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan, Ltd.  
1623-14, Shimotsuruma, Yamato-shi  
Kanagawa 242-8502 Japan

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation  
224A/101  
11400 Burnet Road  
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

## Trademarks

---

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at <http://www.ibm.com/legal/copytrade.shtml>.

Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.



Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

Other company, product, and service names may be trademarks or service marks of others.



