IBM Tivoli Storage Manager
for Linux
Version 6.3.4

Installation Guide

IBM

IBM Tivoli Storage Manager
for Linux
Version 6.3.4

Installation Guide

IBM

> **Note:**
> Before using this information and the product it supports, read the information in "Notices" on page 227.

Contents

Preface

This publication contains installation and configuration instructions for the IBM®
Tivoli® Storage Manager server and client API, server languages, and other Tivoli
Storage Manager components.

Instructions for installing the Tivoli Storage Manager license, device driver, storage
agent, the IBM Tivoli Storage Manager Operations Center, the Tivoli Integrated
Portal and Administration Center, and Tivoli Monitoring for Tivoli Storage
Manager are also included in this publication.

Who should read this guide

This publication is intended for a system administrator installing and configuring a
Version 6.3 or later Tivoli Storage Manager server, the Operations Center, the
Administration Center, or Tivoli Monitoring for Tivoli Storage Manager, or
upgrading from Tivoli Storage Manager Version 6.1 or 6.2.

If you are upgrading an existing 5.5.x Tivoli Storage Manager server to Tivoli
Storage Manager Version 6.3 or later, see the *Upgrade and Migration Guide for V5
Servers*.

If you are upgrading a Tivoli Storage Manager Version 6.1 or Version 6.2 server to
a newer version, see Chapter 5, "Upgrading to Tivoli Storage Manager Version 6.3
or later," on page 77.

If you are upgrading an existing Tivoli Storage Manager Version 6.3 server to a
later level of Version 6.3, see Chapter 4, "Installing a Tivoli Storage Manager server
fix pack," on page 73.

If you are installing Tivoli Monitoring for Tivoli Storage Manager, see Chapter 9,
"Installing Tivoli Monitoring for Tivoli Storage Manager," on page 107.

If you are upgrading Tivoli Monitoring for Tivoli Storage Manager, see Chapter 10,
"Upgrading Tivoli Monitoring for Tivoli Storage Manager to Version 6.3, or later,"
on page 149.

If you are installing the Operations Center, see Part 3, "Installing the Operations
Center," on page 161.

If you are installing the Administration Center, see Chapter 19, "Installing and
configuring the Administration Center," on page 189.

If you are upgrading the Administration Center, see Chapter 21, "Upgrading the
Administration Center to Version 6.3 or later," on page 213.

Installable components

The IBM Tivoli Storage Manager server, client API, and licenses are required components. Other, optional components and products are also available in separate packages.

You can install the following components for Tivoli Storage Manager V6.3.4 or later.
- Tivoli Storage Manager server
- Tivoli Storage Manager server languages
- Tivoli Storage Manager licenses
- Tivoli Storage Manager devices
- Tivoli Storage Manager storage agent
- Tivoli Storage Manager Operations Center
- Tivoli Storage Manager Administration Center
- Tivoli Monitoring for Tivoli Storage Manager

Tivoli Monitoring for Tivoli Storage Manager must not be installed on any system that contains a Tivoli Storage Manager server instance.

Table 1 describes all the installable components. These components are in several different installation packages.

Table 1. Tivoli Storage Manager installable components

Tivoli Storage Manager component:	Description:	Additional information:
Server (required)	Includes the database, client API, GSKit, and tools to help you configure and manage Tivoli Storage Manager.	See the Tivoli Storage Manager server overview in the *Administrator's Guide*.
Language package (optional)	Each language package (one for each language) contains language-specific information for the server.	See "Installing server language packages" on page 42.
Licenses (required)	Includes support for all Tivoli Storage Manager licensed features. After you install this package, you must configure the licenses you purchased.	See the chapter on managing server operations in the *Administrator's Guide*.
Devices (optional)	Extends Tivoli Storage Manager media management capability.	The Tivoli Storage Manager device driver is preferred for use with the Tivoli Storage Manager server. See the chapter on adding devices in the *Administrator's Guide*. A list of devices supported by this driver is available from the Tivoli Storage Manager website, at http://www.ibm.com/ support/entry/portal/Overview/Software/Tivoli/ Tivoli_Storage_Manager.

Table 1. Tivoli Storage Manager installable components (continued)

Tivoli Storage Manager component:	Description:	Additional information:
Storage agent (optional)	Installs the component that allows client systems to write data directly to, or read data directly from, storage devices that are attached to a storage area network (SAN). **Remember:** The IBM Tivoli Storage Manager for Storage Area Networks is a separately licensed product.	See the *Storage Agent User's Guide*.
Operations Center (optional)	Installs the Installation Manager and Operations Center that automatically help you configure and manage Tivoli Storage Manager. Optional components such as Tivoli Common Reporting are also available. **Remember:** The Operations Center is on a separate DVD.	See Part 3, "Installing the Operations Center," on page 161.
Administration Center (optional)	Installs the following components automatically to help you configure and manage Tivoli Storage Manager: • Tivoli Integrated Portal • Integrated Solutions Console • WebSphere® Application Server • Tivoli Storage Manager client performance monitor Optional components such as Tivoli Common Reporting are also available. **Tip:** The Administration Center is on a separate DVD.	See "System requirements" on page 190.
Tivoli Monitoring for Tivoli Storage Manager (optional)	Provides reports and real time monitoring information about Tivoli Storage Manager servers and client activity. **Tip:** Tivoli Monitoring for Tivoli Storage Manager is on a separate DVD.	See Chapter 9, "Installing Tivoli Monitoring for Tivoli Storage Manager," on page 107.

Publications

Publications for the IBM Tivoli Storage Manager family of products are available online. The Tivoli Storage Manager product family includes IBM Tivoli Storage FlashCopy® Manager, IBM Tivoli Storage Manager for Space Management, IBM Tivoli Storage Manager for Databases, and several other storage management products from IBM Tivoli.

To search all publications, search across the appropriate Tivoli Storage Manager information center:

- Version 6.3 information center: http://pic.dhe.ibm.com/infocenter/tsminfo/v6r3
- Version 6.4 information center: http://pic.dhe.ibm.com/infocenter/tsminfo/v6r4

You can download PDF versions of publications from the Tivoli Storage Manager information center or from the IBM Publications Center at http://www.ibm.com/shop/publications/order/.

Go to Tivoli Documentation Central to find information centers that contain official product documentation for current and previous versions of Tivoli products, including the Tivoli Storage Manager product family. You can find Tivoli Documentation Central at http://www.ibm.com/tivoli/documentation.

You can also order some related publications from the IBM Publications Center website at http://www.ibm.com/shop/publications/order/. The website provides information about ordering publications from countries other than the United States. In the United States, you can order publications by calling 1-800-879-2755.

Tivoli Storage Manager publications

The following tables list the publications that make up the Tivoli Storage Manager library.

Table 2. Tivoli Storage Manager server publications

Publication title	Order number
IBM Tivoli Storage Manager for AIX Installation Guide	GC23-9781
IBM Tivoli Storage Manager for AIX Administrator's Guide	SC23-9769
IBM Tivoli Storage Manager for AIX Administrator's Reference	SC23-9775
IBM Tivoli Storage Manager for HP-UX Installation Guide	GC23-9782
IBM Tivoli Storage Manager for HP-UX Administrator's Guide	SC23-9770
IBM Tivoli Storage Manager for HP-UX Administrator's Reference	SC23-9776
IBM Tivoli Storage Manager for Linux Installation Guide	GC23-9783
IBM Tivoli Storage Manager for Linux Administrator's Guide	SC23-9771
IBM Tivoli Storage Manager for Linux Administrator's Reference	SC23-9777
IBM Tivoli Storage Manager for Oracle Solaris Installation Guide	GC23-9784
IBM Tivoli Storage Manager for Oracle Solaris Administrator's Guide	SC23-9772
IBM Tivoli Storage Manager for Oracle Solaris Administrator's Reference	SC23-9778
IBM Tivoli Storage Manager for Windows Installation Guide	GC23-9785
IBM Tivoli Storage Manager for Windows Administrator's Guide	SC23-9773
IBM Tivoli Storage Manager for Windows Administrator's Reference	SC23-9779

Table 2. Tivoli Storage Manager server publications (continued)

Publication title	Order number
IBM Tivoli Storage Manager for z/OS Media Installation and User's Guide	SC27-4018
IBM Tivoli Storage Manager Upgrade and Migration Guide for V5 Servers	GC27-4017
IBM Tivoli Storage Manager Integration Guide for Tivoli Storage Manager FastBack®	SC27-2828

Table 3. Tivoli Storage Manager storage agent publications

Publication title	Order number
IBM Tivoli Storage Manager for SAN for AIX Storage Agent User's Guide	SC23-9797
IBM Tivoli Storage Manager for SAN for HP-UX Storage Agent User's Guide	SC23-9798
IBM Tivoli Storage Manager for SAN for Linux Storage Agent User's Guide	SC23-9799
IBM Tivoli Storage Manager for SAN for Oracle Solaris Storage Agent User's Guide	SC23-9800
IBM Tivoli Storage Manager for SAN for Windows Storage Agent User's Guide	SC23-9553

Table 4. Tivoli Storage Manager client publications

Publication title	Order number
IBM Tivoli Storage Manager for UNIX and Linux: Backup-Archive Clients Installation and User's Guide	SC23-9791
IBM Tivoli Storage Manager for Windows: Backup-Archive Clients Installation and User's Guide	SC23-9792
IBM Tivoli Storage Manager Using the Application Programming Interface	SC23-9793
IBM Tivoli Storage Manager for Space Management for UNIX and Linux: User's Guide	SC23-9794
IBM Tivoli Storage Manager HSM for Windows Administration Guide	SC23-9795

Table 5. Tivoli Storage Manager data protection publications

Publication title	Order number
IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server Installation and User's Guide	GC27-4010
IBM Tivoli Storage Manager for Databases: Data Protection for Oracle for UNIX and Linux Installation and User's Guide	SC27-4019
IBM Tivoli Storage Manager for Databases: Data Protection for Oracle for Windows Installation and User's Guide	SC27-4020
IBM Tivoli Storage Manager for Mail: Data Protection for Microsoft Exchange Server Installation and User's Guide	GC27-4009
IBM Tivoli Storage Manager for Mail: Data Protection for Lotus Domino® UNIX and Linux Installation and User's Guide	SC27-4021
IBM Tivoli Storage Manager for Mail: Data Protection for Lotus Domino for Windows Installation and User's Guide	SC27-4022

Table 5. Tivoli Storage Manager data protection publications (continued)

Publication title	Order number
IBM Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for SAP Installation and User's Guide for DB2	SC33-6341
IBM Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for SAP Installation and User's Guide for Oracle	SC33-6340
IBM Tivoli Storage Manager for Virtual Environments Installation and User's Guide	SC27-2898
IBM Tivoli Storage Manager for Microsoft SharePoint Guide	N/A

Table 6. IBM Tivoli Storage Manager troubleshooting and tuning publications

Publication title	Order number
IBM Tivoli Storage Manager Problem Determination Guide	GC23-9789
IBM Tivoli Storage Manager Optimizing Performance	GC23-9788
IBM Tivoli Storage Manager Client Messages and Application Programming Interface Return Codes	SC27-2878
IBM Tivoli Storage Manager Server Messages and Error Codes	SC27-2877
IBM Tivoli Storage Manager for Mail: Data Protection for Microsoft Exchange Server Messages	GC27-4011
IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server Messages	GC27-4012
IBM Tivoli Storage Manager for Databases: Data Protection for Oracle Messages	SC27-4014
IBM Tivoli Storage Manager for Mail: Data Protection for Lotus Domino Messages	SC27-4015
IBM Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for SAP Messages	SC27-4016

Note: You can find information about IBM System Storage® Archive Manager at the Tivoli Storage Manager v6.3.0 information center.

Support information

You can find support information for IBM products from various sources.

Start at the IBM Support Portal: http://www.ibm.com/support/entry/portal/. You can select the products that you are interested in and search for a wide variety of relevant information.

Getting technical training

Information about Tivoli technical training courses is available online.

Go to the following websites to sign up for training, ask questions, and interact with others who use IBM storage products.

Tivoli software training and certification
> Choose from instructor led, online classroom training, self-paced Web classes, Tivoli certification preparation, and other training options at http://www.ibm.com/software/tivoli/education/

Tivoli Support Technical Exchange
> Technical experts share their knowledge and answer your questions in webcasts at http://www.ibm.com/software/sysmgmt/products/support/supp_tech_exch.html.

Storage Management community
> Interact with others who use IBM storage management products at http://www.ibm.com/developerworks/servicemanagement/sm/index.html

Global Tivoli User Community
> Share information and learn from other Tivoli users throughout the world at http://www.tivoli-ug.org/.

IBM Education Assistant
> View short "how to" recordings designed to help you use IBM software products more effectively at http://publib.boulder.ibm.com/infocenter/ieduasst/tivv1r0/index.jsp

Searching knowledge bases

If you have a problem with your Tivoli Storage Manager family product, there are several knowledge bases that you can search.

Begin by searching the Tivoli Storage Manager Information Center at http://pic.dhe.ibm.com/infocenter/tsminfo/v6r3. From this website, you can search the current Tivoli Storage Manager documentation.

Searching the Internet

If you cannot find an answer to your question in the IBM Tivoli Storage Manager information center, search the Internet for the information that might help you resolve the problem.

To search multiple Internet resources, go to the IBM support website at http://www.ibm.com/support/entry/portal/.

You can search for information without signing in. Sign in using your IBM ID and password if you want to customize the site based on your product usage and information needs. If you do not already have an IBM ID and password, click **Sign in** at the top of the page and follow the instructions to register.

From the support website, you can search various resources including:
- IBM technotes.
- IBM downloads.
- IBM Redbooks® publications.
- IBM Authorized Program Analysis Reports (APARs). Select the product and click **Downloads** to search the APAR list.

If you still cannot find a solution to the problem, you can search forums and newsgroups on the Internet for the latest information that might help you find problem resolution.

An independent user discussion list, ADSM-L, is hosted by Marist College. You can subscribe by sending an email to listserv@vm.marist.edu. The body of the message must contain the following text: SUBSCRIBE ADSM-L *your_first_name your_family_name*.

To share your experiences and learn from others in the Tivoli Storage Manager and Tivoli Storage FlashCopy Manager user communities, go to Service Management Connect (http://www.ibm.com/developerworks/servicemanagement/sm/index.html). From there you can find links to product wikis and user communities.

Using IBM Support Assistant

IBM Support Assistant is a complimentary software product that can help you with problem determination. It is available for some Tivoli Storage Manager and Tivoli Storage FlashCopy Manager products.

To learn about which products are supported, go to the IBM Support Assistant download web page at http://www.ibm.com/software/support/isa/download.html.

IBM Support Assistant helps you gather support information when you must open a problem management record (PMR), which you can then use to track the problem. The product-specific plug-in modules provide you with the following resources:

- Support links
- Education links
- Ability to submit problem management reports

You can find more information at the IBM Support Assistant website:

http://www.ibm.com/software/support/isa/

You can also install the stand-alone IBM Support Assistant application on any workstation. You can then enhance the application by installing product-specific plug-in modules for the IBM products that you use. Find add-ons for specific products at http://www.ibm.com/support/docview.wss?uid=swg27012689.

Finding product fixes

A product fix to resolve your problem might be available from the IBM software support website.

You can determine what fixes are available by checking the IBM software support website at http://www.ibm.com/support/entry/portal/.

- If you previously customized the site based on your product usage:
  1. Click the link for your product, or a component for which you want to find a fix.
  2. Click **Downloads**, and then click **Fixes by version**.
- If you have not customized the site based on your product usage, click **Downloads** and search for your product.

Receiving notification of product fixes

You can receive notifications about fixes, flashes, upgrades, and other news about IBM products.

To sign up to receive notifications about IBM products, follow these steps:

1. From the support page at http://www.ibm.com/support/entry/portal/, click **Sign in to create, manage, or view your subscriptions** in the **Notifications** pane.
2. Sign in using your IBM ID and password. If you do not have an ID and password, click **register now** and complete the registration process.
3. Click **Manage all my subscriptions** in the **Notifications** pane.
4. Click the **Subscribe** tab and then click **Tivoli**.
5. Select the products for which you want to receive notifications and click **Continue**.
6. Specify your notification preferences and click **Submit**.

Contacting IBM Software Support

You can contact IBM Software Support if you have an active IBM subscription and support contract and if you are authorized to submit problems to IBM.

To obtain help from IBM Software Support, complete the following steps:

1. Ensure that you have completed the following prerequisites:
   a. Set up a subscription and support contract.
   b. Determine the business impact of your problem.
   c. Describe your problem and gather background information.
2. Follow the instructions in "Submitting the problem to IBM Software Support" on page xvi.

Setting up a subscription and support contract

Set up a subscription and support contract. The type of contract that you need depends on the type of product you have.

For IBM distributed software products (including, but not limited to, IBM Tivoli, Lotus®, and Rational® products, as well as IBM DB2® and IBM WebSphere products that run on Microsoft Windows or on operating systems such as AIX or Linux), enroll in IBM Passport Advantage® in one of the following ways:

- **Online:** Go to the Passport Advantage website at http://www.ibm.com/software/lotus/passportadvantage/, click **How to enroll**, and follow the instructions.
- **By telephone:** You can call 1-800-IBMSERV (1-800-426-7378) in the United States. For the telephone number to call in your country, go to the IBM Software Support Handbook web page at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html and click **Contacts**.

Determining the business impact

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you must understand and assess the business impact of the problem you are reporting.

Severity 1	**Critical** business impact: You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.
Severity 2	**Significant** business impact: The program is usable but is severely limited.
Severity 3	**Some** business impact: The program is usable with less significant features (not critical to operations) unavailable.
Severity 4	**Minimal** business impact: The problem causes little impact on operations, or a reasonable circumvention to the problem has been implemented.

Describing the problem and gathering background information

When explaining a problem to IBM, it is helpful to be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently.

To save time, know the answers to these questions:

* What software versions were you running when the problem occurred?
* Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
* Can the problem be re-created? If so, what steps led to the failure?
* Have any changes been made to the system? For example, hardware, operating system, networking software, and so on.
* Are you using a workaround for this problem? If so, be prepared to explain it when you report the problem.

Submitting the problem to IBM Software Support

You can submit the problem to IBM Software Support online or by telephone.

Online

> Go to the IBM Software Support website at http://www.ibm.com/support/entry/portal/Open_service_request/Software/Software_support_(general). Sign in to access IBM Service Requests and enter your information into the problem submission tool.

By telephone

> For the telephone number to call in your country, go to the IBM Software Support Handbook at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html and click **Contacts**.

New for Tivoli Storage Manager Version 6.3.4

This section summarizes changes that have been made to IBM Tivoli Storage Manager Version 6.3.4. These changes affect the Tivoli Storage Manager server, the Operations Center, the Administration Center, Tivoli Monitoring for Tivoli Storage Manager, and the upgrade to Version 6.3 or later. Any updates that have been made to the information since the previous edition are marked with a vertical bar (|) in the margin.

The following installation-related features are new for Tivoli Storage Manager in Version 6.3.4. For a complete list of new Version 6.3.4 features, see the "What's new in the products" topic in the Tivoli Storage Manager information center at http://pic.dhe.ibm.com/infocenter/tsminfo/v6r3.

End user license agreement (EULA)
> The license agreement no longer needs to be accepted for the Administration Center and for the Tivoli Monitoring for Tivoli Storage Manager feature. The Tivoli Storage Manager Version 6.3 or later server installation wizard now has a separate license agreement for the following products:
> - Tivoli Storage Manager
> - Tivoli Storage Manager Extended Edition
> - System Storage Archive Manager
> - Tivoli Storage Manager for Storage Area Networks

Tivoli Storage Manager migration to V6.3.4 or later on Linux x86_64
> You can now migrate a Tivoli Storage Manager V5 server that runs on an AIX®, HP-UX, or Solaris operating system to V6.3.4 or later on a Linux x86_64 operating system. Depending on your hardware and software environment, this migration procedure might be useful for achieving server consolidation, load balancing, or standardization on the Linux operating system. For more information about the advantages of migrating the server, see the server database updates overview section in the *Upgrade and Migration Guide for V5 Servers*.

Operations Center V6.4.1 user interface
> The V6.4.1 Operations Center includes an Overview page that shows the interaction of Tivoli Storage Manager servers and clients. You can use the Operations Center to identify potential issues at a glance, manage alerts, and access the Tivoli Storage Manager command line. The Administration Center interface is also available, but the Operations Center is the preferred monitoring interface. For more information about the Operations Center, see Part 3, "Installing the Operations Center," on page 161.

Tivoli Storage Manager V6.4 code levels
> Tivoli Storage Manager Version 6.4 is made up of the following components and code levels:
> - Backup-archive client at V6.4
> - Application programming interface (API) at V6.4
> - Server at V6.3.4, including Administration Center, Tivoli Monitoring for Tivoli Storage Manager, and device driver components, also at V6.3.4
> - Operations Center at V6.4.1

Part 1. Installing and upgrading the server

Install and upgrade the Tivoli Storage Manager server.

Planning to install	➡	Installing components	➡	Taking the first steps
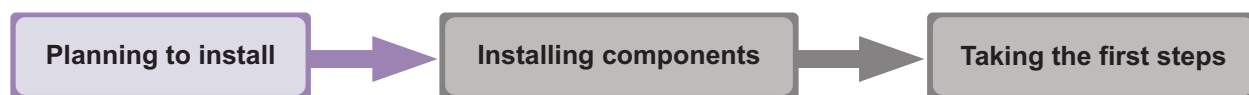
Figure 1. As highlighted in the figure, you are in the planning to install the Tivoli Storage Manager server section. Review this section carefully to ensure that you have the system and other requirements needed to install Tivoli Storage Manager.

Chapter 1. Planning to install the Tivoli Storage Manager server

Install the Tivoli Storage Manager server software on the computer that manages storage devices and install the Tivoli Storage Manager client software on every workstation that transfers data to Tivoli Storage Manager server-managed storage.

Tivoli Storage Manager server maintenance releases, client software, and publications are available from the Tivoli Storage Manager website at http://www.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Storage_Manager.

Allow approximately 30 - 45 minutes to install a Tivoli Storage Manager Version 6.3 or later server, using this guide.

An upgrade from V6.1.x, V6.2.x, or V6.3.x to V6.3 or later takes approximately 20 - 50 minutes. Your environment might produce different results than that obtained in the labs.

The following figure illustrates the main parts for installing a new Tivoli Storage Manager server.
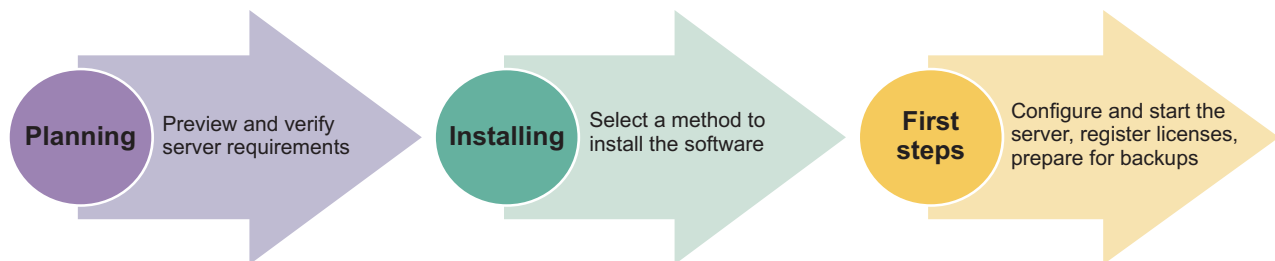
What you should know first

Before installing IBM Tivoli Storage Manager, be familiar with your operating systems, storage devices, communication protocols, and system configurations.

The following figure illustrates an overview of the installation, upgrade, and migration process.

Installing the Tivoli Storage Manager server

I want to...

Install a new release	Install a fix pack update	Upgrade or migrate an existing version
Plan for the installation	Download the code from FTP	Plan the upgrade or migration
Choose an installation method	Install the code	Choose an upgrade or migration method
Complete post-installation tasks		Complete the upgrade or migration process

Optional

- Install Tivoli Monitoring for Tivoli Storage Manager
- Install the Operations Center
- Install the Administration Center

Begin backing up data

Figure 2. Installation, upgrade, migration overview

Table 7. Upgrade information

To upgrade from this version	To this version	See this information
V6.3 or later	V6.3 or later	Chapter 4, "Installing a Tivoli Storage Manager server fix pack," on page 73
V6.2	V6.3 or later	"Upgrading from Tivoli Storage Manager V6.2 to V6.3 or later" on page 78

Table 7. Upgrade information (continued)

To upgrade from this version	To this version	See this information
V6.1	V6.3 or later	"Upgrading from Tivoli Storage Manager V6.1 to V6.3 or later" on page 83
V5.5	V6.3 or later	*Upgrade and Migration Guide for V5 Servers*

If you are migrating a Tivoli Storage Manager server, see the following documentation:

- V5 server on a z/OS® operating system to V6.3 or later on an AIX or Linux on System z® operating system, see the *Upgrade and Migration Guide for V5 Servers*
- V5 server on an AIX, HP-UX, or Solaris operating system to V6.3.4 or later on a Linux x86_64 operating system, see the *Upgrade and Migration Guide for V5 Servers*.

Restriction: You can install and run the Version 6.3 or later server on a system that already has DB2 installed on it, whether DB2 was installed independently or as part of some other application, with some restrictions. For details, see "Compatibility of the Tivoli Storage Manager server with other DB2 products on the system" on page 13.

Experienced DB2 administrators can choose to perform advanced SQL queries and use DB2 tools to monitor the database. Do not, however, use DB2 tools to change DB2 configuration settings from those that are preset by Tivoli Storage Manager, or alter the DB2 environment for Tivoli Storage Manager in other ways, such as with other products. The Tivoli Storage Manager Version 6.3 or later server has been built and tested extensively using the data definition language (DDL) and database configuration that Tivoli Storage Manager deploys.

Attention: Do not alter the DB2 software that is installed with Tivoli Storage Manager installation packages and fix packs. Do not install or upgrade to a different version, release, or fix pack of DB2 software because doing so can damage the database.

System requirements

To install Tivoli Storage Manager server on a Linux system, it is necessary to have a minimum level of hardware and software, including a communication method and the most current device driver.

These tables list the minimum hardware and software requirements for the installation of a Tivoli Storage Manager server. Use these requirements as a starting point. You can use the prerequisite checker to verify most of the requirements. See "Running the installation prerequisite checker" on page 12. You can find the most current information about system requirements at Tivoli Storage Manager Supported Operating Systems.

See *Tivoli Storage Manager Optimizing Performance* for server configuration guidelines and best practices.

The Tivoli Storage Manager device driver package does not contain a device driver for this operating system because a SCSI generic device driver is used. Configure

the device driver before using the Tivoli Storage Manager server with tape devices. The Tivoli Storage Manager driver package contains driver tools and ACSLS daemons. You can locate IBM driver packages at the Fix Central website.

Requirements, supported devices, client installation packages, and fixes are available at the Tivoli Storage Manager website. After you have installed Tivoli Storage Manager and before you customize it for your use, go to this website and download and apply any applicable fixes: http://www.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Storage_Manager.

Linux X86_64 server requirements

The Tivoli Storage Manager server on Linux X86_64 has hardware and software requirements.

Hardware requirements

Table 8 describes the minimum hardware requirements that are needed for your Tivoli Storage Manager server. For more details about planning disk space, see "Capacity planning" on page 15.

Table 8. Hardware requirements

Type of hardware	Hardware requirements
Hardware	An AMD64 or Intel EMT-64 processor
Disk space	The following minimum values for disk space: • 5 MB for the /var directory • 30 MB for the /opt directory if you create mount points • 2 GB for the /opt/tivoli/tsm directory • 390 MB for the /tmp directory • 300 MB for the /usr directory • 2 GB in the home directory **Tip:** Expect to use more space for problem determination. Significant additional disk space is required for database and log files. The size of the database depends on the number of client files to be stored and the method by which the server manages them. The default active log space is 16 GB, the minimum that is needed for most workloads and configurations. Allocate at least three times the active log space for the archive log (48 GB). Ensure that you have sufficient resources if you are using data deduplication or expect a heavy client workload. For optimal performance and to facilitate I/O, specify at least two equally sized containers or Logical Unit Numbers (LUNs) for the database. See *Optimizing Performance* for more information about the configuration of directories for the database. In addition, each active log and archive log should have its own container or LUN. Ensure that you see the capacity planning section for more details about disk space.

Table 8. Hardware requirements (continued)

Type of hardware	Hardware requirements
Memory	• 12 GB. • 16 GB if you are using data deduplication. • At least 32 GB for heavily used servers. Using 32 GB or more of memory enhances performance of the Tivoli Storage Manager server database inventory. • If you plan to run multiple instances, each instance requires the memory listed for one server. Multiply the memory for one server by the number of instances planned for the system. • Node replication processing requires additional memory. Use a minimum of 32 GB of memory for node replication without data deduplication. Node replication with data deduplication requires a minimum of 64 GB of memory.

Software requirements

Table 9 describes the minimum software requirements that are needed for your system.

Table 9. Software requirements

Type of software	Minimum software requirements
Operating system	The Tivoli Storage Manager server on Linux x86_64 requires one of the following operating systems: • Red Hat Enterprise Linux 5, Update 3 or later • Red Hat Enterprise Linux 6 • SUSE Linux Enterprise Server 10, Service Pack 2 or later • SUSE Linux Enterprise Server 11
Libraries	GNU C libraries, Version 2.3.3-98.38 or later that is installed on the Tivoli Storage Manager system. For Red Hat Enterprise Linux and SUSE Linux Enterprise Servers: • libaio.so.1 (32 and 64 bit packages are required) • libstdc++.so.5 (32 and 64 bit packages are required) • libstdc++.so.6 (32 and 64 bit packages are required)
Communication protocol	• TCP/IP Version 4 or Version 6, which is standard with Linux • Shared memory protocol (with Tivoli Storage Manager Version 6.3 or later Linux x86_64 client)
Processing	Asynchronous I/O must be enabled. On Linux kernels at 2.6 or later, install the libaio library to enable Asynchronous I/O.
Web browser	A web browser to retrieve an online installation package. The following browsers are supported: • Microsoft Internet Explorer 7.0 or later • Firefox 3.5 or later Your browser must support the server code page. If your browser does not support the server code page, the windows might be unreadable. If your browser meets these requirements but does not correctly display a Tivoli Storage Manager web-based interface, consider using a different browser.

Table 9. Software requirements (continued)

Type of software	Minimum software requirements
Other software	Korn Shell (ksh)

Linux on System z server requirements

The Tivoli Storage Manager server for Linux on System z has hardware and software requirements.

Hardware requirements

Table 10 describes the minimum hardware requirements that are needed for your Tivoli Storage Manager server. For more details about planning disk space, see "Capacity planning" on page 15.

Table 10. Hardware requirements

Type of hardware	Hardware requirements
Hardware	An IBM zSeries®, IBM System z9®, IBM System z10®, or IBM zEnterprise® System (z114 and z196) 64-bit native logical partition (LPAR) or z/VM® guest.
Disk space	The following minimum values for disk space: • 5 MB for the /var directory • 30 MB for the /opt directory if you create mount points • 2 GB for the /opt/tivoli/tsm directory • 390 MB for the /tmp directory • 300 MB for the /usr directory • 2 GB in the home directory **Tip:** Expect to use more space for problem determination. Significant additional disk space is required for database and log files. The size of the database depends on the number of client files to be stored and the method by which the server manages them. The default active log space is 16 GB, the minimum that is needed for most workloads and configurations. Allocate at least three times the active log space for the archive log (48 GB). Ensure that you have sufficient resources if you are using data deduplication or expect a heavy client workload. For optimal performance and to facilitate I/O, specify at least two equally sized containers or Logical Unit Numbers (LUNs) for the database. See *Optimizing Performance* for more information about the configuration of directories for the database. In addition, each active log and archive log should have its own container or LUN. Ensure that you see the capacity planning section for more details about disk space.

Table 10. Hardware requirements (continued)

Type of hardware	Hardware requirements
Memory	• 12 GB. • 16 GB if you are using data deduplication. • At least 32 GB for heavily used servers. Using 32 GB or more of memory enhances performance of the Tivoli Storage Manager server database inventory. • If you plan to run multiple instances, each instance requires the memory listed for one server. Multiply the memory for one server by the number of instances planned for the system. • Node replication processing requires additional memory. Use a minimum of 32 GB of memory for node replication without data deduplication. Node replication with data deduplication requires a minimum of 64 GB of memory.

Software requirements

Table 11 describes the minimum software requirements that are needed for your system.

Table 11. Software requirements

Type of software	Minimum software requirements
Operating system	The Tivoli Storage Manager server on Linux on System z (s390x 64-bit architecture) requires one of the following operating systems: • Red Hat Enterprise Linux 5, Update 3 or later • Red Hat Enterprise Linux 6 • SUSE Linux Enterprise Server 10, Service Pack 2 or later • SUSE Linux Enterprise Server 11
Library	GNU C library, Version 2.4-31.43.6 is installed on the Tivoli Storage Manager system. For Red Hat Enterprise Linux and SUSE Linux Enterprise Servers: • libaio.so.1 (32 and 64 bit packages are required) • libstdc++.so.5 (32 and 64 bit packages are required) • libstdc++.so.6 (32 and 64 bit packages are required)
Communication protocol	• TCP/IP Version 4 or Version 6, which is standard with Linux • Shared memory protocol (with Tivoli Storage Manager Version 6.3 or later Linux on System z client)
Processing	Asynchronous I/O must be enabled. On Linux kernels at 2.6 or later, install the libaio library to enable Asynchronous I/O.
Web browser	A web browser to retrieve an online installation package. The following browsers are supported: • Microsoft Internet Explorer 7.0 or later • Firefox 3.5 or later Your browser must support the server code page. If your browser does not support the server code page, the windows might be unreadable. If your browser meets these requirements but does not correctly display a Tivoli Storage Manager web-based interface, consider using a different browser.

Table 11. Software requirements (continued)

Type of software	Minimum software requirements
Other software	Korn Shell (ksh)

Linux on Power Systems server requirements

The Tivoli Storage Manager server on a Linux on Power Systems™ server requires a minimum amount of hardware, disk space, memory, and software.

Hardware requirements

Table 12 describes the minimum hardware requirements that are needed for your Tivoli Storage Manager server. For more details about planning disk space, see "Capacity planning" on page 15.

Table 12. Hardware requirements

Type of hardware	Hardware requirements
Hardware	A Linux on Power Systems server on an IBM system, such as one listed in the following website: http://www.ibm.com/systems/power/software/linux/about/index.html
Disk space	The following minimum disk space: • 5 MB for the /var directory • 30 MB for the /opt directory if you create mount points • 2 GB for the /opt/tivoli/tsm directory • 390 MB for the /tmp directory • 300 MB for the /usr directory • 2 GB in the home directory **Tip:** Expect to use more space for problem determination. Significant additional disk space is required for database and log files. The size of the database depends on the number of client files to be stored and the method by which the server manages them. The default active log space is 16 GB, the minimum that is needed for most workloads and configurations. Allocate at least three times the active log space for the archive log (48 GB). Ensure that you have sufficient resources if you are using data deduplication or expect a heavy client workload. For optimal performance and to facilitate I/O, specify at least two equally sized containers or Logical Unit Numbers (LUNs) for the database. See *Optimizing Performance* for more information about the configuration of directories for the database. In addition, each active log and archive log should have its own container or LUN. Ensure that you see the capacity planning section for more details about disk space.

Table 12. Hardware requirements (continued)

Type of hardware	Hardware requirements
Memory	- 12 GB. - 16 GB if you are using data deduplication. - At least 32 GB for heavily used servers. Using 32 GB or more of memory enhances performance of the Tivoli Storage Manager server database inventory. - If you plan to run multiple instances, each instance requires the memory listed for one server. Multiply the memory for one server by the number of instances planned for the system. - Node replication processing requires additional memory. Use a minimum of 32 GB of memory for node replication without data deduplication. Node replication with data deduplication requires a minimum of 64 GB of memory.

Software requirements

Table 13 describes the minimum software requirements that are needed for your system.

Table 13. Software requirements

Type of software	Minimum software requirements
Operating system	The Tivoli Storage Manager server on Linux on Power (ppc64 architecture) requires one of the following operating systems: - Red Hat Enterprise Linux 5, Update 3 or later - Red Hat Enterprise Linux 6 - SUSE Linux Enterprise Server 10, Service Pack 2 or later - SUSE Linux Enterprise Server 11 And the following, additional requirement: - Minimum C++ runtime level with the xlC 8.0.0.0 To download the XL C++ runtime, go to this website: http://www.ibm.com/software/awdtools/xlcpp/. For more details about this system requirement, you can check the following website: http://www.ibm.com/software/data/db2/9/sysreqs.html.
Libraries	GNU C libraries, Version 2.4-31.30 and later. libaio.so.1 for Red Hat Enterprise Linux and SUSE Linux Enterprise Servers (32 and 64 bit packages are required). If you are running SUSE Linux Enterprise Server 11, download the XL C/C++ runtime package V10.1. See the following link for instructions: http://www.ibm.com/support/docview.wss?uid=swg24022673.
Communication protocol	- TCP/IP Version 4 or Version 6, which is standard with Linux - Shared memory protocol (with Tivoli Storage Manager Version 6.3 or later System p® client)
Processing	Asynchronous I/O must be enabled. On Linux kernels at 2.6 or later, install the libaio library to enable Asynchronous I/O.

Table 13. Software requirements (continued)

Type of software	Minimum software requirements
Web browser	A web browser to retrieve an online installation package. The following browsers are supported: • Microsoft Internet Explorer 7.0 or later • Firefox 3.5 or later Your browser must support the server code page. If your browser does not support the server code page, the windows might be unreadable. If your browser meets these requirements but does not correctly display a Tivoli Storage Manager web-based interface, consider using a different browser.
Other software	Korn Shell (ksh)

Remember: Raw logical volumes are not supported.

Running the installation prerequisite checker

The installation prerequisite checker is an optional tool that verifies the operating system, the amount of free disk space for the installation, and other prerequisites.

To ensure that your system environment is appropriate for the installation, you can run the prerequisite checker before each installation.

Tip: The prerequisite checker verifies only the minimum memory that is necessary. More memory is required for additional tasks.

The prerequisite checker presents a summary of results at the end of the check. Any changes that are required in your environment before the installation are listed. Any new directories that are required for the installation are created.

To run the prerequisite checker, complete the following steps.
1. Ensure that the appropriate installation package is downloaded and that its files are extracted. A prerequisite checker is part of the installation package.
2. Choose the graphical interface (the default) or console method to start the installation, and follow the wizard instructions to complete the installation:
   • Issue this command to start the installation wizard using a graphical interface:
     ```
     ./prereqcheck.bin
     ```
   • Issue this command to start the installation wizard using the console method:
     ```
     ./prereqcheck.bin -i console
     ```
3. Select the language for the prerequisite checker user interface.
4. In the welcome and disclaimer panels, review the statements and accept them.

If the Prerequisite Results page indicates that your system passed the checks, you are ready to start the installation.

If an error message is shown in the Prerequisite Results page, make the required corrections before continuing with the installation. The summary page lists the errors and directs you to an error log file.

Compatibility of the Tivoli Storage Manager server with other DB2 products on the system

You can install other products that deploy and use DB2 products on the same system as the Tivoli Storage Manager Version 6.3 or later server on AIX, HP-UX, Linux, and Oracle Solaris platforms, with some limitations.

To install and use other products that use a DB2 product on the same system as the Tivoli Storage Manager server, ensure that the following criteria are met:

Table 14. Compatibility of the Tivoli Storage Manager server with other DB2 products on the system

Criterion	Instructions
Version level	The other products that use a DB2 product must use DB2 version 9 or later. DB2 products include product encapsulation and segregation support beginning with Version 9. Starting with this version, you can run multiple copies of DB2 products, at different code levels, on the same system. For details, see the information about multiple DB2 copies: http://pic.dhe.ibm.com/infocenter/db2luw/v9r7.
User IDs and directories	Ensure that the user IDs, fence user IDs, installation location, other directories, and related information are not shared across DB2 installations. Your specifications must be different from the IDs and locations that you used for the Tivoli Storage Manager server installation and configuration. If you used the `dsmicfgx` wizard or `dsmupgdx` wizard to configure Version 6.3 or later, or upgrade the server from Version 5.5, these are values that you entered when running the wizard. If you used the manual configuration for Version 6.3 or later or upgrade from Version 5.5 procedures, review the procedures that you used if necessary to recall the values that were used for the server.

Table 14. Compatibility of the Tivoli Storage Manager server with other DB2 products on the system (continued)

Criterion	Instructions
Resource allocation	Consider the resources and capability of the system compared to the requirements for both the Tivoli Storage Manager server and the other applications that use the DB2 product. To provide sufficient resources for the other DB2 applications, you might have to change the Tivoli Storage Manager server settings so that the server uses less system memory and resources. Similarly, if the workloads for the other DB2 applications compete with the Tivoli Storage Manager server for processor or memory resources, the performance of the server in handling the expected client workload or other server operations might be adversely affected. To segregate resources and provide more capability for the tuning and allocation of processor, memory, and other system resources for multiple applications, consider using logical partition (LPAR), workload partition (WPAR), or other virtual workstation support. For example, run a DB2 application on its own virtualized system.

Worksheets for planning details for the Tivoli Storage Manager server

You can use the work sheets to help you plan the amount and location of storage needed for the Tivoli Storage Manager server. You can also use them to keep track of names and user IDs.

See *Tivoli Storage Manager Optimizing Performance* for server configuration guidelines and best practices.

Item	Space required	Number of directories	Location of directories
The database			
Active log			
Archive log			
Optional: Log mirror for the active log			
Optional: Secondary archive log (failover location for archive log)			

Item	Names and user IDs	Location
The *instance user ID* for the server, which is the ID you use to start and run the Tivoli Storage Manager server		

Item	Names and user IDs	Location
The *home directory* for the server, which is the directory that contains the instance user ID		
The database instance name		
The *instance directory* for the server, which is a directory that contains files specifically for this server instance (the server options file and other server-specific files)		
Server name, use a unique name for each server		

Capacity planning

Capacity planning for Tivoli Storage Manager includes managing resources such as the database and recovery log. To maximize resources as part of capacity planning, you must estimate space requirements for the database and the recovery log.

For information about the benefits of deduplication and guidance on how to make effective use of the Tivoli Storage Manager deduplication feature, see Optimizing Performance.

Estimating space requirements for the database

To estimate space requirements for the database, you can use the maximum number of files that can be in server storage at one time or you can use storage pool capacity.

Consider using at least 25 GB for the initial database space. Provision file system space appropriately. A database size of 25 GB is adequate for a test environment or a library-manager-only environment. For a production server supporting client workloads, the database size is expected to be larger. If you use random-access disk (DISK) storage pools, more database and log storage space is needed than for sequential-access storage pools.

The maximum size of the Tivoli Storage Manager database is 4 TB.

For information about sizing the database in a production environment that is based on the number of files and on storage pool size, see the following topics.

Estimating database space requirements based on the number of files

If you can estimate the maximum number of files that might be in server storage at a time, you can use that number to estimate space requirements for the database.

To estimate space requirements that is based on the maximum number of files in server storage, use the following guidelines:

- 600 - 1000 bytes for each stored version of a file, including image backups.

  Restriction: The guideline does not include space that is used during data deduplication.

- 100 - 200 bytes for each cached file, copy storage pool file, active-data pool file, and deduplicated file.
- Additional space is required for database optimization to support varying data-access patterns and to support server back-end processing of the data. The amount of extra space is equal to 50% of the estimate for the total number of bytes for file objects.

In the following example for a single client, the calculations are based on the maximum values in the preceding guidelines. The examples do not take into account that you might use file aggregation. In general, when you aggregate small files, it reduces the amount of required database space. File aggregation does not affect space-managed files.

1. Calculate the number of file versions. Add each of the following values to obtain the number of file versions:

   a. Calculate the number of backed-up files. For example, as many as 500,000 client files might be backed up at a time. In this example, storage policies are set to keep up to three copies of backed up files:

      ```
      500,000 files * 3 copies = 1,500,000 files
      ```

   b. Calculate the number of archive files. For example, as many as 100,000 client files might be archived copies.

   c. Calculate the number of space-managed files. For example, as many as 200,000 client files might be migrated from client workstations.

   Using 1000 bytes per file, the total amount of database space that is required for the files that belong to the client is 1.8 GB:

   ```
   (1,500,000 + 100,000 + 200,000) * 1000 = 1.8 GB
   ```

2. Calculate the number of cached files, copy storage-pool files, active-data pool files, and deduplicated files:

   a. Calculate the number of cached copies. For example, caching is enabled in a 5 GB disk storage pool. The high migration threshold of the pool is 90% and the low migration threshold of the pool is 70%. Thus, 20% of the disk pool, or 1 GB, is occupied by cached files.

      If the average file size is about 10 KB, approximately 100,000 files are in cache at any one time:

      ```
      100,000 files * 200 bytes = 19 MB
      ```

   b. Calculate the number of copy storage-pool files. All primary storage pools are backed up to the copy storage pool:

      ```
      (1,500,000 + 100,000 + 200,000) * 200 bytes = 343 MB
      ```

   c. Calculate the number of active storage-pool files. All the active client-backup data in primary storage pools is copied to the active-data storage pool. Assume that 500,000 versions of the 1,500,000 backup files in the primary storage pool are active:

      ```
      500,000 * 200 bytes = 95 MB
      ```

   d. Calculate the number of deduplicated files. Assume that a deduplicated storage pool contains 50,000 files:

      ```
      50,000 * 200 bytes = 10 MB
      ```

   Based on the preceding calculations, about 0.5 GB of extra database space is required for the client's cached files, copy storage-pool files, active-data pool files, and deduplicated files.

3. Calculate the amount of extra space that is required for database optimization. To provide optimal data access and management by the server, extra database space is required. The amount of extra database space is equal to 50% of the total space requirements for file objects.

   ```
   (1.8 + 0.5) * 50% = 1.2 GB
   ```

4. Calculate the total amount of database space that is required for the client. The total is approximately 3.5 GB:

   ```
   1.8 + 0.5 + 1.2 = 3.5 GB
   ```

5. Calculate the total amount of database space that is required for all clients. If the client that was used in the preceding calculations is typical and you have 500 clients, for example, you can use the following calculation to estimate the total amount of database space that is required for all clients:

   ```
   500 * 3.5 = 1.7 TB
   ```

Tip: In the preceding examples, the results are estimates. The actual size of the database might differ from the estimate because of factors such as the number of directories and the length of the path and file names. Periodically monitor your database and adjust its size as necessary.

During normal operations, the Tivoli Storage Manager server might require temporary database space. This space is needed for the following reasons:

- To hold the results of sorting or ordering that are not already being kept and optimized in the database directly. The results are temporarily held in the database for processing.
- To give administrative access to the database through one of the following methods:
  - A DB2 open database connectivity (ODBC) client
  - An Oracle Java™ database connectivity (JDBC) client
  - Structured Query Language (SQL) to the server from an administrative-client command line

Consider using an extra 50 GB of temporary space for every 500 GB of space for file objects and optimization. See the guidelines in the following table. In the example that is used in the preceding step, a total of 1.7 TB of database space is required for file objects and optimization for 500 clients. Based on that calculation, 200 GB is required for temporary space. The total amount of required database space is 1.9 TB.

Database size	Minimum temporary-space requirement
< 500 GB	50 GB
≥ 500 GB and < 1 TB	100 GB
≥ 1 TB and < 1.5 TB	150 GB
≥ 1.5 and < 2 TB	200 GB
≥ 2 and < 3 TB	250 - 300 GB
≥ 3 and < 4 TB	350 - 400 GB

Estimating database space requirements based on storage pool capacity

To estimate database space requirements based on storage pool capacity, use a ratio of 1 - 5%. For example, if you require 200 TB of storage pool capacity, the size of your database is expected to be 2 - 10 TB. As a general rule, make your database as large as possible to prevent running out of space. If you run out of database space, server operations and client-store operations can fail.

The database manager and temporary space

The Tivoli Storage Manager server database manager manages and allocates system memory and disk space for the database. The amount of database space you require depends on the amount of system memory available and the server workload.

The database manager sorts data in a specific sequence, as per the SQL statement that you issue to request the data. Depending on the workload on the server, and if there is more data than the database manager can manage, the data (that is ordered in sequence) is allocated to temporary disk space. Data is allocated to temporary disk space when there is a large result set. The database manager dynamically manages the memory used when data is allocated to temporary disk space.

For example, expiration processing can produce a large result set. If there is not enough system memory on the database to store the result set, some of the data is allocated to temporary disk space. During expiration processing, if a node or file space are selected that are too large to process, the database manager does not have enough memory to sort the data.

To run database operations, consider adding more database space for the following scenarios:

- The database has a small amount of space and the server operation that requires temporary space uses the remaining free space.
- The file spaces are large, or the file spaces has a policy assigned to it which creates many file versions.
- The Tivoli Storage Manager server must run with limited memory. The database uses the Tivoli Storage Manager server main memory to run database operations. However, if there is insufficient memory available, the Tivoli Storage Manager server allocates temporary space on disk to the database. For example, if 10G of memory is available and database operations require 12G of memory, the database uses temporary space.
- An `out of database space` error is displayed when you deploy a Tivoli Storage Manager V6 server. Monitor the server activity log for messages related to database space.

Important: Do not change the DB2 software that is installed with the Tivoli Storage Manager installation packages and fix packs. Do not install or upgrade to a different version, release, or fix pack, of DB2 software to avoid damage to the database.

Recovery log space requirements

In Tivoli Storage Manager, the term *recovery log* comprises the active log, the archive log, the active log mirror, and the archive failover log. The amount of space that you require for the recovery log depends on various factors, including, for example, the amount of client activity with the server.

Active and archive log space

When you estimate space requirements for active and archive logs, include some extra space for contingencies such as occasional heavy workloads and failovers.

In Tivoli Storage Manager servers V6.1 and later, the active log can be a maximum size of 128 GB. The archive log size is limited to the size of the file system that it is installed on.

Use the following general guidelines when you estimate the size of the active log:
- The suggested starting size for the active log is 16 GB.
- Ensure that the active log is at least large enough for the amount of concurrent activity that the server typically handles. As a precaution, try to anticipate the largest amount of work that the server manages at one time. Provision the active log with extra space that can be used if needed. Consider using 20% of extra space.
- Monitor used and available active log space. Adjust the size of the active log as needed, depending upon factors such as client activity and the level of server operations.
- Ensure that the directory that holds the active log is as large as, or larger than, the size of the active log. A directory that is larger than the active log can accommodate failovers, if they occur.
- Ensure that the file system that contains the active log directory has at least 8 GB of free space for temporary log movement requirements.

The suggested starting size for the archive log is 48 GB.

The archive log directory must be large enough to contain the log files that are generated since the previous full backup. For example, if you perform a full backup of the database every day, the archive log directory must be large enough to hold the log files for all the client activity that occurs during 24 hours. To recover space, the server deletes obsolete archive log files after a full backup of the database. If the archive log directory becomes full and a directory for archive failover logs does not exist, log files remain in the active log directory. This condition can cause the active log directory to fill up and stop the server. When the server restarts, some of the existing active-log space is released.

After the server is installed, you can monitor archive log utilization and the space in the archive log directory. If the space in the archive log directory fills up, it can cause the following problems:
- The server is unable to perform full database backups. Investigate and resolve this problem.
- Other applications write to the archive log directory, exhausting the space that is required by the archive log. Do not share archive log space with other applications including other Tivoli Storage Manager servers. Ensure that each server has a separate storage location that is owned and managed by that specific server.

Installing the Tivoli Storage Manager server

For guidance about the layout and tuning of the active log and archive log, see Optimizing Performance.

Example: Estimating active and archive log sizes for basic client-store operations:

Basic client-store operations include backup, archive, and space management. Log space must be sufficient to handle all store transactions that are in progress at one time.

To determine the sizes of the active and archive logs for basic client-store operations, use the following calculation:

```
number of clients  x  files stored during each transaction
   x  log space needed for each file
```

This calculation is used in the example in the following table.

Table 15. Basic client-store operations

Item	Example values	Description
Maximum number of client nodes that back up, archive, or migrate files concurrently at any time	300	The number of client nodes that back up, archive, or migrate files every night.
Files stored during each transaction	4096	The default value of the server option TXNGROUPMAX is 4096.
Log space that is required for each file	3053 bytes	The value of 3053 bytes for each file in a transaction represents the log bytes that are needed when backing up files from a Windows client where the file names are 12 - 120 bytes. This value is based on the results of tests performed under laboratory conditions. The tests consisted of backup-archive clients performing backup operations to a random-access disk (DISK) storage pool. DISK pools result in more log use than sequential-access storage pools. Consider a value larger than 3053 bytes if the data being stored has file names that are longer than 12 - 120 bytes.

Active log: Suggested size	19.5 GB [1]	Use the following calculation to determine the size of the active log. One GB equals 1,073,741,824 bytes.
		
		`(300 clients x 4096 files stored during each transaction x 3053 bytes for each file) ÷ 1,073,741,824 bytes = 3.5 GB`
		
		Increase that amount by the suggested starting size of 16 GB:
		
		`3.5 + 16 = 19.5 GB`

Archive log: Suggested size	58.5 GB [1]	Because of the requirement to be able to store archive logs across three server database-backup cycles, multiply the estimate for the active log by 3 to estimate the total archive log requirement.
		
		`3.5 x 3 = 10.5 GB`
		
		Increase that amount by the suggested starting size of 48 GB:
		
		`10.5 + 48 = 58.5 GB`

Table 15. Basic client-store operations (continued)

Item	Example values	Description
[1] The example values in this table are used only to illustrate how the sizes for active logs and archive logs are calculated. In a production environment that does not use deduplication, 16 GB is the suggested minimum size for an active log. The suggested minimum size for an archive log in a production environment that does not use deduplication is 48 GB. If you substitute values from your environment and the results are larger than 16 GB and 48 GB, use your results to size the active log and archive log.		
Monitor your logs and adjust their size if necessary.		

Example: Estimating active and archive log sizes for clients that use multiple sessions:

If the client option RESOURCEUTILIZATION is set to a value that is greater than the default, the concurrent workload for the server increases.

To determine the sizes of the active and archive logs when clients use multiple sessions, use the following calculation:

```
number of clients  x  sessions for each client  x  files stored
   during each transaction  x  log space needed for each file
```

This calculation is used in the example in the following table.

Table 16. Multiple client sessions

Item	Example values		Description
Maximum number of client nodes that back up, archive, or migrate files concurrently at any time	300	1000	The number of client nodes that back up, archive, or migrate files every night.
Possible sessions for each client	3	3	The setting of the client option RESOURCEUTILIZATION is larger than the default. Each client session runs a maximum of three sessions in parallel.
Files stored during each transaction	4096	4096	The default value of the server option TXNGROUPMAX is 4096.
Log space that is required for each file	3053	3053	The value of 3053 bytes for each file in a transaction represents the log bytes needed when backing up files from a Windows client where the file names are 12 - 120 bytes. This value is based on the results of tests performed under laboratory conditions. Tests consisted of clients performing backup operations to a random-access disk (DISK) storage pool. DISK pools result in more log use than sequential-access storage pools. Consider a value larger than 3053 bytes if the data being stored has file names that are longer than 12 - 120 bytes.

Table 16. Multiple client sessions (continued)

Item	Example values		Description

Active log: Suggested size	26.5 GB [1]	51 GB [1]	The following calculation was used for 300 clients. One GB equals 1,073,741,824 bytes.
			
			`(300 clients x 3 sessions for each client x 4096 files stored during each transaction x 3053 bytes for each file) ÷ 1,073,741,824 = 10.5 GB`
			
			Increase that amount by the suggested starting size of 16 GB:
			
			`10.5 + 16 = 26.5 GB`
			
			The following calculation was used for 1000 clients. One GB equals 1,073,741,824 bytes.
			
			`(1000 clients x  3 sessions for each client x 4096 files store during each transaction x 3053 bytes for each file) ÷ 1,073,741,824 = 35 GB`
			
			Increase that amount by the suggested starting size of 16 GB:
			
			`35 + 16 = 51 GB`

Archive log: Suggested size	79.5 GB [1]	153 GB [1]	Because of the requirement to be able to store archive logs across three server-database backup cycles, the estimate for the active log is multiplied by 3:
			
			`10.5 x 3 = 31.5 GB`
			
			`35 x 3 = 105 GB`
			
			Increase those amounts by the suggested starting size of 48 GB:
			
			`31.5 + 48 = 79.5 GB`
			
			`105 + 48 = 153 GB`

[1] The example values in this table are used only to illustrate how the sizes for active logs and archive logs are calculated. In a production environment that does not use deduplication, 16 GB is the suggested minimum size for an active log. The suggested minimum size for an archive log in a production environment that does not use deduplication is 48 GB. If you substitute values from your environment and the results are larger than 16 GB and 48 GB, use your results to size the active log and archive log.

Monitor your active log and adjust its size if necessary.

Example: Estimating active and archive log sizes for simultaneous write operations:

If client backup operations use storage pools that are configured for simultaneous write, the amount of log space that is required for each file increases.

The log space that is required for each file increases by about 200 bytes for each copy storage pool that is used for a simultaneous write operation. In the example in the following table, data is stored to two copy storage pools in addition to a primary storage pool. The estimated log size increases by 400 bytes for each file. If you use the suggested value of 3053 bytes of log space for each file, the total number of required bytes is 3453.

This calculation is used in the example in the following table.

Table 17. Simultaneous write operations

Item	Example values	Description
Maximum number of client nodes that back up, archive, or migrate files concurrently at any time	300	The number of client nodes that back up, archive, or migrate files every night.
Files stored during each transaction	4096	The default value of the server option TXNGROUPMAX is 4096.
Log space that is required for each file	3453 bytes	3053 bytes plus 200 bytes for each copy storage pool. The value of 3053 bytes for each file in a transaction represents the log bytes that are needed when backing up files from a Windows client where the file names are 12 - 120 bytes. This value is based on the results of tests performed under laboratory conditions. The tests consisted of backup-archive clients performing backup operations to a random-access disk (DISK) storage pool. DISK pools result in more log use than sequential-access storage pools. Consider a value larger than 3053 bytes if the data being stored has file names that are longer than 12 - 120 bytes.

Active log: Suggested size	20 GB [1]	Use the following calculation to determine the size of the active log. One GB equals 1,073,741,824 bytes.
		
		`(300 clients x 4096 files stored during each transaction x 3453 bytes for each file) ÷ 1,073,741,824 bytes = 4.0 GB`
		
		Increase that amount by the suggested starting size of 16 GB:
		
		`4 + 16 = 20 GB`

Archive log: Suggested size	60 GB [1]	Because of the requirement to be able to store archive logs across three server database-backup cycles, multiply the estimate for the active log by 3 to estimate the archive log requirement:
		
		`4 GB  x  3  = 12 GB`
		
		Increase that amount by the suggested starting size of 48 GB:
		
		`12 + 48 = 60 GB`

[1] The example values in this table are used only to illustrate how the sizes for active logs and archive logs are calculated. In a production environment that does not use deduplication, 16 GB is the suggested minimum size for an active log. The suggested minimum size for an archive log in a production environment that does not use deduplication is 48 GB. If you substitute values from your environment and the results are larger than 16 GB and 48 GB, use your results to size the active log and archive log.

Monitor your logs and adjust their size if necessary.

Example: Estimating active and archive log sizes for basic client store operations and server operations:

Migration of data in server storage, identification processes for data deduplication, reclamation, and expiration might run concurrently with client store operations. Administrative tasks such as administrative commands or SQL queries from administrative clients can also run concurrently with client store operations. Server operations and administrative tasks that run concurrently can increase the active log space that is required.

For example, migration of files from the random-access (DISK) storage pool to a sequential-access disk (FILE) storage pool uses approximately 110 bytes of log space for each file that is migrated. For example, suppose that you have 300 backup-archive clients and each one of them backs up 100,000 files every night. The files are initially stored on DISK and then migrated to a FILE storage pool. To estimate the amount of active log space that is required for the data migration, use the following calculation. The number of clients in the calculation represents the maximum number of client nodes that back up, archive, or migrate files concurrently at any time.

```
300 clients  x 100,000 files for each client   x  110 bytes =  3.1 GB
```

Add this value to the estimate for the size of the active log that calculated for basic client store operations.

Example: Estimating active and archive log sizes under conditions of extreme variation:

Problems with running out of active log space can occur if you have many transactions that complete quickly and some transactions that take much longer to complete. A typical case occurs when many workstation or file-server backup sessions are active and a few very large database server-backup sessions are active. If this situation applies to your environment, you might need to increase the size of the active log so that the work completes successfully.

Example: Estimating archive log sizes with full database backups:

The Tivoli Storage Manager server deletes unnecessary files from the archive log only when a full database backup occurs. Consequently, when you estimate the space that is required for the archive log, you must also consider the frequency of full database backups.

For example, if a full database backup occurs once a week, the archive log space must be able to contain the information in the archive log for a full week.

The difference in archive log size for daily and full database backups is shown in the example in the following table.

Table 18. Full database backups

Item	Example values	Description
Maximum number of client nodes that back up, archive, or migrate files concurrently at any time	300	The number of client nodes that back up, archive, or migrate files every night.
Files stored during each transaction	4096	The default value of the server option TXNGROUPMAX is 4096.

Table 18. Full database backups (continued)

Item	Example values	Description
Log space that is required for each file	3453 bytes	3053 bytes for each file plus 200 bytes for each copy storage pool. The value of 3053 bytes for each file in a transaction represents the log bytes needed when backing up files from a Windows client where the file names are 12 - 120 bytes. This value is based on the results of tests performed under laboratory conditions. Tests consisted of clients performing backup operations to a random-access disk (DISK) storage pool. DISK pools result in more log use than sequential-access storage pools. Consider a value larger than 3053 bytes if the data being stored has file names that are longer than 12 - 120 bytes.

Active log: Suggested size	20 GB [1]	Use the following calculation to determine the size of the active log. One GB equals 1,073,741,824 bytes.
		
		`(300 clients x 4096 files per transaction x 3453 bytes per file) ÷ 1,073,741,824 bytes = 4.0 GB`
		
		Increase that amount by the suggested starting size of 16 GB:
		
		`4 + 16 = 20 GB`

Archive log: Suggested size with a full database backup every day	60 GB [1]	Because of the requirement to be able to store archive logs across three backup cycles, multiply the estimate for the active log by 3 to estimate the total archive log requirement:
		
		`4 GB x 3 = 12 GB`
		
		Increase that amount by the suggested starting size of 48 GB:
		
		`12 + 48 = 60 GB`

Archive log: Suggested size with a full database every week	132 GB [1]	Because of the requirement to be able to store archive logs across three server database-backup cycles, multiply the estimate for the active log by 3 to estimate the total archive log requirement. Multiply the result by the number of days between full database backups:
		
		`(4 GB x 3 ) x 7 = 84 GB`
		
		Increase that amount by the suggested starting size of 48 GB:
		
		`84 + 48 = 132 GB`

[1] The example values in this table are used only to illustrate how the sizes for active logs and archive logs are calculated. In a production environment that does not use deduplication, 16 GB is the suggested minimum size for an active log. The suggested starting size for an archive log in a production environment that does not use deduplication is 48 GB. If you substitute values from your environment and the results are larger than 16 GB and 48 GB, use your results to size the active log and archive log.

Monitor your logs and adjust their size if necessary.

Example: Estimating active and archive log sizes for data deduplication operations:

If you deduplicate data, you must consider its effects on space requirements for active and archive logs.

The following factors affect requirements for active and archive log space:

The amount of deduplicated data
> The effect of data deduplication on the active log and archive log space depends on the percentage of data that is eligible for deduplication. If the percentage of data that can be deduplicated is relatively high, more log space is required.

The size and number of extents
> Approximately 1,500 bytes of active log space are required for each extent that is identified by a duplicate-identification process. For example, if 250,000 extents are identified by a duplicate-identification process, the estimated size of the active log is 358 MB:
>
> ```
> 250,000 extents identified during each process x 1,500 bytes
>  for each extent = 358 MB
> ```
>
> Consider the following scenario. Three hundred backup-archive clients back up 100,000 files each night. This activity creates a workload of 30,000,000 files. The average number of extents for each file is two. Therefore, the total number of extents is 60,000,000, and the space requirement for the archive log is 84 GB:
>
> ```
> 60,000,000 extents x 1,500 bytes for each extent = 84 GB
> ```
>
> A duplicate-identification process operates on aggregates of files. An aggregate consists of files that are stored in a given transaction, as specified by the TXNGROUPMAX server option. Suppose that the TXNGROUPMAX server option is set to the default of 4096. If the average number of extents for each file is two, the total number of extents in each aggregate is 8192, and the space required for the active log is 12 MB:
>
> ```
> 8192 extents in each aggregate x 1500 bytes for each extent =
>     12 MB
> ```

The timing and number of the duplicate-identification processes
> The timing and number of duplicate-identification processes also affects the size of the active log. Using the 12 MB active-log size that was calculated in the preceding example, the concurrent load on the active log is 120 MB if 10 duplicate-identification processes are running in parallel:
>
> ```
> 12 MB for each process x 10 processes = 120 MB
> ```

File size
> Large files that are processed for duplicate identification can also affect the size of the active log. For example, suppose that a backup-archive client backs up an 80 GB, file-system image. This object can have a high number of duplicate extents if, for example, the files included in the file system image were backed up incrementally. For example, assume that a file system image has 1.2 million duplicate extents. The 1.2 million extents in this large file represent a single transaction for a duplicate-identification process. The total space in the active log that is required for this single object is 1.7 GB:
>
> ```
> 1,200,000 extents x 1,500 bytes for each extent = 1.7 GB
> ```

If other, smaller duplicate-identification processes occur at the same time as the duplicate-identification process for a single large object, the active log might not have enough space. For example, suppose that a storage pool is enabled for deduplication. The storage pool has a mixture of data, including many relatively small files that range from 10 KB to several hundred KB. The storage pool also has few large objects that have a high percentage of duplicate extents.

To take into account not only space requirements but also the timing and duration of concurrent transactions, increase the estimated size of the active log by a factor of two. For example, suppose that your calculations for space requirements are 25 GB (23.3 GB + 1.7 GB for deduplication of a large object). If deduplication processes are running concurrently, the suggested size of the active log is 50 GB. The suggested size of the archive log is 150 GB.

The examples in the following tables show calculations for active and archive logs. The example in the first table uses an average size of 700 KB for extents. The example in the second table uses an average size of 256 KB. As the examples show, the average deduplicate-extent size of 256 KB indicates a larger estimated size for the active log. To minimize or prevent operational problems for the server, use 256 KB to estimate the size of the active log in your production environment.

Table 19. Average duplicate-extent size of 700 KB

Item	Example values		Description
Size of largest single object to deduplicate	800 GB	4 TB	The granularity of processing for deduplication is at the file level. Therefore, the largest single file to deduplicate represents the largest transaction and a correspondingly large load on the active and archive logs.
Average size of extents	700 KB	700 KB	The deduplication algorithms use a variable block method. Not all deduplicated extents for a given file are the same size, so this calculation assumes an average size for extents.
Extents for a given file	1,198,372 bits	6,135,667 bits	Using the average extent size (700 KB), these calculations represent the total number of extents for a given object. The following calculation was used for an 800 GB object: `(800 GB ÷ 700 KB) = 1,198,372 bits` The following calculation was used for a 4 TB object: `(4 TB ÷ 700 KB) = 6,135,667 bits`
Active log: Suggested size that is required for the deduplication of a single large object during a single duplicate-identification process	1.7 GB	8.6 GB	The estimated active log space that are needed for this transaction.

Installing the Tivoli Storage Manager server

Table 19. Average duplicate-extent size of 700 KB (continued)

Item	Example values		Description

Active log: Suggested total size	66 GB [1]	79.8 GB [1]	After considering other aspects of the workload on the server in addition to deduplication, multiply the existing estimate by a factor of two. In these examples, the active log space required to deduplicate a single large object is considered along with previous estimates for the required active log size.
			
			The following calculation was used for multiple transactions and an 800 GB object:
			
			`(23.3 GB + 1.7 GB) x 2 = 50 GB`
			
			Increase that amount by the suggested starting size of 16 GB:
			
			`50 + 16 = 66 GB`
			
			The following calculation was used for multiple transactions and a 4 TB object:
			
			`(23.3 GB + 8.6 GB) x 2 = 63.8 GB`
			
			Increase that amount by the suggested starting size of 16 GB:
			
			`63.8 + 16 = 79.8 GB`

Archive log: Suggested size	198 GB [1]	239.4 GB [1]	Multiply the estimated size of the active log by a factor of 3.
			
			The following calculation was used for multiple transactions and an 800 GB object:
			
			`50 GB x 3 = 150 GB`
			
			Increase that amount by the suggested starting size of 48 GB:
			
			`150 + 48 = 198 GB`
			
			The following calculation was used for multiple transactions and a 4 TB object:
			
			`63.8 GB x 3 = 191.4 GB`
			
			Increase that amount by the suggested starting size of 48 GB:
			
			`191.4 + 48 = 239.4 GB`

[1] The example values in this table are used only to illustrate how the sizes for active logs and archive logs are calculated. In a production environment that uses deduplication, 32 GB is the suggested minimum size for an active log. The suggested minimum size for an archive log in a production environment that uses deduplication is 96 GB. If you substitute values from your environment and the results are larger than 32 GB and 96 GB, use your results to size the active log and archive log.

Monitor your logs and adjust their size if necessary.

Table 20. Average duplicate-extent size of 256 KB

Item	Example values		Description
Size of largest single object to deduplicate	800 GB	4 TB	The granularity of processing for deduplication is at the file level. Therefore, the largest single file to deduplicate represents the largest transaction and a correspondingly large load on the active and archive logs.

Table 20. Average duplicate-extent size of 256 KB (continued)

Item	Example values		Description
Average size of extents	256 KB	256 KB	The deduplication algorithms use a variable block method. Not all deduplicated extents for a given file are the same size, so this calculation assumes an average extent size.
Extents for a given file	3,276,800 bits	16,777,216 bits	Using the average extent size, these calculations represent the total number of extents for a given object. The following calculation was used for multiple transactions and an 800 GB object: `(800 GB ÷ 256 KB) = 3,276,800 bits` The following calculation was used for multiple transactions and a 4 TB object: `(4 TB ÷ 256 KB) = 16,777,216 bits`
Active log: Suggested size that is required for the deduplication of a single large object during a single duplicate-identification process	4.5 GB	23.4 GB	The estimated size of the active log space that is required for this transaction.
Active log: Suggested total size	71.6 GB [1]	109.4 GB [1]	After considering other aspects of the workload on the server in addition to deduplication, multiply the existing estimate by a factor of 2. In these examples, the active log space required to deduplicate a single large object is considered along with previous estimates for the required active log size. The following calculation was used for multiple transactions and an 800 GB object: `(23.3 GB + 4.5 GB) x 2 = 55.6 GB` Increase that amount by the suggested starting size of 16 GB: `55.6 + 16 = 71.6 GB` The following calculation was used for multiple transactions and a 4 TB object: `(23.3 GB + 23.4 GB) x 2 = 93.4 GB` Increase that amount by the suggested starting size of 16 GB: `93.4 + 16 = 109.4 GB`

Table 20. Average duplicate-extent size of 256 KB (continued)

Item	Example values		Description

Archive log: Suggested size	214.8 GB [1]	328.2 GB [1]	The estimated size of the active log multiplied by a factor of 3.
			
			 The following calculation was used for an 800 GB object:
			
			 `55.6 GB x 3 = 166.8 GB`
			
			 Increase that amount by the suggested starting size of 48 GB:
			
			 `166.8 + 48 = 214.8 GB`
			
			 The following calculation was used for a 4 TB object:
			 `93.4 GB x 3 = 280.2 GB`
			
			 Increase that amount by the suggested starting size of 48 GB:
			
			 `280.2 + 48 = 328.2 GB`

[1] The example values in this table are used only to illustrate how the sizes for active logs and archive logs are calculated. In a production environment that uses deduplication, 32 GB is the suggested minimum size for an active log. The suggested minimum size for an archive log in a production environment that uses deduplication is 96 GB. If you substitute values from your environment and the results are larger than 32 GB and 96 GB, use your results to size the active log and archive log.

Monitor your logs and adjust their size if necessary.

Active-log mirror space

The active log can be mirrored so that the mirrored copy can be used if the active log files cannot be read. There can be only one active log mirror.

Creating a log mirror is a suggested option. If you increase the size of the active log, the log mirror size is increased automatically. Mirroring the log can affect performance because of the doubled I/O activity that is required to maintain the mirror. The additional space that the log mirror requires is another factor to consider when deciding whether to create a log mirror.

If the mirror log directory becomes full, the server issues error messages to the activity log and to the db2diag.log. Server activity continues.

Archive-failover log space

The archive failover log is used by the server if the archive log directory runs out of space.

Specifying an archive failover log directory can prevent problems that occur if the archive log runs out of space. If both the archive log directory and the drive or file system where the archive failover log directory is located become full, the data remains in the active log directory. This condition can cause the active log to fill up, which causes the server to halt.

Server naming best practices

Use these descriptions as a reference when you install or upgrade a Tivoli Storage Manager server.

Instance user ID

The instance user ID is used as the basis for other names related to the server instance. The instance user ID is also called the instance owner.

For example: tsminst1

The instance user ID is the user ID that must have ownership or read/write access authority to all directories that you create for the database and the recovery log. The standard way to run the server is under the instance user ID. That user ID must also have read/write access to the directories that are used for any **FILE** device classes.

Home directory for the instance user ID

The home directory can be created when creating the instance user ID, by using the option (-m) to create a home directory if it does not exist already. Depending on local settings, the home directory might have the form: /home/*instance_user_ID*

For example: /home/tsminst1

The home directory is primarily used to contain the profile for the user ID and for security settings.

Database instance name

The database instance name must be the same as the instance user ID under which you run the server instance.

For example: tsminst1

Instance directory

The instance directory is a directory that contains files specifically for a server instance (the server options file and other server-specific files). It can have any name that you want. For easier identification, use a name that ties the directory to the instance name.

You can create the instance directory as a subdirectory of the home directory for the instance user ID. For example: /home/*instance_user_ID*/ *instance_user_ID*

The following example places the instance directory in the home directory for user ID tsminst1: /home/tsminst1/tsminst1

You can also create the directory in another location, for example: /tsmserver/tsminst1

The instance directory stores the following files for the server instance:
* The server options file, dsmserv.opt
* The server key database file, cert.kdb, and the .arm files (used by clients and other servers to import the Secure Sockets Layer certificates of the server)

- Device configuration file, if the DEVCONFIG server option does not specify a fully qualified name
- Volume history file, if the VOLUMEHISTORY server option does not specify a fully qualified name
- Volumes for **DEVTYPE=FILE** storage pools, if the directory for the device class is not fully specified, or not fully qualified
- User exits
- Trace output (if not fully qualified)

Database name

The database name is always TSMDB1, for every server instance. This name cannot be changed.

Server name

The server name is an internal name for Tivoli Storage Manager, and is used for operations that involve communication among multiple Tivoli Storage Manager servers. Examples include server-to-server communication and library sharing.

The server name is also used when you add the server to the Administration Center so that it can be managed using that interface. Use a unique name for each server. For easy identification in the Administration Center (or from a **QUERY SERVER** command), use a name that reflects the location or purpose of the server.

The server name is also used when you add the server to the Operations Center so that it can be managed using that interface. Use a unique name for each server. For easy identification in the Operations Center (or from a **QUERY SERVER** command), use a name that reflects the location or purpose of the server.

If you use the wizard, the default name that is suggested is the host name of the system that you are using. You can use a different name that is meaningful in your environment. If you have more than one server on the system and you use the wizard, you can use the default name for only one of the servers. You must enter a unique name for each server.

For example:

```
PAYROLL
SALES
```

For more information about server names, see the *Administrator's Guide*.

Directories for database space and recovery log

The directories can be named according to local practices. For easier identification, consider using names that tie the directories to the server instance.

For example, for the archive log:
```
/tsminst1_archlog
```

Installation directories

Installation directories for the Tivoli Storage Manager server include the server, DB2, device, language, and other directories. Each one contains several additional directories.

The default directories and their subdirectories are listed here for the server, DB2, devices, and languages:

- **Server directory** (`/opt/tivoli/tsm/server/bin`), which contains:
  - Server code and licensing
- **Additional server directories**:
  - The command and message help are in the `/opt/tivoli/tsm/server/bin/dsmserv.hlp` directory.
  - Tivoli inventory (`/opt/tivoli/tsm/tivinv`)
- **DB2 directories**

  The DB2 product that is installed as part of the installation of the Tivoli Storage Manager server has the directory structure as documented in DB2 information sources. Protect these directories and files as you do the server directories.
  - `/opt/tivoli/tsm/db2`
- **Device directories**
  - `/opt/tivoli/tsm/devices/bin`
- **Language directory**

  Language-dependent portions of the program are located here:

  `/opt/tivoli/tsm/server/bin`

You can use US English, German, French, Italian, Spanish, Brazilian Portuguese, Korean, Japanese, traditional Chinese, simplified Chinese, Chinese GBK, Chinese Big5, and Russian.

Installing the Tivoli Storage Manager server

Chapter 2. Installing the Tivoli Storage Manager server components

To install the Tivoli Storage Manager 6.3 or later server, you can use the graphical installation wizard, the console wizard, or the command line in silent mode.

Planning to install	→	Installing components	→	Taking the first steps
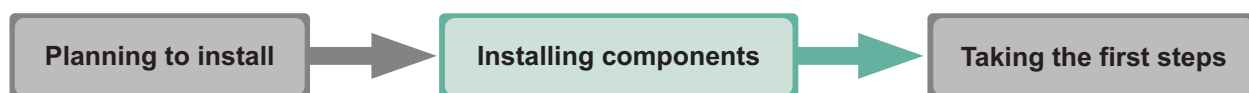
Using the Tivoli Storage Manager installation software, you can install the following components:

- Tivoli Storage Manager Server

  Tip: The Tivoli Storage Manager client application programming interface (API), the database (DB2), and the Global Security Kit (GSKit) are automatically installed when you select the server component.
- Tivoli Storage Manager Server Languages
- Tivoli Storage Manager License
- Tivoli Storage Manager Devices
- Tivoli Storage Manager Storage Agent

  See the *Storage Agent User's Guide* for more details about storage agents.

Important: Use your root user ID to install Tivoli Storage Manager. If you do not, certain key Tivoli Storage Manager functions do not work properly.

1. If you are installing the products using the Tivoli Storage Manager DVD, complete the following steps:

   Insert the Tivoli Storage Manager DVD into a DVD drive. Ensure that the DVD is mounted on directory /dvdrom and change to that directory.

2. If you downloaded the program from Passport Advantage as an executable file, complete the following steps.

   a. Verify that you have enough space to store the installation files when they are extracted from the product package. See the download document for the space requirements:
      - Tivoli Storage Manager: http://www.ibm.com/support/docview.wss?uid=swg24030521
      - Tivoli Storage Manager Extended Edition: http://www.ibm.com/support/docview.wss?uid=swg24030527
      - System Storage Archive Manager: http://www.ibm.com/support/docview.wss?uid=swg24030530

   b. Change to the directory where you downloaded the package file. Be sure to extract the installation files to an empty directory. Do not extract to a directory that contains previously extracted files, or any other files.

Also, ensure that you extract the Tivoli Storage Manager installation wizard to a directory where the root user ID and instance user ID have executable permission.

 c. Change the file permissions by entering the following command:

```
chmod a+x package_name.bin
```

 The *package_name* is typically a name such as CZ1N1ML.

 d. Extract the installation files:

```
./package_name.bin
```

 The package is large, so the extraction takes some time.

3. Optional: After all the files are extracted, locate this file and run it to ensure that your system meets all requirements:

 prereqcheck.bin

See "Running the installation prerequisite checker" on page 12 for details.

4. Ensure that the `/etc/hosts` file is configured. See "Configuring the /etc/hosts file" for details.

5. Ensure that the following command is enabled so that the Tivoli Storage Manager wizards work properly:

 finger

By default, the command is enabled.

6. Select one of the following ways of installing Tivoli Storage Manager:

Installation wizard
 "Installing Tivoli Storage Manager by using the installation wizard" on page 37

Command-line console wizard
 "Installing Tivoli Storage Manager by using the console installation wizard" on page 38

Silent mode
 "Installing Tivoli Storage Manager in silent mode" on page 40

7. After you install Tivoli Storage Manager and before you customize it for your use, go to the Tivoli Storage Manager website: http://www.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Storage_Manager. Click **Support and downloads** and apply any applicable fixes.

Configuring the /etc/hosts file

The /etc/hosts file must have the correct format before you start the Tivoli Storage Manager installation.

Ensure that the /etc/hosts file meets the following requirements:

1. Locate the /etc/hosts file on your system. Open it with an editor, and as a root user if you plan on editing it.

2. Ensure that the following lines were not removed. Replace them if they are missing:

```
127.0.0.1 localhost.localdomain localhost
359.33.9.234 your.server.name
workstation
```

where you replace 359.33.9.234 with the IP address of your system and change `your.server.name` to the fully qualified host name for your system. Include the name of your workstation after the full qualified host name.

3. Save the host file.

Installing Tivoli Storage Manager by using the installation wizard

Using the installation wizard is one method of installing Tivoli Storage Manager.

To install Tivoli Storage Manager by using the installation wizard, complete the following steps:

1. Verify that the operating system is set to the language that you require. By default, the language of the operating system is the language of the installation wizard.

   If you plan to select a different language for the wizard, you might have to change the language of the operating system. By setting the operating system to an ASCII language, such as English or Spanish, you can select an ASCII language for the wizard later in the installation process. By setting the operating system to a non-ASCII language, such as Simplified Chinese, you can select a non-ASCII language later in the installation process.

   For information about setting the language of the operating system, see the operating system documentation.

2. If you are installing locally onto a remote system that uses an X display, and your local system does not have an X Window System server running, the installation might fail. If it fails, ensure that the DISPLAY environment variable is *not* set and restart the installation.

3. If your temporary location is smaller than Tivoli Storage Manager needs, as per the system requirements, use the Install Anywhere environment variable `$IATEMPDIR` as the temporary directory.

4. If you are using Security Enhanced Linux on your system, set `SELINUX=disable` or set `SELINUX=permissive` in the `/etc/sysconfig/selinux` file, at least until the installation process completes. If you do not adjust the setting, you receive this message when you try to install the server:

   ```
   The installation wizard cannot run on your configuration.
   It will now stop. For more details about installation error logs,
   enter the phrase "installation log files" in the Search field
   at this site: http://publib.boulder.ibm.com/infocenter/tsminfo/v6r3.
   ```

5. To start the wizard without saving your responses, enter the following command:

   ```
   ./install.bin
   ```

   To start the wizard and save your responses to later use for a silent installation, enter the following command and specify the -r option.

   ```
   ./install.bin -r /path_name/response.rsp
   ```

   where *path_name* is the full directory path to where you want the response file to be created. If you do not specify a fully qualified name, the response file is placed in a temporary directory.

6. Select the language for your installation and follow the wizard, selecting **Next** to step through the wizard.

   Select the product that you are entitled to use and a license agreement is displayed. You can select only one product on the page. If you select Tivoli Storage Manager, Tivoli Storage Manager Extended Edition, or System Storage

Archive Manager, you are asked if you will be using LAN-free or library sharing. If you select **YES**, you must accept the Tivoli Storage Manager for Storage Area Networks license agreement. This is in addition to the license for the product that you chose on the previous page.

Select the components that you want to install. Components include the server, languages, license, device driver, and storage agent. There is no default, so you must make a selection. If you previously installed a server, ensure that you select the same directory when you install a language package, license, or device driver. If you previously installed a storage agent, ensure that you select the same directory if you return to install a device driver.

A server and a storage agent cannot be installed on the same workstation.

The Tivoli Storage Manager client application programming interface (API), DB2 Version 9.7, and IBM Global Security Kit (GSKit) Version 8 are automatically installed when you select the server component.

If there were any errors during the installation, the summary page lists the errors and directs you to an error log file. The log is in the following directory:

```
/var/tivoli/tsm
```

After you install a new Tivoli Storage Manager server, you must configure it. See Chapter 3, "Taking the first steps after you install Tivoli Storage Manager," on page 45.

Installing Tivoli Storage Manager by using the console installation wizard

Using the console installation wizard is one method of installing Tivoli Storage Manager.

To install Tivoli Storage Manager by using the console installation wizard, complete these steps:

1. Verify that the operating system is set to the language that you require. By default, the language of the operating system is the language of the installation wizard.

   If you plan to select a different language for the wizard, you might have to change the language of the operating system. By setting the operating system to an ASCII language, such as English or Spanish, you can select an ASCII language for the wizard later in the installation process. By setting the operating system to a non-ASCII language, such as Simplified Chinese, you can select a non-ASCII language later in the installation process.

   For information about setting the language of the operating system, see the operating system documentation.

2. If you are installing locally onto a remote system that uses an X display, and your local system does not have an X Window System server running, the installation might fail. If it fails, ensure that the DISPLAY environment variable is *not* set and restart the installation.

3. If your temporary location is smaller than Tivoli Storage Manager needs, as per the system requirements, use the Install Anywhere environment variable $IATEMPDIR as the temporary directory.

4. If you are using Security Enhanced Linux on your system, set SELINUX=disable or set SELINUX=permissive in the /etc/sysconfig/selinux file, at least until the installation process completes. If you do not adjust the setting, you receive this message when you try to install the server:

```
The installation wizard cannot run on your configuration.
It will now stop. For more details about installation error logs,
enter the phrase "installation log files" in the Search field
at this site: http://publib.boulder.ibm.com/infocenter/tsminfo/v6r3.
```

5. To start the wizard without saving your responses, enter the following command:

   `./install.bin -i console`

   To start the wizard and save your responses, enter the following command and specify the -r option.

   `./install.bin -i console -r /path_name/response.rsp`

   where *path_name* is the full directory path to where you want the response file to be created. If you do not specify a fully qualified name, the response file is placed in a temporary directory.

   The Tivoli Storage Manager installation wizard starts.

6. Select the language for your installation and follow the wizard, selecting **Next** to step through the wizard.

   Select the product that you are entitled to use and a license agreement is displayed. You can select only one product on the page. If you select Tivoli Storage Manager, Tivoli Storage Manager Extended Edition, or System Storage Archive Manager, you are asked if you will be using LAN-free or library sharing. If you select **YES**, you must accept the Tivoli Storage Manager for Storage Area Networks license agreement. This is in addition to the license for the product that you chose on the previous page.

   Select the components that you want to install. Components include the server, languages, license, device driver, and storage agent. There is no default, so you must make a selection. If you previously installed a server, ensure that you select the same directory when you install a language package, license, or device driver. If you previously installed a storage agent, ensure that you select the same directory if you return to install a device driver.

   A server and a storage agent cannot be installed on the same workstation.

   The Tivoli Storage Manager client application programming interface (API), DB2 Version 9.7, and IBM Global Security Kit (GSKit) Version 8 are automatically installed when you select the server component.

If there were any errors during the installation, the summary page lists the errors and directs you to an error log file. The log is in the following directory:

   `/var/tivoli/tsm`

After you install a new Tivoli Storage Manager server, you must configure it. See Chapter 3, "Taking the first steps after you install Tivoli Storage Manager," on page 45.

Installing Tivoli Storage Manager in silent mode

Using silent mode is one method of installing Tivoli Storage Manager.

Pass the variables in Table 21 into this file to define the silent installation:

    ./install.bin

Table 21. Variables for the silent installation

Variable	Description
• -DIBM_TSM_LICENSE_ACCEPTED=true • -DIBM_TSMEE_LICENSE_ACCEPTED=true • -DIBM_SSAM_LICENSE_ACCEPTED=true • -DIBM_TSMSAN_LICENSE_ACCEPTED=true (required)	Specify one or two variables or the installation stops. It also stops if you specify more than two variables. The wizard installs the license agreement for the Tivoli Storage Manager product that is selected. **Tip:** If two products are specified, the wizard checks that one of them is the Tivoli Storage Manager for Storage Area Networks license: IBM_TSMSAN_LICENSE_ACCEPTED=true. If one variable is not, the wizard stops.
For command line: -DINSTANCE_CRED="*instance1 userid1 password1, instance2 userid2 password2*" (required for reinstallation only) For response file: INSTANCE_CRED=*instance1 userid1 password1, instance2 userid2 password2* (required for reinstallation only)	Enter the instance credentials used by the installation wizard to redefine the database instance. Use quotation marks around the credentials when you pass them into the command line. Specify multiple instances by separating them with a comma. **Tip:** An instance cannot be in both the INSTANCE_CRED and the INSTANCE_OMIT parameters. All of the instances that exist when an installation package is reinstalled must be listed in either the INSTANCE_CRED or the INSTANCE_OMIT parameters. Or, the silent installation fails.
For command line:-DINSTANCE_OMIT="*instance3, instance4*" (optional for reinstallation only) For response file: INSTANCE_OMIT=*instance3, instance4* (optional for reinstallation only)	Enter any instances that will not be recreated as part of the installation. Use this variable if you have an instance that exists but is not used. Use it if you have removed the instance user ID, forgotten the password, or otherwise do not want to create the instance as part of a reinstallation. Use quotation marks around the credentials when you pass them into the command line. Specify multiple instances by separating them with a comma. **Tip:** An instance cannot be in both the INSTANCE_CRED and the INSTANCE_OMIT parameters. All of the instances that exist when an installation package is reinstalled must be listed in either the INSTANCE_CRED or the INSTANCE_OMIT parameters. Or, the silent installation fails.
-DINSTALL_DEVICES=1 (optional)	Install the Tivoli Storage Manager device driver.

Table 21. Variables for the silent installation (continued)

Variable	Description
-DINSTALL_LICENSE=1 (required for base packages)	Install the Tivoli Storage Manager server license component. This variable should be specified only if the package being installed includes Tivoli Storage Manager server license files or the installation might fail. This option is typically required only for a first-time installation of the base release package. This option should not be used when installing most fix packs and interim fix packages because they do not include the server licenses.
-DINSTALL_SERVER=1 (optional)	Install the Tivoli Storage Manager server component.
-DINSTALL_STAGENT=1 (optional)	Install the Tivoli Storage Manager storage agent.
-DINSTALL_*language_package*=1 (optional)	Install a specific language package. You can install the following server language-packages during the silent installation, using these variables: • INSTALL_GERMAN • INSTALL_SPANISH • INSTALL_FRENCH • INSTALL_ITALIAN • INSTALL_BRPORTUGUESE • INSTALL_KOREAN • INSTALL_JAPANESE • INSTALL_RUSSIAN • INSTALL_SCHINESE • INSTALL_TCHINESE • INSTALL_ENGLISHUTF8 • INSTALL_GERMANUTF8 • INSTALL_SPANISHUTF8 • INSTALL_FRENCHUTF8 • INSTALL_ITALIANUTF8 • INSTALL_PTBUTF8 • INSTALL_KOREANUTF8 • INSTALL_JAPANESEUTF8 • INSTALL_SCHINESEUTF8 • INSTALL_RUSSIANUTF8 • INSTALL_TCHINESEUTF8 • INSTALL_GBKCH • INSTALL_EUCCH For example, to install the German language package, use this variable: -DINSTALL_GERMAN=1

• To enable a component during silent installation, append it to the `install.bin` command on a single line. For example:

```
./install.bin -i silent
-DIBM_TSM_LICENSE_ACCEPTED=true
-DINSTALL_SERVER=1 -DINSTALL_LICENSE=1
-DINSTALL_ENGLISHUTF8=1
```

Or, for a reinstallation:

```
./install.bin -i silent -DINSTANCE_CRED="tsminst1 tsminst1 tsminst1"
-DINSTANCE_OMIT="tsminst2"
-DIBM_TSM_LICENSE_ACCEPTED=true -DINSTALL_SERVER=1
```

- Alternatively, the component variables can be placed into a response file. The path to this response file can then be passed into the `./install.bin` command. To create this file, use the same variables that are in Table 21 on page 40.

  Remove the -D and separate the options on individual lines. Do not use quotation marks. For example:

```
INSTANCE_CRED=tsminst1 tsminst1 tsminst1
INSTANCE_OMIT=tsminst2
IBM_product_LICENSE_ACCEPTED=true
INSTALL_SERVER=1
INSTALL_SPANISH=1
```

- To use an existing response file, issue the following command:

```
./install.bin -i silent -f response_file
```

  where the *response_file* is the full directory path to a file that you created in the Tivoli Storage Manager installation process. The response file contains variables that you selected during a prior installation, by using the GUI or console wizard. You might see a difference between response files, depending on which installation mode you used (GUI or console).

Remember: If you previously installed a server, ensure that you select the same directory when you install a language package, license, or device driver. If you previously installed a storage agent, ensure that you select the same directory if you return to install a device driver.

Fix any errors before continuing. See the following log for more information:

```
/var/tivoli/tsm
```

After you install a new Tivoli Storage Manager server, you must configure it. See Chapter 3, "Taking the first steps after you install Tivoli Storage Manager," on page 45.

Installing server language packages

Translations for the IBM Tivoli Storage Manager server allow the server to display messages and help in languages other than U.S. English. The translations also allow for the use of locale conventions for date, time, and number formatting.

Server language locales

Use either the default language package option or select another language package to display server messages and help.

This language package is automatically installed for the following default language option for Tivoli Storage Manager server messages and help:

- LANGUAGE en_US

For languages or locales other than the default, install the language package that your installation requires.

You can use the languages shown:

Table 22. Server languages for Linux

LANGUAGE	LANGUAGE option value
Chinese, Simplified	zh_CN
	zh_CN.gb18030
	zh_CN.utf8
Chinese, Traditional	Big5 / Zh_TW
	zh_TW
	zh_TW.utf8
English, United States	en_US
	en_US.utf8
French	fr_FR
	fr_FR.utf8
German	de_DE
	de_DE.utf8
Italian	it_IT
	it_IT.utf8
Japanese	ja_JP
	ja_JP.utf8
Korean	ko_KR
	ko_KR.utf8
Portuguese, Brazilian	pt_BR
	pt_BR.utf8
Russian	ru_RU
	ru_RU.utf8
Spanish	es_ES
	es_ES.utf8
Notes: For more information about setting the LANGUAGE option, see the *Administrator's Reference*.	

Restriction: For Administration Center users, some characters might not be displayed properly if the web browser version is not the same language as the server. If this problem occurs, use a browser version that uses the same language as the server.

Configuring a language package

After you configure a language package, messages and help are shown on the Tivoli Storage Manager in languages other than US English. Installation packages are provided with Tivoli Storage Manager.

To set support for a certain locale, complete one of the following tasks:

- Set the `LANGUAGE` option in the server options file to the name of the locale that you want to use. For example:

    To use the `it_IT` locale, set the `LANGUAGE` option to `it_IT`. See "Server language locales" on page 43.

- Set the `LC_MESSAGES` environment variable to match the value that is set in the server options file. For example, to set the environment variable for Italian, enter the following value:

    `export LC_MESSAGES=it_IT`

If the locale is successfully initialized, it formats the date, time, and number for the server. If the locale is not successfully initialized, the server uses the US English message files and the date, time, and number format.

Chapter 3. Taking the first steps after you install Tivoli Storage Manager

After you install Tivoli Storage Manager Version 6.3 or later, prepare for the configuration. Using the configuration wizard is the preferred method of configuring the Tivoli Storage Manager instance.
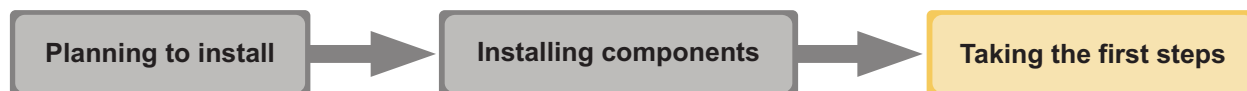
Figure 3. You are in the configuring the Tivoli Storage Manager server section

Configure the Tivoli Storage Manager server instance by completing the following steps:

1. Update the kernel parameter values.

   See "Tuning kernel parameters" on page 46.

2. Create the directories and user ID for the server instance. See "Creating the user ID and directories for the server instance" on page 48.

3. Configure a Tivoli Storage Manager instance. Select one of the following options:

   - Use the Tivoli Storage Manager configuration wizard, the preferred method. See "Configuring Tivoli Storage Manager using the configuration wizard" on page 50.

   - Use the Tivoli Storage Manager configuration wizard in the Administration Center. See "Configuring Tivoli Storage Manager using the Administration Center" on page 52.

   - Manually configure the new Tivoli Storage Manager instance. See "Configuring the server instance manually" on page 54. Complete the following steps during a manual configuration.

     a. Set up your directories and create the Tivoli Storage Manager instance. See "Creating the server instance" on page 54.

     b. Create a new server options file by copying the sample file to set up communications between the server and clients. See "Configuring server and client communications" on page 55.

     c. Issue the DSMSERV FORMAT command to format the database. See "Formatting the database and log" on page 59.

     d. Configure your system for database backup. See "Preparing the database manager for backup" on page 50.

4. Configure options to control when database reorganization runs. See "Configuring server options for server database maintenance" on page 61.

5. Configure access rights to deployment engine files. See "Configuring access rights to deployment engine files" on page 62

6. Start the Tivoli Storage Manager server instance if it is not already started.

   See "Starting the server instance on AIX, HP-UX, Linux, and Solaris systems" on page 63.

7. Register your license. See "Registering licenses" on page 68.

8. Prepare your system for database backups. See "Preparing the system for backups" on page 68.
9. Monitor the server. See "Monitoring the server" on page 69.

Tuning kernel parameters

For IBM Tivoli Storage Manager and DB2 to install and operate correctly on Linux, you must update the kernel configuration parameters.

If you do not update these parameters, the installation of DB2 and Tivoli Storage Manager might fail. Even if installation is successful, operational problems might occur if you do not set parameter values.

Updating kernel parameters

DB2 automatically increases interprocess communication (IPC) kernel parameter values to the preferred settings.

To update the kernel parameters on Linux servers, complete the following steps:

1. Issue the `ipcs -l` command to list the parameter values.
2. Analyze the results to determine whether any changes are required for your system. If changes are required, you can set the parameter in the `/etc/sysctl.conf` file. The parameter value is applied when the system starts.

For Red Hat Enterprise Linux 6 (RHEL6), you must set the `kernel.shmmax` parameter in the `/etc/sysctl.conf` file before automatically starting the Tivoli Storage Manager server on system startup.

The address space layout randomization (ASLR) security technique for Linux might cause DB2 process failures. To change the setting, enter the following parameter in the `/etc/sysctl.conf` file and restart the system:

`kernel.randomize_va_space=0`

For details about the Linux ASLR and DB2, see http://www.ibm.com/support/docview.wss?uid=swg21365583.

For details about the DB2 database for Linux, see the DB2 information center: http://pic.dhe.ibm.com/infocenter/db2luw/v9r7.

Suggested minimum values

Ensure that the values for kernel parameters are sufficient to prevent operational problems from occurring when running the Tivoli Storage Manager server.

The following table contains the suggested minimum values for running DB2 on your system. To run Tivoli Storage Manager with DB2, the values might need to be increased above the minimum values specified here. In addition to implementing the suggestions in this table, other changes are required to run both Tivoli Storage Manager and DB2. For details, see http://www.ibm.com/support/docview.wss?uid=swg27015156.

Parameter	Description	Preferred value
kernel.shmmni	See note. The maximum number of segments	$256 \times size\ of\ RAM$ *in GB*

Parameter	Description	Preferred value
kernel.shmmax	See note. The maximum size of a shared memory segment (bytes)	*size of RAM in bytes*
kernel.shmall	See note. The maximum allocation of shared memory pages (pages)	*2 × size of RAM in bytes* (setting is in 4 KB pages)
kernel.sem (SEMMNI)	See note. The maximum number of arrays	*256 × size of RAM in GB*
kernel.sem (SEMMSL)	See note. The maximum semaphores per array	250
kernel.sem (SEMMNS)	See note. The maximum semaphores per system	256,000
kernel.sem (SEMOPM)	See note. The maximum operations per semaphore call	32
kernel.msgmni	See note. The maximum number of system-wide message queues	*1024 × size of RAM in GB*
kernel.msgmax	See note. The maximum size of messages (bytes)	65,536
kernel.msgmnb	See note. The default maximum size of queue (bytes)	65,536
kernel.randomize_va_space	The `kernel.randomize_va_space` parameter configures the kernels use of memory ASLR. When you set the value to 0, `kernel.randomize_va_space=0`, it disables ASLR. DB2 data servers rely on fixed addresses for certain shared memory objects, and the ASLR can cause errors for some activities. To learn more details about the Linux ASLR and DB2, see the technote at: http://www.ibm.com/support/docview.wss?uid=swg21365583.	0
vm.swappiness	The `vm.swappiness` parameter defines whether the kernel can swap application memory out of physical random access memory (RAM). For more information about kernel parameters, see the DB2 information center.	0
vm.overcommit_memory	The `vm.overcommit_memory` parameter influences how much virtual memory the kernel can permit to be allocated. For more information about kernel parameters, see the DB2 information center.	0
Note: For Linux, DB2 automatically increases interprocess communication (IPC) kernel parameter values to the preferred settings.		

Creating the user ID and directories for the server instance

Create the user ID for the Tivoli Storage Manager server instance and create the directories that the Tivoli Storage Manager server instance needs for database and recovery logs.

Review the information about planning space for the server before completing this task. See "Worksheets for planning details for the Tivoli Storage Manager server" on page 14.

1. Create the user ID that will own the server instance. You use this user ID when you create the server instance in a later step.

   Create a user ID and group that will be the owner of the Tivoli Storage Manager server instance.

   a. The following commands can be run from an administrative user ID that will set up the user and group. Create the user ID and group in the home directory of the user.

      Restriction: In the user ID, only lowercase letters (a-z), numerals (0-9), and the underscore character (_) can be used. The user ID and group name must comply with the following rules:
      - The length must be 8 characters or less.
      - The user ID and group name cannot start with *ibm*, *sql*, *sys*, or a numeral.
      - The user ID and group name cannot be *user*, *admin*, *guest*, *public*, *local*, or any SQL reserved word.

      For example, create user ID `tsminst1` in group `tsmsrvrs`. The following examples show how to create this user ID and group using operating system commands.

      ```
      groupadd tsmsrvrs
      useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
      passwd tsminst1
      ```

   b. Log off, then log in to your system. Change to the user account that you just created. Use an interactive login program, such as telnet, so that you are prompted for the password and can change it if necessary.

2. Create directories that the server requires. Ensure that you are logged in under the new user ID you just created.

   Create empty directories for each of the items shown in the following table. Mount the associated storage to each directory for the active log, archive log and database directories.

Item	Example commands for creating the directories	Your directories
The *instance directory* for the server, which is a directory that will contain files specifically for this server instance (the server options file and other server-specific files)	`mkdir /tsminst1`	

Create empty directories for each of the items shown in the following table. Mount the associated storage to each directory for the active log, archive log and database directories.

Item	Example commands for creating the directories	Your directories

The database directories	`mkdir /home/user_ID/tsmdb001`
	`mkdir /home/user_ID/tsmdb002`
	`mkdir /home/user_ID/tsmdb003`
	`mkdir /home/user_ID/tsmdb004`	

Active log directory	`mkdir /home/user_ID/tsmlog`	
Archive log directory	`mkdir /home/user_ID/` `tsmarchlog`	
Optional: Directory for the log mirror for the active log	`mkdir /home/user_ID/` `tsmlogmirror`	
Optional: Secondary archive log directory (failover location for archive log)	`mkdir /home/user_ID/` `tsmarchlogfailover`	

When a server is initially created, with the **DSMSERV FORMAT** utility or with the configuration wizard, a server database and recovery log are created. In addition, files are created to hold database information that is used by the database manager.

3. If a configuration profile does not exist for the user ID, create the file. For example, create a `.profile` file if you are using the Korn shell (ksh).

4. Log off the new user ID.

Configuring Tivoli Storage Manager

After you have installed Tivoli Storage Manager Version 6.3 or later and prepared for the configuration, configure the Tivoli Storage Manager server instance.

Configure a Tivoli Storage Manager server instance by selecting one of the following options:

- Use the Tivoli Storage Manager configuration wizard on your local system. See "Configuring Tivoli Storage Manager using the configuration wizard" on page 50.
- Use the Tivoli Storage Manager configuration wizard in the Administration Center. See "Configuring Tivoli Storage Manager using the Administration Center" on page 52.
- Manually configure the new Tivoli Storage Manager instance. See "Configuring the server instance manually" on page 54. Complete the following steps during a manual configuration.
  1. Set up the directories and create the Tivoli Storage Manager instance. See "Creating the server instance" on page 54.
  2. Create a new server options file by copying the sample file in order to set up communications between the Tivoli Storage Manager server and clients. See "Configuring server and client communications" on page 55.
  3. Issue the DSMSERV FORMAT command to format the database. See "Formatting the database and log" on page 59.
  4. Configure your system for database backup. See "Preparing the database manager for backup" on page 50.

Configuring Tivoli Storage Manager using the configuration wizard

The wizard offers a guided approach to configuring a server. By using the graphical user interface (GUI), you can avoid some configuration steps that are complex when done manually. Start the wizard on the system where you installed the Tivoli Storage Manager server program.

Before beginning the configuration wizard, you must complete all preceding steps to prepare for the configuration, including installing Tivoli Storage Manager, creating the database and log directories, and creating the directories and user ID for the server instance.

1. Ensure that the following requirements are met:

   - The system where you installed Tivoli Storage Manager must have the X Window System client. You must also be running an X Window System server on your desktop.
   - The system must have one of the following protocols enabled. Ensure that the port that the protocol uses is not blocked by a firewall.
     - Secure Shell (SSH). Ensure that the port is set to the default value, 22. Also ensure that the SSH daemon service has access rights for connecting to the system by using `localhost`.
     - Remote shell (RSH).
     - Remote Execution Protocol (REXEC).
   - You must be able to log in to Tivoli Storage Manager with the user ID that you created for the server instance, by using the SSH, RSH, or REXEC protocol. When using the wizard, you must provide this user ID and password to access that system.

2. Start the local version of the wizard:

   Open the dsmicfgx program in the `/opt/tivoli/tsm/server/bin` directory. This wizard can only be run as a root user.

   Follow the instructions to complete the configuration. The wizard can be stopped and restarted, but the server is not operational until the entire configuration process is complete.

Preparing the database manager for backup

To back up the data in the database to Tivoli Storage Manager, you must enable the database manager and configure the Tivoli Storage Manager application programming interface (API).

If you use the Tivoli Storage Manager configuration wizard to create a Tivoli Storage Manager server instance, you do not have to complete these steps. If you are configuring an instance manually, complete the following steps before issuing either the BACKUP DB or the RESTORE DB commands.

Attention: If the database is unusable, the entire Tivoli Storage Manager server is unavailable. If a database is lost and cannot be recovered, it might be difficult or impossible to recover data managed by that server. Therefore, it is critically important to back up the database. However, even without the database, fragments of data or complete files might easily be read from storage pool volumes that are not encrypted. Even if data is not recovered, security can be compromised. For this reason, sensitive data must always be encrypted by the Tivoli Storage Manager client or the storage device, unless the storage media is physically secured.

In the following commands, the examples use `tsminst1` for the server instance user ID and /home/tsminst1/tsminst1 for the Tivoli Storage Manager server instance directory. Replace these values with your actual values in the commands.

1. Set the Tivoli Storage Manager API environment-variable configuration for the database instance:

   a. Log in using the `tsminst1` user ID.

   b. When user `tsminst1` is logged in, ensure that the DB2 environment is properly initialized. The DB2 environment is initialized by running the /home/tsminst1/sqllib/db2profile script, which normally runs automatically from the profile of the user ID. If /home/tsminst1/.profile does not run the db2profile script,add the following lines to /home/tsminst1/.profile:

      ```
      if [ -f /home/tsminst1/sqllib/db2profile ]; then
            . /home/tsminst1/sqllib/db2profile
         fi
      ```

   c. In the `userprofile` file in the /home/tsminst1/sqllib directory, add or update the following lines:

      Korn or Bash shell:

      ```
      export DSMI_CONFIG=/home/tsminst1/tsminst1/tsmdbmgr.opt
      export DSMI_DIR=/opt/tivoli/tsm/client/api/bin64
      export DSMI_LOG=/home/tsminst1/tsminst1
      ```

      Bourne shell:

      ```
      DSMI_CONFIG=/home/tsminst1/tsminst1/tsmdbmgr.opt
      DSMI_DIR=/opt/tivoli/tsm/client/api/bin64
      DSMI_LOG=/home/tsminst1/tsminst1
      export DSMI_CONFIG DSMI_DIR DSMI_LOG
      ```

      C shell:

      ```
      setenv DSMI_CONFIG=/home/tsminst1/tsminst1/tsmdbmgr.opt
      setenv DSMI_DIR=/opt/tivoli/tsm/client/api/bin64
      setenv DSMI_LOG=/home/tsminst1/tsminst1
      ```

2. Log out and log in again as tsminst1, or issue this command:

   ```
   . ~/.profile
   ```

   Tip: Ensure that you enter a space after the initial dot (.) character.

3. Create a file called `tsmdbmgr.opt` in the /tsminst1 directory and add the following line:

   ```
   SERVERNAME TSMDBMGR_TSMINST1
   ```

   Remember: The name that you use must match your server instance name.

4. Add the following lines to the Tivoli Storage Manager API dsm.sys configuration file. The dsm.sys configuration file is in the following default location:

   ```
   /opt/tivoli/tsm/client/api/bin64/dsm.sys
   ```

   Avoid placing the server name, TSMDBMGR_TSMINST1, first in dsm.sys because it should not be the system-wide default. In this example, the added lines are after the stanza for server_a.

   ```
   Servername server_a
   COMMMethod TCPip
   TCPPort 1500
   TCPServeraddress node.domain.company.COM


   servername TSMDBMGR_TSMINST1
   commmethod tcpip
   ```

```
tcpserveraddr localhost
tcpport 1500
passwordaccess generate
passworddir /home/tsminst1/tsminst1
errorlogname /home/tsminst1/tsminst1/tsmdbmgr.log
nodename $$_TSMDBMGR_$$
```

> **Tip:** Ensure that you enter the same `tcpport` as the server is using. This is specified in the `dsmserv.opt` file.

5. Stop and start the database instance:

   a. Stop DB2:

      ```
      db2stop
      ```

   b. Start DB2:

      ```
      db2start
      ```

6. Set the API password:

   a. Ensure that the Tivoli Storage Manager server is started. See "Starting the server instance on AIX, HP-UX, Linux, and Solaris systems" on page 63 for the details.

   b. Log in using the root user ID.

   c. Source the database manager profile by issuing the following command. Ensure that you enter a dot, a space, and the path to the `db2profile` file. If you do not enter the space, the database backup fails.

      ```
      . /home/tsminst1/sqllib/db2profile
      ```

   d. Change the API password. Use this command:

      ```
      /home/tsminst1/sqllib/adsm/dsmapipw
      ```

   e. When prompted by the dsmapipw command, specify TSMDBMGR as both the original and new password.

   f. Enter this operating system command:

      ```
      rm /home/tsminst1/tsminst1/tsmdbmgr.log
      ```

Configuring Tivoli Storage Manager using the Administration Center

The Administration Center wizard offers a guided approach to configuring a server. By using this wizard, you can avoid some configuration steps that are complex when done manually.

Before beginning the configuration wizard, you must complete all preceding steps to prepare for the configuration. The preceding steps include installing the Version 6.3 or later server program, creating the database and log directories, and creating the directories and user ID for the server instance.

1. Ensure that the following requirements are met:

   - The system must have one of the following protocols enabled. Ensure that the port that the protocol uses is not blocked by a firewall.
     - Secure Shell (SSH). Ensure that the port is set to the default value, 22. Also ensure that the SSH daemon service has access rights for connecting to the system by using `localhost`.
     - Remote shell (RSH).
     - Remote Execution Protocol (REXEC).
   - You must be able to log in to the Version 6.3 or later system with the user ID that you created for the server instance, by using the SSH,

RSH, or REXEC protocol. When using the wizard, you must provide this user ID and password to access that system.

2. Open the Administration Center by entering one of the following addresses in a supported web browser:

```
http://workstation_name:non_secure_port/ibm/console
```

Or:

```
https://workstation_name:secure_port/ibm/console
```

The *workstation_name* is the network name or IP address of the computer on which you installed the Administration Center. The *non_secure_port* is the HTTP port and the *secure_port* is the HTTPS port.

Attention: Use the port number that was shown in the summary panel of the installation wizard, which might be different from the port that you specified in the wizard. If you use an incorrect port, no warning messages are shown but you are not able to complete all Administration Center tasks.

The default HTTP port is 16310. The default HTTPS port is 16311. If you use a different port number from the default, the secure port typically appears as the non-secure port plus 1.

Look in the following file to see the port that is being used. In this file, **WC_defaulthost** contains the value for the HTTP port and **WC_adminhost_secure** contains the value for the HTTPS port.

   TIP_HOME/properties/TIPPortDef.properties

where *TIP_HOME* is the home directory for the Tivoli Integrated Portal installation.

   The default for *TIP_HOME* is /opt/IBM/tivoli/tipv2.

Tips:
* If you use http://*workstation_name*:16310/ibm/console to connect to the Administration Center, you are automatically redirected to the secure port and address.
* A file named Tivoli_Storage_Manager_Administration_Center.htm is created in the tsmac directory of the Administration Center installation directory. Open this file in a web browser to automatically connect to the Administration Center.

3. Log in, using the Tivoli Integrated Portal user ID and password you created during the installation. After you successfully log in, the Tivoli Integrated Portal welcome page is displayed. Expand the Tivoli Storage Manager folder in the Work Items list and click **Getting Started** to display the Tivoli Storage Manager welcome page. This page provides instructions for using the Administration Center.

4. Go to **Tivoli Storage Manager** > **Manage Servers** and use the menu to find the Create Server Instance wizard.

5. After you open the Create Server Instance wizard, a list of tasks for setting up a Tivoli Storage Manager server instance displays. Click **Next** to continue.

6. Enter the TCP/IP server address and system administrator's (root user ID) logon credentials, and click **Next**.

7. Specify the instance and server configuration information, by using the wizard to guide you.

8. Verify the settings on the Summary page. After you have verified the information, click **Finish**. The Tivoli Storage Manager instance is configured in steps as indicated in the progress bar on the following page.

After the configuration is finished, the wizard exits to the Manage Servers page where you can find your new server.

Configuring the server instance manually

After installing Tivoli Storage Manager Version 6.3 or later, you can configure Tivoli Storage Manager manually instead of using the configuration wizard.

Creating the server instance

Create a Tivoli Storage Manager instance by issuing the **db2icrt** command.

You can have one or more server instances on one workstation.

Important: Before you run the **db2icrt** command, verify the following items:

- The home directory for the user (/home/tsminst1) exists. If there is no home directory, you must create it.

  The instance directory stores the following core files that are generated by the Tivoli Storage Manager server:

  – The server options file, dsmserv.opt

  – The server key database file, cert.kdb, and the .arm files (used by clients and other servers to import the Secure Sockets Layer certificates of the server)

  – Device configuration file, if the DEVCONFIG server option does not specify a fully qualified name

  – Volume history file, if the VOLUMEHISTORY server option does not specify a fully qualified name

  – Volumes for **DEVTYPE=FILE** storage pools, if the directory for the device class is not fully specified, or not fully qualified

  – User exits

  – Trace output (if not fully qualified)

- A shell configuration file (for example, .profile) exists in the home directory. The root user and instance user ID must have write permission to this file. For more information, see the section on Linux and UNIX environment variable settings in the DB2 Information Center (http://pic.dhe.ibm.com/infocenter/db2luw/v9r7).

1. Log in using the root user ID and create a Tivoli Storage Manager instance. The name of the instance must be the same name as the user that owns the instance. Use the **db2icrt** command and enter the command on one line:

   ```
   /opt/tivoli/tsm/db2/instance/db2icrt -a server -s ese -u
   instance_name instance_name
   ```

   For example, if your user ID for this instance is tsminst1, use the following command to create the instance. Enter the command on one line.

   ```
   /opt/tivoli/tsm/db2/instance/db2icrt -a server -s ese -u
   tsminst1 tsminst1
   ```

Remember: From this point on, use this new user ID when configuring your Tivoli Storage Manager server. Log out of the root user ID and log in under the new instance-user ID.

2. Change the default directory for the database to be the same as the instance directory for the server. If you have multiple servers, log in under the instance ID for each server. Issue this command:

```
db2 update dbm cfg using dftdbpath instance_directory
```

For example:

```
db2 update dbm cfg using dftdbpath /tsminst1
```

3. Modify the library path to use the version of the IBM Global Security Kit (GSKit) that is installed with the Tivoli Storage Manager server:

   You must update the following files to set the library path when DB2 or the Tivoli Storage Manager server are started:

   instance_directory/sqllib/usercshrc

   instance_directory/sqllib/userprofile

   For the *instance_directory*/sqllib/usercshrc file, add the following lines:

```
setenv LD_LIBRARY_PATH /usr/local/ibm/gsk8_64/lib64:$LD_LIBRARY_PATH
```

   For the *instance_directory*/sqllib/userprofile file, add the following lines:

```
LD_LIBRARY_PATH=/usr/local/ibm/gsk8_64/lib64:$LD_LIBRARY_PATH
export LD_LIBRARY_PATH
```

   Verify the library path settings and that the GSKit is version 8.0.14.14 or later. Issue the following commands:

```
echo $LD_LIBRARY_PATH
gsk8capicmd_64 -version
gsk8ver_64
```

   If your GSKit version is not 8.0.14.14 or later, you must reinstall the Tivoli Storage Manager server. The reinstallation ensures that the correct GSKit version is available.

4. Create a new server options file. See "Configuring server and client communications."

Configuring server and client communications

A default sample server options file, dsmserv.opt.smp, is created during Tivoli Storage Manager installation in the /opt/tivoli/tsm/server/bin directory. You must set up communications between the server and clients by creating a new server options file. To do so, copy the sample file to the directory for the server instance.

Ensure that you have a server instance directory, for example /tsminst1/instance1, and copy the sample file to this directory. Name the new file dsmserv.opt and edit the options. Complete this set-up before you initialize the server database (see "Formatting the database and log" on page 59). Each sample or default entry in the sample options file is a comment, a line beginning with an asterisk (*). Options are not case-sensitive and one or more blank spaces are allowed between keywords and values.

When editing the options file, follow these guidelines:
- Remove the asterisk at the beginning of the line to activate an option.
- Begin entering the options in any column.
- Enter only one option per line, and the option must be on only one line.

- If you make multiple entries for a keyword, the Tivoli Storage Manager server uses the last entry.

If you change the server options file, you must restart the server for the changes to take effect. See the *Administrator's Reference* for a description of all server options.

You can specify one or more of the following communication methods:
- TCP/IP Version 4 or Version 6
- Shared memory
- Simple network management protocol (SNMP) DPI
- Secure Sockets Layer (SSL)

   Note: You can authenticate passwords with the LDAP directory server, or authenticate passwords with the Tivoli Storage Manager server. Passwords that are authenticated with the LDAP directory server can provide enhanced system security. For details, see the managing passwords and logon procedures section in the *Administrator's Guide*.

Setting TCP/IP options:

Select from a range of TCP/IP options for the Tivoli Storage Manager server or retain the default.

The following is an example of a list of TCP/IP options you can use to set up your system.

```
commmethod       tcpip
  tcpport        1500
  tcpwindowsize  0
  tcpnodelay     yes
```

Tip: You can use TCP/IP Version 4, Version 6, or both.

TCPPORT

   The server TCP/IP port address. The default value is 1500.

TCPWINDOWSIZE

   Specifies the size of the TCP/IP buffer that is used when sending or receiving data. The window size that is used in a session is the smaller of the server and client window sizes. Larger window sizes use additional memory but can improve performance.

   You can specify an integer from 0 to 2048. To use the default window size for the operating system, specify 0.

TCPNODELAY

   Specifies whether or not the server sends small messages or lets TCP/IP buffer the messages. Sending small messages can improve throughput but increases the number of packets sent over the network. Specify YES to send small messages or NO to let TCP/IP buffer them. The default is YES.

TCPADMINPORT

   Specifies the port number on which the server TCP/IP communication driver is to wait for requests other than client sessions. The default value is 1500.

SSLTCPPORT

   (SSL-only) Specifies the Secure Sockets Layer (SSL) port number on which

the server TCP/IP communication driver waits for requests for SSL-enabled sessions for the command-line backup-archive client and the command-line administrative client.

SSLTCPADMINPORT

Specifies the port address on which the server TCP/IP communication driver waits for requests for SSL-enabled sessions for the command-line administrative client.

Setting shared memory options:

You can use shared memory communications between clients and servers on the same system. To use shared memory, TCP/IP Version 4 must be installed on the system.

The following example shows a shared memory setting:

```
commmethod      sharedmem
   shmport      1510
```

In this example, SHMPORT specifies the TCP/IP port address of a server when using shared memory. Use the SHMPORT option to specify a different TCP/IP port. The default port address is 1510.

COMMMETHOD can be used multiple times in the IBM Tivoli Storage Manager server options file, with a different value each time. For example, the following example is possible:

```
commmethod tcpip
commmethod sharedmem
```

You might receive the following message from the server when using shared memory:

```
ANR9999D shmcomm.c(1598): ThreadId<39>
Error from msgget (2), errno = 28
```

The message means that a message queue must be created but the system limit for the maximum number of message queues (MSGMNI) would be exceeded.

To find out the maximum number of message queues (MSGMNI) on your system, issue the following command:

```
cat /proc/sys/kernel/msgmni
```

To increase the MSGMNI value on your system, issue the following command:

```
sysctl -w kernel.msgmni=n
```

where **n** is the maximum number of message queues that you want the system to allow.

Setting SNMP DPI subagent options:

Tivoli Storage Manager implements a simple network management protocol (SNMP) subagent. You can configure the SNMP subagent to send traps to an SNMP manager, such as NetView®, and to provide support for a Management Information Base (MIB).

For details about configuring SNMP for use with Tivoli Storage Manager, see the *Administrator's Guide*.

The subagent communicates with the snmp daemon, which in turn communicates with a management application. The snmp daemon must support the DPI protocol. Agents are available on AIX. The subagent process is separate from the Tivoli Storage Manager server process, but the subagent gets its information from a server options file. When the SNMP management application is enabled, it can get information and messages from servers.

Use the following SNMP DPI options as an example of a SNMP setting. You must specify the COMMMETHOD option. For details about the other options, see the *Administrator's Reference*.

```
commmethod                    snmp
   snmpheartbeatinterval      5
   snmpmessagecategory        severity
```

Setting Secure Sockets Layer options:

You can add more protection for your data and passwords by using Secure Sockets Layer (SSL).

SSL is the standard technology for creating encrypted sessions between servers and clients. SSL provides a secure channel for servers and clients to communicate over open communication paths. With SSL, the identity of the server is verified through the use of digital certificates.

To ensure better system performance, use SSL only for sessions when it is needed. Consider adding additional processor resources on the Tivoli Storage Manager server to manage the increased requirements.

Refer to setting up Transport Layer Security (TLS) in the *Administrator's Guide*.

Formatting the database and log

Use the **DSMSERV FORMAT** utility to initialize a server instance. No other server activity is allowed while initializing the database and recovery log.

After you set up server communications, you are ready to initialize the database. Ensure that you log in by using the instance user ID. Do not place the directories on file systems that might run out of space. If certain directories (for example, the archive log) become unavailable or full, the server stops. See "Capacity planning" on page 15 for more details.

For optimal performance and to facilitate I/O, specify at least two equally sized containers or Logical Unit Numbers (LUNs) for the database. See *Optimizing Performance* for more information about the configuration of directories for the database. In addition, each active log and archive log should have its own container or LUN.

Setting the server code page

Set the DB2CODEPAGE system environment variable to 819 for each server instance. Before you issue the **DSMSERV LOADFORMAT** command, log on to the system as the server instance owner and issue this command:

```
db2set -i instance_name DB2CODEPAGE=819
```

For example:

```
db2set -i tsminst1 DB2CODEPAGE=819
```

Initializing a server instance

Use the **DSMSERV FORMAT** utility to initialize a server instance. For example, issue the following command:

```
dsmserv format dbdir=/tsmdb001 activelogsize=8192
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

Tip: If DB2 does not start after you issue the **DSMSERV FORMAT** command, you might need to disable the file system mount option NOSUID. If this option is set on the file system that contains the DB2 instance owner directory, or on any file system that contains the DB2 database, active logs, archive logs, failover logs, or mirrored logs, the option must be disabled to start the system.

After you disable the NOSUID option, remount the file system and then start DB2 by issuing the following command:

```
db2start
```

For more information, see the *Administrator's Reference*.

Preparing the database manager for backup

To back up the data in the database to Tivoli Storage Manager, you must enable the database manager and configure the Tivoli Storage Manager application programming interface (API).

If you use the Tivoli Storage Manager configuration wizard to create a Tivoli Storage Manager server instance, you do not have to complete these steps. If you are configuring an instance manually, complete the following steps before issuing either the BACKUP DB or the RESTORE DB commands.

Installing the Tivoli Storage Manager server

Attention: If the database is unusable, the entire Tivoli Storage Manager server is unavailable. If a database is lost and cannot be recovered, it might be difficult or impossible to recover data managed by that server. Therefore, it is critically important to back up the database. However, even without the database, fragments of data or complete files might easily be read from storage pool volumes that are not encrypted. Even if data is not recovered, security can be compromised. For this reason, sensitive data must always be encrypted by the Tivoli Storage Manager client or the storage device, unless the storage media is physically secured.

In the following commands, the examples use `tsminst1` for the server instance user ID and `/home/tsminst1/tsminst1` for the Tivoli Storage Manager server instance directory. Replace these values with your actual values in the commands.

1. Set the Tivoli Storage Manager API environment-variable configuration for the database instance:

   a. Log in using the `tsminst1` user ID.

   b. When user `tsminst1` is logged in, ensure that the DB2 environment is properly initialized. The DB2 environment is initialized by running the `/home/tsminst1/sqllib/db2profile` script, which normally runs automatically from the profile of the user ID. If `/home/tsminst1/.profile` does not run the db2profile script,add the following lines to `/home/tsminst1/.profile`:

      ```
      if [ -f /home/tsminst1/sqllib/db2profile ]; then
          . /home/tsminst1/sqllib/db2profile
        fi
      ```

   c. In the `userprofile` file in the `/home/tsminst1/sqllib` directory, add or update the following lines:

      Korn or Bash shell:

      ```
      export DSMI_CONFIG=/home/tsminst1/tsminst1/tsmdbmgr.opt
      export DSMI_DIR=/opt/tivoli/tsm/client/api/bin64
      export DSMI_LOG=/home/tsminst1/tsminst1
      ```

      Bourne shell:

      ```
      DSMI_CONFIG=/home/tsminst1/tsminst1/tsmdbmgr.opt
      DSMI_DIR=/opt/tivoli/tsm/client/api/bin64
      DSMI_LOG=/home/tsminst1/tsminst1
      export DSMI_CONFIG DSMI_DIR DSMI_LOG
      ```

      C shell:

      ```
      setenv DSMI_CONFIG=/home/tsminst1/tsminst1/tsmdbmgr.opt
      setenv DSMI_DIR=/opt/tivoli/tsm/client/api/bin64
      setenv DSMI_LOG=/home/tsminst1/tsminst1
      ```

2. Log out and log in again as tsminst1, or issue this command:

   ```
   . ~/.profile
   ```

   Tip: Ensure that you enter a space after the initial dot (.) character.

3. Create a file called `tsmdbmgr.opt` in the `/tsminst1` directory and add the following line:

   ```
   SERVERNAME TSMDBMGR_TSMINST1
   ```

   Remember: The name that you use must match your server instance name.

4. Add the following lines to the Tivoli Storage Manager API dsm.sys configuration file. The dsm.sys configuration file is in the following default location:

   ```
   /opt/tivoli/tsm/client/api/bin64/dsm.sys
   ```

Avoid placing the server name, TSMDBMGR_TSMINST1, first in dsm.sys because it should not be the system-wide default. In this example, the added lines are after the stanza for server_a.

```
Servername server_a
COMMMethod TCPip
TCPPort 1500
TCPServeraddress node.domain.company.COM


servername TSMDBMGR_TSMINST1
commmethod tcpip
tcpserveraddr localhost
tcpport 1500
passwordaccess generate
passworddir /home/tsminst1/tsminst1
errorlogname /home/tsminst1/tsminst1/tsmdbmgr.log
nodename $$_TSMDBMGR_$$
```

Tip: Ensure that you enter the same `tcpport` as the server is using. This is specified in the `dsmserv.opt` file.

5. Stop and start the database instance:

   a. Stop DB2:

      `db2stop`

   b. Start DB2:

      `db2start`

6. Set the API password:

   a. Ensure that the Tivoli Storage Manager server is started. See "Starting the server instance on AIX, HP-UX, Linux, and Solaris systems" on page 63 for the details.

   b. Log in using the root user ID.

   c. Source the database manager profile by issuing the following command. Ensure that you enter a dot, a space, and the path to the `db2profile` file. If you do not enter the space, the database backup fails.

      `. /home/tsminst1/sqllib/db2profile`

   d. Change the API password. Use this command:

      `/home/tsminst1/sqllib/adsm/dsmapipw`

   e. When prompted by the dsmapipw command, specify TSMDBMGR as both the original and new password.

   f. Enter this operating system command:

      `rm /home/tsminst1/tsminst1/tsmdbmgr.log`

Configuring server options for server database maintenance

To help avoid problems with database growth and server performance, the server automatically monitors its database tables and reorganizes them when needed. Before starting the server for production use, set server options to control when reorganization runs. If you plan to use deduplication, ensure that the option to run index reorganization is enabled.

Table and index reorganization requires significant processor resources, active log space, and archive log space. Because database backup takes precedence over reorganization, select the time and duration for reorganization to ensure that the processes do not overlap and reorganization can complete. For more information about scheduling reorganization, see *Administrator's Guide*.

If you update these server options while the server is running, you must stop and restart the server before the updated values take effect.

1. Modify the server options.

   Edit the server options file, `dsmserv.opt`, in the server instance directory. Follow these guidelines when editing the server options file:

   - To activate an option, remove the asterisk at the beginning of the line.
   - Begin entering an option on any line.
   - Enter only one option per line. The entire option with its value must be on one line.
   - If you have multiple entries for an option in the file, the server uses the last entry.
   - To view available server options, see the sample file, `dsmserv.opt.smp`, in the `/opt/tivoli/tsm/server/bin` directory.

2. If you plan to use deduplication, enable the **ALLOWREORGINDEX** server option. Add the following option and value to the server options file:

   `allowreorgindex yes`

3. Set two server options that control when reorganization starts and how long it runs. Select a time and duration so that reorganization runs when you expect that the server is least busy. These server options control both table and index reorganization processes.

   a. Set the time for reorganization to start by using the **REORGBEGINTIME** server option. Specify the time by using the 24-hour system. For example, to set the start time for reorganization as 8:30 p.m., specify the following option and value in the server options file:

      `reorgbegintime 20:30`

   b. Set the interval during which the server can start reorganization. For example, to specify that the server can start reorganization for four hours after the time set by the **REORGBEGINTIME** server option, specify the following option and value in the server options file:

      `reorgduration 4`

4. If the server was running while you updated the server options file, stop and restart the server.

Configuring access rights to deployment engine files

When you install the Tivoli Storage Manager server, the deployment engine is installed automatically on the same system. The deployment engine installs Tivoli Storage Manager components. You can configure access rights to the files that are controlled by the deployment engine.

The deployment engine is installed globally by using the root user ID. The deployment engine makes it possible for administrators with non-root user IDs to upgrade and install the components that were installed by the deployment engine. The deployment engine also makes certain files accessible to all system users.

The following table describes how to set access levels for the files that are controlled by the deployment engine. To view, set, or refresh the access level, issue the specified command on one line.

Table 23. Commands for setting access rights to files that are controlled by the deployment engine

Action	Description	Command/File path
View access level	Shows the current access level	`/usr/ibm/common/acsi/bin/de_security.sh`
Set single-user write access	Grants only the user who installed the deployment engine write access to the deployment engine files	`/usr/ibm/common/acsi/bin/de_security.sh -singleUser`
Set group access	Grants the current user and members of the specified group write access to the deployment engine files	`/usr/ibm/common/acsi/bin/de_security.sh -group` *groupname*
Set global access rights	Grants all users write access to the deployment engine files	`/usr/ibm/common/acsi/bin/de_security.sh -global`
Refresh access levels	Shows updated access levels	`/usr/ibm/common/acsi/bin/de_security.sh -refreshDB`

Starting the server instance on AIX, HP-UX, Linux, and Solaris systems

Verify that the server instance is correctly set up by starting the Tivoli Storage Manager instance. You can start the server when logged in to the system with the user ID that you created for this instance. Before you start the server, ensure that the server options file, `dsmserv.opt`, exists and that ulimit values are set correctly.

Verify that the `dsmserv.opt` file exists in the server instance directory, and that the file includes parameters for the server instance. If you have not yet created a `dsmserv.opt` file, see "Configuring server and client communications" on page 55.

Starting the server is an operating system-level operation and has certain restrictions. If you do not have the permissions to use the dsmserv program, you cannot start it. If you do not have authority to read/write files in the instance directory, you cannot start that instance of the server. If you do not have authority for the server DB2 database, you cannot start that instance of the server.

Important: When you start the Tivoli Storage Manager server, the server attempts to change certain ulimit values to unlimited. In general, this server action helps to ensure optimal performance and facilitates debugging. If you are a non-root user when you start the server, attempts to change the ulimit values might fail. To ensure correct server operation if you are running the server as a non-root user, set the ulimit values as high as possible before you start the server.

This task includes setting DB2 user limits as high as possible. DB2 relies on private data memory for sort memory allocations during SQL processing. Insufficient shared heap memory can lead to Tivoli Storage Manager server failures during

interaction with DB2. For more information about setting the appropriate values, see Technote 1212174 (http://www.ibm.com/support/docview.wss?uid=swg21212174).

For guidance in setting ulimit values, see the following table:

Table 24. Ulimit values

Ulimit type	Standard value
Maximum size of core files created	Unlimited
Maximum size of a data segment for a process	Unlimited
Maximum file size	Unlimited
Maximum number of open files	• For servers on which replication, data deduplication, or both are enabled, specify a minimum value of 16384. • For all other servers, specify a minimum value of 8192.
Maximum amount of processor time in seconds	Unlimited

For instructions about setting ulimit values, see the documentation for your operating system.

The default value for the user limit of maximum user processes (nproc) has changed on some distributions and versions of the Linux operating system. The new default value is 1024. This value can cause unexpected behavior in the Tivoli Storage Manager server. For the Red Hat Enterprise Linux (RHEL) 6 operating system, the default value for nproc was decreased to 1024. This value might have changed in other versions and distributions of Linux that are supported by the Tivoli Storage Manager server. Increase the user limit of maximum user processes to the minimum suggested value of 16384. If the value is not updated, the server might display unexpected behavior, including hangs or failures. To verify the current user limit, issue the following command as the instance user:

```
ulimit -u
```

For example:

```
[user@Machine ~]$ ulimit -u
16384
```

To display the current values of all user limits, issue the following command:

```
ulimit -a
```

For example:

```
[user@Machine ~]$ ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority             (-e) 0
file size               (blocks, -f) unlimited
pending signals                 (-i) 128098
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) unlimited
open files                      (-n) 1024
pipe size            (512 bytes, -p) 8
POSIX message queues     (bytes, -q) 819200
real-time priority              (-r) 0
```

```
stack size              (kbytes, -s) 10240
cpu time                (seconds, -t) unlimited
max user processes            (-u) 16384
virtual memory          (kbytes, -v) unlimited
file locks                    (-x) unlimited
```

To update the user limit of maximum user processes, add a line to the /etc/security/limits.conf file. On the RHEL 6 operating system, the user limit for nproc is set in the /etc/security/limits.d/90-nproc.conf file. This file overrides the settings in the /etc/security/limits.conf file. To update the user limit on the RHEL 6 operating system, you must either edit the file in the /etc/security/limits.d directory or remove the file and add a line to the /etc/security/limits.conf file.

Starting the server from the instance user ID

The instance user ID has a user profile that enables it to run the server with the required permissions.

To start a Tivoli Storage Manager server from the instance user ID, complete the following steps:

1. Log in to the system where Tivoli Storage Manager is installed by using the instance user ID for the Tivoli Storage Manager server.
2. If you do not have a user profile that runs the db2profile script, issue the following command:

   ```
   . /home/tsminst1/sqllib/db2profile
   ```

   Tip: For information about updating the user ID login script to run the db2profile script automatically, see the DB2 documentation.
3. Start the server by issuing the following command from the server instance directory:

   ```
   /opt/tivoli/tsm/server/bin/dsmserv
   ```

   Tip: The command runs in the foreground so that you can set an administrator ID and connect to the server instance.

   For example, if the name of the Tivoli Storage Manager server instance is tsminst1, you can start the instance by issuing the following commands:

   ```
   cd /tsminst1
   . ~/sqllib/db2profile
   /opt/tivoli/tsm/server/bin/dsmserv
   ```
4. Optional: To start the server in the background, issue the following command:

   ```
   /opt/tivoli/tsm/server/bin/dsmserv -q &
   ```

Starting the server from the root user ID

The standard way to start the server is by using the instance user ID. However, in some cases, it might be necessary to use another user ID to start the server. For example, you might want to use the root user ID to ensure that the server can access specific devices.

For information about authorizing root users and starting the server by using the root user ID, see the *Administrator's Guide*.

Automatically starting servers on AIX, HP-UX, Linux, and Oracle systems

You can configure servers to start automatically at system startup. If the server is installed on an AIX, HP-UX, or Solaris operating system, use the `rc.dsmserv` script, which is provided for this purpose.

The `rc.dsmserv` script is in the `/opt/tivoli/tsm/server/bin` directory.

If the server is installed on a Linux operating system, you must use the `dsmserv.rc` script to automatically start the server.

To configure a server to start automatically on a Linux operating system, see "Automatically starting servers on Linux systems."

Automatically starting servers on Linux systems

To automatically start a Tivoli Storage Manager server on a Linux operating system, use the `dsmserv.rc` script.

Before you begin, review details about kernel parameter tuning for Tivoli Storage Manager here: http://www.ibm.com/support/docview.wss?uid=swg27015156.

The `dsmserv.rc` script:
- can be used either to start the server manually or to start the server automatically by adding entries to the `/etc/rc.d/init.d` directory
- can be used to stop the server
- works with Linux utilities such as **CHKCONFIG** and **SERVICE**

The `dsmserv.rc` script is in the `/opt/tivoli/tsm/server/bin` directory. The server instance directory structure must either be set up by the Tivoli Storage Manager configuration wizard or in the same way as the wizard sets it up. The instance directory structure must meet the following requirements:
- The Tivoli Storage Manager server instance runs under a non-root user ID with the same name as the instance owner.
- The home directory for the instance user is `/home/instance_name`.
- The instance directory for the server is in a subdirectory of the home directory called `/home/instance_name/instance_name`.

For each server instance that you want to automatically start, complete the following steps:
1. Place a copy of the `dsmserv.rc` script in the `/etc/rc.d/init.d` directory.
2. Rename the script so that it has the same name as the server instance owner.
3. After the script is in place, use tools such as the **CHKCONFIG** utility to configure the run level in which the server will automatically start. Specify a value that corresponds to a multiuser mode, with networking turned on. Typically, the run level to use is 2, 3, or 5, depending on the operating system and its configuration. Ensure that the run level in the script matches the run level of the operating system. For details about run levels, see the documentation for your operating system.

In this example, the instance owner is tsminst1 and the server instance directory is /home/tsminst1/tsminst1. Create a copy of the dsmserv.rc script called /etc/rc.d/init.d/tsminst1. Use the **CHKCONFIG** utility to configure the script to start at run level 5.

```
cp /opt/tivoli/tsm/server/bin/dsmserv.rc /etc/rc.d/init.d/tsminst1
chkconfig --list tsminst1
service tsminst1 supports chkconfig, but is not referenced in any runlevel
(run 'chkconfig --add tsminst1')
chkconfig --add tsminst1
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:off 4:off 5:off 6:off
chkconfig --level 5 tsminst1 on
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:off 4:off 5:on 6:off
```

4. Optional: After the script is in place, use a tool like the service utility to manually start or stop the server. For example:

```
service tsminst1
Usage: /etc/init.d/tsminst1 {start|stop|status|restart}
service tsminst1 status
Status of dsmserv instance tsminst1: stopped
service tsminst1 start
Starting dsmserv instance tsminst1 ... Succeeded

service tsminst1 status
Status of dsmserv instance tsminst1: running
service tsminst1 stop
Stopping dsmserv instance tsminst1 ...dsmserv instance tsminst1
stopped Successfully

service tsminst1 status
Status of dsmserv instance tsminst1: stopped
```

Stopping the server

You can stop the server without warning if an unexpected problem requires you to return control to the operating system. To avoid losing administrative and client node connections, stop the server only after current sessions have completed or been canceled.

To stop the server, issue the following command from the Tivoli Storage Manager command prompt:

```
halt
```

The server console stops.

If you cannot connect to the server with an administrative client and you want to stop the server, you must cancel the process by using the kill command with the process ID number (pid) that is displayed at initialization.

Important: Before you issue the kill command, ensure that you know the correct process ID for the Tivoli Storage Manager server.
The dsmserv.v6lock file, in the directory from which the server is running, can be used to identify the process ID of the process to kill. To display the file enter:

```
cat /instance_dir/dsmserv.v6lock
```

Issue the following command to stop the server:

```
kill -36 dsmserv_pid
```

where *dsmserv_pid* is the process ID number.

Registering licenses

Immediately register any Tivoli Storage Manager licensed functions that you purchase so you do not lose any data after you start server operations, such as backing up your data.

Use the **REGISTER LICENSE** command for this task.

Example: Register a license

Register the base Tivoli Storage Manager license.

```
register license file=tsmbasic.lic
```

Preparing the system for backups

To prepare the system for automatic and manual database backups, you must specify the device class to be used.

Before you begin the setup, ensure that you have defined a tape or file device class. See the defining device classes section of the *Administrator's Guide*.

To set up your system for database backups, issue the **SET DBRECOVERY** command to specify a device class to be used for the backups. You can also change the device class to be used for database backups with the **SET DBRECOVERY** command.

Perform the following setup procedure:

1. If you did not use the configuration wizard (dsmicfgx) to configure the server, ensure that you have completed the steps to manually configure the system for database backups.
2. Select the device class to be used for backups of the database. Issue the following command from a IBM Tivoli Storage Manager administrative command line.

   ```
   set dbrecovery device_class_name
   ```

   The device class that you specify is used by the database manager for database backups. If you do not specify a device class with the **SET DBRECOVERY** command, the backup fails.

For example, to specify that the **DBBACK** device class is to be used, issue this command:

```
set dbrecovery dbback
```

When you are ready to back up your database, see the **BACKUP DB** command in the *Administrator's Reference*.

Running multiple server instances on a single system

You can create more than one server instance on your system. Each server instance has its own instance directory, and database and log directories.

Multiply the memory and other system requirements for one server by the number of instances planned for the system.

The set of files for one instance of the server is stored separately from the files used by another server instance on the same system. Use the steps in "Creating the server instance" on page 54 for each new instance, including creation of the new instance user.

To manage the system memory that is used by each server, use the DBMEMPERCENT server option to limit the percentage of system memory. If all servers are equally important, use the same value for each server. If one server is a production server and other servers are test servers, set the value for the production server to a higher value than the test servers.

If you are upgrading from Tivoli Storage Manager Version 6.1 to V6.2 or V6.3 or later and have multiple servers on your system, you must run the upgrade wizard only once. The upgrade wizard collects the database and variables information for all of your original server instances.

If you are upgrading from Tivoli Storage Manager Version 6.1 to V6.3 or later and have multiple servers on your system, all instances that exist in DB2 Version 9.5 are dropped and recreated in DB2 Version 9.7. The wizard issues the db2 upgrade db dbname command for each database. The database environment variables for each instance on your system are also reconfigured during the upgrade process.

For information about the Server Initialization wizard, see the *Tivoli Storage Manager Administrator's Guide*.

Monitoring the server

When you start using server in production operation, monitor the space used by the server to ensure that the amount of space is adequate. Make adjustments as needed.

1. Monitor the active log, to ensure that the size is correct for the workload that is handled by the server instance.

   When the server workload is up to its typical expected level, and the space that is used by the active log is 80 - 90% of the space that is available to the active log directory, you might need to increase the amount of space. Whether you need to increase the space depends on the types of transactions in the server's workload, because transaction characteristics affect how the active log space is used.

   The following transaction characteristics can affect the space usage in the active log:

   - The number and size of files in backup operations
     - Clients such as file servers that back up large numbers of small files can cause large numbers of transactions that complete during a short period of time. The transactions might use a large amount of space in the active log, but for a short period of time.

- Clients such as a mail server or a database server that back up large chunks of data in few transactions can cause small numbers of transactions that take a long time to complete. The transactions might use a small amount of space in the active log, but for a long period of time.
- Network connection types
  - Backup operations that occur over fast network connections cause transactions that complete more quickly. The transactions use space in the active log for a shorter period of time.
  - Backup operations that occur over relatively slower connections cause transactions that take a longer time to complete. The transactions use space in the active log for a longer period of time.

If the server is handling transactions with a wide variety of characteristics, the space that is used for the active log might go up and down by a large amount over time. For such a server, you might need to ensure that the active log typically has a smaller percentage of its space used. The extra space allows the active log to grow for transactions that take a very long time to complete, for example.

2. Monitor the archive log to ensure that space is always available.

   Remember: If the archive log becomes full, and the failover archive log becomes full, the active log can become full and the server will stop. The goal is to make enough space available to the archive log so that it never uses all its available space.
   You are likely to notice the following pattern:

   a. Initially, the archive log grows rapidly as typical client-backup operations occur.
   b. Database backups occur regularly, either as scheduled or done manually.
   c. After at least two full database backups occur, log pruning occurs automatically. The space used by the archive log decreases when the pruning occurs.
   d. Normal client operations continue, and the archive log grows again.
   e. Database backups occur regularly, and log pruning occurs as often as full database backups occur.

   With this pattern, the archive log grows initially, then decreases, then might grow again. Over a period of time, as normal operations continue, the amount of space used by the archive log should reach a relatively constant level.

   If the archive log continues to grow, consider taking one or both of these actions:

   - Add space to the archive log. This might mean moving the archive log to a different file system.

     For information about moving the archive log, see the *Tivoli Storage Manager Administrator's Guide*.

   - Increase the frequency of full database backups, so that log pruning occurs more frequently.

3. If you defined a directory for the failover archive log, determine whether any logs get stored in that directory during normal operations. If the failover log space is being used, consider increasing the size of the archive log. The goal is that the failover archive log is used only under unusual conditions, not in normal operation.

For details about monitoring, see the *Administrator's Guide*.

Monitoring space utilization for the database and recovery logs

To determine the amount of used and available active log space, you issue the **QUERY LOG** command. To monitor space utilization in the database and recovery logs, you can also check the activity log for messages.

Active log

If the amount of available active log space is too low, the following messages are displayed in the activity log:

ANR4531I: IC_AUTOBACKUP_LOG_USED_SINCE_LAST_BACKUP_TRIGGER
   This message is displayed when the active log space exceeds the maximum specified size. The Tivoli Storage Manager server starts a full database backup.

   To change the maximum log size, halt the server. Open the `dsmserv.opt` file, and specify a new value for the `ACTIVELOGSIZE` option. When you are finished, restart the server.

ANR0297I: IC_BACKUP_NEEDED_LOG_USED_SINCE_LAST_BACKUP
   This message is displayed when the active log space exceeds the maximum specified size. You must back up the database manually.

   To change the maximum log size, halt the server. Open the `dsmserv.opt` file, and specify a new value for the `ACTIVELOGSIZE` option. When you are finished, restart the server.

ANR4529I: IC_AUTOBACKUP_LOG_UTILIZATION_TRIGGER
   The ratio of used active-log space to available active-log space exceeds the log utilization threshold. If at least one full database backup has occurred, the Tivoli Storage Manager server starts an incremental database backup. Otherwise, the server starts a full database backup.

ANR0295I: IC_BACKUP_NEEDED_LOG_UTILIZATION
   The ratio of used active-log space to available active-log space exceeds the log utilization threshold. You must back up the database manually.

Archive log

If the amount of available archive log space is too low, the following message is displayed in the activity log:

ANR0299I: IC_BACKUP_NEEDED_ARCHLOG_USED
   The ratio of used archive-log space to available archive-log space exceeds the log utilization threshold. The Tivoli Storage Manager server starts a full automatic database backup.

Database

If the amount of space available for database activities is too low, the following messages are displayed in the activity log:

ANR2992W: IC_LOG_FILE_SYSTEM_UTILIZATION_WARNING_2
   The used database space exceeds the threshold for database space utilization. To increase the space for the database, use the **EXTEND DBSPACE** command, the **EXTEND DBSPACE** command, or the DSMSERV FORMAT utility with the **DBDIR** parameter.

ANR1546W: FILESYSTEM_DBPATH_LESS_1GB

The available space in the directory where the server database files are located is less than 1 GB.

When a Tivoli Storage Manager server is created with the DSMSERV FORMAT utility or with the configuration wizard, a server database and recovery log are also created. In addition, files are created to hold database information used by the database manager. The path specified in this message indicates the location of the database information used by the database manager. If space is unavailable in the path, the server can no longer function.

You must add space to the file system or make space available on the file system or disk.

Chapter 4. Installing a Tivoli Storage Manager server fix pack

Tivoli Storage Manager maintenance updates, which are also referred to as fix packs, bring your server up to the current maintenance level.

To install a fix pack or interim fix to the server, install the server at the level on which you want to run it. You do not have to start the server installation at the base release level. For example, if you currently have V6.1.2.1 installed, you can go directly to the latest fix pack for V6.3 or later. You do not have to start with the V6.3.0 installation if a maintenance update is available.

You must have the Tivoli Storage Manager license package installed. The license package is provided with the purchase of a base release. Alternatively, you can obtain the license package when download a fix pack from the Passport Advantage website. After the fix pack or interim fix is installed, install the license for the server. To display messages and help in a language other than US English, install the language package of your choice.

For information about the estimated time required to install a fix pack, see Techdoc 7023591.

If you upgrade the server to V6.3.4 or later, and then revert the server to a level that is earlier than V6.3.4, you must restore the database to a point in time before the upgrade. During the upgrade process, complete the required steps to ensure that the database can be restored: back up the database, the volume history file, the device configuration file, and the server options file. For more information, see Chapter 6, "Reverting from Version 6.3 or later to the previous Version 6 server," on page 95.

Before you upgrade the Tivoli Storage Manager server, ensure that you retain the installation media from the base release of the installed server. If you installed Tivoli Storage Manager from a DVD, ensure that the DVD is available. If you installed Tivoli Storage Manager from a downloaded package, ensure that the downloaded files are available. If the upgrade fails, and the server license module is uninstalled, the installation media from the server base release are required to reinstall the license.

Visit this website: http://www.ibm.com/support/entry/portal/Overview/ Software/Tivoli/Tivoli_Storage_Manager for the following information:

- A list of the latest maintenance and download fixes. Click **Support and downloads** and apply any applicable fixes.
- Details about obtaining a base license package. Search for **Warranties and licenses**.
- Supported platforms and system requirements. Click **Server requirements**.

To install a fix pack or interim fix, complete the following steps.

Attention: Do not alter the DB2 software that is installed with Tivoli Storage Manager installation packages and fix packs. Do not install or upgrade to a different version, release, or fix pack of DB2 software because doing so can damage the database.

   1. Log in as the root user.

Installing a Tivoli Storage Manager fix pack

2. Obtain the package file for the fix pack or interim fix that you want to install from the Tivoli Storage Manager FTP downloads site: ftp:// public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/server.

3. Change to the directory where you placed the executable file and complete the following steps.

   Tip: The files are extracted to the current directory. Ensure that the executable file is in the directory where you want the extracted files to be located.

   a. Change file permissions by entering the following command:

   ```
   chmod a+x 6.x.x.x-TIV-TSMALL-platform.bin
   ```

   where *platform* denotes the architecture that Tivoli Storage Manager is to be installed on.

   b. Issue the following command to extract the installation files:

   ```
   ./6.x.x.x-TIV-TSMALL-platform.bin
   ```

4. Back up the database. The preferred method is to use a snapshot backup. A snapshot backup is a full database backup that does not interrupt any scheduled database backups. For example, issue the following Tivoli Storage Manager administrative command:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

   See the *Administrator's Guide* for more details.

5. Back up the device configuration information. Issue the following Tivoli Storage Manager administrative command:

   ```
   backup devconfig filenames=file_name
   ```

   where *file_name* specifies the name of the file in which to store device configuration information.

6. Save the volume history file to another directory or rename the file. Issue the following Tivoli Storage Manager administrative command:

   ```
   backup volhistory filenames=file_name
   ```

   where *file_name* specifies the name of the file in which to store the volume history information.

7. Save a copy of the server options file, typically named dsmserv.opt. The file is in the server instance directory.

8. Halt the server before installing a fix pack or interim fix. Use the **HALT** command.

9. Ensure that extra space is available in the installation directory. The installation of this fix pack might require additional temporary disk space in the installation directory of the server. The amount of additional disk space can be as much as that required for installing a new database as part of a Tivoli Storage Manager installation. The Tivoli Storage Manager installation wizard displays the amount of space that is required for installing the fix pack and the available amount. If the required amount of space is greater than the available amount, the installation stops. If the installation stops, add the required disk space to the file system and restart the installation.

10. Select one of the following ways of installing Tivoli Storage Manager.

    Important: After a fix pack is installed, it is not necessary to go through the configuration again. You can stop after completing the installation, fix any errors, then restart your servers.

Installation wizard
"Installing Tivoli Storage Manager by using the installation wizard" on page 37

Command-line console wizard
"Installing Tivoli Storage Manager by using the console installation wizard" on page 38

Silent mode
"Installing Tivoli Storage Manager in silent mode" on page 40

Fix any errors before continuing. The installation log, `installFixPack.log`, is stored in the following location:

coi/plan/tmp

Installing a Tivoli Storage Manager fix pack

Chapter 5. Upgrading to Tivoli Storage Manager Version 6.3 or later

You can upgrade an IBM Tivoli Storage Manager server from any version of 6.1 or 6.2 directly to Version 6.3 or later.

Table 25. Upgrade information

To upgrade from this version	To this version	See this information
V6.3 or later	V6.3 or later	Chapter 4, "Installing a Tivoli Storage Manager server fix pack," on page 73
V6.2	V6.3 or later	"Upgrading from Tivoli Storage Manager V6.2 to V6.3 or later" on page 78
V6.1	V6.3 or later	"Upgrading from Tivoli Storage Manager V6.1 to V6.3 or later" on page 83
V5.5	V6.3 or later	*Upgrade and Migration Guide for V5 Servers*

For information about upgrades in a clustered environment, see "Upgrading Tivoli Storage Manager in a clustered environment" on page 94.

If a Tivoli Storage Manager V5 server is installed, and you prefer to upgrade the server to V6 on a different operating system, see the instructions for server migration:

Table 26. Migration information

To migrate the server from this operating system	To this operating system	See this information
AIX	Linux x86_64	Section about migrating Tivoli Storage Manager V5 servers on AIX, HP-UX, or Solaris systems to V6.3.4 on Linux in the *Upgrade and Migration Guide for V5 Servers*
HP-UX	Linux x86_64	Section about migrating Tivoli Storage Manager V5 servers on AIX, HP-UX, or Solaris systems to V6.3.4 on Linux in the *Upgrade and Migration Guide for V5 Servers*
Solaris	Linux x86_64	Section about migrating Tivoli Storage Manager V5 servers on AIX, HP-UX, or Solaris systems to V6.3.4 on Linux in the *Upgrade and Migration Guide for V5 Servers*

Table 26. Migration information (continued)

To migrate the server from this operating system	To this operating system	See this information
z/OS	AIX	Section about migrating Tivoli Storage Manager V5 servers on z/OS systems to V6 on AIX or Linux on System z in the *Upgrade and Migration Guide for V5 Servers*
z/OS	Linux on System z	Section about migrating Tivoli Storage Manager V5 servers on z/OS systems to V6 on AIX or Linux on System z in the *Upgrade and Migration Guide for V5 Servers*

To revert to an earlier version of Tivoli Storage Manager after an upgrade or migration, you must have a full database backup and the installation software for the original server. You must also have key configuration files:

- Volume history file
- Device configuration file
- Server options file
- dsmserv.dsk file

Restriction: Multiple server instances on a system all use the same installed code, so all the server instances on a system must be upgraded at the same time.

Upgrading from Tivoli Storage Manager V6.2 to V6.3 or later

You can upgrade the server directly from Tivoli Storage Manager Version 6.2 to V6.3.1, V6.3.2, V6.3.3, or V6.3.4 without installing V6.3 first. You also do not need to uninstall V6.2.

To upgrade to the Tivoli Storage Manager V6.3 or later server, install the V6.3 license package. The license package is provided with the purchase of a base release. Alternatively, you can obtain the license package when you download a fix pack from Passport Advantage, an IBM license acquisition and software maintenance website, at http://www.ibm.com/software/lotus/passportadvantage/pacustomers.html.

Before you upgrade the Tivoli Storage Manager server, ensure that you retain the installation media from the base release of the installed server. If you installed Tivoli Storage Manager from a DVD, ensure that the DVD is available. If you installed Tivoli Storage Manager from a downloaded package, ensure that the downloaded files are available. If the upgrade fails, and the server license module is uninstalled, the installation media from the server base release are required to reinstall the license.

The upgrade process consists of three phases:
1. Planning the upgrade
2. Preparing the system
3. Installing the software and verifying the upgrade

To plan the upgrade, complete the following steps:
1. Optional: To review hardware and software requirements before you start the upgrade process, see the requirements for your operating system:

   "System requirements" on page 5

   For the latest updates related to system requirements, see the Tivoli Storage Manager support website at http://www.ibm.com/support/docview.wss?uid=swg21243309.

   Tip: At a later stage in the process, after you extract the installation files, you can run the prerequisite checker to automatically verify hardware and software requirements.
2. For special instructions or specific information for your operating system, review the release notes or readme files: http://publib.boulder.ibm.com/infocenter/tsminfo/v6r3/topic/com.ibm.itsm.relnotes.doc/relnote_server630.html. Alternatively, review the readme file on the Tivoli Storage Manager installation DVD or in the directory where you extract the package.
3. If the server that you are upgrading is at a release level that is earlier than V6.2.3.000, review Technote 1452146 (http://www.ibm.com/support/docview.wss?uid=swg21452146). The technote describes improvements in the database reorganization process, and configuration changes that you might be required to make.
4. Select an appropriate day and time to upgrade your system to minimize the impact on production operations. Upgrading the server from V6.2 to V6.3 or later takes approximately 20 - 50 minutes. Your environment might produce different results from these lab results. The time that is required to update the system depends on the database size and many other factors. When you start the upgrade process, clients cannot connect to the server until the new software is installed and any required licenses are registered again.

To prepare the system for the upgrade, complete the following steps:
1. Log on to the system where you are planning to upgrade the Tivoli Storage Manager server.

   Use the root user ID.
2. Back up the Tivoli Storage Manager database. The preferred method is to use a snapshot backup. A snapshot backup is a full database backup that does not interrupt any scheduled database backups. For example, you can create a backup by issuing the Tivoli Storage Manager administrative command:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

   For more information about this command and other Tivoli Storage Manager administrative commands, see the *Administrator's Reference*.
3. Back up the device configuration information by issuing the Tivoli Storage Manager administrative command:

   ```
   backup devconfig filenames=file_name
   ```

   where *file_name* specifies the name of the file in which to store device configuration information.
4. Back up the volume history file to another directory or rename the file. Issue the Tivoli Storage Manager administrative command:

   ```
   backup volhistory filenames=file_name
   ```

where *file_name* specifies the name of the file in which to store the volume history information.

Important: By taking this step, you ensure that the file is not overwritten during the upgrade process. If you decide to restore the database, this file is required.

5. Save a copy of the server options file, typically named `dsmserv.opt`. The file is in the server instance directory.

6. Back up the deployment engine by issuing the following system commands:
```
. /var/ibm/common/acsi/setenv.sh
cd /usr/ibm/common/acsi/bin
./de_backupdb
```

7. For each existing server instance, gather information about the corresponding DB2 instance. Note the default database path, actual database path, database name, database alias, and any DB2 variables that are configured for the instance. Keep the record for future reference.

   a. Ensure that you are logged on with the instance user ID, and not the root user ID, when you issue the system commands to obtain DB2 instance information.

   b. Obtain a list of DB2 instances by issuing the following system commands:
   ```
   su - instance
   /opt/tivoli/tsm/db2/instance/db2ilist
   ```

   c. Obtain the default database path of the DB2 instance by issuing the following system commands:
   ```
   su - instance
   . ~instance/sqllib/db2profile; LC_ALL=C db2 get dbm cfg | grep DFTDBPATH
   ```

   d. Obtain information about the DB2 instance databases by issuing the following system commands:
   ```
   su - instance
   . ~instance/sqllib/db2profile; LC_ALL=C db2 list database directory
   ```

   e. Obtain the DB2 instance variables by issuing the following system commands:
   ```
   su - instance
   . ~instance/sqllib/db2profile; LC_ALL=C db2set -all
   ```

   f. Obtain more DB2 instance information by saving the following files:
   ```
   ~instance/sqllib/userprofile
   ~instance/sqllib/usercshrc
   ```

   For example, issue the following system commands:
   ```
   cp ~instance/sqllib/userprofile copy_location
   cp ~instance/sqllib/usercshrc copy_location
   ```

   where *instance* is the DB2 instance and *copy_location* is the location where the copied file is saved.

8. Prevent activity on the server by disabling new sessions. Issue the following Tivoli Storage Manager administrative commands:
```
disable sessions client
disable sessions server
```

9. Prevent administrative activity from any user ID other than the administrator ID that is being used for the upgrade preparation tasks. Lock out other administrator IDs, if necessary, by using the Tivoli Storage Manager administrative command:
```
lock admin administrator_name
```

10. Verify whether any sessions exist, and notify the users that the server will be stopped. To check for existing sessions, issue the following Tivoli Storage Manager administrative command:

    `query session`

11. Cancel sessions that are running by issuing the following Tivoli Storage Manager administrative command:

    `cancel session all`

12. Halt the server by issuing the following Tivoli Storage Manager administrative command:

    `halt`

13. In the server instance directory of your installation, delete or rename the `NODELOCK` file. The `NODELOCK` file contains the previous licensing information for your installation. This licensing information is replaced when the upgrade is complete.

To install the software and verify that the upgrade was successful, complete the following steps:

1. If you are installing the products by using the Tivoli Storage Manager DVD, insert the DVD into a DVD drive.

   Ensure that the DVD is mounted on directory `/dvdrom` and navigate to that directory.

2. If you downloaded the program from Passport Advantage as an executable file, verify that you have enough space to store the installation files when you extract them from the product package. For space requirements, see the download document for your product:

   - Tivoli Storage Manager: http://www.ibm.com/support/docview.wss?uid=swg24030521
   - Tivoli Storage Manager Extended Edition: http://www.ibm.com/support/docview.wss?uid=swg24030527
   - System Storage Archive Manager: http://www.ibm.com/support/docview.wss?uid=swg24030530

3. If you are installing the program from Passport Advantage, ensure that the executable file for the installation package is in the directory where you want the installation package to be. The directory for the installation package must not contain previously extracted files, or any other files.

4. If you downloaded the program from Passport Advantage, navigate to the directory where you placed the executable file and complete the following steps:

   a. Change the file permissions by issuing the following system command:

      `chmod a+x 6.x.x.x-TIV-TSMALL-platform.bin`

      where *6.x.x.x.* specifies the version number and *platform* specifies the architecture that Tivoli Storage Manager is to be installed on.

   b. To extract the installation files, issue the following system command:

      `./6.x.x.x-TIV-TSMALL-platform.bin`

5. To ensure that your system meets all requirements, locate the following file and run it:

   `prereqcheck.bin`

   For details, see "Running the installation prerequisite checker" on page 12.

6. Install the Tivoli Storage Manager software by using one of the following methods:

   Installation wizard
   > The installation wizard guides you through the process with a graphical user interface.
   >
   > For instructions, see "Upgrading Tivoli Storage Manager by using the installation wizard" on page 88

   Console installation wizard
   > The console installation wizard guides you through the process with a text-based interface. You provide input by issuing commands. This option is useful if you are installing Tivoli Storage Manager from a system that does not support a graphical user interface.
   >
   > For instructions, see "Upgrading Tivoli Storage Manager by using the console installation wizard" on page 90

   Silent mode
   > You start the process by specifying the values of variables, and the installation runs on its own. You are freed from the tasks of monitoring the installation and providing input during the process.
   >
   > For instructions, see "Upgrading Tivoli Storage Manager in silent mode" on page 91

   Tip: If you have multiple server instances on your system, run the installation wizard only once. The installation wizard upgrades all server instances. For more information about running multiple servers, see "Running multiple server instances on a single system" on page 69.

7. Correct any errors that are detected during the installation process. Errors are listed in the summary page of the wizard.

   You can also review the error log files in the `/var/tivoli/tsm` directory.

8. Verify that the upgrade was successful:

   a. Start the server instances as described in "Starting the server instance on AIX, HP-UX, Linux, and Solaris systems" on page 63.

   b. Monitor the messages that the server issues as it starts. Watch for error and warning messages, and resolve any issues.

   c. Verify that you can connect to the server by using the administrative client. To start an administrative client session, issue the following Tivoli Storage Manager administrative command:

      `dsmadmc`

   d. Run **QUERY** commands to obtain information about the upgraded system. For example, to obtain consolidated information about the system, issue the following Tivoli Storage Manager administrative command:

      `query system`

      To obtain information about the database, issue the following Tivoli Storage Manager administrative command:

      `query db format=detailed`

9. Register the licenses for the Tivoli Storage Manager server components that are installed on your system by issuing the following Tivoli Storage Manager administrative command:

   `register license file=*.lic`

Restriction: You cannot register licenses for IBM Tivoli Storage Manager for Mail, IBM Tivoli Storage Manager for Databases, IBM Tivoli Storage Manager for Enterprise Resource Planning, and IBM Tivoli Storage Manager for Space Management.

10. Back up the deployment engine again by issuing the following system commands:

```
. /var/ibm/common/acsi/setenv.sh
cd /usr/ibm/common/acsi/bin
./de_backupdb
```

After you upgrade the server to V6.3.3 or later, you can authenticate passwords with the LDAP directory server, or authenticate passwords with the Tivoli Storage Manager server. Passwords that are authenticated with the LDAP directory server can provide enhanced system security. For details, see the section about managing passwords and logon procedures in the *Administrator's Guide*.

Upgrading from Tivoli Storage Manager V6.1 to V6.3 or later

You can upgrade your system directly from Tivoli Storage Manager V6.1 to V6.3.1, V6.3.2, V6.3.3, or V6.3.4 without installing V6.3 first. You also do not need to uninstall V6.1.

To upgrade to the Tivoli Storage Manager V6.3 or later server, install the V6.3 license package. The license package is provided with the purchase of a base release. Alternatively, you can obtain the license package when you download a fix pack from Passport Advantage, an IBM license acquisition and software maintenance website, at http://www.ibm.com/software/lotus/passportadvantage/pacustomers.html.

Before you upgrade the Tivoli Storage Manager server, ensure that you retain the installation media from the base release of the installed server. If you installed Tivoli Storage Manager from a DVD, ensure that the DVD is available. If you installed Tivoli Storage Manager from a downloaded package, ensure that the downloaded files are available. If the upgrade fails, and the server license module is uninstalled, the installation media from the server base release are required to reinstall the license.

The upgrade process consists of three phases:
1. Planning the upgrade
2. Preparing the system
3. Installing the software and verifying the upgrade

To plan the upgrade, complete the following steps:
1. Optional: To review hardware and software requirements before you start the upgrade process, see the requirements for your operating system:

   "System requirements" on page 5

   For the latest updates related to system requirements, see the Tivoli Storage Manager support website at http://www.ibm.com/support/docview.wss?uid=swg21243309.

   Tip: At a later stage in the process, after you extract the installation files, you can run the prerequisite checker to automatically verify hardware and software requirements.

2. For special instructions or specific information for your operating system, review the release notes: http://publib.boulder.ibm.com/infocenter/tsminfo/ v6r3/topic/com.ibm.itsm.relnotes.doc/relnote_server630.html. Alternatively, review the readme file on the Tivoli Storage Manager installation DVD or in the directory where you extract the package.

3. If the server that you are upgrading is at a release level earlier than V6.1.5.10, review Technote 1452146 (http://www.ibm.com/support/ docview.wss?uid=swg21452146). The technote describes improvements in the database reorganization process, and configuration changes that you might be required to make.

4. To minimize the impact on production operations, select an appropriate day and time to upgrade your system. Upgrading the server from V6.1 to V6.3 or later takes approximately 20 - 50 minutes. Your environment might produce different results than these lab results. The time that is required to update the system depends on the database size and many other factors. When you start the upgrade process, clients cannot connect to the server until the new software is installed and any required licenses are registered again.

To prepare the system for the upgrade, complete the following steps:

1. Log on to the system where you are planning to upgrade the Tivoli Storage Manager server.

   Use the root user ID.

2. Back up the database. The preferred method is to use a snapshot backup. A snapshot backup is a full database backup that does not interrupt any scheduled database backups. For example, you can create a backup by issuing the Tivoli Storage Manager administrative command:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

   For more information about this command and other Tivoli Storage Manager administrative commands, see the *Administrator's Reference*.

3. Back up the device configuration information by issuing the following Tivoli Storage Manager administrative command:

   ```
   backup devconfig filenames=file_name
   ```

   where *file_name* specifies the name of the file in which to store device configuration information.

4. Back up the volume history file to another directory or rename the file. Issue the following Tivoli Storage Manager administrative command:

   ```
   backup volhistory filenames=file_name
   ```

   where *file_name* specifies the name of the file in which to store the volume history information.

   Important: By taking this step, you ensure that the file is not overwritten during the upgrade process. If you decide to restore the database, this file is required.

5. Save a copy of the server options file, typically named `dsmserv.opt`. The file is in the server instance directory.

6. Back up the deployment engine by issuing the following system commands:

   ```
   . /var/ibm/common/acsi/setenv.sh
   cd /usr/ibm/common/acsi/bin
   ./de_backupdb
   ```

7. Prevent activity on the server by disabling new sessions. Issue the following Tivoli Storage Manager administrative commands:

```
disable sessions client
disable sessions server
```

8. Prevent administrative activity from any user ID other than the administrator ID that is being used to prepare the upgrade. Lock out other administrator IDs, if necessary, by using the Tivoli Storage Manager administrative command:

```
lock admin administrator_name
```

9. Verify whether any sessions exist, and notify the users that the server will be stopped. To check for existing sessions, issue the following Tivoli Storage Manager administrative command:

```
query session
```

10. Cancel sessions that are running by issuing the following Tivoli Storage Manager administrative command:

```
cancel session all
```

11. Halt the server by issuing the following Tivoli Storage Manager administrative command:

```
halt
```

12. In the server instance directory of your installation, delete or rename the NODELOCK file. The NODELOCK file contains the previous licensing information for your installation. This licensing information is replaced when the upgrade is complete.

13. For each existing server instance, gather information about the corresponding DB2 instance. Note the default database path, actual database path, database name, database alias, and any DB2 variables that are configured for the instance. Keep the record for future reference.

    a. Ensure that you are logged on with the instance user ID, and not the root user ID, when you issue the system commands to obtain DB2 instance information.

    b. Obtain a list of DB2 instances by issuing the following system commands:

    ```
    su - instance
    /opt/tivoli/tsm/db2/instance/db2ilist
    ```

    c. Obtain the default database path of the DB2 instance by issuing the following system commands:

    ```
    su - instance
    . ~instance/sqllib/db2profile; LC_ALL=C db2 get dbm cfg | grep DFTDBPATH
    ```

    d. Obtain information about the DB2 instance databases by issuing the following system commands:

    ```
    su - instance
    . ~instance/sqllib/db2profile; LC_ALL=C db2 list database directory
    ```

    e. Obtain the DB2 instance variables by issuing the following system commands:

    ```
    su - instance
    . ~instance/sqllib/db2profile; LC_ALL=C db2set -all
    ```

    f. Obtain more DB2 instance information by saving the following files:

    ```
    ~instance/sqllib/userprofile
    ```

    ```
    ~instance/sqllib/usercshrc
    ```

    For example, issue the following system commands:

    ```
    cp ~instance/sqllib/userprofile copy_location
    cp ~instance/sqllib/usercshrc copy_location
    ```

where *instance* is the DB2 instance and *copy_location* is the location where the copied file is saved.

To verify requirements and install the software, complete the following steps:

1. If you downloaded the program from Passport Advantage as an executable file, verify that you have enough space to store the installation files when you extract them from the product package. For space requirements, see the download document for your product:

    - Tivoli Storage Manager: http://www.ibm.com/support/docview.wss?uid=swg24030521
    - Tivoli Storage Manager Extended Edition: http://www.ibm.com/support/docview.wss?uid=swg24030527
    - System Storage Archive Manager: http://www.ibm.com/support/docview.wss?uid=swg24030530

2. If you are installing the program from Passport Advantage, ensure that the executable file for the installation package is in the directory where you want the installation package to be. The directory for the installation package must not contain previously extracted files, or any other files.

3. If you downloaded the program from Passport Advantage, navigate to the directory where you placed the executable file and complete the following steps:

    a. Change the file permissions by issuing the following system command:

    ```
    chmod a+x 6.x.x.x-TIV-TSMALL-platform.bin
    ```

    where *6.x.x.x.* specifies the version number and *platform* specifies the architecture that Tivoli Storage Manager is to be installed on.

    b. To extract the installation files, issue the following system command:

    ```
    ./6.x.x.x-TIV-TSMALL-platform.bin
    ```

    where *6.x.x.x.* specifies the version number and *platform* specifies the architecture that Tivoli Storage Manager is to be installed on.

4. If you are installing the products by using the Tivoli Storage Manager DVD, insert the DVD into a DVD drive.

    Ensure that the DVD is mounted on directory `/dvdrom` and navigate to that directory.

5. To ensure that your system meets all requirements, locate the following file and run it:

    ```
    prereqcheck.bin
    ```

    For details, see "Running the installation prerequisite checker" on page 12.

6. Review the installation methods:

    Installation wizard
    The installation wizard guides you through the process with a graphical user interface.

    Console installation wizard
    The console installation wizard guides you through the process with a text-based interface. You provide input by issuing commands. This option is useful if you are installing Tivoli Storage Manager from a system that does not support a graphical user interface.

Silent mode

You start the process by specifying the values of variables, and the installation runs on its own. You are freed from the tasks of monitoring the installation and providing input during the process.

7. If you plan to use the installation wizard or console installation wizard for the upgrade, ensure that the following requirements are met:

- The system must have one of the following protocols enabled. Ensure that the port that the protocol uses is not blocked by a firewall.

   Secure Shell (SSH)

   Ensure that the port is set to the default value, 22. Also, ensure that the SSH daemon service has access rights for connecting to the system by using `localhost`.

   Remote shell (rsh)

   Remote Execution Protocol (REXEC)

- You must be able to log on to the V6.3 or later system with the user ID that you created for the server instance, by using the SSH, rsh, or REXEC protocol. When you use the wizard, use this user ID and password to access that system.

   Tip: If "su" is enabled for the instance owner user ID, the listed requirements are not mandatory.

If you cannot establish a connection by using the SSH, rsh, or REXEC protocols, manually upgrade the Tivoli Storage Manager server instance from Version 6.1. For details, see http://www.ibm.com/support/docview.wss?uid=swg27018195.

8. Install the Tivoli Storage Manager software by using one of the following methods:

   Installation wizard

   For instructions, see "Upgrading Tivoli Storage Manager by using the installation wizard" on page 88.

   Console installation wizard

   For instructions, see "Upgrading Tivoli Storage Manager by using the console installation wizard" on page 90.

   Silent mode

   For instructions, see "Upgrading Tivoli Storage Manager in silent mode" on page 91.

   Tips: If you have multiple server instances on your system, run the installation wizard only once. The installation wizard upgrades all server instances. For more information about running multiple servers, see "Running multiple server instances on a single system" on page 69. After Tivoli Storage Manager is upgraded, do not configure the system again.

9. Correct any database errors that are detected during the installation process. Review the output from the **db2ckupgrade** command. The log names for each database have the following structure:

   /tmp/db2ckupgrade_*instance_name_db_name*.log

The wizard automatically corrects some errors in the database during the upgrade to V6.3 or later and DB2 V9.7. You might need to correct other errors manually. For more information about database errors, see the information about DB2 log files in the *Problem Determination Guide*.

10. Correct any other errors that were detected during the installation process. Errors are listed in the summary page of the wizard.

    You can also review the error log files in the `/var/tivoli/tsm` directory.

11. Verify that the upgrade was successful:

    a. Start the server instances as described in "Starting the server instance on AIX, HP-UX, Linux, and Solaris systems" on page 63.

    b. Monitor the messages that the server issues as it starts. Watch for error and warning messages, and resolve any issues.

    c. Verify that you can connect to the server by using the administrative client. To start an administrative client session, issue the following Tivoli Storage Manager administrative command:

       `dsmadmc`

    d. Run **QUERY** commands to obtain information about the upgraded system. For example, to obtain consolidated information about the system, issue the following Tivoli Storage Manager administrative command:

       `query system`

       To obtain information about the database, issue the following Tivoli Storage Manager administrative command:

       `query db format=detailed`

12. Register the licenses for the Tivoli Storage Manager server components that are installed on your system by issuing the following Tivoli Storage Manager administrative command:

    `register license file=*.lic`

    Restriction: You cannot register licenses for IBM Tivoli Storage Manager for Mail, IBM Tivoli Storage Manager for Databases, IBM Tivoli Storage Manager for Enterprise Resource Planning, and IBM Tivoli Storage Manager for Space Management.

13. Back up the deployment engine again by issuing the following system commands:

    ```
    . /var/ibm/common/acsi/setenv.sh
    cd /usr/ibm/common/acsi/bin
    ./de_backupdb
    ```

After you upgrade the server to V6.3.3 or later, you can authenticate passwords with the LDAP directory server, or authenticate passwords with the Tivoli Storage Manager server. Passwords that are authenticated with the LDAP directory server can provide enhanced system security. For details, see the section about managing passwords and logon procedures in the *Administrator's Guide*.

Upgrading Tivoli Storage Manager by using the installation wizard

Using the installation wizard is one method of upgrading Tivoli Storage Manager from Version 6.

See Chapter 5, "Upgrading to Tivoli Storage Manager Version 6.3 or later," on page 77 for an overview of the upgrade steps, before starting the upgrade.

To upgrade Tivoli Storage Manager from Version 6 by using the installation wizard, complete the following steps:

1. If you are installing locally onto a remote system that uses an X display, and your local system does not have an X Window System server running, the installation might fail. If it fails, ensure that the DISPLAY environment variable is *not* set and restart the installation.

2. If your temporary location is smaller than Tivoli Storage Manager needs, as per the system requirements, use the Install Anywhere environment variable `$IATEMPDIR` as the temporary directory.

3. If you are using Security Enhanced Linux on your system, set `SELINUX=disable` or set `SELINUX=permissive` in the `/etc/sysconfig/selinux` file, at least until the installation process completes. If you do not adjust the setting, you receive this message when you try to install the server:

```
The installation wizard cannot run on your configuration.
It will now stop. For more details about installation error logs,
enter the phrase "installation log files" in the Search field
at this site: http://publib.boulder.ibm.com/infocenter/tsminfo/v6r3.
```

4. To start the wizard without saving your responses, enter the following command:

   `./install.bin`

   To start the wizard and save your responses to later use for a silent installation, enter the following command and specify the -r option.

   `./install.bin -r /path_name/response.rsp`

   where *path_name* is the full directory path to where you want the response file to be created. If you do not specify a fully qualified name, the response file is placed in a temporary directory.

5. Select the language for your installation and follow the wizard, selecting **Next** to step through the wizard.

   Select the product that you are entitled to use and a license agreement is displayed. You can select only one product on the page. If you select Tivoli Storage Manager, Tivoli Storage Manager Extended Edition, or System Storage Archive Manager, you are asked if you will be using LAN-free or library sharing. If you select **YES**, you must accept the Tivoli Storage Manager for Storage Area Networks license agreement. This is in addition to the license for the product that you chose on the previous page.

   Select the components that you want to install. Components include the server, languages, license, device driver, and storage agent. There is no default, so you must make a selection. If you previously installed a server, ensure that you select the same directory when you install a language package, license, or device driver. If you previously installed a storage agent, ensure that you select the same directory if you return to install a device driver.

   A server and a storage agent cannot be installed on the same workstation.

   The Tivoli Storage Manager client application programming interface (API), DB2 Version 9.7, and IBM Global Security Kit (GSKit) Version 8 are automatically installed when you select the server component.

At the end of the upgrade, a summary is provided. If errors occurred during the upgrade, another summary page lists the errors and directs you to an error log file. The installation log is stored in the following location:

`/var/tivoli/tsm`

Upgrading Tivoli Storage Manager by using the console installation wizard

Using the console installation wizard is one method of upgrading Tivoli Storage Manager from Version 6.

See Chapter 5, "Upgrading to Tivoli Storage Manager Version 6.3 or later," on page 77 for an overview of the upgrade steps, before starting the upgrade.

To upgrade the Tivoli Storage Manager server from Version 6 by using the console installation wizard, complete the following steps:

1. If you are installing locally onto a remote system that uses an X display, and your local system does not have an X Window System server running, the installation might fail. If it fails, ensure that the DISPLAY environment variable is *not* set and restart the installation.

2. If your temporary location is smaller than Tivoli Storage Manager needs, as per the system requirements, use the Install Anywhere environment variable $IATEMPDIR as the temporary directory.

3. If you are using Security Enhanced Linux on your system, set SELINUX=disable or set SELINUX=permissive in the /etc/sysconfig/selinux file, at least until the installation process completes. If you do not adjust the setting, you receive this message when you try to install the server:

   ```
   The installation wizard cannot run on your configuration.
   It will now stop. For more details about installation error logs,
   enter the phrase "installation log files" in the Search field
   at this site: http://publib.boulder.ibm.com/infocenter/tsminfo/v6r3.
   ```

4. To start the wizard without saving your responses, enter the following command:

   ```
   ./install.bin -i console
   ```

   To start the wizard and save your responses, enter the following command and specify the -r option.

   ```
   ./install.bin -i console -r /path_name/response.rsp
   ```

   where *path_name* is the full directory path to where you want the response file to be created. If you do not specify a fully qualified name, the response file is placed in a temporary directory.

5. Select the language for your installation and follow the wizard, selecting **Next** to step through the wizard.

   Select the product that you are entitled to use and a license agreement is displayed. You can select only one product on the page. If you select Tivoli Storage Manager, Tivoli Storage Manager Extended Edition, or System Storage Archive Manager, you are asked if you will be using LAN-free or library sharing. If you select **YES**, you must accept the Tivoli Storage Manager for Storage Area Networks license agreement. This is in addition to the license for the product that you chose on the previous page.

   Select the components that you want to install. Components include the server, languages, license, device driver, and storage agent. There is no default, so you must make a selection. If you previously installed a server, ensure that you select the same directory when you install a language package, license, or device driver. If you previously installed a storage agent, ensure that you select the same directory if you return to install a device driver.

   A server and a storage agent cannot be installed on the same workstation.

The Tivoli Storage Manager client application programming interface (API), DB2 Version 9.7, and IBM Global Security Kit (GSKit) Version 8 are automatically installed when you select the server component.

At the end of the upgrade, a summary is provided. If errors occurred during the upgrade, another summary page lists the errors and directs you to an error log file. The installation log is stored in the following location:

```
/var/tivoli/tsm
```

Upgrading Tivoli Storage Manager in silent mode

Using silent mode is one method of upgrading Tivoli Storage Manager from Version 6.

See Chapter 5, "Upgrading to Tivoli Storage Manager Version 6.3 or later," on page 77 for an overview of the upgrade steps, before starting the upgrade.

Pass the variables in Table 27 into this file to define the silent upgrade:

```
./install.bin
```

Table 27. Variables for the silent upgrade

Variable	Description
• -DIBM_TSM_LICENSE_ACCEPTED=true • -DIBM_TSMEE_LICENSE_ACCEPTED=true • -DIBM_SSAM_LICENSE_ACCEPTED=true • -DIBM_TSMSAN_LICENSE_ACCEPTED=true (required)	Specify one or two variables or the installation stops. It also stops if you specify more than two variables. The wizard installs the license agreement for the Tivoli Storage Manager product that is selected. **Tip:** If two products are specified, the wizard checks that one of them is the Tivoli Storage Manager for Storage Area Networks license: IBM_TSMSAN_LICENSE_ACCEPTED=true. If one variable is not, the wizard stops.
For command line: -DINSTANCE_CRED="*instance1 userid1 password1*, *instance2 userid2 password2*" (required) For response file: INSTANCE_CRED=*instance1 userid1 password1*, *instance2 userid2 password2* (required)	Enter the instance credentials used by the upgrade wizard to redefine the database instance in an upgrade from V6.1. Use quotation marks around the credentials when you pass them into the command line. Specify multiple instances by separating them with a comma. To find the existing server instances, issue this command: /opt/tivoli/tsm/db2/instance/db2ilist **Tip:** An instance cannot be in both the INSTANCE_CRED and the INSTANCE_OMIT parameters. All of the instances that exist when an installation package is upgraded must be listed in either the INSTANCE_CRED or the INSTANCE_OMIT parameters. Or, the silent upgrade fails.

Upgrading the Tivoli Storage Manager server

Table 27. Variables for the silent upgrade (continued)

Variable	Description

For command line:-
`DINSTANCE_OMIT="instance3, instance4"`
(optional)
For response file:
`INSTANCE_OMIT=instance3, instance4`
(optional)
	Enter any instances that will not be recreated as part of the upgrade from V6.1. Use this variable if you have an instance that exists but is not used. Use it if you removed the instance user ID, forgot the password, or otherwise do not want to create the instance as part of an upgrade.
	
	Use quotation marks around the credentials when you pass them into the command line. Specify multiple instances by separating them with a comma.
	Tip: An instance cannot be in both the INSTANCE_CRED and the INSTANCE_OMIT parameters. All of the instances that exist when an installation package is upgraded must be listed in either the INSTANCE_CRED or the INSTANCE_OMIT parameters. Or, the silent upgrade fails.

`-DINSTALL_DEVICES=1` (optional)	Upgrade the Tivoli Storage Manager device driver.
`-DINSTALL_LICENSE=1` (required for base packages)	Upgrade the Tivoli Storage Manager server license component. This variable should be specified only if the package being upgraded includes Tivoli Storage Manager server license files or the installation might fail. This option is typically required only for a first-time upgrade of the base release package. This option should not be used when installing most fix packs and interim fix packages because they do not include the server licenses.
`-DINSTALL_SERVER=1` (optional)	Upgrade the Tivoli Storage Manager server component.
`-DINSTALL_STAGENT=1` (optional)	Upgrade the Tivoli Storage Manager storage agent. A server and a storage agent cannot be installed on the same workstation.

Table 27. Variables for the silent upgrade (continued)

Variable	Description
-DINSTALL_*language_package*=1 (optional)	Upgrade a specific language pack. You can install the following server language-packages during the silent installation, using these variables: • INSTALL_GERMAN • INSTALL_SPANISH • INSTALL_FRENCH • INSTALL_ITALIAN • INSTALL_BRPORTUGUESE • INSTALL_KOREAN • INSTALL_JAPANESE • INSTALL_RUSSIAN • INSTALL_SCHINESE • INSTALL_TCHINESE • INSTALL_ENGLISHUTF8 • INSTALL_GERMANUTF8 • INSTALL_SPANISHUTF8 • INSTALL_FRENCHUTF8 • INSTALL_ITALIANUTF8 • INSTALL_PTBUTF8 • INSTALL_KOREANUTF8 • INSTALL_JAPANESEUTF8 • INSTALL_SCHINESEUTF8 • INSTALL_RUSSIANUTF8 • INSTALL_TCHINESEUTF8 • INSTALL_GBKCH • INSTALL_EUCCH For example, to install the German language package, use this variable: -DINSTALL_GERMAN=1

- To enable a component during silent upgrade, append it to the **install.bin** command on a single line. For example:

```
./install.bin -i silent
-DIBM_TSM_LICENSE_ACCEPTED=true
-DINSTALL_SERVER=1 -DINSTALL_LICENSE=1
-DINSTALL_ENGLISHUTF8=1
```

- Alternatively, the component variables can be placed into a response file. The path to this response file can then be passed into the `./install.bin` command. To create this file, use the same variables that are in Table 27 on page 91.

  Remove the -D and separate the options on individual lines. Do not use quotation marks. For example:

```
INSTANCE_CRED=tsminst1 tsminst1 tsminst1
INSTANCE_OMIT=tsminst2
IBM_product_LICENSE_ACCEPTED=true
INSTALL_SERVER=1
INSTALL_SPANISH=1
```

- To use an existing response file, issue the following command:

```
./install.bin -i silent -f response_file
```

where the *response_file* is the full directory path to a file that you created in the Tivoli Storage Manager installation process. The response file contains variables that you selected during a prior installation, by using the GUI or console wizard. You might see a difference between response files, depending on which installation mode you used (GUI or console).

Fix any errors before continuing. For more information, review the following log:

```
/var/tivoli/tsm
```

Upgrading Tivoli Storage Manager in a clustered environment

To upgrade a Tivoli Storage Manager server to V6.3 or later in a clustered environment, you must complete preparation and installation tasks. The procedures vary, depending on the operating system and release.

Follow the procedure for your operating system, source release, and target release:

Table 28. Procedures for upgrading the server in a clustered environment on a Linux operating system

Source release	Target release	Procedure
V5 or V6	V6.3 or later	"Upgrading Tivoli Storage Manager to V6.3 or later in a clustered environment"

Upgrading Tivoli Storage Manager to V6.3 or later in a clustered environment

A clustering option is available for the Tivoli Storage Manager for Linux V6.3 server by using Tivoli System Automation for Multiplatforms V3.2.1.

You can download a deployment guide and configuration scripts at https://www.ibm.com/software/brandcatalog/ismlibrary/ details?catalog.label=1TW10SM35. Select the Download link to access the files.

Chapter 6. Reverting from Version 6.3 or later to the previous Version 6 server

If you must revert to the previous version of the server after an upgrade, you must have a full database backup from your original version. You must also have the server installation media for your original version and key configuration files. Carefully follow the preparation steps before you upgrade the server. By doing so, it might be possible to revert to the previous version of the Tivoli Storage Manager server with minimal loss of data.

You must have the following items from the earlier version of the server:
- Server database backup
- Volume history file
- Device configuration file
- Server options file

Use the same instructions whether you are reverting within releases or to an earlier release, for example, from 6.2.2 to 6.2.0 or from 6.2.2 to 6.1.2. The older version must match the version that you used before the upgrade to 6.3 or later.

Attention: Specify the **REUSEDELAY** parameter to help prevent backup-archive client data loss when you revert the server to a previous version.

Steps for reverting to the previous server version

Complete the following steps on the system that has the Version 6.3 or later server.
1. Back up the Version 6.3 or later database. Save the contents of the instance directory, including the volume history file, the device configuration file, and server options file. Keep these files if you want to return to the Version 6.3 or later version of the server.
2. Halt the server to shut down all server operations by using the **HALT** command.
3. Remove the database from the database manager, then delete the database and recovery log directories.
   a. Manually remove the database. One way to remove it is by issuing this command:

      `dsmserv -k instance_name removedb tsmdb1`

   b. If you must reuse the space that is occupied by the database and recovery log directories, you can now delete these directories.
4. Use the uninstallation program to uninstall the Version 6.3 or later server. Uninstallation removes the server and the database manager, with their directories. For details, see Chapter 8, "Uninstalling Tivoli Storage Manager," on page 103.
5. Reinstall the version of the server program that you were using before the upgrade to Version 6.3 or later. This version must match the version that your server was running when you created the database backup that you restore in a later step. For example, the server was at version 6.2.2.0 before the upgrade, and you intend to use the database backup that was in use on this server. You must install the 6.2.2.0 fix pack to be able to restore the database backup.
6. Copy the following files to the instance directory.

- Device configuration file
- Volume history file
- The server options file (typically `dsmserv.opt`)

7. If you are reverting to a version at or earlier than 6.1.2, complete the following steps.

   a. Locate the instance file:

      /etc/tivoli/tsm/instance.info

   b. Recreate each of the instances in the instance file by issuing the **db2icrt** command:

      ```
      /opt/tivoli/tsm/db2/instance/db2icrt -a server -u
      InstanceName InstanceName
      ```

   c. Recreate the variables in the instance file by issuing the **db2set -i** command. Issue this command for each variable in your instance file. Ensure that the variable is in quotation marks:

      ```
      /opt/tivoli/tsm/db2/instance/db2set —i InstanceName "Variable"
      ```

8. Format the database by using the **DSMSERV FORMAT** utility. For details, see the information for the version of the server that you are reinstalling.

   Information for Version 6.2 is available at this information center: http://pic.dhe.ibm.com/infocenter/tsminfo/v6r2.

   Information for Version 6.1 is available at this information center: http://publib.boulder.ibm.com/infocenter/tsminfo/v6.

9. Restore the database to a point in time before the upgrade. For more details, see the restoring the server database to a point in time section in the *Administrator's Guide*.

10. If you enabled data deduplication for any FILE-type storage pools that existed before the upgrade, or if you moved data that existed before the upgrade into new storage pools while using the Version 6.3 or later server, you must complete additional recovery steps. For more details, see "Additional recovery steps if you created new storage pools or enabled data deduplication" on page 97.

11. If the **REUSEDELAY** parameter setting on storage pools is less than the age of the database that you restored, restore volumes on any sequential-access storage pools that were reclaimed after that database backup. Use the **RESTORE VOLUME** command.

    If you do not have a backup of a storage pool, audit the reclaimed volumes by using the **AUDIT VOLUME** command, with the **FIX=YES** parameter to resolve inconsistencies. For example:

    ```
    audit volume volume_name fix=yes
    ```

12. If client backup or archive operations were completed using the Version 6.3 or later server, audit the storage pool volumes on which the data was stored.

13. If you were using active-data pools before you upgraded to Version 6.3 or later, you must recreate them.

    The amount of time required to recreate the active-data pools might be significant, depending on the number and size of the active-data pools to be recreated.

Additional recovery steps if you created new storage pools or enabled data deduplication

If you created new storage pools, turned on data deduplication for any FILE-type storage pools, or did both while your server was running as a Version 6.3 or later server, you must complete more steps to return to the previous server version.

To complete this task, you must have a complete backup of the storage pool that was created before the upgrade to Version 6.3 or later.

Use this information if you did either or both of the following actions while your server was running as a Version 6.3 or later server:

- You enabled the data deduplication function for any storage pools that existed before the upgrade to Version 6.3 or later program. Data deduplication applies only to storage pools that use a FILE device type.
- You created new, primary storage pools after the upgrade, *and* moved data that was stored in other storage pools into the new storage pools.

Perform these steps after the server is again restored to V6.1 or V6.2.

- For each storage pool for which you enabled the data deduplication function, restore the entire storage pool by using the **RESTORE STGPOOL** command.
- For storage pools that you created after the upgrade, determine what action to take. Data that was moved from existing, V6.1 or V6.2 storage pools into the new storage pools might be lost because the new storage pools no longer exist in your restored V6.1 or V6.2 server. Possible recovery depends on the type of storage pool:
  - If data was moved from V6.1 or V6.2 DISK-type storage pools into a new storage pool, space that was occupied by the data that was moved was probably reused. Therefore, you must restore the original, V6.1 or V6.2 storage pools, by using the storage pool backups that were created before the upgrade to Version 6.3 or later.

    If *no* data was moved from V6.1 or V6.2 DISK-type storage pools into a new storage pool, then audit the storage pool volumes in these DISK-type storage pools.
  - If data was moved from V6.1 or V6.2 sequential-access storage pools into a new storage pool, that data might still exist and be usable in storage pool volumes on the restored V6.1 or V6.2 server. The data might be usable if the **REUSEDELAY** parameter for the storage pool was set to a value that prevented reclamation while the server was running as a Version 6.3 or later server. If any volumes were reclaimed while the server was running as a Version 6.3 or later server, restore those volumes from storage pool backups that were created before the upgrade to Version 6.3 or later.

Chapter 7. Reference: DB2 commands for Tivoli Storage Manager server databases

Use this list as reference when you are directed to issue DB2 commands by IBM support.

Purpose

After using the wizards to install and configure Tivoli Storage Manager, you seldom need to issue DB2 commands. A limited set of DB2 commands that you might use or be asked to issue are listed in Table 29. This list is supplemental material only and is not a comprehensive list. There is no implication that a Tivoli Storage Manager administrator will use it on a daily or ongoing basis. Samples of some commands are provided. Details of output are not listed.

For a full explanation of the commands described here and of their syntax, see http://pic.dhe.ibm.com/infocenter/db2luw/v9r7.

Table 29. DB2 commands

Command	Description	Example

db2icrt	Creates DB2 instances in the home directory of the instance owner. **Tip:** The Tivoli Storage Manager configuration wizard creates the instance used by the server and database. After a server is installed and configured through the configuration wizard, the **db2icrt** command is generally not used.
	
	This utility is in the `DB2DIR/instance` directory, where `DB2DIR` represents the installation location where the current version of the DB2 database system is installed.
		Manually create a Tivoli Storage Manager instance. Enter the command on one line:
		
		`/opt/tivoli/tsm/db2/instance/`
		`db2icrt -a server -s ese -u`
		`instance_name instance_name`

db2set	Displays DB2 variables.	List DB2 variables: `db2set`
CATALOG DATABASE	Stores database location information in the system database directory. The database can be located either on the local workstation or on a remote database partition server. The server configuration wizard takes care of any catalog needed for using the server database. Run this command manually, after a server is configured and running, only if something in the environment changes or is damaged.	Catalog the database: `db2 catalog database tsmdb1`
CONNECT TO DATABASE	Connects to a specified database for command-line interface (CLI) use.	Connect to the Tivoli Storage Manager database from a DB2 CLI: `db2 connect to tsmdb1`

Reference: DB2 commands for Tivoli Storage Manager server databases

Table 29. DB2 commands (continued)

Command	Description	Example

GET DATABASE CONFIGURATION	Returns the values of individual entries in a specific database configuration file. **Important:** This command and parameters are set and managed directly by DB2. They are listed here for informational purposes and a means to view the existing settings. Changing these settings might be advised by IBM support or through service bulletins such as APARs or Technical Guidance documents (technotes). Do not change these settings manually. Change them only at the direction of IBM and only through the use of Tivoli Storage Manager server commands or procedures.	Show the configuration information for a database alias:
		`db2 get db cfg for tsmdb1`
		
		Retrieve information in order to verify settings such as database configuration, log mode, and maintenance.
		`db2 get db config for tsmdb1 show detail`

GET DATABASE MANAGER CONFIGURATION	Returns the values of individual entries in a specific database configuration file. **Important:** This command and parameters are set and managed directly by DB2. They are listed here for informational purposes and a means to view the existing settings. Changing these settings might be advised by IBM support or through service bulletins such as APARs or Technical Guidance documents (technotes). Do not change these settings manually. Change them only at the direction of IBM and only through the use of Tivoli Storage Manager server commands or procedures.	Retrieve configuration information for the database manager: `db2 get dbm cfg`
GET HEALTH SNAPSHOT	Retrieves the health status information for the database manager and its databases. The information returned represents a snapshot of the health state at the time the command was issued. Tivoli Storage Manager monitors the state of the database using the health snapshot and other mechanisms that are provided by DB2. There might be cases where the health snapshot or other DB2 documentation indicates that an item or database resource might be in an alert state. Such a case indicates that action must be considered to remedy the situation. Tivoli Storage Manager monitors the condition and responds appropriately. Not all declared alerts by the DB2 database are acted on.	Receive a report on DB2 health monitor indicators: `db2 get health snapshot for database on tsmdb1`

GRANT (Database Authorities)	Grants authorities that apply to the entire database rather than privileges that apply to specific objects within the database.	Grant access to the user ID itmuser:
		`db2 GRANT CONNECT ON DATABASE TO USER itmuser`
		`db2 GRANT CREATETAB ON DATABASE TO USER itmuser`

Table 29. DB2 commands (continued)

Command	Description	Example

RUNSTATS	Updates statistics about the characteristics of a table and associated indexes or statistical views. These characteristics include number of records, number of pages, and average record length.
	
	To see a table, issue this utility after updating or reorganizing the table.
	
	A view must be enabled for optimization before its statistics can be used to optimize a query. A view that is enabled for optimization is known as a statistical view. Use the DB2 **ALTER VIEW** statement to enable a view for optimization. Issue the **RUNSTATS** utility when changes to underlying tables substantially affect the rows returned by the view.
	Tip: The server configures DB2 to run the **RUNSTATS** command as needed.
		Update statistics on a single table.
		
		`db2 runstats on table`
		`SCHEMA_NAME.TABLE_NAME`
		`with distribution and sampled`
		`detailed indexes all`

SET SCHEMA	Changes the value of the **CURRENT SCHEMA** special register, in preparation for issuing SQL commands directly through the DB2 CLI. **Tip:** A special register is a storage area that is defined for an application process by the database manager. It is used to store information that can be referenced in SQL statements.	Set the schema for Tivoli Storage Manager: `db2 set schema tsmdb1`
START DATABASE MANAGER	Starts the current database manager instance background processes. The Tivoli Storage Manager server starts and stops the instance and database whenever the server starts and halts. **Important:** Allow the Tivoli Storage Manager server to manage the starting and stopping of the instance and database unless otherwise directed by IBM support.	Start the database manager: `db2start`
STOP DATABASE MANAGER	Stops the current database manager instance. Unless explicitly stopped, the database manager continues to be active. This command does not stop the database manager instance if any applications are connected to databases. If there are no database connections, but there are instance attachments, the command forces the instance attachments to stop first. Then, it stops the database manager. This command also deactivates any outstanding database activations before stopping the database manager. This command is not valid on a client. The Tivoli Storage Manager server starts and stops the instance and database whenever the server starts and halts. **Important:** Allow the Tivoli Storage Manager server to manage the starting and stopping of the instance and database unless otherwise directed by IBM support.	Stop the database manager: `db2 stop dbm`

Chapter 8. Uninstalling Tivoli Storage Manager

You can use the following procedures to uninstall Tivoli Storage Manager. Before you remove Tivoli Storage Manager, there are several steps to complete to ensure that you do not lose your backup and archive data.

Complete the following steps before you uninstall Tivoli Storage Manager:
- Complete a full database backup.
- Save a copy of the volume history and device configuration files.
- Store the output volumes in a safe location.

Important: Uninstalling Tivoli Storage Manager removes all components of the Tivoli Storage Manager server Version 6.3 or later. It is not possible to uninstall a single component of the product by itself. For example, you cannot uninstall only the Tivoli Storage Manager device driver and leave the Tivoli Storage Manager server.

To uninstall Tivoli Storage Manager, complete the following steps:
1. Change to the following directory: /opt/tivoli/tsm/_uninst by issuing this command:

   `cd /opt/tivoli/tsm/_uninst`
2. Use one of the following methods to uninstall Tivoli Storage Manager:
   - To use the installation wizard (GUI) to uninstall Tivoli Storage Manager, issue this command:

      `./Uninstall_Tivoli_Storage_Manager`
   - To use the console to uninstall Tivoli Storage Manager, issue this command:

      `./Uninstall_Tivoli_Storage_Manager -i console`
   - To silently uninstall Tivoli Storage Manager, issue this command:

      `./Uninstall_Tivoli_Storage_Manager -i silent`
3. Follow the prompts to uninstall Tivoli Storage Manager.
4. You see a message that the Tivoli Storage Manager uninstallation was successful.

See Chapter 2, "Installing the Tivoli Storage Manager server components," on page 35 for installation steps to reinstall the Tivoli Storage Manager components.

Uninstalling and reinstalling Tivoli Storage Manager

If you plan to manually reinstall Tivoli Storage Manager instead of using the wizard, there are a number of steps to take to preserve your server instance names and database directories. During an uninstallation, any server instances you had set up are removed, but the database catalogs for those instances still exist.

If you are using the wizard to upgrade from Tivoli Storage Manager Version 6.1 or Version 6.2, it is not necessary to complete these steps, the wizard completes them automatically. To manually uninstall and reinstall Tivoli Storage Manager complete the following steps:
1. Make a list of your current server instances before proceeding to the uninstallation. Run the following command:

```
/opt/tivoli/tsm/db2/instance/db2ilist
```

2. Run the following commands for every server instance:

```
db2 attach to instance_name
db2 get dbm cfg show detail
db2 detach
```

Keep a record of the database path for each instance.

3. Uninstall Tivoli Storage Manager. See Chapter 8, "Uninstalling Tivoli Storage Manager," on page 103.

4. When you uninstall any version of Tivoli Storage Manager 6.1 or later, including a fix pack, an instance file is created. The instance file is created to help reinstall Tivoli Storage Manager. Check this file and use the information when you are prompted for the instance credentials when reinstalling. In silent installation mode, you provide these credentials using the INSTANCE_CRED variable.

You can find the instance file in the following location:

```
/etc/tivoli/tsm/instance.info
```

5. Reinstall Tivoli Storage Manager. See Chapter 2, "Installing the Tivoli Storage Manager server components," on page 35.

6. Recreate your server instances. See "Creating the server instance" on page 54.

Tip: The installation wizard configures the server instances but you must verify that they exist. If they do not exist, you must manually configure them.

7. Catalog the database. Log in to each server instance as the instance user, one at a time, and issue the following commands:

```
db2 catalog database tsmdb1
db2 attach to instance_name
db2 update dbm cfg using dftdbpath instance_directory
db2 detach
```

8. Verify that the server instance was created successfully. Issue this command:

```
/opt/tivoli/tsm/db2/instance/db2ilist
```

9. Verify that Tivoli Storage Manager recognizes the server instance by listing your directories. Your home directory appears if you did not change it. Your instance directory does appear if you used the configuration wizard. Issue this command:

```
db2 list database directory
```

If you see TSMDB1 listed, you can start the server.

Part 2. Installing and upgrading Tivoli Monitoring for Tivoli Storage Manager

IBM Tivoli Monitoring for Tivoli Storage Manager brings together multiple components to monitor Tivoli Storage Manager servers, and to produce historical reports about server and client activities.

Chapter 9. Installing Tivoli Monitoring for Tivoli Storage Manager

Tivoli Monitoring for Tivoli Storage Manager brings together multiple components, to provide real-time monitoring, and historical reporting for your Tivoli Storage Manager servers.
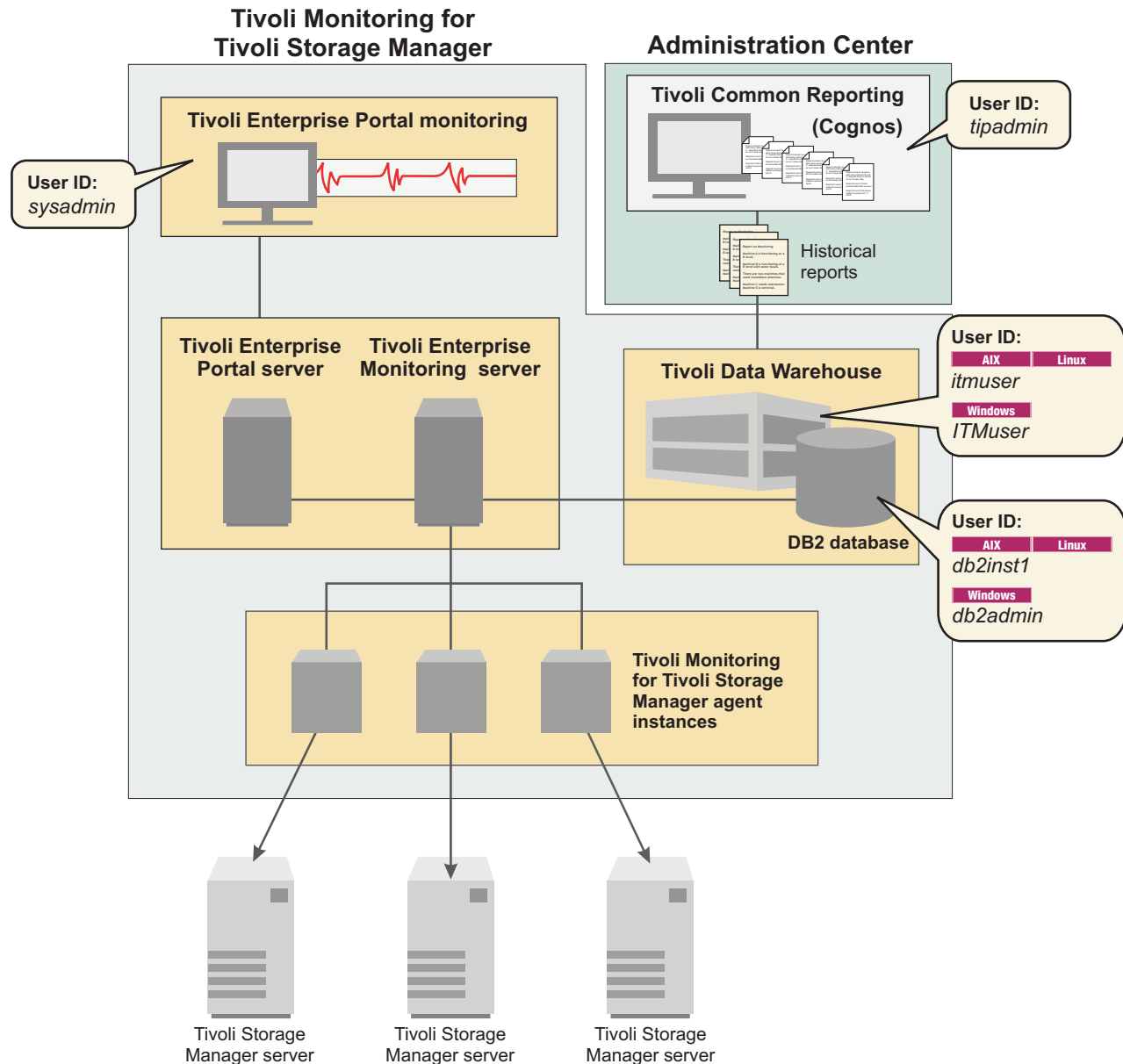
Figure 4. Tivoli Monitoring for Tivoli Storage Manager components that provide the reporting and monitoring capabilities

Building a system that can monitor data and produce reports includes the following tasks:

107

Installing Tivoli Monitoring for Tivoli Storage Manager

1. Installing Tivoli Monitoring for Tivoli Storage Manager, which includes these components:
   - IBM DB2
   - IBM Tivoli Monitoring, which includes:
     - Tivoli Enterprise Portal server
     - Tivoli Data Warehouse
     - Tivoli Enterprise Monitoring server
     - Summarization Pruning agent
     - Warehouse Proxy agent
     - Tivoli Monitoring for Tivoli Storage Manager agent
2. Creating and configuring the agent instance to point to the Tivoli Storage Manager servers that you want to monitor.
3. Installing the Administration Center, including the Tivoli Common Reporting component, to view historical reports.

   Note: The Administration Center, Tivoli Monitoring for Tivoli Storage Manager, and the monitoring agents must all be at version 6.3 or later. The Tivoli Storage Manager server that you want to monitor can be V5.4 - V6.3 or later.

   Related tasks:

   "Installing on AIX and Linux systems" on page 120

   Chapter 19, "Installing and configuring the Administration Center," on page 189

   "Creating and configuring the agent instance" on page 125

   Related reference:

   "Installation checklist" on page 117

Planning to install

Be sure to review all applicable planning information, including system requirements, capacity planning, and installation scenarios, before installing.

Before you install the software, complete these tasks:
1. Choose an installation scenario that best suits your needs.
2. Read the system requirements that are required for your operating system.
3. Review the capacity planning information.
4. Review the installation work sheet and note the user IDs, passwords, and other values that are required during installation.
5. Optionally run the prerequisite checker to verify the readiness of your installation environment.

To view historical reports, you must install the Administration Center, including the Tivoli Common Reporting component, on the same system where you installed Tivoli Monitoring for Tivoli Storage Manager. You can install either one first, but you must select the Tivoli Common Reporting component during the Administration Center installation.

If you installed the Administration Center without the Tivoli Common Reporting component, you must rerun the Administration Center installer to install the Tivoli Common Reporting component and to view historical reports.

Restriction: Install the Administration Center and Tivoli Monitoring for Tivoli Storage Manager on a system that is different than the system where the Tivoli

Storage Manager server is installed.

Installation scenarios

Before installing Tivoli Monitoring for Tivoli Storage Manager, choose the scenario that best meets the needs of your business.

- Scenario 1: New installation, intending to monitor 1 - 5 Tivoli Storage Manager servers.
- Scenario 2: New installation, intending to monitor more than 5 Tivoli Storage Manager servers.
- Scenario 3: Installing in to an existing IBM Tivoli Monitoring environment, intending to monitor 1 - 5 Tivoli Storage Manager servers.
- Scenario 4: Installing in to an existing IBM Tivoli Monitoring environment, intending to monitor more than 5 Tivoli Storage Manager servers.

Important Notes:

1. If you have a Tivoli Storage Manager server that is in a different timezone than the system with Tivoli Monitoring for Tivoli Storage Manager, install the monitoring agent on the Tivoli Storage Manager server. See Scenario 2 to install the agent directly on the Tivoli Storage Manager server.
2. If you have more than five servers, installing the monitoring agent on each of the Tivoli Storage Manager servers is the most efficient use of memory on both the Tivoli Storage Manager server, and the Tivoli Monitoring for Tivoli Storage Manager server.

Table 30. Installation scenarios

Scenario Number	Description	Tasks that you must complete
Scenario 1	Use this scenario for a new installation with a plan to monitor and report on 1- 5 Tivoli Storage Manager servers.	Perform all the tasks in this scenario on the same system: 1. Install Tivoli Monitoring for Tivoli Storage Manager. The approximate installation time is 45 - 90 minutes, depending on the speed of your system. 2. Configure the agent instance that was installed as part of the Tivoli Monitoring for Tivoli Storage Manager installation package. The approximate configuration time is 10 minutes. 3. Install the Administration Center on the same system as Tivoli Monitoring for Tivoli Storage Manager. Ensure that you select the Tivoli Common Reporting component during installation. The approximate installation time is 45 - 90 minutes, depending on the speed of your system. **Notes:** 1. You cannot install IBM Tivoli Monitoring for Tivoli Storage Manager on a system where Tivoli Storage Manager server is installed. 2. However, you can install the monitoring agent on any remote Tivoli Storage Manager server that you want to monitor.

Installing Tivoli Monitoring for Tivoli Storage Manager

Table 30. Installation scenarios (continued)

Scenario Number	Description	Tasks that you must complete
Scenario 2	Use this scenario for a new installation with a plan to monitor and report on more than 5 Tivoli Storage Manager servers.	1. Install Tivoli Monitoring for Tivoli Storage Manager. The approximate installation time is 45 - 90 minutes, depending on the speed of your system. 2. Install monitoring agents on each Tivoli Storage Manager server that you want to monitor. The approximate installation time is 15 - 30 minutes per additional agent. 3. Configure the agents to point to the Tivoli Enterprise Monitoring server host installed in Step 1. The approximate configuration time is 10 minutes per agent. 4. Install the Administration Center on the same system as Tivoli Monitoring for Tivoli Storage Manager. Ensure that you select the Tivoli Common Reporting component during installation. The approximate installation time is 45 - 90 minutes, depending on the speed of your system. **Notes:** 1. You cannot install IBM Tivoli Monitoring for Tivoli Storage Manager on a system where Tivoli Storage Manager server is installed. 2. However, you can install the monitoring agent on any remote Tivoli Storage Manager server that you want to monitor. **Restriction:** The monitoring agent is not supported on Solaris, HP, and Linux ppc64.
Scenario 3	Use this scenario when you install the software into an existing IBM Tivoli Monitoring environment with a plan to monitor up to 5 Tivoli Storage Manager servers.	1. Install the new monitoring agent on the IBM Tivoli Monitoring server where Tivoli Enterprise Monitoring server and Tivoli Enterprise Portal server are installed. The approximate installation time is 15 - 30 minutes per additional agent. 2. Configure each agent to point to the system where the Tivoli Enterprise Monitoring server and Tivoli Enterprise Portal server are installed. The approximate configuration time is 10 minutes per agent. **Notes:** 1. You cannot install IBM Tivoli Monitoring for Tivoli Storage Manager on a system where Tivoli Storage Manager server is installed. 2. However, you can install the monitoring agent on any remote Tivoli Storage Manager server that you want to monitor.

Table 30. Installation scenarios (continued)

Scenario Number	Description	Tasks that you must complete
Scenario 4	Use this scenario when you install the software into an existing IBM Tivoli Monitoring environment with a plan to monitor more than 5 Tivoli Storage Manager servers.	1. Install the new monitoring agent on the Tivoli Storage Manager server that you want to monitor. The approximate installation time is 15 - 30 minutes per additional agent. 2. Configure each agent to point to the system where the Tivoli Enterprise Monitoring server and Tivoli Enterprise Portal server are installed. The approximate configuration time is 10 minutes per agent. **Notes:** 1. You cannot install IBM Tivoli Monitoring for Tivoli Storage Manager on a system where Tivoli Storage Manager server is installed. 2. However, you can install the monitoring agent on any remote Tivoli Storage Manager server that you want to monitor. **Restriction:** The monitoring agent is not supported on Solaris, HP, and Linux ppc64.

Related tasks:

"Installing on AIX and Linux systems" on page 120

Related reference:

"Installation worksheet" on page 115

"Installation checklist" on page 117

System requirements for Tivoli Monitoring for Tivoli Storage Manager

Review the hardware and software requirements applicable for your system before you install Tivoli Monitoring for Tivoli Storage Manager.

Other than installing the Tivoli Monitoring for Tivoli Storage Manager, you can install the monitoring agent separately on your Tivoli Storage Manager servers. The monitoring agent is supported on any Tivoli Storage Manager server except for the following operating systems:

- Solaris
- HP
- Linux PPC

Related tasks:

"Capacity planning" on page 115

"Running the prerequisite checker" on page 119

Related reference:

"Installation worksheet" on page 115

"Installation checklist" on page 117

System requirements

There are hardware and software requirements that your system must meet before you install Tivoli Monitoring for Tivoli Storage Manager on a Linux system.

Hardware requirements

These tables list the minimum hardware and software requirements required for Tivoli Monitoring for Tivoli Storage Manager. Use these requirements as a starting point, but you can find the latest information at http://www.ibm.com/support/docview.wss?uid=swg21569311.

Table 31 describes the hardware requirements for the Tivoli Monitoring for Tivoli Storage Manager.

Table 31. Hardware requirements

Type of hardware	Hardware requirements
Hardware	• Dual core Intel Pentium compatible processor or multiprocessor-based computer with a 2 GHz or greater processor • Network interface card
Disk space	If you are installing the full Tivoli Monitoring for Tivoli Storage Manager application, verify that your system meets the following minimum requirements: • 500 MB free disk space in the db2inst1 instance directory. By default, the location is /home/db2inst1. The preferred amount of free disk space is 10 GB. This is where the warehouse data is stored. As historical data is gathered and stored in Tivoli Data Warehouse, the requirements increase approximately to 500 GB each year. If pruning options are set up for each attribute group, it helps to reduce the rate at which the database grows. For more information about pruning, see Configuring summarization and pruning settings. • 10 MB free disk space in the / directory. • 5 MB free disk space in the /var directory. • 350 MB free disk space in the /usr directory. • 200 MB free disk space in the /tmp directory. If you are installing only the Tivoli Monitoring for Tivoli Storage Manager agent, ensure that your system meets the following minimum requirements: • 10 MB free disk space in the / directory. • 5 MB free disk space in the /var directory. • 350 MB free disk space in the /usr directory. • 200 MB free disk space in the /tmp directory.
Memory	• 3-GB minimum • If Tivoli Storage Manager monitoring agents are installed on the Tivoli Monitoring server, memory requirements increase quickly as the number of Tivoli Storage Manager servers are monitored from that one IBM Tivoli Monitoring server. Each agent instance requires approximately a 150 MB of additional memory to run. • If a Tivoli Storage Manager monitoring agent is installed on a Tivoli Storage Manager server, there is only a single instance of the agent is running on the Tivoli Storage Manager server and no increases in memory requirements are needed by the IBM Tivoli Monitoring server.

Table 31. Hardware requirements (continued)

Type of hardware	Hardware requirements
Monitor	Set your monitor resolution to 1024 x 768 (minimum) to view the entire window.

Software requirements

Table 32 describes the minimum software requirements for Tivoli Monitoring for Tivoli Storage Manager.

Table 32. Software requirements

Type of software	Minimum software requirements

Operating systems	• RHEL 5 x86 32-bit (update 2)
	• RHEL 5 x86_64 (update 2)
	• SLES 10, 11 x86 32-bit (service pack 2)
	• SLES 10, 11 x86_64 (service pack 2)
	
	Security-enhanced Linux considerations
	    On RHEL 5 systems, if Security-enhanced Linux (SELinux) is enabled and in enforcing mode, the installer might fail due to SELinux restrictions.
	
	To determine if SELinux is installed and in enforcing mode, perform one of the following:
	    1. Check the /etc/sysconfig/selinux file
	    2. Run the **sestatus** command
	    3. Check the /var/log/messages file for SELinux notices
	
	To disable SELinux, you can do one of the following:
	    1. Set it in permissive mode and run the setenforce 0 command as a superuser
	    2. Modify /etc/sysconfig/selinux and reboot the machine
	
	If your DB2 database product installs successfully on a RHEL 5 system, DB2 processes will run in the unconfined domain. To assign DB2 processes to their own domains, modify the policy. A sample SELinux policy is provided in the sqllib/samples directory
	Important: If you are installing a Tivoli Monitoring for Tivoli Storage Manager agent, and you previously installed an IBM Tivoli Monitoring server, you must install the agent on the existing Tivoli Enterprise Monitoring server. Tivoli Monitoring for Tivoli Storage Manager is only supported with IBM Tivoli Monitoring, version 6.2.2 FP2 or later.

Installing Tivoli Monitoring for Tivoli Storage Manager

Table 32. Software requirements (continued)

Type of software	Minimum software requirements
Web browser	A web browser to log on and use the console. The web browser can be installed on the same or a separate system. The following browsers can be used: • Microsoft Internet Explorer 7 • Microsoft Internet Explorer 8 • Firefox 3.5 IBM Java version 5 is required to launch Tivoli Enterprise Portal. If the Common Reporting portlet is blank when opened in Internet Explorer 7, the default security settings might be too restrictive. Complete these steps to modify the security settings: 1. In an Internet Explorer version 7 window, click **Tools** > **Internet Options**, and on the Security tab, click **Custom level**. 2. Locate the **Miscellaneous** category, disable the **Access data sources across domains** option, and click OK to apply the changes. **Tip:** If your browser still does not display correctly, consider using a different browser. To avoid potential compatibility issues with Web browsers you can view the Tivoli Enterprise Portal remotely using the Java Web Start applet: • Connect to http://*hostname:1920*. • Click **IBM Tivoli Enterprise Portal Web Start Client** to start the Java Web Start Client. • Optionally create a desktop shortcut to start the Tivoli Enterprise Portal in the future.

Libraries	**GNU C libraries**
	    Version 2.3.3-98.38 or later that is installed on the Tivoli Storage Manager system.
	
	Red Hat Enterprise Linux (RHEL) and SUSE Linux Enterprise Servers:
	    For Linux x86_32 server:
	
	``
	compat-libstdc++-33-3.2.3-61 (RHEL)
	libstdc++-33-3.2.3-61 (Suse Linux)
	``
	
	For Linux x86_64 server:
	    libaio.so.1 is required for DB2 database servers using asynchronous I/O.
	
	    libstdc++.so.5 is required for DB2 Net Search Extender
	
	    libstdc++.so.6 is required for DB2 database servers and clients.
	
	If IBM Tivoli System Automation for Multiplatforms, or IBM Tivoli Monitoring for Databases: DB2 Agent is used, libstdc++.so.5 is needed.

Communication Protocol	At least one of the following communication protocols: • Named Pipes • TCP/IP Version 4 or Version 6
Other software and software considerations	• Eclipse 3.3 and Business Intelligence and Reporting Tools (BIRT), version 2.2.1 are required for creating custom BIRT reports. • Korn Shell (ksh)
X Window System or X11 GUI	Supplied with Linux software.

Related tasks:

"Capacity planning"

"Running the prerequisite checker" on page 119

"Installing on AIX and Linux systems" on page 120

Related reference:

"Installation worksheet"

"Installation checklist" on page 117

Capacity planning

Planning details include determining how many servers that you want to monitor, how many agents and agent instances are required, and how much memory, and space is necessary for growth over time.

The following list provides planning guidelines so you can anticipate the growth of your system over time, depending on how many monitoring agents are in your environment:

- Each agent instance, whether it is an IBM Tivoli Monitoring agent, or a Tivoli Monitoring for Tivoli Storage Manager agent, requires approximately 150 MB of memory.
- Each agent also requires up to 15% processor resources during data collection.
- During a one-year period, the data *WAREHOUS* can grow to approximately 500 GB for each Tivoli Storage Manager server that is being monitored using the installation defaults. This value depends on the number of nodes that are being backed up and archived to that server, and the frequency that backups are occurring. Enabling pruning on the monitoring server can reduce the size of the WAREHOUS database by approximately 50 percent.

Related tasks:

"Configuring summarization and pruning settings" on page 130

Related reference:

"Installation worksheet"

"Installation checklist" on page 117

Installation worksheet

Use this worksheet to record information that you need when you install and administer Tivoli Monitoring for Tivoli Storage Manager. The worksheet includes several passwords for user accounts that are created during the installation. The worksheet is intended to help you remember the values that you chose after completing the installation.

Installing Tivoli Monitoring for Tivoli Storage Manager

Table 33. Tivoli Monitoring for Tivoli Storage Manager installation worksheet

Item	Description	Default value*	Your value
DB2 user IDs db2inst1	Database administrator This is the Tivoli Data Warehouse user name and password. This user has permission to complete all the administrative tasks in DB2.	**User name:** db2inst1 **Password:** The password must be 8 - 14 characters in length and can include letters, numbers, @, or #.	
DB2 port	Default port number	The default port number is: 50000. Valid port numbers are 1024 - 65535.	
db2grp1	This is the group that the DB2 instance user ID belongs to.		
encryption key	A default encryption key is provided and the fields are prefilled with the default key. You can specify a different key, however, it is not necessary. The encryption key is used to establish a secure connection (using SSL protocol) between the Hub TEMS and the other components of the IBM Tivoli Monitoring environment. The encryption key must be the same for all of the agents accessing the Tivoli Enterprise Monitoring server.	IBMTivoliMonitoringEncryptionKey Must be exactly 32 characters in length. Valid characters are A-Z, a-z, 0-9, @, !, and #.	
sysadmin	Tivoli Enterprise Portal user name and password. This user ID is not automatically generated during the installation process. You can log in to the Tivoli Enterprise Portal without specifying a password. If you want this ID to require a password during login, you can manually create the sysadmin ID, and specify a password.	**User name:** sysadmin **Password:** The password must be 8 - 14 characters in length and can include letters, numbers, @, or #.	
itmuser	Tivoli Data Warehouse user name and password. This user has access to read the information from the *WAREHOUS* database. **Note:** You are only prompted for this information during configuration of the warehouse, not at installation time.	**User name:** itmuser **Password:** The password must be 8 - 14 characters in length and can include letters, numbers, @, or #.	
DB2 home directory	You can specify which directory that you want to store the DB2 instance information. This is where the database is stored by default. If you specify /home, the instance information is stored in /home/db2inst1. If you specify /information/db2, the instance information is stored in /information/db2/db2inst1. Ensure that there is enough space available in this directory and that the directory has write-access. For additional planning help see Capacity planning.	The default value is /home.	

Table 33. Tivoli Monitoring for Tivoli Storage Manager installation worksheet (continued)

Item	Description	Default value*	Your value
Monitoring agent instance name	You can specify the name of the monitoring agent instance. If you intend to monitor more than one Tivoli Storage Manager server, you must have unique agent instance names for each instance. When specifying an instance name, the best practice is to specify the host name of the Tivoli Storage Manager server, or the server name from the **QUERY STATUS** command as your agent instance name. Instance names cannot exceed 20 characters. **Note:** The monitoring agent instances can be created and configured after the installation.	**Your first agent instance name:** **Your second agent instance name:** **Your third agent instance name:** **More agent instance names...:**	
Administration Center information	Ensure that you have the Administration Center installation information ready during the installation, such as the port number, fully qualified host name, and Tivoli Integrated Portal user ID and password.	The default port is 1500 Fully qualified host name: Tivoli Integrated Portal **User name:** **Password:**	
Location and the name of the SSL certificate	Needed when using the SSL feature instead of TCP IP.		
*Best practices are to use the default values listed here. If you change these values ensure that you document them because they are needed later.			

Related tasks:

Related reference:

"Installation checklist"

Installation checklist

This checklist summarizes the steps that are required to install and configure a system that can monitor Tivoli Storage Manager server and client data and produce reports. You can print out this checklist and use it as a guide to verify that all required steps are completed.

Table 34. Installation checklist

Step	Installation task or topic	Task description
1._____	Hardware and software requirements	Ensure that your system meets the system and hardware requirements.
2._____	Capacity planning	Review the capacity planning information to ensure that you adequately plan for growth.
3._____	Installation worksheet	Complete the installation worksheet to record password values and other installation information that you need.

Installing Tivoli Monitoring for Tivoli Storage Manager

Table 34. Installation checklist (continued)

Step	Installation task or topic	Task description
4._____	Prerequisite checker	Optionally, run the prerequisite checker to ensure that your system meets all installation requirements.
5._____	Installation scenarios	Choose an installation scenario. The scenario you choose depends on the number of servers that you intend to monitor, and if there is an existing Tivoli Monitoring environment before this installation.
6._____	Installing on AIX and Linux systems	Run the Tivoli Monitoring for Tivoli Storage Manager installer. The following components are installed: • DB2 • Tivoli Monitoring, which includes the following components: – Tivoli Enterprise Portal server – Tivoli Data Warehouse – Tivoli Enterprise Monitoring server – Summarization pruning agent – Warehouse proxy agent • Tivoli Monitoring for Tivoli Storage Manager agent **Note:** If there is an existing Tivoli Monitoring environment, install only the monitoring agent.
7._____	Creating and configuring the agent instance	Install or configure the monitoring agents to connect to the Tivoli Storage Manager server. If you plan to monitor five or less Tivoli Storage Manager servers, configure the monitoring agent that was installed on this system. Otherwise, install and configure only the monitoring agent on each Tivoli Storage Manager server to be monitored. **Tip:** Create 1 agent per Tivoli Storage Manager server instance.
8._____	Configuring historical data collection using the command-line interface on AIX and Linux systems	Configure history configuration to allow data to be pruned from the *WAREHOUS* database.
9._____	Verifying the installation	Verify that the installation was complete and successful.

Table 34. Installation checklist (continued)

Step	Installation task or topic	Task description
10.____	Chapter 19, "Installing and configuring the Administration Center," on page 189	Install Tivoli Common Reporting, which is selected as part of the Administration Center installation package. **Important:** The Administration Center and Tivoli Monitoring for Tivoli Storage Manager must be installed on the same system to use Tivoli Common Reporting.

Tips:

1. To view real-time Tivoli Storage Manager server activity, use Tivoli Enterprise Portal.
2. To view historical reports, use Tivoli Common Reporting, which is part of the Administration Center.
3. For additional help, see Tivoli Monitoring for Tivoli Storage Manager troubleshooting topics.

Running the prerequisite checker

The installation prerequisite checker is an optional tool that verifies the operating system, the amount of free disk space for the installation, and other prerequisites.

To ensure that your system environment is appropriate for the installation, you can run the prerequisite checker before each installation.

Tip: The prerequisite checker verifies only the minimum memory that is necessary. More memory is required for additional tasks.

The prerequisite checker presents a summary of results at the end of the check. Any changes that are required in your environment before the installation are listed. Any new directories that are required for the installation are created.

To run the prerequisite checker, complete the following steps.

1. Ensure that the appropriate installation package is downloaded and that its files are extracted. A prerequisite checker is part of the installation package.
2. Choose the graphical interface (the default) or console method to start the installation, and follow the wizard instructions to complete the installation:
   - Issue this command to start the installation wizard using a graphical interface:

     ```
     ./prereqcheck.bin
     ```
   - Issue this command to start the installation wizard using the console method:

     ```
     ./prereqcheck.bin -i console
     ```
3. Select the language for the prerequisite checker user interface.
4. In the welcome and disclaimer panels, review the statements and accept them.

If an error message is shown in the Prerequisite Results page, make the required corrections before continuing with the installation. The summary page lists the errors and directs you to an error log file.

Related tasks:

"Installing on AIX and Linux systems"

Related reference:

"Installation checklist" on page 117

Installing on AIX and Linux systems

You can install Tivoli Monitoring for Tivoli Storage Manager using the installation wizard with either the graphical interface, or the console method.

Before you begin, ensure that you read and satisfy the installation prerequisites.

- Packages can be downloaded from Passport Advantage or from the FTP site at ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/ reporting/v6r3/LATEST.
- If you uninstalled a previous version of Tivoli Monitoring for Tivoli Storage Manager, confirm that you completed a successful uninstallation before attempting to reinstall. That includes ensuring that the db2inst1 user ID does not exist.

  Tip: The db2inst1 user ID can remain, but it must belong to the db2grp1 group. Or, you can delete the ID and it will automatically be re-created and added to the group during the installation.

  To learn more about uninstalling, see Chapter 11, "Uninstalling Tivoli Monitoring for Tivoli Storage Manager," on page 157.
- Ensure that your system meets all system requirements. See "System requirements for Tivoli Monitoring for Tivoli Storage Manager" on page 111.
- If you are installing on a remote system using an X display, and the local server does not have an X server running, the installation might fail. If this happens, you must run the wizard in console mode.
- Print a copy of the installation worksheet, or refer to it during installation. The worksheet describes the ports, directories, user IDs, and privileges that are required during installation, and any default values. The worksheet can be used to record the values that you need during installation. See Installation worksheet.

Complete the following steps to install Tivoli Monitoring for Tivoli Storage Manager:

1. Choose whether you want to install from the DVD, or a downloaded package file, and complete the steps in the following table to begin the installation:

Install from DVD media:	Install from downloaded package file:

1. Insert the DVD into the DVD drive.
Tip: Ensure that the DVD is mounted on directory `/dvdrom`
2. Optionally, run the **`prereqcheck.bin`** file to ensure that your system meets all system requirements.
3. Begin the installation using the graphical interface by issuing the following command:
`./install.bin`
 	
Experienced users: You can also run the installation wizard in console mode, by issuing the following command:
`./install.bin -i console`
	1. Change to the directory where you downloaded the package file, and ensure that this file system has approximately 6.5 GB to 7 GB of free disk space.
	Important: Ensure that you extract the installation files to an empty directory. Do not extract to a directory that contains previously extracted files, or any other files.
	2. Change the permissions on the package file, and extract the files:
	
	AIX and Linux 64-bit systems
	`chmod +x C`*xxxxxx*`.bin`
	
	where *xxxxxx* is the part number, for example: CZ1N1ML
	`./C`*xxxxxx*`.bin`
	
	Linux 32-bit:
	`tar -xvf C`*xxxxxx*`.tar`
	
	where *xxxxxx* is the part number, for example: CZ1N1ML
	3. Optionally, locate the **`prereqcheck.bin`** file and run it to ensure that your system meets all requirements.
	4. Start the graphical interface installation wizard by issuing the following command:
	`./install.bin`
	
	Experienced users: You can also run the installation wizard in console mode, by issuing the following command:
	`./install.bin -i console`

2. Verify that the installation was successful by using the steps in Verifying the installation.

To begin collecting data, you must create and configure an agent instance. See "Creating and configuring the agent instance" on page 125.

To begin working with reports, you must install the Administration Center, including the Tivoli Common Reporting component. See Chapter 19, "Installing and configuring the Administration Center," on page 189.

> **Related tasks**:
>
> "Running the prerequisite checker" on page 119
>
> Chapter 19, "Installing and configuring the Administration Center," on page 189
>
> "Creating and configuring the agent instance" on page 125
>
> **Related reference**:
>
> "Installation checklist" on page 117

Verifying the installation

After you install Tivoli Monitoring for Tivoli Storage Manager, verify that all of the components are installed and configured correctly.

To verify that the installation was successful, complete these steps:

1. Verify that the **Tivoli Enterprise Portal server** version is 06.22.02.00:

   a. Open the Manage Tivoli Enterprise Management Services application:

      - Run the CandleManage program by using the following commands:
        ```
        cd install_dir/itm/bin
        ./CandleManage &
        ```

        where *install_dir* is the installation directory. The default installation directory is /opt/tivoli/tsm/reporting.

   b. Verify that the version of **Tivoli Enterprise Portal server** is 06.22.02.00 in the **Version** column.

2. Verify that the **Monitoring Agent for Tivoli Storage Manager template** version is 06.34.00.00:

   a. Open the Manage Tivoli Enterprise Management Services application as described in Step 1.a.

   b. Verify that the version of the **Monitoring Agent for Tivoli Storage Manager template** is 06.34.00.00 in the **Version** column.

3. Verify database connectivity:

   a. Log on to the Tivoli Enterprise Portal with your sysadmin user ID and password by using one of the following methods:

      - Use the Web Client

         1) Open a web browser and go to: http://*hostname*:1920, where *hostname* is the name of your operating system.

         2) Select **IBM Tivoli Enterprise Portal Web Client**.

      - Open a web browser and specify the address of the server where the Tivoli Enterprise Portal was installed, similar to the following example:
        http://*hostname*:1920///cnp/kdh/lib/cnp.html

        where *hostname* is the server name and 1920///cnp/kdh/lib/cnp.html is the port and location of the Java Tivoli Enterprise Portal web Client.

        Tip: Always use this port number and location.

   b. Click the **Warehouse Proxy** node to highlight it in the **Navigator** pane.

      Note: The **Warehouse Proxy** node can be found in the following location:

      Enterprise > **Linux System** > *hostname* > **Warehouse Proxy**

   c. In the **Database Information** table, verify that the **DB Connectivity** has a value of YES and that the **DB Version** has a value of 9.7.

    d. Click the **Summarization and Pruning Agent** node to highlight it in the **Navigator** pane.

    e. In the Connectivity table, verify that the **TEPS Connectivity** value and the **DB Connectivity** values are YES.

4. Verify that the history configuration is configured:

    a. Log on to the Tivoli Enterprise Portal by following the steps in Step 3.a.

    b. Click **Edit** > **History Configuration**.

    c. Verify that there are several KSK_* attribute groups under the **Tivoli Storage Manager** node in the navigation pane.

    d. In the content pane, under the **Group** column, verify that there are several groups with the ![icon] icon that precedes the name. The icon indicates that the attribute is running to summarize and store data.

5. If you completed a new installation, verify that pruning is configured:

    a. Log on to the Tivoli Enterprise Portal by following the steps in Step 3.a.

    b. Click **Edit** > **History Configuration**.

    c. Click the **Tivoli Storage Manager** node to highlight it.

    d. Click any of the attribute groups with the ![icon] icon, and view the **Pruning** section in the window. If configured, all the check boxes are selected and there are numerical values in the fields. For more information, see "Configuring summarization and pruning settings" on page 130.

6. Optional: If you configured the monitoring agent and installed the Administration Center, you can verify the configuration and begin working with the reports.

    a. Log on to the Tivoli Enterprise Portal by following the steps in Step 3.a. with the *sysadmin* user ID and password and review the workspaces to verify that data is being collected.

    Note: The workspaces can be found in the **Navigator** pane under the following node:

    Enterprise > **Linux System** > *hostname* > **Tivoli Storage Manager**

    If you created multiple instances of the agent, click each agent instance that is listed under the Tivoli Storage Manager branch in the **Navigator** panel. Each agent instance has its own list of workspaces. Review a few workspaces to verify that data is coming in from the Tivoli Storage Manager server.

    You can also navigate to the **Agent Log** workspace and look for messages such as TSM login succeeded. If you see a message that indicates that the login failed, you probably specified an incorrect ID or password when you were configuring your agent instance. If data is not being collected, see the information about resolving problems with Tivoli Monitoring for Tivoli Storage Manager, in the *Problem Determination Guide*.

    b. Log on to the Administration Center:

      1) Open a web browser and enter the following address to start the Administration Center:

```
https://hostname:port/ibm/console
```

      where *port* is the port number that is specified when you installed the Tivoli Integrated Portal. The default port is 16311. The *hostname* is the host name of the system where the Administration Center is installed.

2) Enter the `tipadmin` user ID and password. The default user ID is `tipadmin`.

c. Navigate to **Reporting** > **Common Reporting**. You can view Cognos® reports by selecting **IBM Tivoli Storage Manager Cognos Reports**. You can view BIRT reports by selecting **Tivoli Products**.

Note: You might need to wait one or two hours after configuration before you can see historical data in Tivoli Common Reporting.

If you experience issues with your installation such as data not displaying in your reports, or other issues, review the information in the *Problem Determination Guide* about resolving problems with Tivoli Monitoring for Tivoli Storage Manager.

For more information about reports, see the monitoring operations section in the *Administrator's Guide*.

Taking the first steps after installation

After you install Tivoli Monitoring for Tivoli Storage Manager, there are steps you must follow to complete your setup. After the setup is complete, you can start real-time monitoring of your Tivoli Storage Manager servers and start collecting historical data so you can run Tivoli Common Reporting reports.

Complete these two steps after the installation:

1. Create an agent instance for each Tivoli Storage Manager that you want to monitor.

   You must create and configure a monitoring agent instance for each Tivoli Storage Manager server that you want to monitor. You can create up to 5 agent instances on the monitoring server. If you intend to monitor more than 5 Tivoli Storage Manager servers, you must use the installer to install only the Monitoring Agent directly on the additional Tivoli Storage Manager servers you want to monitor.

   - See "Creating and configuring the agent instance using CandleManage" on page 125.
   - See "Creating and configuring the agent instance using the command-line interface" on page 127.

2. Install the Administration Center, including the Tivoli Common Reporting component. See Chapter 19, "Installing and configuring the Administration Center," on page 189.

   To run historical reports on the Tivoli Storage Manager servers that you create agent instances for, you must install the Tivoli Common Reporting component. The Administration Center must be installed on the same system as Tivoli Monitoring for Tivoli Storage Manager. If you installed the Administration Center without the Tivoli Common Reporting component, you must rerun the Administration Center installer to install the Tivoli Common Reporting component.

Related tasks:

Chapter 19, "Installing and configuring the Administration Center," on page 189

"Creating and configuring the agent instance" on page 125

Related reference:

"Installation checklist" on page 117

Creating and configuring the agent instance

After you install Tivoli Monitoring for Tivoli Storage Manager, you must create and configure the agent instance to begin collecting data.

If your environment has less than five Tivoli Storage Manager servers, you can use the monitoring agent template that was installed as part of the Tivoli Monitoring for Tivoli Storage Manager installation to create and configure up to 5 agent instances.

If your environment has more than five Tivoli Storage Manager servers, you must install additional monitoring agents on each Tivoli Storage Manager servers that you want to monitor.

This configuration provides the most efficient use of memory on both the Tivoli Storage Manager server, and the IBM Tivoli Monitoring server.

Related tasks:

"Creating and configuring the agent instance using CandleManage"

"Creating and configuring the agent instance using the command-line interface" on page 127

"Verifying the installation" on page 122

Related reference:

"Installation checklist" on page 117

Creating and configuring the agent instance using CandleManage

After installing the Tivoli Monitoring for Tivoli Storage Manager agent, you can use the CandleManage graphical interface to create and configure an agent instance.

Complete these steps to create and configure the agent instance using the CandleManage graphical interface, or you can use the command-line interface: "Creating and configuring the agent instance using the command-line interface" on page 127.

You can monitor approximately five Tivoli Storage Manager servers from the same IBM Tivoli Monitoring server, but you must create and configure an agent instance for each server that you want to monitor. If you plan to monitor more than five servers, you should install additional monitoring agents on each of your Tivoli Storage Manager servers.

Note: The term, *agent*, is synonymous with the Tivoli Monitoring for Tivoli Storage Manager agent. This term is used throughout the CandleManage program.

To configure an agent instance, complete the following steps:

1. Run the CandleManage program using the following command:
   a. Go to the directory where the CandleManage program is located by issuing the following command:
      ```
      cd /opt/tivoli/tsm/reporting/itm/bin
      ```
   b. Run the CandleManage program by issuing this command:
      ```
      ./CandleManage &
      ```

2. In the CandleManage window, right-click **Monitoring Agent for Tivoli Storage Manager**, and select **configure**, to create an instance of the Tivoli Monitoring for Tivoli Storage Manager agent.

3. In the Manage Application Instances window, click **Add instance**.

4. In the Input window, specify an agent instance name and click **OK** For example SERVER1.

   Tip: When specifying an instance name, the best practice is to specify the host name of the Tivoli Storage Manager server, or the server name from the **QUERY STATUS** command as your instance name. Instance names must be unique, and cannot exceed 20 characters.

5. In the Agent Configuration window, complete the following fields for the Tivoli Storage Manager server to be monitored:

   a. In the **Server Address** field, enter the fully qualified IP server address for the Tivoli Storage Manager server.

   b. In the **Port Number** field, enter the port number that is used to communicate with the Tivoli Storage Manager server.

      Tip: For normal TCP/IP traffic, you can determine the port number by issuing one of the following commands:
      ```
      QUERY OPT TCPPORT
      QUERY OPT TCPADMINPORT
      ```

      For SSL encrypted TCP/IP traffic, you can determine the port number by issuing one of the following commands:
      ```
      QUERY OPT SSLTCPPORT
      QUERY OPT SSLTCPADMINPORT
      ```

   c. In the **TSM Administrator** field, enter the Tivoli Storage Manager Administrator ID used to access the server.

      Note: The IBM Tivoli Monitoring agent runs only queries on the Tivoli Storage Manager server and does not change anything. The administrator that you choose to run the queries can be an administrator ID without the following privileges:
      - System Privileges
      - Policy Privileges
      - Storage Privileges
      - Operator Privileges
      - Client Access Privileges
      - Client Owner Privileges

   d. In the **TSM Administrator Password** field, enter the password twice for the Tivoli Storage Manager Administrator ID

   e. In the **File System Location and Name of SSL Certificate** field, either browse to the location where the SSL certificates are located, or leave the field blank if you do not intend to use SSL to encrypt network traffic from the agent to the Tivoli Storage Manager server.

      Notes: If you intend to use SSL to encrypt network traffic, ensure that your Tivoli Storage Manager server is enabled for this type of secure communication and that you specified the correct port number. For additional information, see Configuring Tivoli Storage Manager client/server communication with Secure Sockets Layer.

  f. Click **OK** to save the settings.

6. Specify the Tivoli Enterprise Monitoring server information, but before you click **Save**, ensure that all the settings in the Tivoli Enterprise Monitoring server connection tab are correct:

    *   Ensure that there is no check mark in the **No TEMS** connection box.
    *   Enter the name of the host where Tivoli Enterprise Monitoring server is installed. If the **TEMS Hostname** field is prefilled, verify that the host name is correct.
    *   Ensure that the Protocol field indicates **IP.PIPE**.
    *   The Port Number should indicate 1918.

    The Manage Tivoli Enterprise Monitoring Services window opens with the new Tivoli Monitoring for Tivoli Storage Manager agent instance displayed.

7. If the agent was installed separately on an existing IBM Tivoli Monitoring server, you might need to seed the Tivoli Enterprise Monitoring server and Tivoli Enterprise Portal server, to allow it to pick up the new agent configuration. Issue these commands:

    ```
    ./itmcmd config -A cq
    ./itmcmd support -t tems_name sk
    ```

    Tip: The `itmcmd` program is in the `bin` directory under the `ITM` installation directory. The default is: `/opt/IBM/ITM/bin`.

8. Stop and restart the Tivoli Enterprise Monitoring server and the Tivoli Enterprise Portal server. From the CandleManage program, select the **Tivoli Enterprise Portal server**, right-click, and select **stop**. Wait for the process to stop and click **Start**. Repeat this step for the Tivoli Enterprise Monitoring server.

9. Start the Tivoli Monitoring for Tivoli Storage Manager agent instance. Select **Monitoring Agent for Tivoli Storage Manager**, right-click **Start Service**. Select the agent instance you want to start and click **Start Agent**.

    If an error occurs, examine the `$CANDLE_HOME/logs` directory for the most recent *hostname*`_sk_`*instancename*`_timestamp.log` file. This file contains error messages from when the agent starts.

Related tasks:

"Verifying the installation" on page 122

Related reference:

"Installation checklist" on page 117

Creating and configuring the agent instance using the command-line interface

After installing the Tivoli Monitoring for Tivoli Storage Manager agent, you can manually create and configure the agent instance using the command-line interface method.

Create and configure the agent instance using this command-line interface method, or you can use the CandleManage graphical interface method: "Creating and configuring the agent instance using CandleManage" on page 125.

You can monitor multiple Tivoli Storage Manager servers from the same IBM Tivoli Monitoring server, but you must create and configure an agent instance for each server that you want to monitor.

Installing Tivoli Monitoring for Tivoli Storage Manager

Note: The term, *monitoring agent*, that is displayed in the following examples is synonymous with the Tivoli Monitoring for Tivoli Storage Manager agent.

To configure a Tivoli Monitoring for Tivoli Storage Manager agent instance using the command-line interface, complete the following steps:

1. Run the following command from the directory where you installed the Tivoli Monitoring for Tivoli Storage Manager agent. The default directory is: `/opt/tivoli/tsm/reporting/itm/bin`.

   `./itmcmd config -A sk`

   The command returns the following instruction:

   ```
   Enter the instance name
   ```

2. Enter a name for the Tivoli Monitoring for Tivoli Storage Manager agent instance. For example, SERVER1.

   Tip: When specifying an instance name, the best practice is to include the host name of the Tivoli Storage Manager server. You can find the server name by issuing the **QUERY STATUS** command. Instance names must be unique, and cannot exceed 20 characters.
   The command returns the following question:

   ```
   Edit "Monitoring Agent for Tivoli Storage Manager" settings?
   [ 1=Yes, 2=No ] (default is: 1): myserver.mycompany.com
   ```

3. Enter 1. The command returns the following question: `Edit 'TSM Server Connection Information' settings? [ 1=Yes, 2=No ] (default is: 1):`

4. Enter 1. The command returns the following prompts for your response:

   ```
   Server Address (default is: ):
   Port Number (default is: 1500):
   TSM Administrator (default is: ):
   TSM Administrator Password (default is: ):
   ```

   a. For the Server Address, enter the address of the Tivoli Storage Manager server to be monitored.

   b. In the `Port Number` field, specify the port number that is used to communicate with the Tivoli Storage Manager server.

   Tip: For normal TCP/IP traffic, you can determine the port number by issuing one of the following commands:

   `QUERY OPT TCPPORT`

   `QUERY OPT TCPADMINPORT`

   For SSL encrypted TCP/IP traffic, you can determine the port number by issuing one of the following commands:

   `QUERY OPT SSLTCPPORT`

   `QUERY OPT SSLTCPADMINPORT`

   c. For the `TSM Administrator ID`, enter the Tivoli Storage Manager administrator ID to access the server where the monitoring agent is installed.

   Note: The IBM Tivoli Monitoring agent runs only queries on the Tivoli Storage Manager server and does not change anything. The administrator that you choose to run the queries can be an administrator ID without the following privileges:

- System Privileges
- Policy Privileges
- Storage Privileges
- Operator Privileges
- Client Access Privileges
- Client Owner Privileges

d. For the `TSM Administrator Password`, enter the correct password for the administrator ID. The command returns the following question:

```
Will this agent connect to a TEMS?
[1=YES, 2=NO] (Default is: 1):
```

5. In the `File System Location and Name of SSL Certificate` field, specify the location where the SSL certificates are located, or leave the field blank if you do not intend to use SSL to encrypt network traffic from the agent to the Tivoli Storage Manager server

   Notes: If you intend to use SSL to encrypt network traffic, ensure that your Tivoli Storage Manager server is enabled for this type of secure communication and that you specified the correct port number. For more information see Configuring Tivoli Storage Manager client/server communication with Secure Sockets Layer.

6. Enter 1, and specify the name of the host that Tivoli Enterprise Monitoring server is installed on. The host name is set by default, and requires changing only if Tivoli Enterprise Monitoring server is installed on a system other than the local host. The command returns the following prompts, for your response:

```
TEMS Host Name (Default is the host name where the agent was installed):
Network Protocol [ip, sna, ip.pipe or ip.spipe] (Default is: ip.pipe):
      Now choose the next protocol number from one of these:
      - ip
      - sna
      - ip.spipe
      - 0 for none
Network Protocol 2 (Default is: 0):
IP.PIPE Port Number (Default is: 1918):
Enter name of KDC_PARTITION (Default is: null):
```

7. Enter a protocol name or enter the default `ip.pipe`. The command returns the following information:

```
Configure connection for a secondary TEMS? [1=YES, 2=NO] (Default is: 2):
```

8. To have this agent connect to another Tivoli Enterprise Monitoring server, enter 1. Otherwise, enter 2 and go to step 12 on page 130.

   If you entered 1 to connect to another server, the command returns the following information:

```
Enter Optional Primary Network Name or 0 for "none" (Default is: 0):
```

9. If the agent was installed separately on to an existing IBM Tivoli Monitoring server, you might need to seed the Tivoli Enterprise Monitoring server and Tivoli Enterprise Portal server to allow it to pick up the new agent configuration settings. Complete this task by issuing these commands:

```
./itmcmd config -A cq
./itmcmd support -t tems_name sk
```

> **Tip:** The `itmcmd` program is in the bin directory under the IBM Tivoli Monitoring installation directory. The default is: `/opt/IBM/ITM/bin`.

10. Enter the following commands to stop and restart the Tivoli Enterprise Monitoring server, and the Tivoli Enterprise Portal server:

    ```
    ./itmcmd server stop tems_server
    ./itmcmd server start tems_server
    ```

11. Enter the following commands to stop and restart the agent:

    ```
    ./itmcmd agent stop cq
    ./itmcmd agent start cq
    ```

12. Enter the following command to start the Tivoli Monitoring for Tivoli Storage Manager agent you configured in step 3 on page 128:

    ```
    # ./itmcmd agent -o myinstance start sk
    ```

    If successful, the command returns the following information:

    ```
    Starting Monitoring Agent for Tivoli Storage Manager
     Agent Started Successfully
    ```

    If there is a problem with starting the Tivoli Monitoring for Tivoli Storage Manager agent instance, the command returns the following information:

    ```
    Starting Monitoring Agent for Tivoli Storage Manager ...
    KCIIN0198E Unable to start agent. Please, check log file.
    # exit
    ```

    If an error occurs, examine the `$CANDLE_HOME/logs` directory for the most recent *hostname*`_sk_`*instancename*`_timestamp.log` file. This file contains error messages from when the agent starts.

Related tasks:

"Verifying the installation" on page 122

Related reference:

"Installation checklist" on page 117

Manually configuring agents and services

After you install Tivoli Monitoring for Tivoli Storage Manager, you can manually configure the IBM Tivoli Monitoring agents and the data source if necessary.

Configuring summarization and pruning settings

After you install Tivoli Monitoring for Tivoli Storage Manager, you can configure summarization and pruning settings on the WAREHOUS database.

The summarization and pruning settings control how often data is collected and pruned from the WAREHOUS database. The values are set independently for each attribute group. The attribute groups correspond to a workspace in the Tivoli Enterprise Portal. The summarized data is stored in the WAREHOUS database for Tivoli Common Reporting reports to use. When the summarized data is periodically pruned, the data is removed from the WAREHOUS database.

Summarization values are automatically configured during installation. Pruning values are configured only during new installations. If you upgraded the application, you must manually configure the pruning settings. Pruning can help reduce the amount of data that is stored in the database, in some cases by as much as 50%. Pruning can also help with performance issues if the database becomes too large. You can adjust the values so that they are appropriate for your organization.

Note: DB2 allocates space for the database size to increase. Pruning reduces the amount of data that is stored in the database. To reduce the size of the database, go to the DB2 information center: http://pic.dhe.ibm.com/infocenter/db2luw/ v9r7/index.jsp and search for *reducing databases*.

To configure summarization and pruning settings, complete the following steps:

1. Log on to the Tivoli Enterprise Portal by using the sysadmin ID and password.
2. From the main menu, click **Edit** > **History Configuration** > **Tivoli Storage Manager**.
3. In the Select Attribute Groups pane, highlight the rows that contain the groups that you want to modify. The summarization and pruning fields below the table become active.
4. Select the summarization and pruning values that you want to modify, specify how long you want to keep the data, and click **OK**.

   The following table shows one example of a modified pruning setup. Your settings can vary depending on the data that you collect, how often you collect it, how long you keep it, and how often you prune it.

Table 35. Default pruning setup

Summarization value	Pruning value	Numeric value	Time units
Yearly	Yearly	7	Years
Quarterly	Quarterly	2	Years
Monthly	Monthly	2	Years
Weekly	Weekly	6	Months
Daily	Daily	2	Months
Hourly	Hourly	2	Weeks
	Detailed data	3	Months

As a best practice, start with the default settings, and test your system to ensure that data is being collected. When you are satisfied that the data is being collected correctly, you can adjust the collection interval and pruning values to suit the needs of your organization. Be sure to allow sufficient time to elapse before expecting data to display in reports. Data is displayed in the reports that are based upon the intervals that you choose.

You cannot run a report on data that has been removed through pruning.

Manually configuring the Tivoli Enterprise Portal server

When Tivoli Monitoring for Tivoli Storage Manager is installed, a script is run to configure the Tivoli Enterprise Portal server. You can verify that the service is configured correctly, or you can manually reconfigure this service if necessary.

1. Log on to the Manage Tivoli Enterprise Monitoring Services application:
   - Run the CandleManage program by using the following commands:
     - `cd install_dir/itm/bin`
     - `./CandleManage &`
2. From the Manage Tivoli Enterprise Monitoring Services window, select **Tivoli Enterprise Portal Server**, right-click, and select **Reconfigure**.
3. Click **OK** in the TEP Server Configuration window to accept the defaults and continue.

4. Verify that the host name and port numbers specify where the Tivoli Enterprise Monitoring server is located, and click **OK**. Click **Yes**.

5. Click **OK** in the Warehouse Proxy Database Selection window to accept **DB2** as the default database type, and click **OK** to continue.

    Restriction: There are other choices that are listed, but DB2 is the database that is required for Tivoli Monitoring for Tivoli Storage Manager.

6. Verify that the following fields are correct:
    - **Data Source Name:** `ITM Warehouse`
    - **Database Name:** `WAREHOUS`
    - **Admin User ID:** `db2inst1`
    - **Database User ID:** `itmuser`

7. Remove, and retype the password in the **Database Password** field and the **Admin Password** field.

8. Click **OK**.

    Note: The message `Successfully configured warehouse data source` displays. If you do not receive this message, there is at least one empty field or an error in configuring the service.

    Tip: There is no check for valid passwords, therefore it is important to retype the passwords correctly.

9. Click **Yes** to complete the configuration process.

10. From the Manage Tivoli Enterprise Monitoring Services window, select **Tivoli Enterprise Portal Server**, right-click, and select **Start**.

Manually configuring the Warehouse Proxy agent on AIX and Linux

When Tivoli Monitoring for Tivoli Storage Manager is installed, a script is run to configure the Warehouse Proxy agent. Sometimes you might need to verify that the agent is configured correctly, or manually reconfigure the agent if necessary.

The agent on AIX and Linux uses a JDBC connection. To configure the Warehouse Proxy agent, complete the following steps:

1. Start the Manage Tivoli Enterprise Monitoring Services window by changing to the *install_dir*/bin directory and run the following command:

    `./CandleManage`

    where *install_dir* is the installation directory for Tivoli Monitoring for Tivoli Storage Manager. The default installation directory is `/opt/tivoli/tsm/reporting/itm`.

2. Right-click **Warehouse Proxy** and click **Configure**. The Configure Warehouse Proxy window is displayed.

3. Click the **Agent Parameters** tab.

4. Ensure that the following values are correctly specified:
    - **JDBC Drivers:**

        ```
        /opt/tivoli/tsm/reporting/db2/java/db2jcc.jar
        /opt/tivoli/tsm/reporting/db2/java/db2jcc_license_cu.jar
        ```
    - **Database:** DB2
    - In the **Warehouse URL** field, ensure that the following information is correct:

– The URL should be similar to this example: `jdbc:db2://`*`myserver`*`:50000/`
`WAREHOUS`
– The *myserver* variable can be the IP address or host name of the system.
You can also use `localhost`.
– The default DB2 port number is 50000.
– Ensure that the default Tivoli Warehouse database name `WAREHOUS` is
appended to the end of the Warehouse URL.
- **Warehouse Driver:** `com.ibm.db2.jcc.DB2Driver`
- In the **Warehouse User** field, specify the IBM Tivoli Monitoring user ID. The
default user ID is: `itmuser`.
- In the **Warehouse Password** field, specify the password that you entered for
Tivoli Data Warehouse during the IBM Tivoli Monitoring installation.
5. Click **Test database connection** to test the connection.
6. Verify that **Use Batch** is selected.
7. Click **Save** to save your settings and close the window.
8. From the Manage Tivoli Enterprise Monitoring Services window, select
Warehouse Proxy, right-click, and select **Start**.

Manually configuring the Warehouse Summarization and Pruning agent

When Tivoli Monitoring for Tivoli Storage Manager is installed, a script is run to
configure the Warehouse Summarization and Pruning agent. Sometimes you might
need to verify that the agent is configured correctly, or manually reconfigure this
agent if necessary.

1. Log on to the Manage Tivoli Enterprise Monitoring Services application:
   - Run the CandleManage program by using the following commands:
     – `cd `*`install_dir`*`/itm/bin`
     – `./CandleManage &`
2. From the Manage Tivoli Enterprise Monitoring Services window, select
   Warehouse Summarization and Pruning Agent, right-click, and select
   Reconfigure.

   Tip: If **Reconfigure** is not available, double-click **Warehouse Summarization
   and Pruning Agent** in the Manage Tivoli Monitoring Services application, to
   start the initial configuration wizard.
3. Ensure that the **primary TEMS connection** field indicates **IP.PIPE**.
4. Verify that the host name and port numbers specify where the Tivoli Enterprise
   Monitoring server is located, and click **OK**. Click **Yes**.
5. Click the **Sources** tab and ensure that the following values are correctly
   specified, and click **Save**:
   - **JDBC Drivers:**
     `/opt/tivoli/tsm/reporting/db2/java/db2jcc.jar`
     `/opt/tivoli/tsm/reporting/db2/java/db2jcc_license_cu.jar`
   - **Database:** DB2
   - In the **Warehouse URL** field, ensure that the following information is correct:
     – The URL should be similar to this example: `jdbc:db2://`*`myserver`*`:50000/`
     `WAREHOUS`
     – The *myserver* variable can be the IP address or host name of the system.
     You can also use `localhost`.
     – The default DB2 port number is 50000

- Ensure that the default Tivoli Warehouse database name WAREHOUS is appended to the end of the Warehouse URL.
- **Warehouse Driver:** com.ibm.db2.jcc.DB2Driver
- In the **Warehouse User** field, specify the IBM Tivoli Monitoring user ID. The default user ID is:

  itmuser
- **Warehouse Password:** my_password Specify the password that you entered for Tivoli Data Warehouse during the IBM Tivoli Monitoring installation.
- Click **Test database connection** to test the connection.
- In the **TEP Server Host** field, accept the default localhost.
- In the **TEP Server Port** field, accept 1920 as the default server port or enter a different port number.

6. Click **Save** and then click **Close** to close the Configure Summarization and Pruning Agent window.

7. From the Manage Tivoli Enterprise Monitoring Services window, select **Warehouse Summarization and Pruning Agent**, right-click, and select **Start**.

Configuring a data source by using the configuration wizard

A data source is automatically configured during the Tivoli Monitoring for Tivoli Storage Manager installation. The data source must be configured correctly to allow the Administration Center to connect to the WAREHOUS database and generate reports.

The data source defines the connection to the WAREHOUS database. It is automatically configured during installation, but you can use the data source configuration wizard to reconfigure the data source if necessary.

To configure a data source by using the configuration wizard, complete these steps:

1. Locate the data configuration wizard executable file, which is named datasrc. If you installed Tivoli Monitoring for Tivoli Storage Manager in the default directory, the executable file can be found in this directory:

   /opt/tivoli/tsm/reporting/datasrc.bin

2. Start the configuration wizard and follow the instructions to specify the DB2 host name, port, user ID, and password. You must also specify the Tivoli Integrated Portal user ID and password that was defined when you installed the Administration Center.

Installing monitoring agents

You can install monitoring agents on any remote Tivoli Storage Manager server that you want to monitor.

The Tivoli Monitoring for Tivoli Storage Manager agent gathers data from each Tivoli Storage Manager server, and sends it to the Tivoli Monitoring server.

Before deciding whether you need to install the monitoring agent directly on your Tivoli Storage Manager server, consider the following items:

- The monitoring server can handle up to five monitoring agents. For more agents, you must install a monitoring agent directly on each of the Tivoli Storage Manager servers that you want to monitor.

- If you create and configure a single agent instance on the Tivoli Storage Manager server, instead of the monitoring server, you can help avoid an increase in memory requirements on the monitoring server.
- Review the requirements for the operating systems that the monitoring agent installation is supported on. See "System requirements for Tivoli Monitoring for Tivoli Storage Manager" on page 111.

Restrictions:

1. To use the agent in an existing Tivoli Monitoring environment, you must install the agent on the existing Tivoli Enterprise Monitoring server.
2. If you plan to monitor a Tivoli Storage Manager server in a different timezone than the monitoring server, install the monitoring agent on the Tivoli Storage Manager server.
3. The monitoring agent is not supported on Solaris, HP, and Linux ppc64.

Related tasks:

"Installing monitoring agents on Tivoli Storage Manager servers"

"Installing and deploying monitoring agents in an existing Tivoli Monitoring environment" on page 136

"Remotely deploying monitoring agents" on page 139

Related reference:

"System requirements for Tivoli Monitoring for Tivoli Storage Manager" on page 111

"Remote deployment preinstallation requirements" on page 139

Installing monitoring agents on Tivoli Storage Manager servers

You can install a Tivoli Monitoring for Tivoli Storage Manager agent on any supported Tivoli Storage Manager server that you want to monitor.

Important: Do not use a domain ID to install or configure agents. The Windows user ID that you use when installing must be a local ID with Administrator privileges, and cannot be a domain ID.

To install the Tivoli Monitoring for Tivoli Storage Manager agent on the Tivoli Storage Manager server, complete these steps:

1. Start the installation wizard from the DVD or package file.
2. Accept the license agreement and click **Next**.
3. On the **Component Selection** page, select **Tivoli Monitoring for Tivoli Storage Manager agent**, and click **Next**.
4. Follow the wizard instructions to specify the installation location and encryption key.

   Requirements:

   a. If you are installing into an existing IBM Tivoli Monitoring environment, you must choose the same directory where IBM Tivoli Monitoring is installed. For example, if you installed IBM Tivoli Monitoring in the `/opt/IBM/ITM` directory, you must specify `/opt/IBM/ITM` as the destination folder for this installation.
   b. All agents must use the same encryption key that was specified during installation of the monitoring server. The default encryption key is: `IBMTivoliMonitoringEncryptionKey`.

5. Review the installation summary page and click **Next** to start the installation.

   At the end of the installation, the installation results are displayed. If there were any errors during the installation, the summary lists the errors and directs you to an error log file.

6. Click **Finish**.

After you install the agent, create and configure the agent instance. See Creating and configuring the agent instance.

Installing and deploying monitoring agents in an existing Tivoli Monitoring environment

Remotely deploying monitoring agents is intended only for users who purchased IBM Tivoli Monitoring separately from Tivoli Storage Manager, and who are already running a Tivoli Monitoring server. By remotely deploying monitoring agents, you can monitor Tivoli Storage Manager servers with the existing Tivoli Monitoring server.

The operating system agent that is required for remote deployment is not included in the version of IBM Tivoli Monitoring that is embedded in Tivoli Monitoring for Tivoli Storage Manager. Therefore, you cannot use remote deployment without purchasing IBM Tivoli Monitoring.

Installing monitoring agents, or application support files in an existing IBM Tivoli Monitoring environment on AIX and Linux systems

If you have an existing IBM Tivoli Monitoring system that does not have Tivoli Monitoring for Tivoli Storage Manager installed, you can run the native IBM Tivoli Monitoring installation wizard to install more monitoring agents. If you do not want to install the agent, you can install only the application support files, which are required by the Tivoli Enterprise Monitoring server and Tivoli Enterprise Portal server to monitor Tivoli Storage Manager servers.

Restrictions to know before you begin:
• These procedures are for experienced IBM Tivoli Monitoring users only, and are not intended for novice Tivoli Monitoring for Tivoli Storage Manager users.
• Do not install this option if you have previously installed Tivoli Monitoring for Tivoli Storage Manager. Doing so can interfere with future uninstallations or upgrades of Tivoli Monitoring for Tivoli Storage Manager.
• You must use Tivoli Monitoring for Tivoli Storage Manager only with IBM Tivoli Monitoring, version 6.2.2 FP2 or later. See the system requirements for your platform for more requirements.
• Ensure that you meet all system requirements.

Complete these steps to install the monitoring agent or application support files with a user ID that has root privileges:

1. Download the appropriate executable file from Passport Advantage, or the FTP download site at ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/reporting/v6r3/LATEST. The file name for installing only the monitoring agent, or only the application support files, can be recognized by the word **AGENT** in capital letters. For example:

   `6.3.3.000-TIV-TSMRPT-AGENT-Linux.bin`

2. Stop all of the Tivoli Storage Manager processes and agent instances using the CandleManage application, or the command-line interface.

> **Tip:** Always stop processes by issuing the **itmcmd** commands, or from the Manage Tivoli Enterprise Monitoring Services application. Do not stop processes by using the operating system.

Stop the processes using CandleManage:	Stop the processes using the command-line interface:

1. Go to the directory where the CandleManage application is installed. For example:
 	
  `cd install_dir/itm/bin`
 	
2. Run the CandleManage program by issuing the following command:
 	
  `./CandleManage &`
	1. Display the agents that are running by issuing the following command, and checking the output for the list of services that are running:
	
	  `./cinfo`
	  `-r`
	
	2. Stop the Summarization and Pruning agent by issuing the following command:
	
	  `./itmcmd agent stop sy`
	
	3. Stop the Warehouse Proxy by issuing the following command:
	
	  `./itmcmd`
	  `agent stop hd`
	
	4. Stop the Tivoli Enterprise Portal server by issuing the following command:
	
	  `./itmcmd agent stop cq`
	
	5. Stop the Tivoli Enterprise Monitoring server by issuing the following command:
	
	  `./itmcmd server stop tems_server`
	
	6. Stop all of the Tivoli Storage Manager instances by issuing the following command:
	
	  `./itmcmd agent -o instance_name stop`
	  `sk`
	
	7. Stop all of the IBM Eclipse server by issuing the following command:
	
	  `./itmcmd`
	  `server -o stop kf`

3. Type the following command in the directory where you extracted the installation files:

   `./install.sh`

   Optionally: If you are installing from the DVD media, navigate to the top-level directory on the DVD and issue the following command:

   `./small_agent_install.sh`

4. Press `Enter` to accept the /opt/IBM/ITM path as the default directory, or specify the full path to a different directory. If the specified directory does not exist, type **y** when prompted to create it.

   Tip: If you are installing into an existing IBM Tivoli Monitoring environment, choose the same directory where IBM Tivoli Monitoring is installed. For example, if you installed IBM Tivoli Monitoring in the /opt/IBM/ITM directory, specify /opt/IBM/ITM as the destination folder for this installation.

5. Type **1** at the prompt to Install products to the local host. For example:

Installing Tivoli Monitoring for Tivoli Storage Manager

```
Select one of the following:

1) Install products to the local host.
2) Install products to depot for remote deployment (requires TEMS).
3) Install TEMS support for remote seeding
4) Exit install.

Please enter a valid number:  1
```

6. Type 1 to accept the license agreement.
7. When the list of products that can be installed is displayed, you can choose to install the monitoring agent, or you can install only the application support files. To install the monitoring agent, you would select number 1 and after that completes you would specify a value of 2, to install the support files for Tivoli Enterprise Portal Browser Client support. After that completes, you would specify a value of 3, and so on, until you specified all of the support files. If you are installing only the application support files, you would begin by selecting 2, then 3, then 4, and finally 5. For example:

```
Product packages are available for this operating system and component support
categories:

 1) IBM Tivoli Monitoring components for this operating system
 2) Tivoli Enterprise Portal Browser Client support
 3) Tivoli Enterprise Portal Desktop Client support
 4) Tivoli Enterprise Portal Server support
 5) Tivoli Enterprise Monitoring Server support
 6) Other operating systems

Type the number or type "q" to quit selection
[number "1" or "IBM Tivoli Monitoring components for this operating system"
is default]:2
```

Installing the monitoring agent:	Installing the application support files:
Use this option if you intend to create and configure an agent instance on the Tivoli Enterprise Monitoring server. 1. Specify the number that corresponds to the IBM Tivoli Monitoring components for this operating system option. 2. Specify a 32-character encryption key, or press Enter to use the default key. **Restriction:** All agents must use the same encryption key that was specified during installation of the monitoring server. The default encryption key is: IBMTivoliMonitoringEncryptionKey.	You must install the application support files so that the Tivoli Monitoring for Tivoli Storage Manageragent can display Tivoli Storage Manager data in Tivoli Enterprise Monitoring server and Tivoli Enterprise Portal server. 1. Specify the number that corresponds to the Tivoli Enterprise Portal Browser Client Support option. 2. Specify the number that corresponds to the Tivoli Enterprise Portal Desktop Client Support option. 3. When prompted again, specify the number that corresponds to the Tivoli Enterprise Portal Server Support option. 4. When prompted again, specify the number that corresponds to the Tivoli Enterprise Monitoring Server Support option.

8. Reconfigure the Tivoli Enterprise Portal server by issuing the following command, follow the prompts, and accept all default values:

   `/opt/IBM/ITM/bin/itmcmd config -A cq`

9. Start the Tivoli Enterprise Portal server by issuing the following command:

```
/opt/IBM/ITM/bin/itmcmd agent start cq
```

10. Restart any agents that you stopped at the beginning of this installation.

After you complete the installation, you must configure Tivoli Enterprise Portal to collect and retain historical data for reports. See "Configuring historical data collection by using the command-line interface on AIX and Linux systems" on page 146.

You can also create and configure an agent instance. See "Creating and configuring the agent instance" on page 125.

Related reference:

"System requirements for Tivoli Monitoring for Tivoli Storage Manager" on page 111

"Remote deployment preinstallation requirements"

Remotely deploying monitoring agents

Remote deployment provides the ability to add the monitoring agent installation packages to a central location called an *agent depot*. From this central location, the packages can then be pushed out to remote locations and installed silently by using the IBM Tivoli Monitoring operating system agent. Remote deployment is useful for larger-scale deployments such as deploying five or more monitoring agents.

Remote deployment can be used to deploy monitoring agents to systems that already have the IBM Tivoli Monitoring operating system agent that is installed on them. Remote deployment can be used for new installations or to upgrade existing monitoring agents to new versions.

There are multiple tasks that must be completed to use remote deployment. These tasks include the following items:

- Add the agents that you want to deploy to the agent depot on the Tivoli Enterprise Monitoring server hub.

  Requirement: The IBM Tivoli Monitoring operating system agents on the systems that you want to deploy to must be configured to use this Tivoli Enterprise Monitoring server hub.
- Initiate the remote deployment.
- Configure historical data collection.

Remote deployment preinstallation requirements:

Before you begin any remote deployment tasks, ensure that you meet the preinstallation requirements for your system.

Remote deployment prerequisites include the following tasks:

1. Install IBM Tivoli Monitoring and configure the Tivoli Enterprise Monitoring server hub.
2. Install the IBM Tivoli Monitoring 6.2.2 operating system agent on each system that you want to remotely deploy a monitoring agent to, and configure it to point to the Tivoli Enterprise Monitoring server.
3. You must also install the IBM Tivoli Monitoring application support files and configure the Tivoli Enterprise Monitoring server hub. These steps can be completed before or after any remote deployment tasks, but are required to view data in historical reports.

You can verify whether these prerequisites are met by logging in to Tivoli Enterprise Portal, selecting the systems that you want to deploy to, and verifying that the operating system agent is displaying information. For example, select the **Memory** workspace in Tivoli Enterprise Portal, and verify that data is displayed.

If you must install the IBM Tivoli Monitoring operating system agent to the agent depot, the easiest method is to copy the agent to the agent depot by issuing the `tacmd addbundles` command, and then install it by issuing the `tacmd createNode` command. For example:

- Extract the Tivoli Monitoring 6.2.2 operating system agent, then copy the operating system agent to the depot by issuing the following command:

  `./tacmd addbundles -i /path_to_agent/unix`

- Deploy the operating system agent by issuing the following command:

  `./tacmd createNode -h host_name -u user_name -w password`

Populating the agent depot on AIX and Linux systems:

Before you can remotely deploy a monitoring agent, you must populate the *agent depot*. The agent depot is an installation directory on the monitoring server that you must copy the agent to, and then deploy from, to remote systems.

Before you begin, ensure that you meet all of the remote deployment preinstallation requirements.

Complete these steps to add the monitoring agent to the agent depot for remote deployment:

1. Copy and extract the agent installation package to a directory that is accessible by the Tivoli Enterprise Monitoring server hub. For example, you can copy the package to the following directory:

   `/tmp/tsmrptagent`

   Tip: Ensure that you select the appropriate executable file from the Passport Advantage, FTP download site, or from the DVD media. The file name for installing only the monitoring agent, or the application support files can be identified by the word AGENT, in capital letters. For example:

   `6.3.3.000-TIV-TSMRPT-AGENT-Linux.bin`

2. Optional: Modify the silent response file that will be used during the agent installation to specify items such as the installation directory and the encryption key that is required to communicate with the Tivoli Enterprise Monitoring server hub.

   Tips:
   a. The default encryption key value is `IBMTivoliMonitoringEncryptionKey`
   b. The silent response file names are:
      - Linux versions and applicable silent response file names:
        – Linux Intel R2.4 (32 bit) - Linux kernel version 2.4 `skli6243.txt`
        – Linux Intel R2.6 (32 bit) - Linux kernel version 2.6 `skli6263.txt`
        – Linux Intel R2.6 (64 bit) - Linux kernel version 2.6 `sklx8266.txt`

3. Add the agent to the agent depot. This process copies the files to a directory on the Tivoli Enterprise Monitoring server.
   a. Change directories to the location where the `tacmd` command is located. For example:

```
/opt/IBM/ITM/bin
```

b. Log in to Tivoli Enterprise Monitoring server by issuing the following command:

```
./tacmd login -s host_name -u sysadmin -p password
```

c. Add the agent to the agent depot by issuing the following command:

```
./tacmd addbundles -i /path_to_agent/unix
```

If the command was successful, the following message is displayed:

```
KUICAB020I: Adding bundles to the /opt/IBM/ITM/tables/TEMS/depot depot.
The time required to complete this operation depends on the number and size of
the added bundles.

 KUICAB022I: The following bundles were successfully added to the
 /opt/IBM/ITM/tables/TEMS/depot depot:

Product Code : sk
Deployable   : True
Version      : 063300000
Description  : Monitoring Agent for Tivoli Storage Manager
Host Type    : li6243
Host Version : li6243
Prerequisites: ci:062202000 la:010001000 gs:074027000 jr:043000000
               ui:062202000 ax:062202000


Product Code : sk
Deployable   : True
Version      : 063300000
Description  : Monitoring Agent for Tivoli Storage Manager
Host Type    : li6263
Host Version : li6263
Prerequisites: ci:062202000 la:010001000 gs:074027000 jr:050900000
               ui:062202000 ax:062202000


Product Code : sk
Deployable   : True
Version      : 063300000
Description  : Monitoring Agent for Tivoli Storage Manager
Host Type    : lx8266
Host Version : lx8266
Prerequisites: ci:062202000 la:010001000 gs:074027000 jr:050900000
               ui:062202000 ax:062202000
```

4. Verify that the bundles exist in the agent depot by navigating to the /opt/IBM/ITM/tables/TEMS/depot directory, or by issuing the following command:

```
./tacmd viewdepot -t sk
```

Tip: You can limit the output to only the Tivoli Monitoring for Tivoli Storage Manager monitoring agent by using the SK product code.
Example output:

Installing Tivoli Monitoring for Tivoli Storage Manager

```
Product Code : sk
Version      : 063300000
Description  : Monitoring Agent for Tivoli Storage Manager
Host Type    : li6243
Host Version : li6243
Prerequisites: ci:062000000,la:010001000,ui:062000000,ax:062000000

Product Code : sk
Version      : 063000000
Description  : Monitoring Agent for Tivoli Storage Manager
Host Type    : unix
Host Version : aix523,aix526,aix533,aix536,aix613,aix616,hp11,hp116,hpi116,lx8266,
               lia266,lpp266,li6223,li6242,li6243,li6245,li6246,li6262,li6263,li6265,
               li6266,ls3223,ls3226,ls3242,ls3243,ls3245,ls3246,ls3262,ls3263,ls3265,
               ls3266,sol283,sol286,sol293,sol296,sol503,sol506,sol606
Prerequisites:
```

Tip: You can remove older bundles if they are no longer needed by issuing the `tacmd removebundles` command. For example:

```
./tacmd removebundles -t sk -i /opt/IBM/ITM/tables/TEMS/depot
```

After you populated the agent depot with the monitoring agent, you can deploy the agent to remote sites from this central location. For detailed procedures, see Remotely deploying monitoring agents.

Related reference:

"System requirements for Tivoli Monitoring for Tivoli Storage Manager" on page 111

"Remote deployment preinstallation requirements" on page 139

Remotely deploying monitoring agents on AIX and Linux systems:

After you have populated the agent depot, you can deploy the monitoring agent to remote systems.

Before you begin, ensure that your system meets all of the remote deployment preinstallation requirements, and that the operating system agent on the remote system is started and has root access.

Complete these steps to install the monitoring agent, and initiate the deployment:

1. Navigate to where the `tacmd` command is located. For example, the default directory is:

   ```
   /opt/IBM/ITM/bin
   ```

2. Log in to the remote system using the sysadmin user ID and password:

   ```
   ./tacmd login -s host_name -u sysadmin -p password
   ```

3. Locate the nodes that you want to deploy the monitoring agent to, by issuing the following command:

   ```
   ./tacmd listSystems -t LZ
   ```

4. Deploy the monitoring agent by issuing the following command:

   ```
   ./tacmd addSystem -t sk -n Primary:yourhost:LZ -p INSTANCE=yourhost
    TSM_AUTHENTICATION_INFORMATION.KSK_SERVER_ADDR=yourhost.yourcompany.com
    TSM_AUTHENTICATION_INFORMATION.KSK_PORT_NUMBER=1500
    TSM_AUTHENTICATION_INFORMATION.KSK_USER=tsmusername
    TSM_AUTHENTICATION_INFORMATION.KSK_PASSWORD=tsmpassword
   ```

   where:

   `TSM_AUTHENTICATION_INFORMATION.KSK_SERVER_ADDR` indicates the server IP address of the Tivoli Storage Manager server

TSM_AUTHENTICATION_INFORMATION.KSK_PORT_NUMBER indicates the port that is required to access the Tivoli Storage Manager server

TSM_AUTHENTICATION_INFORMATION.KSK_USER indicates the user ID that is used to access the Tivoli Storage Manager server

TSM_AUTHENTICATION_INFORMATION.KSK_PASSWORD indicates the password for the user ID that is used to access the Tivoli Storage Manager server

TSM_AUTHENTICATION_INFORMATION.KSK_KEYSTORE indicates the file system location if your agent will be communicating with the Tivoli Storage Manager server through an SSL connection. Leave this blank to use the default non-SSL authentication method.

If your agent will be communicating with the server through an SSL connection, specify a value using the TSM_AUTHENTICATION_INFORMATION.KSK_KEYSTORE option.

Tip: When specifying a monitoring agent instance name, as a best practice, you can specify the name of the Tivoli(r) Storage Manager server, or the host name of the server as your instance name.
For example:

```
./tacmd addSystem -t sk -n Primary:yourhost:UX -p INSTANCE=yourhost
 TSM_AUTHENTICATION_INFORMATION.KSK_SERVER_ADDR=yourhost.yourcompany.com
 TSM_AUTHENTICATION_INFORMATION.KSK_PORT_NUMBER=1500
 TSM_AUTHENTICATION_INFORMATION.KSK_USER=tsmusername
 TSM_AUTHENTICATION_INFORMATION.KSK_PASSWORD=tsmpassword

KUICAR010I: The agent type SK is being deployed.

KUICAR028I: The operation has been successfully queued for deployment,
the transaction id is 1329702031328000000000041,
use the getDeployStatus CLI to view the status.
```

5. Review the deployment status by issuing the following command:

   ```
   ./tacmd getDeployStatus -t sk
   ```

   For example:

   ```
   Transaction ID : 1334178758871657000027663
   Command        : INSTALL
   Status         : SUCCESS
   Retries        : 0
   TEMS Name      : TEMS
   Target Hostname: yourhost:UX
   Platform       : aix526
   Product        : SK
   Version        : 063300000
   Error Message  : KDY0028I: Request completed successfully. Deployment request was
                    processed successfully and is now completed.
   ```

After you deployed the agent, verify that the Tivoli Storage Manager data is being collected and displayed in Tivoli Enterprise Portal. Log in to Tivoli Enterprise Portal, select the system that the monitoring agent was deployed to, and verify that data is displayed correctly in the workspaces.

Related tasks:

"Configuring historical data collection from within Tivoli Enterprise Portal"

"Configuring historical data collection by using the command-line interface on AIX and Linux systems" on page 146

Related reference:

"Remote deployment preinstallation requirements" on page 139

Configuring historical data collection from within Tivoli Enterprise Portal:

After installing monitoring agents in to an existing IBM Tivoli Monitoring environment, you must configure historical data collection if you intend to generate reports based on this data. You can configure historical data collection from within Tivoli Enterprise Portal, but consider using the command-line interface instead because it is quicker than doing it from within Tivoli Enterprise Portal.

If you installed Tivoli Monitoring for Tivoli Storage Manager using the standard installation method, historical data collection was configured for you automatically. If you are using the native IBM Tivoli Monitoring installer, then you must manually configure historical data collection.

You must configure history configuration to have the data from the monitored servers stored in the *WAREHOUS* database. This is a requirement if you plan to use the Administration Center to view historical reports.

You can use the following steps to start data collection. In the steps, example values are used. Your selections depend on your criteria.

1. Start the Tivoli Enterprise Portal:
   a. Open a web browser and specify the address of the server where the Tivoli Enterprise Portal was installed, similar to the following example:
      `http://hostname:1920///cnp/kdh/lib/cnp.html`

      where *hostname* is the server name and `1920///cnp/kdh/lib/cnp.html` is the port and location of the Java™ Tivoli Enterprise Portal web client.
2. Log on to the Tivoli Enterprise Portal by using the `sysadmin` user ID, and the password that was specified during installation.
3. From the Tivoli Enterprise Portal menu, click **Edit** > **History Configuration**.
4. Specify collection settings by completing the following steps for each of the following attribute groups:
   - KSK CLIENT NODE STORAGE
   - KSK CLIENT MISSED FILES
   - KSK CLIENT NODE STATUS
   - KSK DATABASE
   - KSK SCHEDULE
   - KSK STORAGE POOL
   - KSK TAPE USAGE
   - KSK TAPE VOLUME
   - KSK NODE ACTIVITY
   - KSK SERVER
   - KSK STORAGE DEVICE
   - KSK ACTIVITY LOG
   - KSK OCCUPANCY

- KSK REPLSTATUS (Listed as Replication Status)
- KSK REPLDETAILS (Listed as Replication Details)
- KSK ACTIVITY SUMMARY

Tip: KSK denotes the Tivoli Monitoring for Tivoli Storage Manager product code.

a. Right-click Tivoli Storage Manager, and select **Create new collection setting**.

b. Select the attribute group from the menu.

c. Specify a name for the new collection setting, and optionally provide a description. As a best practice, include the attribute group in the name.

d. In the **Collection interval** field, set the value to 1 hour. This value specifies how often the data is retrieved from the monitoring agent.

e. In the **Collection location** field, select **Tivoli Enterprise Monitoring server, TEMA**. This server is where the historical data files are stored.

f. In the **Warehouse interval** field, select **1 day** for how often you want the warehouse data to store data. If you select 1 day, you cannot view reports for at least a day.

Note: These settings are examples. Your selections depend on how often, and how much data you want to collect. To test the data that is collected, start with a short interval such as 1 hour. After you are sure that the data is being collected correctly, you can adjust the collection interval to every 12 or 24 hours.

To verify that historical collection is activated, you can look for the **History Configuration** icon next to each attribute group.

5. After the historical data collection settings are configured, complete the following steps to configure summarization and pruning of the data in the Tivoli Data Warehouse.

Tip: Summarization combines multiple data points into a single data point across a date range such as a monthly or quarterly. Pruning removes older data that is no longer needed to save database space.

a. Left-click on **Tivoli Storage Manager** to open the summarization and pruning settings window.

b. Select all of the attributes that are configured for historical data collection. A blue icon next to the attribute group indicates that data collection is running.

c. In the summarization settings, enable summarization for Yearly, Quarterly, Monthly, Weekly, Daily, and Hourly.

d. In the Pruning section, you can also optionally enable pruning. By default no pruning is enabled. If your Tivoli Data Warehouse database size is growing too large, pruning older data can be enabled here for each attribute group.

Note: Pruning too vigorously can result in no data, or not enough data being displayed in the Tivoli Common Reporting reports.

Configuring historical data collection by using the command-line interface on AIX and Linux systems:

After installing monitoring agents in an existing IBM Tivoli Monitoring environment, you must configure historical data collection if you intend to generate reports based on this data.

If you installed Tivoli Monitoring for Tivoli Storage Manager using the standard installation method, historical data collection was configured for you automatically. If you are using the native IBM Tivoli Monitoring installer, then you must manually configure historical data collection.

You can also configure historical data collection from within the Tivoli Enterprise Portal. However, it is much quicker using the command-line interface because there are many attribute groups that must be configured.

You must configure history configuration to have the data from the monitored servers stored in the *WAREHOUS* database. This is a requirement if you plan to use the Administration Center to view historical reports.

The following commands can be copied and pasted into a terminal session window. Be sure to adjust any of the variables such as your password, to match your installation environment before pasting them in to a terminal session.

Complete the following steps to configure historical data collection and summarization and pruning:

1. Issue the following commands to specify your user ID and password, and the CandleManage directory:

   ```
   export itmuser=sysadmin
   export password=your_password export CANDLE_HOME=/opt/IBM/ITM
   ```

2. Paste the following text in the same terminal window:

   Tip: Remember to change the user ID and password variables to match the values that you specified during installation.

   ```
   export warehouseinterval=1h
   export collectioninterval=1h
   export summarizationdetails=HDWMQY
   cd %CANDLE_HOME%/bin
   ./tacmd histconfiguregroups -u $itmuser -w $password -t SK -i $warehouseinterval
     -c $collectioninterval -d $summarizationdetails -o "KSK CLIENT NODE STORAGE"
   ./tacmd histconfiguregroups -u $itmuser -w $password -t SK -i $warehouseinterval
     -c $collectioninterval -d $summarizationdetails -o "KSK CLIENT MISSED FILES"
   ./tacmd histconfiguregroups -u $itmuser -w $password -t SK -i $warehouseinterval
     -c $collectioninterval -d $summarizationdetails -o "KSK CLIENT NODE STORAGE"
   ./tacmd histconfiguregroups -u $itmuser -w $password -t SK -i $warehouseinterval
     -c $collectioninterval -d $summarizationdetails -o "KSK DATABASE"
   ./tacmd histconfiguregroups -u $itmuser -w $password -t SK -i $warehouseinterval
     -c $collectioninterval -d $summarizationdetails -o "KSK SCHEDULE"
   ./tacmd histconfiguregroups -u $itmuser -w $password -t SK -i $warehouseinterval
     -c $collectioninterval -d $summarizationdetails -o "KSK STORAGE POOL"
   ./tacmd histconfiguregroups -u $itmuser -w $password -t SK -i $warehouseinterval
     -c $collectioninterval -d $summarizationdetails -o "KSK TAPE USAGE"
   ./tacmd histconfiguregroups -u $itmuser -w $password -t SK -i $warehouseinterval
     -c $collectioninterval -d $summarizationdetails -o "KSK TAPE VOLUME"
   ./tacmd histconfiguregroups -u $itmuser -w $password -t SK -i $warehouseinterval
     -c $collectioninterval -d $summarizationdetails -o "KSK NODE ACTIVITY"
   ./tacmd histconfiguregroups -u $itmuser -w $password -t SK -i $warehouseinterval
     -c $collectioninterval -d $summarizationdetails -o "KSK SERVER"
   ./tacmd histconfiguregroups -u $itmuser -w $password -t SK -i $warehouseinterval
   ```

```
     -c $collectioninterval -d $summarizationdetails -o "KSK STORAGE DEVICE"
./tacmd histconfiguregroups -u $itmuser -w $password -t SK -i $warehouseinterval
     -c $collectioninterval -d $summarizationdetails -o "KSK ACTIVITY LOG"
./tacmd histconfiguregroups -u $itmuser -w $password -t SK -i $warehouseinterval
     -c $collectioninterval -d $summarizationdetails -o "KSK OCCUPANCY"
./tacmd histconfiguregroups -u $itmuser -w $password -t SK -i $warehouseinterval
     -c $collectioninterval -d $summarizationdetails -o "KSK REPLSTATUS"
./tacmd histconfiguregroups -u $itmuser -w $password -t SK -i $warehouseinterval
     -c $collectioninterval -d $summarizationdetails -o "KSK REPLDETAILS"
./tacmd histconfiguregroups -u $itmuser -w $password -t SK -i $warehouseinterval
     -c $collectioninterval -d $summarizationdetails -o "KSK ACTIVITY SUMMARY"
```

3. Start collecting data by issuing the following commands:

```
./tacmd histstartcollection -u $itmuser -w $password -t SK -o "KSK
    CLIENT NODE STORAGE"
./tacmd histstartcollection -u $itmuser -w $password -t SK -o "KSK
    CLIENT MISSED FILES"
./tacmd histstartcollection -u $itmuser -w $password -t SK -o "KSK
    CLIENT NODE STORAGE"
./tacmd histstartcollection -u $itmuser -w $password -t SK -o "KSK
    DATABASE"
./tacmd histstartcollection -u $itmuser -w $password -t SK -o "KSK
    SCHEDULE"
./tacmd histstartcollection -u $itmuser -w $password -t SK -o "KSK
    STORAGE POOL"
./tacmd histstartcollection -u $itmuser -w $password -t SK -o "KSK
    TAPE USAGE"
./tacmd histstartcollection -u $itmuser -w $password -t SK -o "KSK
    TAPE VOLUME"
./tacmd histstartcollection -u $itmuser -w $password -t SK -o "KSK
    NODE ACTIVITY"
./tacmd histstartcollection -u $itmuser -w $password -t SK -o "KSK
    SERVER"
./tacmd histstartcollection -u $itmuser -w $password -t SK -o "KSK
    STORAGE DEVICE"
./tacmd histstartcollection -u $itmuser -w $password -t SK -o "KSK
    ACTIVITY LOG"
./tacmd histstartcollection -u $itmuser -w $password -t SK -o "KSK
    OCCUPANCY"
./tacmd histstartcollection -u $itmuser -w $password -t SK -o "KSK
    REPLSTATUS"
./tacmd histstartcollection -u $itmuser -w $password -t SK -o "KSK
    REPLDETAILS"
./tacmd histstartcollection -u $itmuser -w $password -t SK -o "KSK
    ACTIVITY SUMMARY"
```

Installing software for custom BIRT reports

You can create your own reports using the Business Intelligence and Reporting Tools (BIRT) software.

Ensure that you have fulfilled the IBM JDK and JRE requirements listed in the software requirements section for installing optional software. See "System requirements" on page 112.

For help regarding setup, configuration, and troubleshooting of BIRT reports visit: BIRT Report Designer, v2.2.1, for Tivoli Common Reporting

To create your own custom reports using BIRT and Tivoli Common Reporting, complete the following steps:

1. Download and install BIRT, version 2.2.1, All-In-One software by using one of the following websites:

- For the BIRT software that you need to download and install, go to the following IBM Tivoli Integrated Service Management Library website: BIRT Report Designer, v2.2.1, for Tivoli Common Reporting
- If you cannot access the Integrated Service Management Library, you can obtain the software from the BIRT website: BIRT Report Downloads

2. Import the data, configure the data source, and customize the reports following the directions in *Customizing Tivoli Common Reporting Report Designs* found at: Customizing Tivoli Common Reporting Report Designs

Related information:

➡ Tivoli Common Reporting Information Center

Chapter 10. Upgrading Tivoli Monitoring for Tivoli Storage Manager to Version 6.3, or later

You can upgrade Tivoli Monitoring for Tivoli Storage Manager from V6.1 and V6.2 to V6.3, or later. The monitoring agents that are installed on any of your Tivoli Monitoring for Tivoli Storage Manager servers must be upgraded to the same level.

Upgrade scenarios

Before upgrading Tivoli Monitoring for Tivoli Storage Manager, choose the scenario that best meets the needs of your company.

- Scenario 1: Your environment is monitoring 1-5 Tivoli Storage Manager servers.
- Scenario 2: Your environment is monitoring more than 5 Tivoli Storage Manager servers.
- Scenario 3: You have an existing IBM Tivoli Monitoring environment that was not installed as part of Tivoli Monitoring for Tivoli Storage Manager.

Important Notes:

1. If you have a Tivoli Storage Manager server that is in a different timezone than the system with Tivoli Monitoring for Tivoli Storage Manager, install the monitoring agent on the Tivoli Storage Manager server. See Scenario 2 to install the agent directly on the Tivoli Storage Manager server.
2. If you have more than five servers, installing the monitoring agent on each of the servers is the most efficient use of memory on both the Tivoli Storage Manager server, and the Tivoli Monitoring for Tivoli Storage Manager server.

Upgrading Tivoli Monitoring for Tivoli Storage Manager

Table 36. Upgrade scenarios

Upgrade scenario number	Description	Tasks that you must perform
Scenario 1	Use this scenario for an upgraded installation, with a plan to monitor and report on 1-5 Tivoli Storage Manager servers.	Perform all of the tasks in this scenario on the same system: 1. Upgrade Tivoli Monitoring for Tivoli Storage Manager. The approximate installation time is 45 - 90 minutes, depending on the speed of your system. 2. Upgrade the Administration Center. Ensure that you select the Tivoli Common Reporting component during the installation to install new reports. The approximate installation time is 45 - 90 minutes, depending on the speed of your system. **Notes:** 1. You cannot install IBM Tivoli Monitoring for Tivoli Storage Manager on a system where Tivoli Storage Manager server is installed. 2. However, you can install the monitoring agent on any remote Tivoli Storage Manager server that you want to monitor.
Scenario 2	Use this scenario for an upgraded installation, with a plan to monitor and report on more than 5 Tivoli Storage Manager servers.	1. Upgrade Tivoli Monitoring for Tivoli Storage Manager. The approximate installation time is 45 - 90 minutes. 2. Upgrade the monitoring agents that are installed on any of your Tivoli Storage Manager servers. Optionally, install and configure additional agents on any Tivoli Storage Manager servers that you want to monitor. The approximate upgrade time for the agent is 15 - 30 minutes, and an additional 10 minutes, per agent, to manually configure each agent. 3. Upgrade the Administration Center. Ensure that you select the Tivoli Common Reporting component during the installation to install new reports. The approximate installation time is 45 - 90 minutes, depending on the speed of your system. **Notes:** 1. You cannot install IBM Tivoli Monitoring for Tivoli Storage Manager on a system where Tivoli Storage Manager server is installed. 2. However, you can install the monitoring agent on any remote Tivoli Storage Manager server that you want to monitor. **Restriction:** The monitoring agent is not supported on Solaris, HP, and Linux ppc64.

Table 36. Upgrade scenarios (continued)

Upgrade scenario number	Description	Tasks that you must perform
Scenario 3	Use this scenario for upgrading an existing IBM Tivoli Monitoring environment.	Prerequisite: You must have IBM Tivoli Monitoring version 6.2.2 FP2, or later installed. 1. Upgrade the monitoring agent on the IBM Tivoli Monitoring server where Tivoli Enterprise Monitoring server and Tivoli Enterprise Portal server are installed. During the agent upgrade, you must specify the same directory as you did when you installed IBM Tivoli Monitoring. 2. Upgrade the monitoring agents that are installed on any of your Tivoli Storage Manager servers. Optionally, install and configure additional agents on any Tivoli Storage Manager servers that you want to monitor. The approximate upgrade time for the agent is 15 - 30 minutes, and an additional 10 minutes, per agent, to manually configure each agent. 3. Upgrade the Administration Center. Ensure that you select the Tivoli Common Reportingcomponent during the installation to install new reports. The approximate installation time is 45 - 90 minutes, depending on the speed of your system. **Notes:** 1. You cannot install IBM Tivoli Monitoring for Tivoli Storage Manager on a system where Tivoli Storage Manager server is installed. 2. However, you can install the monitoring agent on any remote Tivoli Storage Manager server that you want to monitor. **Restriction:** The monitoring agent is not supported on Solaris, HP, and Linux ppc64.

Upgrading to version 6.3 or later, on AIX and Linux systems

You can upgrade Tivoli Monitoring for Tivoli Storage Manager to version 6.3 or later, from the graphical user interface, or console method installation wizard.

Before you begin the upgrade:

- Download the upgrade package from Passport Advantage, or from the FTP site at: ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/ server.
- Review the upgrade scenarios, and choose the one that best suits your needs.
- Optionally, perform a backup of your existing system.
- If you uninstalled a previous version of Tivoli Monitoring for Tivoli Storage Manager, before you reinstall, confirm that the process was successful. That includes ensuring that the DB2 user db2inst1 and db2fenc1 do not exist. Learn more about uninstalling at: Uninstalling on AIX and Linux systems.
- Close all applications, including Tivoli Enterprise Portal.

Attention: Do not alter the DB2 software that is installed with IBM Tivoli Monitoring for Tivoli Storage Manager installation packages and fix packs. Do not install or upgrade to a different version, release, or fix pack of DB2 software because doing so can damage the database. IBM Tivoli Monitoring for Tivoli Storage Manager can use only components and versions that are installed as part of the IBM Tivoli Monitoring for Tivoli Storage Manager installation.

---

1. Confirm that you have the required access privileges, including user IDs and passwords. See "Installation worksheet" on page 115.
2. Ensure that your system meets all system requirements. See "System requirements for Tivoli Monitoring for Tivoli Storage Manager" on page 111.
3. Stop all of the Tivoli Storage Manager agent instances using the CandleManage application, or the command-line interface.

Tips:

- The upgrade wizard stops all agents and services before the upgrade except for the Tivoli Storage Manager agent instances. These agents must be stopped manually with the above command.
- Always stop processes by issuing the **itmcmd** commands, or from the Manage Tivoli Enterprise Monitoring Services application. Do not kill processes by using the operating system.

Stop the agent using CandleManage:
Go to the directory where the CandleManage application is installed. For example:

```
cd /opt/tivoli/tsm/reporting/itm/bin
```

Run the CandleManage program by issuing the following command:

```
./CandleManage &
```

Stop the agent instances by using the command-line interface:
Display the agents that are running by issuing the following command, and then refer to the output:

```
./cinfo -r
```

Issue the following command for each agent instance:

```
./itmcmd agent -o instance_name stop sk
```

4. Choose whether you want to upgrade from the DVD, or a downloaded package file, and complete the steps in the following table to begin the upgrade:

Upgrade from DVD media:	Upgrade from a downloaded package file:

1. Insert the DVD into the DVD drive.
Tip: Ensure that the DVD is mounted on directory /dvdrom
2. Optionally, run the **prereqcheck.bin** file to ensure that your system meets all system requirements.
3. Begin the upgrade using the graphical interface by issuing the following command:
`./install.bin`
 	
Experienced users: You can also run the installation wizard in console mode, by issuing the following command:
`./install.bin -i console`
	1. Change to the directory where you downloaded the package file, and ensure that this file system has approximately 7 GB of free disk space.
	Important: Ensure that you extract the installation files to an empty directory. Do not extract to a directory that contains previously extracted files, or any other files.
	2. Change the permissions on the package file, and extract the files:
	
	AIX and Linux 64-bit systems
	  `chmod +x C`*xxxxxx*`.bin`
	
	  where *xxxxxx* is the part number, for example: CZ1N1ML
	  `./C`*xxxxxx*`.bin`
	
	Linux 32-bit:
	  `tar -xvf C`*xxxxxx*`.tar`
	
	  where *xxxxxx* is the part number, for example: CZ1N1ML
	3. Optionally, locate the **prereqcheck.bin** file and run it to ensure that your system meets all requirements.
	4. Start the graphical interface installation wizard by issuing the following command:
	`./install.bin`
	
	Experienced users: You can also run the installation wizard in console mode, by issuing the following command:
	`./install.bin -i console`

5. Restart all of the Tivoli Storage Manager agent instances that you stopped at the beginning of this procedure.
6. Verify that the upgrade was successful.
   - Open the Manage Tivoli Enterprise Management Services application and look at the Tivoli Enterprise Portal server version and verify that it is 06.22.02.00. Look at the Monitoring Agent for Tivoli Storage Manager template and verify that the version is 06.33.00.00.
   - Open a DB2 command window and issue db2level to verify that the version of DB2 is 9.7.4.
   - Review the tsmCustomClient.jar file timestamp to ensure that it is recent.

   Note: If there were any errors during the upgrade, review the following steps for assistance:

- The summary page lists any errors that were encountered during the upgrade, and directs you to an error log file. If you accepted the default directory during the upgrade, the log file can be found at: /var/tivoli/tsm/log.txt.
- The logs.zip file contains all of installation log files for or all of the different components, and can be found at: *install_dir*/. For example, /opt/tivoli/tsm/reporting/logs.zip.
- For more help, see the section on reviewing the logs.zip file to resolve installation failures in the *Problem Determination Guide*.

Upgrade any existing monitoring agents that were installed directly on any of your Tivoli Storage Manager servers.

Tip: Monitoring agents that are already at version 6.3 or later, do not need to be upgraded unless you want to use the new SSL feature in V6.3.3. The monitoring agents do not need to be re-created. You can select the existing agent, right-click, and select **Reconfigure** instead.

After you complete the upgrade, you must install the Version 6.3 or later Administration Center, including the Tivoli Common Reporting component. See Chapter 19, "Installing and configuring the Administration Center," on page 189.

Remember: The data source and all previous reports are overwritten during the Administration Center installation. If you customized any BIRT or Cognos reports that you want to save, you must export them before you install the Administration Center. After the installation is complete, you can import the customized reports.

Upgrading the monitoring agent

You can upgrade monitoring agents that are at an earlier version without having to uninstall them.

You do not need to upgrade monitoring agents that are already at V6.3, or later unless you want to use the new SSL feature that is in V6.3.3. The monitoring agents do not need to be re-created. You can select the existing agent, right-click, and select **Reconfigure** instead.

To upgrade your existing monitoring agents to version 6.3, complete these steps:
1. Review the upgrade scenarios and the capacity planning information to determine whether to install more agents on an existing Tivoli Monitoring system, or on a remote Tivoli Storage Manager server.
2. Stop all existing monitoring agents by using one of the following methods:
   - From the Manage Tivoli Enterprise Monitoring Services window, select each monitoring agent instance, and click **Actions** > **Stop**.
   - To stop the agents by using the command line, complete the following steps:
     a. Display the agents that are running by issuing the following command, and then review the output to determine which services are running:
        ./cinfo -r
     b. Stop all of the Tivoli Storage Manager instances by issuing the following command:
        ./itmcmd agent -o *instance_name* stop sk

3. Install a version 6.3 or later monitoring agent on the remote Tivoli Storage Manager that you want to monitor, or on an existing IBM Tivoli Monitoring system. For details, see Installing monitoring agents.

4. Return to the Manage Tivoli Enterprise Monitoring Services window, select each monitoring agent instance, right-click, and select **Start**, or you can restart the agents by issuing the following command:

   ```
   ./itmcmd agent -o instance_name start sk
   ```

After you upgrade the agent, verify that the upgrade was successful. Open the Manage Tivoli Enterprise Monitoring Services application and look at the Monitoring Agent for Tivoli Storage Manager template to verify that the version of the agent is correct.

Chapter 11. Uninstalling Tivoli Monitoring for Tivoli Storage Manager

You can uninstall Tivoli Monitoring for Tivoli Storage Manager if it is no longer needed.

Uninstalling Tivoli Monitoring for Tivoli Storage Manager

You can uninstall Tivoli Monitoring for Tivoli Storage Manager by using this procedure. If you plan to reinstall, this procedure helps to ensure that all previous versions and directories are deleted from your system.

To uninstall Tivoli Monitoring for Tivoli Storage Manager using the wizard, complete these steps:

> **Tip:** Always stop processes by issuing the `itmcmd` commands, or from the Manage Tivoli Enterprise Monitoring Services application. Do not kill processes by using the operating system.

1. Stop all of the Tivoli Storage Manager agent instances using the CandleManage application, or the command-line interface.

   Stop the agent using CandleManage:
   Go to the directory where the CandleManage application is installed. For example:
   ```
   cd /opt/tivoli/tsm/reporting/itm/bin
   ```

   Run the CandleManage program by issuing the following command:
   ```
   ./CandleManage &
   ```

   Stop the agent instances by using the command-line interface:
   Display the agents that are running by issuing the following command, and then refer to the output:
   ```
   ./cinfo  -r
   ```

   Issue the following command for each agent instance:
   ```
   ./itmcmd agent -o instance_name stop sk
   ```
2. Change to the directory where the software is installed. For example: cd /opt/tivoli/tsm/reporting/_uninst
3. To uninstall the product, run one of the following commands:
   - If you are using a graphical interface, issue the following command:
     ```
     ./uninstall
     ```
   - If you are using the command line, issue the following command:
     ```
     ./uninstall -i console
     ```
   a. To continue the uninstallation, press `Enter`.
   b. Enter 1 to continue, or 2 to exit.
   c. After the uninstallation is complete, a message displays stating that all items were successfully uninstalled.
4. To avoid any issues with future installations, after uninstalling Tivoli Monitoring for Tivoli Storage Manager, complete the following steps to delete the `ITMAgents1` file.

a. Change directories to the directory where the `ITMAgents1` file is located, for example: `cd /etc/init.d`

b. Delete the file, `ITMAgents1`. The value appended to the end of the file name can vary.

5. After you complete the uninstallation, the DB2 entry, `db2_tsm1` *portnumber*/`tcp` still exists in the `/etc/services` file. Issue these commands to remove the entry:

   a. `cd /etc`
      `cp services services.mmddyy`

      where mm = month, dd = day, and yy = year. For example: `cp services services.041209`

   b. Open the `services` file and search for and delete this line:

      `db2_tsm1 portnumber/tcp`

   c. Delete the entry, and save the file.

6. You can also remove the DB2 database data if it is no longer needed. By default these files are in the `/home/db2inst1` directory.

   Attention: If you remove this file, you are removing any database data and all the files that are stored under this directory.

   `rm -rf /home/db2inst1`

7. Check for the existence of the `db2inst1` user with this command:

   `cat /etc/passwd | grep db2inst1`

8. If this user ID exists, remove it with this command:

   `userdel db2inst1`

9. If this DB2 group exists, remove it with this command:

   Edit the `/etc/groups` file, and remove these two lines:

   `db2grp1:!:112:root`
   `db2fgrp1:!:113:root`

10. Delete the directories for Tivoli Monitoring for Tivoli Storage Manager and DB2 with these commands:

    `rm -rf /opt/tivoli/tsm/reporting`
    `rm -rf /var/db2`

11. Restart the system.

Uninstalling monitoring agents

Uninstalling monitoring agents and application support files

If you installed Tivoli Monitoring for Tivoli Storage Manager agents by using the IBM Tivoli Monitoring installer, you can uninstall the agents by using the command-line interface.

To uninstall Tivoli Monitoring for Tivoli Storage Manager agents, complete the following steps:

1. Stop all of the Tivoli Storage Manager agent instances using the CandleManage application, or the command-line interface.

   Tip: Always stop processes by issuing the **itcmd** commands, or from the Manage Tivoli Enterprise Monitoring Services application. Do not kill processes by using the operating system.

Stop the agent using CandleManage:
> Go to the directory where the CandleManage application is installed. For example:
>
> ```
> cd /opt/tivoli/tsm/reporting/itm/bin
> ```
>
> Run the CandleManage program by issuing the following command:
>
> ```
> ./CandleManage &
> ```

Stop the agent instances by using the command-line interface:
> Display the agents that are running by issuing the following command, and then refer to the output:
>
> ```
> ./cinfo  -r
> ```
>
> Issue the following command for each agent instance:
>
> ```
> ./itmcmd agent -o instance_name stop sk
> ```

2. Change to the directory where the agent is installed, for example:

   ```
   cd /opt/IBM/ITM/bin
   ```

3. Issue the following command:

   ```
   ./uninstall.sh
   ```

4. In the list of features, locate an agent to uninstall. Agents are identified by the name `Reporting Agent for Tivoli Storage Manager`. Uninstall an agent by entering the feature number of the agent and pressing the Enter key. To confirm your choice, enter 1 and press the Enter key. An updated list of features is displayed. Repeat this step to uninstall all monitoring agents.

5. Exit the window by entering 99 and pressing the Enter key.

6. Identify the support files for the monitoring agents. Issue the `./cinfo` command. For example:

   ```
   /opt/IBM/ITM/bin # ./cinfo -i -t sk
   ```

   The result is similar to the following list:

   ```
   PC   APPLICATION SUPPORT DESC                     PLAT    APP VER

   sk   Monitoring Agent for Tivoli Storage Manager  tpd     06.30.00.
   sk   Monitoring Agent for Tivoli Storage Manager  tps     06.30.00.
   sk   Monitoring Agent for Tivoli Storage Manager  tpw     06.30.00.
   ```

7. Uninstall the support files for the monitoring agents by using the `./uninstall.sh` command. For example, if the entry in the PLAT column is `tpd`, enter the following command to uninstall the corresponding support files:

   ```
   /opt/IBM/ITM/bin # ./uninstall.sh sk tpd
   ```

8. For each support file that you uninstall, confirm the choice by entering 1 and pressing the Enter key.

9. When you finish the uninstall process, to exit the window, enter 99 and press the Enter key.

10. Restart any agents that you stopped.

Part 3. Installing the Operations Center

This overview summarizes key concepts to understand before you install and configure the IBM Tivoli Storage Manager Operations Center. It also summarizes the methods for installing or uninstalling the Operations Center.

Table 37 lists the key concepts to understand and indicates where to find information about these concepts.

Table 38 lists the methods for installing or uninstalling and indicates where to find the associated instructions.

Table 37. Key concepts to understand before you install and configure the Operations Center

Key concepts to understand	Where to find the information
System requirements **Restriction:** To manage a server with the Operations Center, the server must have Tivoli Storage Manager V6.3.4 or later installed.	"System requirements for the Operations Center" on page 163 • "Operating system requirements" on page 165 • "Web browser requirements" on page 165 • "Language requirements" on page 165
IBM Installation Manager	"IBM Installation Manager" on page 166
Prerequisite checks	"Prerequisite checks" on page 167
Operations Center installation package	"Opening the Operations Center installation package" on page 171
Installation credentials	"Installation credentials for the Operations Center" on page 167
Installation directories	"Installation directories" on page 167
Port numbers	"Port numbers" on page 168
Password for secure communications	"Password for secure communications" on page 168
Hub and spoke servers	"Hub and spoke servers" on page 177

Table 38. Methods for installing or uninstalling the Operations Center

Installation method	Where to find the instructions
Graphical	• "Installing the Operations Center by using a graphical wizard" on page 171 • "Uninstalling the Operations Center by using a graphical wizard" on page 185
Console	• "Installing the Operations Center in console mode" on page 172 • "Uninstalling the Operations Center in console mode" on page 185
Silent mode	• "Installing the Operations Center in silent mode" on page 172 • "Uninstalling the Operations Center in silent mode" on page 186

Chapter 12. Planning to install the Operations Center

Before you install the Operations Center, you must understand some key concepts such as system requirements, installation credentials, and the default location of installation directories.

System requirements for the Operations Center

Before you install the Operations Center, ensure that your system meets the minimum requirements.

Operations Center requirements

The following resources are required to run the Operations Center:
- One processor core
- 4 GB of memory
- 1 GB of disk space

You can install the Operations Center on the same computer as a Tivoli Storage Manager server, or on a separate computer.

To use the same computer, it must meet the Operations Center system requirements in addition to the requirements that apply for the Tivoli Storage Manager server.

Hub and spoke server requirements

The first Tivoli Storage Manager server that you connect to the Operations Center is designated as a *hub server*. In a multiple-server environment, you can connect additional servers, called *spoke servers*. The spoke servers send alerts and status information to the hub server.

When you configure a Tivoli Storage Manager server as a hub or spoke server, status monitoring is automatically enabled. Additional system resources are required to support status monitoring.

The hub and spoke server requirements are based on the default monitoring settings. If you reduce the default data refresh interval for the Operations Center, the servers require further resources.

Hub and spoke servers must have Tivoli Storage Manager V6.3.4 or later installed.

Tip: If only one Tivoli Storage Manager server is monitored by the Operations Center, that server is still called a hub server, even though no spoke servers are connected to it.

A hub or spoke server that manages 1000 Tivoli Storage Manager clients (client nodes or virtual machine file spaces) requires the following additional resources to support Operations Center monitoring:
- Approximately 1.1 processor cores
- 2 GB of disk space for the server database

- 10 GB of disk space for the archive log (assumes that a full database backup runs every 24 hours)

Spoke servers send approximately 30 - 60 MB of data to the hub server every hour. Each data collection cycle on the spoke server generates approximately 2.5 - 5 MB of upstream network-session traffic.

Even if a hub or spoke server manages fewer than 1000 clients, consider implementing the minimum requirements.

For every additional 1000 clients that are managed by a hub or spoke server, add 2 GB of database space, 10 GB of log space, and reserve one-tenth of a processor core. For a spoke server, expect an extra 30 - 60 MB of network traffic.

In a multiple-server environment, the hub server must also meet the following requirements:
- Additional database and log space, equal to the total requirement for all the spoke servers.
- Additional processor resources, equal to the total requirement for all clients in the environment.
- Additional I/O capability for the database volumes, to support approximately 200 I/O operations per second (IOPS) for every 1000 clients in the environment. This estimate assumes an average I/O size of 8 KB.

Tips:
- To support the additional I/O requirements, the hub server database should be located on a solid-state drive (SSD) or on an external SAN disk storage device with multiple volumes or multiple spindles under each volume.
- In an environment with fewer than 1000 clients, consider establishing a baseline capability of 1000 IOPS for the hub server database if the hub server manages any spoke servers.

Requirements example

Consider an environment that has the following configuration:
- A hub server that manages 1000 clients
- Five spoke servers, each of which manages 2000 clients

In this example, the servers require the following resources to support Operations Center monitoring, in addition to the resources that are needed to provide backup services to clients:

Spoke servers
> Each spoke server requires the following additional resources:
> - Approximately 1.2 processor cores
> - 4 GB of disk space for the server database
> - 20 GB of disk space for the archive log
>
> Each spoke server sends approximately 60 - 120 MB of data to the hub server every hour.

Hub server
> The hub server requires the following additional resources:
> - Approximately two processor cores

- 22 GB of disk space for the server database
- 110 GB of disk space for the archive log
- 2200 IOPS capability for the server database volumes

Tip: Consider exceeding the disk space requirements for the database and log by 25% - 50% to handle additional processing needs that might occur.

For more information, see *Tivoli Storage Manager Optimizing Performance* and the IBM Support Portal at http://www.ibm.com/support/entry/portal/.

Related concepts:

"Hub and spoke servers" on page 177

Operating system requirements

The Operations Center is available for AIX, Linux, and Windows systems.

- The following are the Linux x86_64 and zSeries systems on which you can install the Operations Center:
  - Red Hat Enterprise Linux 5, update 6 or later
  - Red Hat Enterprise Linux 6, all updates
  - SUSE Linux Enterprise Server 10, Service Pack 3 or later
  - SUSE Linux Enterprise Server 11, all updates

The Operations Center can monitor any server that runs Tivoli Storage Manager V6.3.4 or later. Servers are not limited to the operating systems that are supported for the Operations Center.

Web browser requirements

The Operations Center supports multiple web browsers.

The following web browsers are supported:
- Apple Safari on the iPad
- Google Chrome
- Microsoft Internet Explorer 9 and 10
- Mozilla Firefox ESR 10 or later

For optimal viewing, ensure that the screen resolution for your system is set to a minimum of 1024 X 768 pixels.

Language requirements

By default, the Operations Center uses the language that the web browser uses. However, the installation process uses the language that the operating system uses. Verify that the operating system and the web browser are set to the language that you require.

You can use the languages that are shown:

Table 39. Operations Center languages on Linux systems

Language	Language option value
Chinese, Simplified	zh_CN
Chinese, Simplified (GBK)	zh_CN.gb18030
Chinese, Simplified (UTF-8)	zh_CN.utf8

Table 39. Operations Center languages on Linux systems (continued)

Language	Language option value
Chinese, Traditional (Big5)	Zh_TW
Chinese, Traditional (euc_tw)	zh_TW
Chinese, Traditional (UTF-8)	zh_TW.utf8
English, United States	en_US
English (UTF-8)	en_US.utf8
French	fr_FR
French (UTF-8)	fr_FR.utf8
German	de_DE
German (UTF-8)	de_DE.utf8
Italian	it_IT
Italian (UTF-8)	it_IT.utf8
Japanese (EUC)	ja_JP
Japanese (UTF-8)	ja_JP.utf8
Korean	ko_KR
Korean (UTF-8)	ko_KR.utf8
Portuguese, Brazilian	pt_BR
Portuguese, Brazilian (UTF-8)	pt_BR.utf8
Russian	ru_RU
Russian (UTF-8)	ru_RU.utf8
Spanish	es_ES
Spanish (UTF-8)	es_ES.utf8

IBM Installation Manager

The Operations Center uses IBM Installation Manager, which is an installation program that can use remote or local software repositories to install or update many IBM products.

If the required version of IBM Installation Manager is not already installed, it is automatically installed or upgraded when you install the Operations Center. It must remain installed on the system so that the Operations Center can be updated or uninstalled later as needed.

The following terms represent key concepts that relate to IBM Installation Manager:

Offering
> An installable unit of a software product. The Operations Center offering contains all of the media that IBM Installation Manager requires to install the Operations Center.

Package
> The group of software components that are required to install an offering. The Operations Center package contains the following components: IBM Installation Manager installer and the Operations Center offering.

Package group
A set of packages that share a common parent directory. The default package group for the Operations Center package is IBM Tivoli Storage Manager.

Repository
A remote or local storage area for data and other application resources. The Operations Center package is stored in a repository on IBM Fix Central.

Shared resources directory
A directory that contains software files or plug-ins that are shared by packages. IBM Installation Manager stores installation-related files on the shared resources directory, including files that are used for rolling back to a previous version.

Prerequisite checks

The installation program for the Operations Center verifies that prerequisite requirements are met.

The prerequisite checks verify the following items:
- The minimum memory requirement, as described in "System requirements for the Operations Center" on page 163
- The operating system requirements, as described in "Operating system requirements" on page 165
- The host name of the computer where the web server for the Operations Center is to be installed.

  The host name must not contain double-byte character set (DBCS) characters or the underscore character (_). Although it can contain the hyphen character (-), it cannot have a hyphen as the last character in the name.
- The installation location, as described in "Installation directories"

Installation credentials for the Operations Center

To install the Operations Center, you must have the appropriate credentials.

You must use the following user account:

      root

Installation directories

During the installation process, you must specify the installation directory paths for the Operations Center and for IBM Installation Manager.

Operations Center installation directory

The Operations Center is installed in the ui subdirectory of the installation directory.

The following path is the default path for the Operations Center installation directory:

      /opt/tivoli/tsm

The installation directory path must meet the following criteria:

- The path must contain no more than 128 characters.
- The path must include only ASCII characters.
- The path cannot include non-displayable control characters.
- The path cannot include any of the following characters:

  ```
  % | < > ' " $ & ; *
  ```

Installation Manager installation directory

The following path is the default path for the Installation Manager installation directory:

```
/opt/IBM/InstallationManager
```

Port numbers

During the installation process, you must specify the port numbers that are used by the web server for the Operations Center.

The values for the nonsecure (http) and secure (https) port numbers must meet the following criteria:

- Each port number must be an integer in the range 1024 - 65535.
- Each port number must be unique. The same port number cannot be used for both ports.
- The port numbers cannot be already in use or allocated to other programs.

If you do not specify a port number, the following default values are used:

Nonsecure port (http)
 11080

Secure port (https)
 11090

After you install the Operations Center, if you do not remember which port numbers you specified, refer to the following file, which contains the Tivoli Storage Manager server connection information:

```
installation_dir/ui/Liberty/usr/servers/guiServer/
bootstrap.properties
```

where *installation_dir* represents the directory where the Operations Center is installed.

Password for secure communications

The Operations Center uses the HTTPS protocol to communicate with web browsers. You can optionally use the Secure Sockets Layer (SSL) protocol to secure communications between the Operations Center and the hub server, and between servers.

The truststore file of the Operations Center contains the SSL certificate that the Operations Center uses for HTTPS communication with web browsers. During installation of the Operations Center, you create a password for the truststore file.

Important: Remember the password because, if you later choose to set up SSL communication between the Operations Center and the hub server, you must use the same password to add the SSL certificate of the hub server to the truststore file.

Password length

> Minimum: 6 characters

> Maximum: 64 characters

The password must contain at least the following characters:

> One uppercase letter (A – Z)

> One lowercase letter (a – z)

> One digit (0 – 9)

> Two non-alphanumeric characters: ~ ! @ # $ % ^ & * _ - + = ` | ( ) { } [ ] : ; < > , . ? /

Related tasks:

"Resetting the password for the truststore file of the Operations Center" on page 183

Chapter 13. Installing the Operations Center

You can install the Operations Center by using any of the following methods: a graphical wizard, the command line in console mode, or silent mode.

You cannot configure the Operations Center until you install, configure, and start the Tivoli Storage Manager server. Therefore, before you install the Operations Center, install the Tivoli Storage Manager V6.3.4 server package.

You can install the Operations Center on a computer with the Tivoli Storage Manager server or on a separate computer.

Opening the Operations Center installation package

You can obtain the installation package from the product DVD or from the IBM download site.

Use one of the following procedures to access the Operations Center installation files:

- To use the product DVD, complete the following steps:

  Insert the Tivoli Storage Manager Operations Center DVD. Ensure that the DVD is mounted and the installation files are visible.

- To extract the installation files from a package that you obtain from the IBM download site, complete the following steps:

  1. Obtain one of the following package files: `6.4.1.000-TIV-TSMOC-LinuxS390.bin` or `6.4.1.000-TIV-TSMOC-Linuxx64.bin`.
  2. Ensure that you have executable permission for the package file.

     You can change the file permissions by entering the following command:

     `chmod a+x package_name.bin`
  3. Run the following command to extract the installation files:

     `./package_name.bin`

     The self-extracting package file is extracted to the current directory.

Installing the Operations Center by using a graphical wizard

You can install or update the Operations Center by using the graphical wizard of IBM Installation Manager.

1. From the directory where the Operations Center installation package file is extracted, issue the following command:

   `./install.sh`
2. Follow the wizard instructions to install the IBM Installation Manager and Operations Center packages.

See Chapter 16, "Configuring the Operations Center," on page 177.

Installing the Operations Center in console mode

You can install or update the Operations Center by using the command line in console mode.

1. From the directory where the installation package file is extracted, run the following program:

   `./install.sh -c`

2. Follow the console instructions to install the Installation Manager and Operations Center packages.

Configure the Operations Center, as described in Chapter 16, "Configuring the Operations Center," on page 177.

Installing the Operations Center in silent mode

You can install or update the Operations Center in silent mode without any user interaction.

The `input` directory, in the directory where the installation package is extracted, contains the following sample response files for installing, updating, and uninstalling the Operations Center:

- `install_response_sample.xml`
- `update_response_sample.xml`
- `uninstall_response_sample.xml`

Rather than creating new response files, you can use these sample files as they are, with the default values, or you can customize them.

1. Create a response file, or use one of the following default response files:

   - `install_response_sample.xml`
   - `update_response_sample.xml`

   If you use a default response file, modify the following line of the file to create a password for the truststore file of the Operations Center:

   `<data key='user.SSL_PASSWORD' value='`*mypassword*`'/>`

   where *mypassword* represents the password that you want to create.

   To generate a response file as part of a console-mode installation, complete the selection of the console-mode installation options. In the Summary panel, enter `G` to generate the response file according to the previously selected options.

2. From the directory where the installation package file is extracted, issue the following commands as appropriate:

   To start the installation by accepting the default values, issue the following command:

   `./install.sh -s -acceptLicense`

   To start the installation with a custom response file, issue the following command, where *response_file* represents the response file path, including the file name:

   `./install.sh -s -input `*response_file*` -acceptLicense`

Configure the Operations Center, as described in Chapter 16, "Configuring the Operations Center," on page 177.

Chapter 14. Rolling back to a previous version of the Operations Center

By default, IBM Installation Manager saves earlier versions of a package to roll back to if you experience issues with later versions of updates, fixes, or packages. When the IBM Installation Manager rolls back a package to a previous version, the current version of the files is uninstalled, and an earlier version is reinstalled.

The rollback function is available only after the Operations Center is updated.

To roll back to a previous version of the Operations Center, use the **Roll Back** option on the first page of the IBM Installation Manager.

Chapter 15. Stopping and starting the web server

The web server of the Operations Center runs as a service and starts automatically.

If you must stop and start the web server for the Operations Center, for example, to restart the initial configuration wizard, use the following methods:
Run the following commands:
- To restart the server:

  ```
  service opscenter.rc restart
  ```
- To stop the server:

  ```
  service opscenter.rc stop
  ```
- To start the server:

  ```
  service opscenter.rc start
  ```

Tip: You can use the following command to determine whether the server is running:

```
service opscenter.rc status
```

Chapter 16. Configuring the Operations Center

When you open the Operations Center for the first time after you install it, you must configure it to manage your storage environment.

Hub and spoke servers

The first Tivoli Storage Manager server that you connect to the Operations Center is designated as a *hub server*. In a multiple-server environment, you can connect more servers, called *spoke servers*. The spoke servers send alerts and status information to the hub server.

The Operations Center shows you a consolidated view of alerts and status information for the hub server and any spoke servers.

You can install the Operations Center on the same computer as a Tivoli Storage Manager server or on a different computer.

When you open the Operations Center for the first time, you connect it to one Tivoli Storage Manager server instance, which becomes the dedicated hub server. You can then connect more Tivoli Storage Manager servers as spoke servers.

Tip: If you use library sharing, and the library manager server meets the Operations Center system requirements, consider designating this server as the hub server. Few, if any, Tivoli Storage Manager clients are typically registered to the library manager server. The smaller client workload of this server can make it a good candidate to take on the additional processing requirements of a hub server.

To support the additional input/output requirements of a hub server, the server database must be on an SSD or on an external SAN disk storage device with multiple volumes or multiple spindles under each volume.

Performance

As a rule, a hub server can support 10-20 spoke servers. This number can vary, depending on your configuration.

The following factors have the most significant impact on system performance:
- The number of Tivoli Storage Manager clients or virtual machine file systems that are managed by the hub and spoke servers.
- The frequency at which data is refreshed in the Operations Center.
- The length of time for which status data is retained in the Operations Center.

Consider grouping hub and spoke servers by geographic location. For example, managing a set of hub and spoke servers within the same data center can help prevent issues that can be caused by firewalls or the lack of appropriate network bandwidth between different locations.

If necessary, you can further divide servers according to one or more of the following characteristics:
- The administrator who manages the servers
- The organizational entity that funds the servers

- Server operating systems

Multiple hub servers

You can manage a hub server and multiple spoke servers from the same instance of the Operations Center.

If you have more than 10-20 spoke servers, or if resource limitations require the environment to be partitioned, you can configure multiple hub servers and connect a subset of the spoke servers to each hub server.

Restrictions:
- A single server cannot be both a hub server and a spoke server.
- Each spoke server can be assigned to only one hub server.
- Each hub server requires a separate instance of the Operations Center, each of which has a separate web address.

Administrator IDs and passwords

An administrator must have a valid ID and password on the hub server to log in to the Operations Center. An administrator ID is also assigned to the Operations Center so that the Operations Center can monitor servers.

The following Tivoli Storage Manager administrator IDs are required to use the Operations Center:

Operations Center administrator IDs
> Any administrator ID that is registered on the hub server can be used to log in to the Operations Center. The authority level of the ID determines which tasks can be completed. You can create new administrator IDs by using the **REGISTER ADMIN** command. For information about this command, see the *Administrator's Reference*.

> **Restriction:** To use an administrator ID in a multi-server configuration, the ID must be registered on the hub and spoke servers with the same password and authority level.

> Consider using a Lightweight Directory Access Protocol (LDAP) server to manage authentication for these servers.

> Another way to keep the credentials synchronized is to use the Tivoli Storage Manager enterprise configuration functions to automatically distribute changes to the administrator definitions.

> For more information about the enterprise configuration functions, see *Managing a network of Tivoli Storage Manager servers* in the *Administrator's Guide.*.

Monitoring administrator ID
> When you initially configure the hub server, an administrator ID named IBM-OC-*server_name* is registered with system authority on the hub server and is associated with the initial password that you specify. This ID, which is sometimes called the *monitoring administrator*, is intended for use only by the Operations Center.

> Do not delete, lock, or modify this ID. The same administrator ID with the same password is registered on any spoke servers that you add. The

password is automatically changed on the hub and spoke servers every 90 days. You do not need to use or manage this password.

Opening the Operations Center

You can open the Operations Center with a web browser.

You can open the Operations Center by using any supported web browser. For a list of supported web browsers, see the chapter about web browser requirements in the *Installation Guide.*

Start your browser, and enter `https://hostname:secure_port/oc`, where *hostname* represents the name of the computer where the Operations Center is installed, and *secure_port* represents the port number that the Operations Center uses for HTTPS communication on that computer.

Configuring the hub server: If you are connecting to the Operations Center for the first time, you are redirected to the initial configuration wizard. In that wizard, you must provide the following information:
- Connection information for the Tivoli Storage Manager server that you designate as a hub server
- Login credentials for an administrator who is defined to that Tivoli Storage Manager server

If the event-record retention period of the Tivoli Storage Manager server is less than 14 days, the value automatically increases to 14 days when you configure the server as a hub server.

If you have multiple Tivoli Storage Manager servers in your environment, add the other Tivoli Storage Manager servers as spoke servers to the hub server, as described in "Adding spoke servers."

Related concepts:

"Port numbers" on page 168

"Hub and spoke servers" on page 177

Adding spoke servers

After you configure the hub server for the Operations Center, you can add one or more spoke servers to that hub server.

1. In the menu bar at the top of the Operations Center, click **Servers**. The TSM Servers page opens.

   Tip: In the table on the TSM Servers page, a server might have a status of **Unmonitored**. An *unmonitored* server is a server that an administrator defined to the hub server by using the **DEFINE SERVER** command, but which is not yet configured as a spoke server.

2. Complete one of the following steps:
   - Click the server to highlight it, and from the table menu bar, click **Monitor Spoke**.

   - If the server that you want to add is not shown in the table, click **Connect Spoke** in the table menu bar.

3. Provide the necessary information, and complete the steps in the spoke configuration wizard.

> **Note:** If the event-record retention period of the server is less than 14 days, the value automatically increases to 14 days when you configure the server as a spoke server.

Sending alerts by email

Tivoli Storage Manager can send an email when an alert is triggered. An alert represents one or more error messages that are issued by a Tivoli Storage Manager server. Alerts can be shown in the Operations Center and can be sent from the server to administrators by email.

An SMTP server is required to send and receive alerts by email.

For detailed information about the commands that are mentioned here, see the *Administrator's Reference*.

An administrator with system privilege can complete the following steps on the server to enable alerts to be sent by email:

1. Issue the **QUERY MONITORSETTINGS** command to verify that alert monitoring is set to ON. If the monitoring settings output indicates Off, issue the **SET ALERTMONITOR** command to start alert monitoring on the server:

   set alertmonitor on

   Tip: If alert monitoring is on, alerts are displayed in the Operations Center even though the alert email feature might not be enabled.
2. Enable alerts to be sent by email by issuing the **SET ALERTEMAIL** command:

   set alertemail on
3. Define the SMTP host server that is used to send email by issuing the **SET ALERTEMAILSMTPHOST** command:

   set alertemailsmtphost
4. Set the SMTP port by issuing the **SET ALERTEMAILSMTPPORT** command:

   set alertemailsmtpport *port_number*

   Tip: The default port is 25.
5. Define the email address of the sender of the alerts by issuing the **SET ALERTEMAILFROMADDR** command:

   set alertemailfromaddr *email_address*
6. Add the administrator IDs that want to receive alerts by email to one or more alert triggers by issuing the **DEFINE ALERTTRIGGER** or **UPDATE ALERTTRIGGER** command:

   define alerttrigger *message_number* ADmin=*admin1*,*admin2*

   update alerttrigger *message_number* ADDadmin=*admin3* deladmin=*admin1*
7. Register the administrator ID, or update an administrator ID to enable email alerts and set the email address. Specify alert=yes, and ensure that the administrator ID is updated on the server with the corresponding email address by issuing the **REGISTER ADMIN** or **UPDATE ADMIN** command:

   register admin *admin_name* alert=yes emailaddress=*email_address*

   update admin *admin_name* alert=yes emailaddress=*email_address* or

   Tip: You can suspend email alerts for an administrator by using one of the following methods:
   - Use the **UPDATE ADMIN** command, and specify ALERT=no.

| • Use the **ALERTTRIGGER** command, and specify the **DELADMIN** parameter.

Example: Enabling multiple administrators to receive an alert

The following example describes the commands that are used to enable the administrators myadmin, djadmin, and csdadmin to receive email alerts for ANR1075E messages.

```
set alertmonitor on
set alertmaiil on
set alertemailsmtphost mymailserver.domain.com
set alertemailsmtpport 450
set alertemailfromaddr srvadmin@mydomain.com
update admin myadmin alert=yes emailaddress=myaddr@example.com
update admin djadmin alert=yes emailaddress=djaddr@example.com
update admin csadmin alert=yes emailaddress=csaddr@example.com
define alerttrigger anr0175e admin=myadmin,djadmin,csdadmin
```

Chapter 17. Troubleshooting the Operations Center installation

Descriptions of possible installation problems and their solutions are provided.

Resetting the password for the truststore file of the Operations Center

To add the SSL certificate of the hub server to the truststore file of the Operations Center, you must know the truststore-file password, which was created when the Operations Center was installed. If you do not know the password, you can reset it.

In the following procedure, you create a new password, delete the truststore file of the Operations Center, and restart the web server of the Operations Center. A new truststore file is automatically created, and the SSL certificate of the Operations Center is automatically placed into the truststore file.

1. Stop the web server of the Operations Center. For instructions, see Chapter 15, "Stopping and starting the web server," on page 175.
2. Go to the following directory:

   installation_dir/ui/Liberty/usr/servers/guiServer

   where *installation_dir* represents the directory where the Operations Center is installed.
3. Open the `bootstrap.properties` file.

   The `bootstrap.properties` file contains the truststore-file password in encrypted or unencrypted format.

   - The following example shows an encrypted password, `{xor}MiYPPiwsKDAtOw==`, in the password line of the file. Encrypted passwords begin with the text string `{xor}`.

     `tsm.trustore.pswd={xor}MiYPPiwsKDAtOw==`

   - The following example shows an unencrypted password, `J8b%^B`, in the password line of the file:

     `tsm.truststore.pswd=J8b%^B`

     Tip: If the password is unencrypted, you can use it to open the truststore file, and you are not required to reset the password.
4. Reset the password by replacing the password in the `bootstrap.properties` file with a new password. You can replace the password with an unencrypted or encrypted password. Remember the unencrypted version of the password for future use.

   - To create an unencrypted password, use the following rules:

     Password length:
     > Minimum: 6 characters

     > Maximum: 64 characters

     The password must contain at least the following characters:
     > One uppercase letter (A – Z)

     > One lowercase letter (a – z)

     > One digit (0 – 9)

> Two non-alphanumeric characters: ~ ! @ # $ % ^ & * _ - + = ` | ( ) { }
> [ ] : ; < > , . ? /

- To create an encrypted password, complete the following steps:
   a. Create an unencrypted password.
   b. From the operating-system command line, go to the following directory:

      `installation_dir/ui/Liberty/bin`

   c. Issue the following command:

      `securityUtility encode myPassword`

      where `myPassword` represents the unencrypted password.

      The command returns an encrypted password. For example:
      `{xor}MiYPPiwsKDAtOw==`

5. Close the `bootstrap.properties` file.
6. Go to the following directory:

   `installation_dir/ui/Liberty/usr/servers/guiServer`

7. Delete the truststore file of the Operations Center. The truststore file is the following file:

   `gui-truststore.jks`

8. Start the web server of the Operations Center.

A new truststore file is automatically created for the Operations Center, and the SSL certificate of the Operations Center is automatically placed into the truststore file.

For information about configuring the Operations Center to use the SSL protocol for communications with the hub server, search for "SSL" in the embedded help system of the Operations Center. In one step of the configuration procedure, you are required to enter the unencrypted form of the truststore-file password.

Related concepts:

"Password for secure communications" on page 168

Chinese, Japanese, or Korean fonts display incorrectly

Chinese, Japanese, or Korean fonts might be displayed incorrectly in the Tivoli Storage Manager Operations Center on Red Hat Enterprise Linux 5 (RHEL5).

Solution

Install the following font packages, which are available from Red Hat:
- fonts-chinese
- fonts-japanese
- fonts-korean

For information about these font packages, search the Red Hat Customer Portal.

Chapter 18. Uninstalling the Operations Center

You can uninstall the Operations Center by using any of the following methods: a graphical wizard, the command line in console mode, or silent mode.

Uninstalling the Operations Center by using a graphical wizard

You can uninstall the Operations Center by using IBM Installation Manager installation wizard.

For information about the default path for the Installation Manager installation directory, see "Installation directories" on page 167.

1. To uninstall the Operations Center, start the Installation Manager.

   In the directory where the Installation Manager is installed, go to the `eclipse` subdirectory, and issue the following command:

   `./IBMIM`

2. Click **Uninstall**.
3. Select **IBM Tivoli Storage Manager Operations Center**, and click **Next**.
4. Click **Uninstall**.
5. Click **Finish**.

Uninstalling the Operations Center in console mode

To uninstall the Operations Center by using the command line, you must run the uninstall program of IBM Installation Manager from the command line with the parameter for console mode.

1. In the directory where IBM Installation Manager is installed, go to the following subdirectory:

   `eclipse/tools`

   For example:

   `/opt/IBM/InstallationManager/eclipse/tools`

2. From the `tools` directory, issue the following command:

   `./imcl -c`

3. To uninstall, enter 5.
4. Choose to uninstall from the IBM Tivoli Storage Manager package group.
5. Enter N for Next.
6. Choose to uninstall the IBM Tivoli Storage Manager Operations Center package.
7. Enter N for Next.
8. Enter U for Uninstall.
9. Enter F for Finish.

Uninstalling the Operations Center in silent mode

To uninstall the Operations Center in silent mode, you must run the uninstall program of IBM Installation Manager from the command line with the parameters for silent mode.

The `input` directory, in the directory where the installation package is extracted, contains the following sample response files for installing, updating, and uninstalling the Operations Center:

- `install_response_sample.xml`
- `update_response_sample.xml`
- `uninstall_response_sample.xml`

Rather than creating new response files, you can use these sample files as they are, with the default values, or you can customize them.

1. In the directory where IBM Installation Manager is installed, go to the following subdirectory:

    `eclipse/tools`

    For example:

    `/opt/IBM/InstallationManager/eclipse/tools`

2. From the `tools` directory, issue the following command, where *response_file* represents the response file path, including the file name:

    `./imcl -input response_file -silent`

    The following command is an example:

    `./imcl -input /tmp/input/uninstall_response.xml -silent`

Part 4. Installing and upgrading the Administration Center

Use the Administration Center to administer Tivoli Storage Manager and Tivoli Monitoring for Tivoli Storage Manager from a supported browser anywhere in your network.

Chapter 19. Installing and configuring the Administration Center

Use the Administration Center to administer Tivoli Storage Manager and Tivoli Monitoring for Tivoli Storage Manager from a supported browser anywhere in your network.

A standard installation without Tivoli Common Reporting takes approximately 35 minutes. If you install the Tivoli Common Reporting feature, the installation takes approximately 90 minutes. The installation time depends on the speed of your processor and the memory that is available in your system.

Important: The deployment engine is automatically installed with the Administration Center. Do not uninstall the deployment engine. Uninstalling this component can cause problems when upgrading the Administration Center.

If you are upgrading the Administration Center, see Chapter 21, "Upgrading the Administration Center to Version 6.3 or later," on page 213.

Use the following steps to install the Administration Center and other components, including Tivoli Integrated Portal:

1. Download and install the Administration Center. See "Installing the Administration Center components" on page 198.
2. Optional: Configure a Lightweight Directory Access Protocol (LDAP) server. See "Configuring LDAP user authentication" on page 204.
3. Verify the Administration Center installation. See "Verifying the Administration Center installation" on page 208.
4. Start the Tivoli Integrated Portal. See "Starting and stopping the Tivoli Integrated Portal server" on page 207.
5. Define your Tivoli Integrated Portal users. See "Defining Administration Center users to the Tivoli Integrated Portal" on page 209.
6. Add connections for the Tivoli Storage Manager servers that you want to manage. See "Defining Administration Center users to the Tivoli Integrated Portal" on page 209.
7. Set session length and Java heap size. See "Estimating Java heap memory size" on page 194.

Related tasks:

Chapter 21, "Upgrading the Administration Center to Version 6.3 or later," on page 213

"Creating and configuring the agent instance" on page 125

Planning to install the Administration Center

To administer servers from a browser, plan to install the Administration Center.

Ensure that you review all applicable planning information, including system requirements, capacity planning, and installation scenarios.

Before you install the software, complete these tasks:

1. Read the system requirements that are required for your operating system.
2. Review the capacity planning information.
3. Choose an installation scenario that best suits your needs.
4. Review the installation worksheet and note the user IDs, passwords, and other values that are required during installation.
5. Optionally, run the prerequisite checker to verify the readiness of your installation environment.

System requirements

The Tivoli Storage Manager server can require a large amount of memory, network bandwidth, and processor resources. In many cases, the server performs best when other applications are not installed on the same system. If the system meets the combined requirements for the server and the Administration Center, it can support both applications.

If you plan to use the Administration Center to manage an environment with many servers or administrators, consider installing the Administration Center on a separate system. See the capacity planning section.

For Administration Center system requirements, see the following website: http://www.ibm.com/support/docview.wss?uid=swg21515628.

You can install the Administration Center Version 6.3 and later on the following architectures:

- Linux x86 (32-bit and 64-bit)
- Linux s390x (64-bit)

The optional Tivoli Common Reporting feature cannot be used with the Linux s390x architecture or Red Hat Enterprise Linux 6.

Administration Center capacity planning

Capacity planning is important in determining the setup of your environment. For large environments, you can estimate how many Tivoli Storage Manager Administration Center servers are required to support administrators and Tivoli Storage Manager servers.

With this information, you can allocate sufficient resources to meet the peak application demands with little or no performance degradation and loss of function. If the Administration Center server shares a system with other applications, add the processing and memory requirements of those applications to the Administration Center requirements. In this way, you can determine the total system requirements.

Tip: The Tivoli Storage Manager Administration Center Capacity Planner tool can simplify issuing capacity planning equations. It can provide recommendations for Administration Center hardware sizings. See your IBM representative to obtain this

tool.

Maximum number of active administrators

It is possible to define many administrators to one Administration Center, however, the number of administrators who are active at the same time is limited.

An administrative task is best thought of as an interaction within the administration interface that produces some usable information or completes a preferred operation.

The maximum number of administrators who are logged in and conducting administrative tasks at a certain time for one Administration Center instance is 16. If too many administrators are logged in to the Administration Center at the same time, it is likely to result in an unacceptable rate of task failures and lost administrator productivity.

More administrators can likely be logged in at the same time if they run just a few tasks. For example, if more than 16 administrators are logged in at the same time, three or four, non-concurrent tasks per hour are possible. If the needs of your business require that several administrators be logged in at the same time, completing many tasks, plan for multiple Administration Center instances.

Processing capacity

You can meet high performance requirements for an Administration Center by using a dual-processor system with a speed of 3 GHz or faster.

The Administration Center server can use more processors, but there might not be a noticeable effect on the application performance. Adjust the processor utilization further by multiplying by the ratio of 3.4 GHz relative to the planned processor speed. Then, multiply by the ratio of two processors to the planned number of processors.

To help with planning your sizing, you can estimate the Administration Center processor utilization by using the following equation:

```
processor utilization (%) = 0.15 + tasks completed (per hour) * 0.006
```

The tasks that are completed per hour rate is the highest total number of tasks per hour that is expected to be run with or on the Administration Center server. It includes tasks that are run by all administrators who are logged in at the time. If only one administrator is logged in, the number of tasks that are run per hour can be 20 - 100. This number is not to exceed 2850 tasks per hour.

I/O throughput

Administration Center disk and network input/output (I/O) requirements are not particularly demanding, so there is no need for sustained high I/O throughput.

Application response time suffers if network delays or disk I/O delays occur. A low latency network provides the best administrator response time. Networks that are poorly tuned, currently saturated by other applications, or with higher latency (WANs) might significantly affect Administration Center performance.

Processing memory

The most important resource requirement for the Administration Center is memory.

The Administration Center uses significant memory. The memory is based on the number of Tivoli Storage Manager servers or libraries that are controlled in the Administration Center, and the number of the other applications, such as Tivoli Common Reporting.

The Administration Center uses Java. To increase memory in Java, set a higher value for the Java heap size. A heap is a stack of data that tracks memory allocations. The Java heap size determines how much memory can be allocated to a particular Java Runtime Environment.

The maximum Java heap size is the value that is specified for the Administration Center server. The default is 512 MB. The largest value that can be configured for the maximum Java heap size is 1536 MB.

Add the additional memory that is required by the operating system to the memory required by any other applications on the Administration Center server. Configure the server with at least this much real memory. It is important that the required real memory is available. Without adequate real memory, significant response time degradation can occur as the result of system memory paging.

Minimizing memory usage

You can take steps to keep the Administration Center server memory available for those users and tasks that need it the most.

For the best results, complete these configuration items:
- Turn off all Administration Center server traces, except as needed for problem determination.
- Do not increase the Tivoli Integrated Portal session timeout above 30 minutes. Idle sessions can hold on to large amounts of memory until the session is canceled because of the timeout. To configure the session timeout, see "Configuring the session timeout period" on page 193.

You also achieve better results by completing the following operational tasks regularly:
- Close portlet pages when you are finished. Closing the pages frees up any memory that is held by those pages.
- Use available filtering options where provided when you view data in large tables. The additional search criteria reduces the amount of data that the Administration Center receives from the Tivoli Storage Manager server. It also reduces the amount of data that is sent to the browser and the amount of memory required.

Configuring the session timeout period:

Configure the Administration Center session timeout period by using the Administration Center Support Utility.

This utility is located in the IBM Tivoli Storage Manager installation directory under *install_root*\tsmac\bin. Run the supportUtil script from a command window and follow the instructions.

Start the tool by issuing: supportUtil.sh.

The following text is an example of the output:

```
User ID: iscadmin
Password: <enter password>

Administration Center Support Utility - Main Menu
==================================================
1.  Manage Administration Center tracing
2.  Manage the maximum memory size the Administration Center can use
3.  Manage the Administration Center session timeout setting
4.  Collect trace files, logs and system information to send to support
5.  Generate a heap dump of the Java virtual machine
6.  Generate a Java core dump of the Java virtual machine
7.  View the log file for this utility
9.  Exit
Enter Selection: 3

Administration Center Support Utility - Manage the Session
============================================================
1.  Update the Administration Center session timeout setting
2.  View the Administration Center session timeout setting
99. Return to main menu
Enter Selection: 1

The session timeout setting determines how long a session can be idle before
it times out. After a timeout occurs the user must log in again. The default
timeout setting is 30 minutes. The minimum timeout setting is 10 minutes. To
cancel this operation enter an empty value.
Enter the new session timeout (minutes): 30
Updating the session timeout to 30 minutes.........
Session timeout successfully updated. Restart ISC for changes to take effect.
Press Enter to continue . . .<return>

Administration Center Support Utility - Manage the Session
============================================================
1.  Update the Administration Center session timeout setting
2.  View the Administration Center session timeout setting
99. Return to main menu  Enter Selection: 99

Administration Center Support Utility - Main Menu
==================================================
1.  Manage Administration Center tracing
2.  Manage the maximum memory size the Administration Center can use
3.  Manage the Administration Center session timeout setting
4.  Collect trace files, logs and system information to send to support
5.  Generate a heap dump of the Java virtual machine
6.  Generate a Java core dump of the Java virtual machine
7.  View the log file for this utility
9.  Exit  Enter Selection: 2

Administration Center Support Utility - Manage the JVM
=======================================================
1.  Update the maximum memory size the Administration Center can use
2.  View the maximum memory size the Administration Center can use
99. Return to main menu
Enter Selection: 1
```

```
The maximum memory size determines the largest amount of memory that can be
used by the Administration Center. A minimum heap size of 512 MB is
recommended. When used by 10 or more users, the recommendation is at least
1024 MB. To cancel this operation enter an empty value.
Enter the new JVM max memory size (MB): 1536
Updating the maximum memory size to 1536 MB......
Maximum memory size successfully updated.
Press Enter to continue . . .<return>
```

Estimating Java heap memory size

The Administration Center maintains information for each active administrative session as a set of objects in the configured Java heap memory. The memory requirements of an administrative session depend on the activities that the administrator runs during the session.

In the browser, each open page requires memory. Each open table requires more memory. The amount of memory depends on the number of rows and columns in the table.

Estimate the Administration Center Java heap size by issuing the following equation:

```
JavaHeapAllocated (MB) = 206 + ActiveAdmins * 30
```

`ActiveAdmins` is the maximum number of administrators who are logged in at one time. Additional administrators can be defined in the IBM Tivoli Integrated Portal, but if they are not logged in, no additional memory is required. The number of Tivoli Storage Manager server connections that are defined by an administrator in the Administration Center is not an important variable in determining the Java heap size requirements. More servers, however, imply that more actual work might be required. A larger maximum Java heap size provides more memory in the case of unexpected administration activity or workload growth. More real memory would be required as well.

Using a maximum Java heap size that is too small for the amount of work that is run in the Administration Center can affect performance. The Java Virtual Machine (JVM) completes garbage collection more frequently, there is higher processor utilization, and slower application response time. In certain conditions, the application is unable to complete the requested action because of memory allocation failure. It then becomes necessary to free up memory by closing work pages or logging out sessions.

Suggestions for reducing administrator session memory requirements include:

- Close work pages as soon as you are finished with them.
- Log out if you are not using any administrative functions for more than 30 minutes.
- Do not set the session timeout period to more than 30 minutes.

Configuring the maximum memory size (Java heap size):

Configure the Administration Center maximum memory size (Java heap size) by using the Administration Center Support Utility.

This utility is located in the IBM Tivoli Storage Manager installation directory under *install_root*\tsmac\bin. Run the supportUtil script from a command window and follow the instructions.

Start the tool by issuing: supportUtil.sh.

The following text is an example of the output:

```
User ID: iscadmin
Password: <enter password>

Administration Center Support Utility - Main Menu
=================================================
1.  Manage Administration Center tracing
2.  Manage the maximum memory size the Administration Center can use
3.  Manage the Administration Center session timeout setting
4.  Collect trace files, logs and system information to send to support
5.  Generate a heap dump of the Java virtual machine
6.  Generate a Java core dump of the Java virtual machine
7.  View the log file for this utility
9.  Exit
Enter Selection: 3

Administration Center Support Utility - Manage the Session
==========================================================
1.  Update the Administration Center session timeout setting
2.  View the Administration Center session timeout setting
99. Return to main menu
Enter Selection: 1

The session timeout setting determines how long a session can be idle before
it times out. After a timeout occurs the user must log in again. The default
timeout setting is 30 minutes. The minimum timeout setting is 10 minutes. To
cancel this operation enter an empty value.
Enter the new session timeout (minutes): 30
Updating the session timeout to 30 minutes.........
Session timeout successfully updated. Restart ISC for changes to take effect.
Press Enter to continue . . .<return>

Administration Center Support Utility - Manage the Session
==========================================================
1.  Update the Administration Center session timeout setting
2.  View the Administration Center session timeout setting
99. Return to main menu  Enter Selection: 99

Administration Center Support Utility - Main Menu
=================================================
1.  Manage Administration Center tracing
2.  Manage the maximum memory size the Administration Center can use
3.  Manage the Administration Center session timeout setting
4.  Collect trace files, logs and system information to send to support
5.  Generate a heap dump of the Java virtual machine
6.  Generate a Java core dump of the Java virtual machine
7.  View the log file for this utility
9.  Exit  Enter Selection: 2

Administration Center Support Utility - Manage the JVM
======================================================
1.  Update the maximum memory size the Administration Center can use
2.  View the maximum memory size the Administration Center can use
99. Return to main menu
Enter Selection: 1
```

```
The maximum memory size determines the largest amount of memory that can be
used by the Administration Center. A minimum heap size of 512 MB is
recommended. When used by 10 or more users, the recommendation is at least
1024 MB. To cancel this operation enter an empty value.
Enter the new JVM max memory size (MB): 1536
Updating the maximum memory size to 1536 MB......
Maximum memory size successfully updated.
Press Enter to continue . . .<return>
```

Remember: Do not configure the maximum memory size (Java heap size) to be greater than the available real system memory, or significant performance degradation might occur.

Choosing a location for the Administration Center

Where you install your Administration Center can affect its performance.

During administration activities, more network traffic occurs between the Administration Center system and the administrator's browser than between the Administration Center system and a Tivoli Storage Manager server. Therefore, install the Administration Center close, in network topology, to the administrators, rather than close to the Tivoli Storage Manager servers. For example, if you are in Chicago and administer Tivoli Storage Manager servers in Los Angeles, Paris, and Tokyo, install the Administration Center in Chicago.

You can use a single Administration Center installation to administer multiple Tivoli Storage Manager servers. For availability reasons, you might prefer to install multiple Administration Center instances.

Consider the following statements to further determine where you can install the Administration Center.

You can install the Administration Center on the same system as the Tivoli Storage Manager server if this condition is true:
- You do not plan to install and use the Tivoli Common Reporting component to view historical reports from Tivoli Monitoring for Tivoli Storage Manager

You must install the Administration Center on a different system from the Tivoli Storage Manager server if one or more of the following conditions are true:
- The Administration Center is to be used with multiple Tivoli Storage Manager servers and administrators
- Your Tivoli Storage Manager server is large and heavily active.
- The Administration Center is to be used on a heavily active system.
- You plan to install Tivoli Monitoring for Tivoli Storage Manager. It is a requirement that the Tivoli Monitoring for Tivoli Storage Manager and the Administration Center are installed on the same system so that you can generate Tivoli Common Reporting reports.

Worksheet for planning details for the Administration Center

Use this worksheet to record information that you need to install the Administration Center.

Item	Description	Default value	Your value
Installation location	Specify the base directory path for the installation. Subdirectories are automatically created for the Administration Center itself, the Tivoli Integrated Portal application, and other components. You can create a new directory or install into an existing Tivoli Integrated Portal instance.	`/opt/IBM/tivoli`	
Tivoli Integrated Portal Migration	When upgrading from version 6.2.x, and earlier, you have the option to migrate your existing Tivoli Integrated Portal settings. These settings include information like server connections and Administration Center preferences. If you are also installing the Tivoli Common Reporting component, your configuration settings will be migrated.	No	
Upgrade	If the installer detects an earlier version of 6.3 on your system, you have the option of installing into an existing Tivoli Integrated Portal or to create a new instance. **Note:** When upgrading from version 6.2.x, and earlier, the Administration Center is installed as a new instance. Previous instances can be removed.	Install into an existing Tivoli Integrated Portal	
Tivoli Common Reporting	Use this optional feature to view historical reports for your Tivoli Storage Manager environment. **Tip:** To upgrade an existing Tivoli Common Reporting installation to the current version, select the following wizard options: • Install Tivoli Common Reporting	Tivoli Common Reporting is not installed	
Cognos port number	If you install Tivoli Common Reporting, you must specify a port number for the IBM Cognos Content Database. The IBM Congos Content Database is a relational database that contains data that IBM Cognos 8 needs to operate, such as report specifications, connection information for data sources, and information about scheduling and emailing reports.	Port number: 1527	
Client Performance Monitor	Use the Client Performance Monitor to view and analyze performance data for client backup and restore operations. The *time interval* setting specifies how long state information is kept for ongoing client operations. The *operation save time* setting specifies how long operational data is kept for historical reporting. **Tip:** To use this feature, some additional parameters must be specified in the client options file. For more information, see the *Using the Application Programming Interface* publication.	Port number: 5129 Time interval: 24 hours Operation save time: 14 days	

Item	Description	Default value	Your value
Administrator account information	Create the user account that is used to manage access to the Administration Center. For example, you can log on with this user ID to create and manage additional administrative user accounts. **Tip:** If you are installing into an existing Tivoli Integrated Portal instance, you must specify an existing user account that has the iscadmins role assigned. For a new installation, you must also specify the port number that is used to access the Administration Center through a web browser.	Port number: 16310 Password: No default value User ID: tipadmin	

Installation directories

Administration Center components are installed into several directories. The components include Websphere, Tivoli Integrated Portal, Tivoli Common Reporting, and Administration Center.

The default installation directory for the Administration Center is: `/opt/IBM/tivoli`. It contains the following directories:

- WebSphere (`/opt/IBM/tivoli/tipv2`)
- Tivoli Integrated Portal (`/opt/IBM/tivoli/tipv2`)
- Tivoli Common Reporting (`/opt/IBM/tivoli/tipv2Components/TCRComponent`)
- Administration Center (`/opt/IBM/tivoli/tsmac`)

Installing the Administration Center components

To install the Administration Center components, you can use the graphical installation wizard, the console wizard, or the command line in silent mode.

Install the Tivoli Storage Manager Administration Center, using the installation software. The client performance monitor is installed as part of the Administration Center and more information about this is available within the Administration Center.

Restriction: If access rights for deployment engine files are set to single user mode, you cannot install the Administration Center on the same system by using a non-root user ID. If single user mode is specified, install the Administration Center by logging in as the root user or modify the access rights for deployment engine files. For details, see "Configuring access rights to deployment engine files" on page 62.

1. Log in with a user account that has the required directory access permissions. For more information, see "Preparing the Administration Center environment" on page 199.
2. If you are installing the Administration Center using the DVD, complete the following steps:

   Insert the Tivoli Storage Manager Administration Center DVD into a DVD drive. Ensure that the DVD is mounted on directory /dvdrom and change to that directory.
3. If you are installing the Administration Center from the Tivoli Storage Manager FTP downloads site, obtain the package file here: ftp://public.dhe.ibm.com/

storage/tivoli-storage-management/maintenance/admincenter/. Change to the directory where you placed the executable file and complete the following steps:

Important: The files are extracted to the current directory. Ensure that the executable file is in an empty directory. Do not extract the files into a directory where another Administration Center installation package or any other files are located.

    a. Change file permissions by entering the following command:

       `chmod a+x 6.3.3.0-TIV-TSMAC-`*platform*`.bin`

       where *platform* denotes the architecture that the Administration Center is to be installed on.

    b. Run the following command to extract the installation files:

       `./6.3.3.0-TIV-TSMAC-`*platform*`.bin`

4. Optional: After all the files are extracted, locate this file and run it to ensure that your system meets all requirements:

    prereqcheck.bin

See "Running the installation prerequisite checker" on page 12 for details.

5. If you changed the default, ensure that the following command is enabled so that the Tivoli Storage Manager wizards work properly.

    finger

6. Ensure that there are no processes using *install_dir*/tipv2/java. To check, issue this command:

    `ps -ef | grep `*install_dir*`/tipv2/java`

7. Select one of the following ways to install the Administration Center:

Installation wizard
    "Installing the Administration Center using the installation wizard" on page 201

Command-line console wizard
    "Installing the Administration Center using the console installation wizard" on page 202

Silent mode
    "Installing the Administration Center in silent mode" on page 203

8. After installing the Administration Center, configure and customize it for your use.

Preparing the Administration Center environment

Prepare the environment to install the Administration Center with a non-root user account, which is the standard way to complete the installation.

Use a non-root user account for the installation if the components that are being installed might later be integrated with other Tivoli applications within the same Tivoli Integrated Portal instance. You can use a root account for the installation, but doing so can limit future integration options. Also, if you use a root account, you will be unable to start the Administration Center or Tivoli Common Reporting, using a non-root user account.

Restriction: If you use a non-root user account for the installation, you must use the same user account to install future fix packs or upgrades. If you use a non-root user account for the installation, it is possible to use a root user to start the Administration Center and Tivoli Common Reporting. A non-root user, however, cannot be used again without changing authorities of the file system to non-root.

Complete the following steps to prepare for a non-root installation:
1. Log in using the root user ID and password.
2. If necessary, create a new non-root user account. For example, issue the appropriate **useradd** command for your operating system.
3. If the following directory structure does not already exist, create the directories:

    `/usr/ibm`

    `/var/ibm`

    `/var/tivoli`

    `/opt/IBM/tivoli` (This is the default Administration Center installation directory. You can specify a different directory during the installation process.)

Running the installation prerequisite checker

The installation prerequisite checker is an optional tool that verifies the operating system, the amount of free disk space for the installation, and other prerequisites.

To ensure that your system environment is appropriate for the installation, you can run the prerequisite checker before each installation.

Tip: The prerequisite checker verifies only the minimum memory that is necessary. More memory is required for additional tasks.

The prerequisite checker presents a summary of results at the end of the check. Any changes that are required in your environment before the installation are listed. Any new directories that are required for the installation are created.

To run the prerequisite checker, complete the following steps.
1. Ensure that the appropriate installation package is downloaded and that its files are extracted. A prerequisite checker is part of the installation package.
2. Choose the graphical interface (the default) or console method to start the installation, and follow the wizard instructions to complete the installation:
   - Issue this command to start the installation wizard using a graphical interface:

       `./prereqcheck.bin`
   - Issue this command to start the installation wizard using the console method:

       `./prereqcheck.bin -i console`
3. Select the language for the prerequisite checker user interface.
4. In the welcome and disclaimer panels, review the statements and accept them.

If the Prerequisite Results page indicates that your system passed the checks, you are ready to start the installation.

If an error message is shown in the Prerequisite Results page, make the required corrections before continuing with the installation. The summary page lists the errors and directs you to an error log file.

Installing the Administration Center using the installation wizard

Using the installation wizard is one method of installing the Administration Center.

To install the Administration Center using the installation wizard, complete the following steps:

1. Grant the required directory access permissions.

   For example, issue the following commands to enable the *ac_installer* user account to install the Administration Center using the default installation directory:

   ```
   chown -R ac_installer /usr/ibm
   chown -R ac_installer /var/ibm
   chown -R ac_installer /var/tivoli
   chown -R ac_installer /opt/IBM/tivoli
   ```

   Tip: The non-root user account must also have read and write access to the /tmp directory.

2. Verify that the operating system is set to the language that you require. By default, the language of the operating system will be the language of the Administration Center and its installation wizard.

   If you plan to select a different language for the wizard, you might have to change the language of the operating system. By setting the operating system to an ASCII language, such as English or Spanish, you can select an ASCII language for the wizard later in the installation process. By setting the operating system to a non-ASCII language, such as Simplified Chinese, you can select a non-ASCII language later in the installation process.

   For information about setting the language of the operating system, see the operating system documentation.

3. If you are installing locally onto a remote system that uses an X display, and your local system does not have an X Window System server running, the installation might fail. If it fails, ensure that the DISPLAY environment variable is *not* set and restart the installation.

4. If you are using Security Enhanced Linux on your system, set SELINUX=disable or set SELINUX=permissive in the /etc/sysconfig/selinux file, at least until the installation process completes. If you do not adjust the setting, you receive this message when you try to install the server:

   ```
   The installation wizard cannot run on your configuration.
   It will now stop. For more details about installation error logs,
   enter the phrase "installation log files" in the Search field
   at this site: http://publib.boulder.ibm.com/infocenter/tsminfo/v6r3.
   ```

5. To start the wizard, enter the following command:

   ```
   ./install.bin
   ```

   The Administration Center installation wizard starts.

6. Select the language for your installation and follow the prompts. Tivoli Integrated Portal, the Administration Center, and the Client Performance Monitor are installed by default.

   The default Tivoli Integrated Portal user name is tipadmin. You must specify a password for this ID, or for a new ID you create. You use the ID and password later to log on to the Tivoli Integrated Portal and the Administration Center.

> **Important:** Save the user name and password or you are unable to uninstall
> the Administration Center. Refer to the Worksheet for planning details for the
> Administration Center to record the username and password.

At the end of the installation, a summary is provided. Make a note of the port
number that is listed in the summary panel. It might be different from the one that
you entered in the wizard, depending on port availability and your system
requirements. You need this port to log on to the Administration Center.

Tip: A file named `Tivoli_Storage_Manager_Administration_Center.htm` is created
in the `tsmac` directory of the Administration Center installation directory. Open this
file in a web browser to automatically connect to the Administration Center.

If there are any errors during the installation, another summary page lists the
errors and directs you to an error log file. The installation log is in the following
location:

```
/var/tivoli/tsm.
```

To change the language of the Administration Center, change the language of the
web browser. For a list of available languages for the Administration Center, see
"Server language locales" on page 43.

Installing the Administration Center using the console installation wizard

Using the console installation wizard is one method of installing the
Administration Center.

To install the Administration Center using the console installation wizard, complete
these steps:

1. Grant the required directory access permissions.

   For example, issue the following commands to enable the *ac_installer* user
   account to install the Administration Center using the default installation
   directory:

   ```
   chown -R ac_installer /usr/ibm
   chown -R ac_installer /var/ibm
   chown -R ac_installer /var/tivoli
   chown -R ac_installer /opt/IBM/tivoli
   ```

   Tip: The non-root user account must also have read and write access to the
   `/tmp` directory.

2. Verify that the operating system is set to the language that you require. By
   default, the language of the operating system will be the language of the
   Administration Center and its installation wizard.

   If you plan to select a different language for the wizard, you might have to
   change the language of the operating system. By setting the operating system
   to an ASCII language, such as English or Spanish, you can select an ASCII
   language for the wizard later in the installation process. By setting the
   operating system to a non-ASCII language, such as Simplified Chinese, you can
   select a non-ASCII language later in the installation process.

   For information about setting the language of the operating system, see the
   operating system documentation.

3. If you are installing locally onto a remote system that uses an X display, and your local system does not have an X Window System server running, the installation might fail. If it fails, ensure that the DISPLAY environment variable is *not* set and restart the installation.

4. If you are using Security Enhanced Linux on your system, set `SELINUX=disable` or set `SELINUX=permissive` in the `/etc/sysconfig/selinux` file, at least until the installation process completes. If you do not adjust the setting, you receive this message when you try to install the server:

```
The installation wizard cannot run on your configuration.
It will now stop. For more details about installation error logs,
enter the phrase "installation log files" in the Search field
at this site: http://publib.boulder.ibm.com/infocenter/tsminfo/v6r3.
```

5. To start the wizard, enter this command:

   `./install.bin -i console`

6. Select the language for your installation and follow the prompts. Tivoli Integrated Portal, the Administration Center, and the Client Performance Monitor are installed by default.

   The default Tivoli Integrated Portal user name is `tipadmin`. You must specify a password for this ID, or for a new ID you create. You use the ID and password later to log on to the Tivoli Integrated Portal and the Administration Center.

   Important: Save the user name and password or you are unable to uninstall the Administration Center. Refer to the Worksheet for planning details for the Administration Center to record the username and password.

At the end of the installation, a summary is provided. Make a note of the port number that is listed in the summary panel. It might be different from the one that you entered in the wizard, depending on port availability and your system requirements. You need this port to log on to the Administration Center.

Tip: A file named `Tivoli_Storage_Manager_Administration_Center.htm` is created in the `tsmac` directory of the Administration Center installation directory. Open this file in a web browser to automatically connect to the Administration Center.

If there are any errors during the installation, another summary page lists the errors and directs you to an error log file. The installation log is in the following location:

   `/var/tivoli/tsm.`

To change the language of the Administration Center, change the language of the web browser. For a list of available languages for the Administration Center, see "Server language locales" on page 43.

Installing the Administration Center in silent mode

Use the silent installation option to automatically install the Administration Center and the optional Tivoli Common Reporting feature without any user interaction.

To run a silent installation, complete the following steps:

1. Create a response file. A sample response file named `sample_response.txt` is located in the Tivoli Storage Manager installation media root directory. Use this sample file as a template to create your response file.

2. To start a silent installation, enter the following command on a single line:

   `./install.bin -i silent -f `*`full_path_name_to_response_file`*

If there are any errors during the installation, another summary page lists the
errors and directs you to an error log file. The installation log is in the following
location:

> /var/tivoli/tsm.

Taking the first steps after you install the Administration Center

After installing the Administration Center, prepare for the post-installation tasks.
These tasks include verifying the installation and starting the Administration
Center.

Configure the Administration Center by completing the following tasks:

Configuring LDAP user authentication

To use a Lightweight Directory Access Protocol (LDAP) server to authenticate
access to the Administration Center, you must complete some additional
configuration tasks after you install the Administration Center.

Tips:
* If you use a non-root user account to install the Administration Center, you
  must manually start the Tivoli Integrated Portal server after you complete the
  installation. For more information, see "Starting and stopping the Tivoli
  Integrated Portal server" on page 207.
* Before you change the user authentication method, you must import the Secure
  Sockets Layer (SSL) certificate. For more information, see Configuring an SSL
  connection to an LDAP server.

To change the user authentication method from the local operating system to
LDAP federated repositories, complete the following steps:

1. Open a web browser and log on to the Administration Center with a user
   account that has administrator privileges. To ensure that you are viewing all
   of the available tasks, click the **View** list in the upper left corner of the page
   and select **All tasks**.
2. Click **Settings** > **WebSphere Administrative Console** > **Launch WebSphere
   administrative console**.
3. In the WebSphere administrative console window, click **Security** > **Global
   security**.
4. From the **Available realm definitions** list, select **Federated Repositories** and
   click **Configure**.
5. Under **Related Items**, click **Manage repositories**.
6. Add the LDAP repository that you want to use for authentication by clicking
   Add and entering the following parameters:

   Repository identifier
   > A unique identifier for the repository within the cell, for example:
   > LDAP1.

   Directory type
   > The type of server that you want to connect to.

   Primary host name
   > The host name of the primary LDAP server. This host name is either
   > an IP address or a domain name service (DNS) name.

   Port   The LDAP server port. The default value is 389, which is not a Secure

Sockets Layer (SSL) connection. Port 636 can be an SSL connection. For some LDAP servers, you can specify a different port for non-SSL and SSL connections. If you do not know the port to use, contact your LDAP server administrator.

Bind distinguish name
> The distinguished name (DN) for the application server to use when binding to the LDAP repository. If no name is specified, the application server binds anonymously. In most cases, bind DN and bind password are needed. However, when anonymous bind can satisfy all of the required functions, bind DN and bind password are unnecessary.

Bind password
> The password that the application server uses when binding to the LDAP repository.

7. Click **OK**.

8. In the message box, click **Save directly to the master configuration**.

9. In the repository identifier column, click the identifier for the repository that you want to use.

10. On the configuration panel, under **Additional Properties**, click the LDAP entity types.

11. In the **Entity Type** column, click the link for Group, OrgContainer, and PersonAccount. Complete the search bases field. The search bases field specifies the search bases that are used to search this entity type. The search bases specified must be subtrees of the base entry in the repository. The following example search bases have o=ibm,c=us as the base entry in the repository:

    ```
    o=ibm,c=us or cn=users,o=ibm,c=us or ou=austin,o=ibm,c=us
    ```

    You can use a semicolon to delimit the search bases. For example:

    ```
    ou=austin,o=ibm,c=us;ou=raleigh,o=ibm,c=us
    ```

12. Click **OK** and then click **Save to the master configuration**. You must save to the master configuration every time that you update the search bases field.

13. Return to the federated repositories page and click **Supported Entity Types** under **Additional Properties**.

14. In the **Entity type** column, click the link for Group, OrgContainer, and PersonAccount and complete the base entry for the default parent and **Relative Distinguished Name** properties fields.

    a. In the Base entry for the default parent field, enter the same value that you entered in the Search bases field in step 11.

    b. In the **Relative Distinguished Name** properties field, enter the appropriate LDAP attribute name. In most cases, the values for this field are cn for Group, o;ou;dc;cn for OrgContainer, and uid for PersonAccount.

15. Click **OK** and then click **Save to the master configuration**. You must save to the master configuration every time that you update the base entry for the default parent field.

16. Return to the federated repositories page and click **Apply**, then click **Save to the master configuration**.

17. Under **Repositories in the realm**, click **Add base entry to Realm**.

18. On the repository reference page, select the repository that you created in step 6 on page 204 from the repository list.

19. Enter the distinguished name of a base entry that uniquely identifies the repository in the realm. You must enter the information in the **Distinguished name of a base entry uniquely identifying this set of entries in the realm** field. In most instances, this value is the same value that you entered in the **Search bases** field in step 11 on page 205.

20. In the **Distinguished name of a base entry in this repository** field, enter the distinguished name of the base entry within the repository. In most instances, this value is the same value that you entered in the **Distinguished name of a base entry that uniquely identifies this set of entries in the realm** field.

21. Click **OK** and then click **Save to the master configuration**. You must save to the master configuration every time that you update the distinguished name of a base entry. The base entry identifies the set of entries in the realm field. Two repositories are displayed under repositories in the realm on the federated repositories page: the repository you added, and a default repository.

22. Change the realm name or leave the value in the **Realm name** field as it is.

23. In the primary administrative user name field, enter the name of a user that you added in the repository. The named user is granted administrative privileges for the Tivoli Integrated Portal server.

24. Click the server identity that is stored in the repository.

25. In the server user ID or the administrative user node field, enter the ID that you entered in the primary administrative user name field. Enter the password for the user ID.

26. Select the default file repository that shows **File** in the **Repository type** column and remove it.

27. Click **OK** and then click **Save to the master configuration**.

28. Return to the secure administration, applications, and infrastructure page.

29. In the available realm definition list, select **Federated repositories** and click **Set as current**.

30. Click **Apply** and then click **Save to the master configuration**.

31. Stop and restart the Tivoli Integrated Portal server.

Configuring an SSL connection to an LDAP server

Your implementation of Tivoli Integrated Portal might use an external LDAP-based user repository. You can configure the Tivoli Integrated Portal to communicate over a secure sockets layer (SSL) channel.

This task assumes that you have an existing connection to an LDAP server setup.

Your LDAP server (for example, an IBM Tivoli Directory Server), must be configured to accept SSL connections and run on a secured port number (636). Refer to your LDAP server documentation if you must create a trusted certificate. The trusted certificate must be imported from your LDAP server into the Tivoli Integrated Portal Server key database file (cert.kdb).

Complete these steps to configure the Tivoli Integrated Portal Server to communicate over a secure SSL channel with an external LDAP server. All application server instances must be configured for the LDAP server.

1. Log in to the portal.

2. Follow these steps to import your LDAP server's trusted certificate into the application server key database file.

    a. Click **Settings** > **Websphere Administrative Console**. Click **Launch Websphere administrative console**.

    b. Click **Security** > **SSL certificate and key management**.

    c. In the Related Items area, click **Key stores and certificates**.

    d. In the table, click **NodeDefaultTrustStore**.

    e. In the Additional Properties area, click **Signer certificates** link.

    f. Click **Retrieve from port**.

    g. In the relevant fields, provide the host name, the port, the SSL configuration details, and the alias of the certificate for your LDAP server and click **Retrieve signer information**. Then, click **OK**.

3. Complete the following steps to enable SSL communications to your LDAP server:

    a. Click **Security** > **Secure administration, applications, and infrastructure**.

    b. Select **Federated repositories** from the **Available realm definitions** menu list and click **Configure**.

    c. Select your LDAP server from the **Repository** menu list.

    d. Enable the **Require SSL communications** check box and the select the **Centrally managed** option.

    e. Click **OK**.

4. For the changes to take effect, save, stop, and restart all Tivoli Integrated Portal Server instances.

Starting and stopping the Tivoli Integrated Portal server

Depending on your operating system, you might need to manually start the Tivoli Integrated Portal.

If you use a root user account to install the Administration Center, the IBM Tivoli Integrated Portal server starts automatically. If you use a non-root user account for the installation or if you later shut down the system, you must manually start the Tivoli Integrated Portal server.

To manually start or stop the Tivoli Integrated Portal server, use a Tivoli Storage Manager administrative user ID that is defined to the Tivoli Integrated Portal. The administrative user ID must have the iscadmins role assigned. For details, see "Defining Administration Center users to the Tivoli Integrated Portal" on page 209.

Use the command line to start and stop Tivoli Integrated Portal servers.

When you start and stop the Tivoli Integrated Portal using the command line, the variables in the commands have these meanings:

- *TIP_HOME* is the Tivoli Integrated Portal installation directory.

    The default for *TIP_HOME* is /opt/IBM/tivoli/tipv2.

- *TCR_HOME* is the Tivoli Common Reporting installation directory.

    The default for TCR_HOME is /opt/IBM/tivoli/tipv2Components/ TCRComponent.

- *tip_admin* is the administrator user ID for the Administration Center.

- *tip_pw* is the password for the administrator.

- *tip_profile* is the DB2 profile name for the administrator. The default is TIPProfile, as provided by Tivoli Integrated Portal.

Start or stop the Tivoli Integrated Portal server by using one of the following methods.

If Tivoli Common Reporting is installed:

Change to the *TCR_HOME*/bin directory and issue one of the following commands:

- To start Tivoli Common Reporting and the Tivoli Integrated Portal server, issue this command:

  ./startTCRserver.sh

- To stop Tivoli Common Reporting and the Tivoli Integrated Portal server, issue this command:

  ./stopTCRserver.sh *tip_admin tip_pw*

If Tivoli Common Reporting is not installed:

Change to the *TIP_HOME*/bin directory and issue one of the following commands:

- To start a Tivoli Integrated Portal server, issue this command:

  ./startServer.sh server1

- To stop a Tivoli Integrated Portal server, issue the following command on a single line:

  ./stopServer.sh server1 -username *tip_admin* -password *tip_pw*
  -profileName *tip_profile*

Verifying the Administration Center installation

After you install the Administration Center, verify the installation by opening the Administration Center and logging in.

Complete the following steps:

1. If you used a non-root user account to install the Administration Center, start the Tivoli Integrated Portal server. For more information, see "Starting and stopping the Tivoli Integrated Portal server" on page 207.

2. Open the Administration Center by entering one of the following addresses in a supported web browser:

   http://*workstation_name*:*non_secure_port*/ibm/console

   Or:

   https://*workstation_name*:*secure_port*/ibm/console

   The *workstation_name* is the network name or IP address of the computer on which you installed the Administration Center. The *non_secure_port* is the HTTP port and the *secure_port* is the HTTPS port.

   Attention: Use the port number that was shown in the summary panel of the installation wizard, which might be different from the port that you specified in the wizard. If you use an incorrect port, no warning messages are shown but you are not able to complete all Administration Center tasks.

The default HTTP port is 16310. The default HTTPS port is 16311. If you use a different port number from the default, the secure port typically appears as the non-secure port plus 1.

Look in the following file to see the port that is being used. In this file, **WC_defaulthost** contains the value for the HTTP port and **WC_adminhost_secure** contains the value for the HTTPS port.

   TIP_HOME/properties/TIPPortDef.properties

where *TIP_HOME* is the home directory for the Tivoli Integrated Portal installation.

   The default for *TIP_HOME* is /opt/IBM/tivoli/tipv2.

Tips:
- If you use http://*workstation_name*:16310/ibm/console to connect to the Administration Center, you are automatically redirected to the secure port and address.
- A file named Tivoli_Storage_Manager_Administration_Center.htm is created in the tsmac directory of the Administration Center installation directory. Open this file in a web browser to automatically connect to the Administration Center.

3. To get started, log in using the Tivoli Integrated Portal user ID and password that you created during the Administration Center installation. Save this password in a safe location because it is also needed to uninstall the Administration Center.

4. After you successfully log in, the Tivoli Integrated Portal welcome page is shown. Expand the Tivoli Storage Manager folder in the **Work Items** list and click **Getting Started** to display the Tivoli Storage Manager welcome page. This page provides instructions for using the Administration Center.

Defining Administration Center users to the Tivoli Integrated Portal

When you install the Administration Center, you must define the users to the Tivoli Integrated Portal.

You can create a separate Tivoli Integrated Portal user ID for each Tivoli Storage Manager administrator, or for a group of administrators. Give each Tivoli Storage Manager administrator their own Tivoli Integrated Portal administrator ID. Creating separate Tivoli Integrated Portal administrator IDs can help you control access for administrators who manage different servers, or have different privilege classes. After logging in using this ID, they can use their Tivoli Storage Manager administrator name and password to manage connections for the servers they manage.

Complete the following steps to define Administration Center users to the Tivoli Integrated Portal:

1. In the navigation tree, expand **Users and Groups**.
2. Click **Manage Users**.
3. Click **Create**.
4. Click **Group Membership**.
5. Select **Group name**, then click **Search**.
6. Add TSM_AdminCenter to the Current groups list.

> **Tip:** To add the appropriate roles for users to access the Tivoli Common Reporting reports, see ../com.ibm.itsm.tshoot.doc/ ts_pdg_no_existing_group.dita.

7. Click **Close**. The TSM_AdminCenter group is a shell for you to populate with users. You must manually enter the user credentials.

8. To ensure that an administrative user ID can start or stop the Tivoli Integrated Portal server, assign the iscadmins role to the administrative user ID.

9. Complete the form and click **Create**.

Resetting the Tivoli Integrated Portal installation wizard password

When the Tivoli Integrated Portal installation wizard password is unknown, you can reset it.

When you upgrade or uninstall the Administration Center, you need to use the *tipadmin* password. If the password is unknown, you must reset it.

Complete the following steps to reset the *tipadmin* password:

1. Log in to the operating system where the Administration Center is installed.

2. Open a command window and go to the *tip_home*\profiles\TIPProfile\bin directory.

   The default *tip_home* is /opt/ibm/tivoli/tipv2.

3. To access the wsadmin prompt, issue the following command:

   ```
   ./wsadmin -conntype none -profileName TIPProfile
   ```

4. From the wsadmin command prompt, issue the following three commands to reset the password.

   ```
   wsadmin>$AdminTask changeFileRegistryAccountPassword {-userId username
   -password newpassword}
   wsadmin>$AdminConfig save
   wsadmin>exit
   ```

   The *username* is **tipadmin** and the *newpassword* is the new password you want to use for the tipadmin user ID.

5. For the new password to be recognized, you must restart the Tivoli Integrated Portal server. Go to the *tip_home*\profiles\TIPProfile\bin directory and issue the **stopServer** and **startServer** commands:

   ```
   ./stopServer.sh server1
   ./startServer.sh server1
   ```

Chapter 20. Uninstalling the Administration Center

Uninstall the Administration Center either by using one of two wizards or in silent mode.

Tip: To uninstall a version 6.2 Administration Center, see the instructions at the following website: http://publib.boulder.ibm.com/infocenter/tsminfo/v6r2. To uninstall a version 6.1 Administration Center, see the instructions at the following website: http://publib.boulder.ibm.com/infocenter/tsminfo/v6.

To uninstall the current version of the Administration Center, complete the following steps:

1. If you have the WebSphere server automatic restart set up, remove it before uninstalling the Administration Center.
   * Log in to the operating system with the root user ID.
   * Change to the installation directory. For example, the default directory is `/opt/IBM/tivoli/tsmac/bin`.
   * Run the following script:
     ```
     ./setTSMUnixLinks.sh uninstall
     ```
2. Change to the `/opt/IBM/tivoli/tsmac/_uninst` directory.
3. Use one of the following methods to uninstall the Administration Center:

   Tip: Regardless of the method that you choose, you must provide a valid Administration Center user ID and password to uninstall the Administration Center.
   * To use the installation wizard (GUI) to uninstall the Administration Center, issue this command:
     ```
     ./uninstall
     ```
   * To use the console to uninstall the Administration Center, issue this command:
     ```
     ./uninstall -i console
     ```
   * To silently uninstall the Administration Center, issue the following command. Sample response files (`uninstall_response.txt`) are available with the Administration Center installation driver. Use one of the sample files to run a silent installation. Ensure that you enter the full path name to the sample response file.
     ```
     ./uninstall -i silent -f path_name_to_response_file
     ```
4. Follow the prompts to uninstall the Administration Center. You see a message that the Administration Center uninstallation was successful.

See Chapter 19, "Installing and configuring the Administration Center," on page 189 for the installation steps to reinstall the Administration Center.

Chapter 21. Upgrading the Administration Center to Version 6.3 or later

To administer IBM Tivoli Storage Manager Version 6.3 or later servers, you must upgrade to the Administration Center Version 6.3 or later. The upgrade process consists of installing the new version and completing some manual configuration tasks.

If you are installing the Administration Center for the first time, see Chapter 19, "Installing and configuring the Administration Center," on page 189.

The IBM Tivoli Integrated Portal is a graphical user interface (GUI) framework. The Administration Center is installed into the Tivoli Integrated Portal as a plug-in.

Restriction: The Administration Center Version 6.3 or later is compatible only with the Tivoli Integrated Portal Version 2.1. If you have earlier versions of these applications installed, you must upgrade them both.

You can automatically migrate your Tivoli Integrated Portal settings, like your server connections and user preferences, from a Version 6.2 Administration Center during the installation process. However, some manual configuration is still required after you complete the installation.

Tip: If there is enough disk space, consider temporarily maintaining both the previous and current versions of the Administration Center. This coexistence strategy provides a functioning Administration Center during the upgrade and ensures that the configuration settings of the previous version remain available.

To support coexistence, assign non-conflicting ports for each Administration Center instance. You can use the same port definitions and run only one instance at a time, or you can assign separate ports and run the two instances concurrently.

You can also install the Administration Center into an existing Tivoli Integrated Portal Version 2.1 instance. This option also applies to fix packs.

Previous versions of the Administration Center are not automatically removed during an upgrade installation. You can manually uninstall a previous version after you complete and verify the upgrade installation.

Related tasks:

Chapter 19, "Installing and configuring the Administration Center," on page 189

Chapter 10, "Upgrading Tivoli Monitoring for Tivoli Storage Manager to Version 6.3, or later," on page 149

Upgrading the Administration Center

To upgrade from a previous version of the Administration Center, you must install the new version and then recreate the previous Tivoli Integrated Portal or Integrated Solutions Console user accounts. In some cases, you must also recreate the previous Tivoli Storage Manager server connections.

When you upgrade the Administration Center to Version 6.3 or later, use the same user ID that was used to install the Version 6.2 Administration Center. If you use a different user ID to upgrade the Administration Center to Version 6.3 or later, you must change the ownership of the Version 6.2 Administration Center folders accordingly.

If you do not know your Tivoli Integrated Portal password, reset it by following these instructions: "Resetting the Tivoli Integrated Portal installation wizard password" on page 210.

To upgrade the Administration Center, complete the following steps:
1. If you do not plan to automatically migrate a Version 6.2 Administration Center during the installation process, obtain information about the previously defined Tivoli Storage Manager server connections:
   - For a version 5.5 or earlier Administration Center, save the `tsmservers.xml` file that is in the Administration Center installation directory.
   - For a Version 6.1 or later Administration Center, download the server connections file. From the navigation tree in the Administration Center interface, expand **Tivoli Storage Manager** and click **Manage Servers** > **Download Connection File**.

     Tip: For more details about the server connections file, see the online help for the Manage Servers page.
2. Collect the administrative user account information from the previous Administration Center. For more information, see "Obtaining user account information in a Version 5.5 Administration Center" on page 216 or "Obtaining user account information in a Version 6.1 or later Administration Center" on page 215.
3. Install the Administration Center Version 6.3 or later.

   Important:
   - If you have Tivoli Monitoring for Tivoli Storage Manager installed, the upgrade overwrites any existing reports and data source connections. Before you upgrade, see ../com.ibm.itsm.srv.doc/t_rpt_bkup_itm4tsm.dita for instructions to export and import your customized BIRT and Cognos reports.
   - Extract the installation files into an empty directory. Do not extract to a directory that contains previously extracted files, or any other files.
4. Recreate the previous configuration in the new Administration Center:
   a. Define each Integrated Solutions Console or Tivoli Integrated Portal user account. For more information, see "Defining Administration Center users to the Tivoli Integrated Portal" on page 216.
   b. Edit the `tsmservers.xml` server connections file to specify the TIPRealm domain for each iscuser definition:

      `<iscuser id="TIPRealm/userID" />`

   c. Upload the server connections file. From the navigation tree in the Administration Center interface, expand **Tivoli Storage Manager** and click **Manage Servers** > **Upload Connection File**.

   When administrators log on to the Tivoli Integrated Portal, they are prompted to provide a Tivoli Storage Manager administrative user ID and password for the servers that they manage.

   Tip: If administrators manage many Tivoli Storage Manager servers, they can edit the `tsmservers.xml` file and add the Tivoli Storage Manager administrative credentials.

   Adding administrative credentials to the `tsmservers.xml` file prevents an administrator from having to provide the credentials after logging on to the Tivoli Integrated Portal, but including the passwords in the file can create a security exposure.

5. If you used one user ID to install the Administration Center Version 6.2 and a different user ID to upgrade to Version 6.3 or later, change the ownership of the Administration Center Version 6.2 folders to the ID that is performing the installation. For example:

```
chmod -R <user_id> <AC_6.2_install_location>
```

6. Optional: Uninstall the previous version of the Administration Center.

   To uninstall a Version 6.2 Administration Center, see the instructions at the following website: http://publib.boulder.ibm.com/infocenter/tsminfo/v6r2.

   To uninstall a Version 6.1 Administration Center, see the instructions at the following website: http://publib.boulder.ibm.com/infocenter/tsminfo/v6.

Obtaining user account information in a Version 6.1 or later Administration Center

To access the Version 6.3 or later Administration Center, a Tivoli Integrated Portal user account is required. Tivoli Integrated Portal or Integrated Solutions Console user accounts that are defined in a previous version of the Administration Center must be manually recreated after upgrading to the latest version.

Complete the following steps to obtain information about the defined user IDs:

1. In the navigation tree, expand **Users and Groups** and click **Manage Users**.
2. In the **Search by** list, select **User ID**.
3. In the **Search for** list, enter an asterisk (*).
4. Click **Search**. The table shows all the defined user IDs. Capture this information for later use.
5. Determine the password for each of these user IDs.

Obtaining user account information in a Version 5.5 Administration Center

To access the Version 6.3 or later Administration Center, a Tivoli Integrated Portal user account is required. Integrated Solutions Console user accounts that are defined in a previous version of the Administration Center must be manually recreated after upgrading to the latest version.

Complete the following steps to obtain information about the defined user IDs:

1. In the navigation tree, expand **Console Settings** and click **User and Group Management**.
2. In the **Search** list, select **Users**.
3. In the **Search by** list, select **uid**.
4. In the **Search** field, enter an asterisk (*).
5. Click **Search**. The table shows all the defined user IDs. Capture this information for later use.
6. Determine the password for each of these user IDs.

Defining Administration Center users to the Tivoli Integrated Portal

When you upgrade the Administration Center to Version 6.3 or later, you must define the previous user accounts to the IBM Tivoli Integrated Portal.

Consider creating a separate Tivoli Integrated Portal user account for each Tivoli Storage Manager administrator. The administrators can then log on and use their Tivoli Storage Manager administrative credentials to create connections for the servers that they manage.

Complete the following steps to define the administrative user accounts:

1. In the navigation tree, expand **Users and Groups**.
2. Click **Manage Users**.
3. Click **Create**.
4. Click **Group Membership**.
5. Select **Group name**, then click **Search**.
6. Add TSM_AdminCenter to the Current groups list.

   Tip: To add the appropriate roles for users to access the Tivoli Common Reporting reports, see ../com.ibm.itsm.tshoot.doc/ ts_pdg_no_existing_group.dita.
7. Click **Close**. The TSM_AdminCenter group is a shell for you to populate with users. You must manually enter the user credentials.
8. To ensure that an administrative user ID can start or stop the Tivoli Integrated Portal server, assign the `iscadmins` role to the administrative user ID.
9. Complete the form and click **Create**.

Server connections to the Administration Center

To use the Administration Center, administrators must create connections to one or more Tivoli Storage Manager servers. You can download a file that contains information about existing server connections from the Administration Center. You can then upload the file to quickly redefine server connections after an upgrade installation.

The Administration Center stores Tivoli Storage Manager server connection information in a file named `tsmservers.xml`. This file is located in the Administration Center installation directory.

When you install the Version 6.3 Administration Center you can choose to automatically migrate the configuration of an existing Version 6.2 Administration Center:

* If you select this option, the `tsmservers.xml` file is copied from the previous installation.
* If you do not select this option, or if you are upgrading an earlier version of the Administration Center, you can manually upload the connections file after you complete the installation.

By default, the `tsmservers.xml` file does not include Tivoli Storage Manager administrative user IDs and passwords for each server connection. Server connections that do not include these administrative credentials are treated as incomplete connections, which cannot be used until the credentials are provided.

After you upload the `tsmservers.xml` file, you can handle the incomplete server connections in two ways:

* Leave the connections in the incomplete state. When administrators log on to the Tivoli Integrated Portal, they are prompted to provide the administrative credentials for the servers that they manage.
* Use the **Change Password** action in the Manage Servers table to specify the administrative credentials for one or more server connections.

Tip: You can also edit the `tsmservers.xml` file directly and add the administrative credentials, if this is permitted by the security policies of your company. For more information, see the Administration Center online help for the Manage Servers page.

Part 5. Appendixes

Appendix A. Installation log files

If you experience errors during installation, these errors are recorded in several log files that are distributed in various locations.

- If you are using Security Enhanced Linux on your system, set `SELINUX=disable` or set `SELINUX=permissive` in the `/etc/sysconfig/selinux` file, at least until the installation process completes. If you do not adjust the setting, you receive this message when you try to install the server:

```
The installation wizard cannot run on your configuration.
It will now stop. For more details about installation error logs,
enter the phrase "installation log files" in the Search field
at this site: http://publib.boulder.ibm.com/infocenter/tsminfo/v6r3.
```

Table 40 shows the files that are created when you install or uninstall Tivoli Storage Manager and recommends which files to check when looking for information that might help you troubleshoot problems:

Table 40. Contents of the `log.zip` file

File Name	Description	Location

The `log.txt` file contains information about the following Environment Checks:
- Platform
- Version
- Architecture
- Prerequisites
	Contains general information about an installation. Review this log file when any installation failures occur.	This file is located in:
		  `/var/tivoli/tsm`
		
		The InstallAnywhere exit codes show you the state of the installation. The codes are in the `log.txt` file and can also be called by command. You can retrieve the exit codes after the installation is completed. The exit codes are for both the Tivoli Storage Manager installation and upgrade wizards and the Tivoli Monitoring for Tivoli Storage Manager installation wizard.
		
		To use the command line, issue the following command:
		`echo $?`
		
		See Table 41 on page 223 for all the InstallAnywhere exit codes.

`logs.zip`	The Tivoli Storage Manager server `logs.zip` file contains the following subdirectories: - coi: contains installation log files - de: contains deployment engine log files - ia: contains the `log.txt` file and native installer log files, for example, `tsm_server.log`, `tsm_license.log`, and `db2_inst.log`	This file is located in: `/var/tivoli/tsm`

Table 40. Contents of the `log.zip` *file (continued)*

File Name	Description	Location
`DE_Install.log`	Contains information about the deployment engine installation. Review this log file if the deployment engine installation fails.	`de/root`
`db2setup.log`	Contains information about the DB2 installation. Review this log file if the DB2 installation fails.	`coi/plan/tmp`
`db2_uninst.log`	Contains information about the DB2 uninstallation	`coi/plan/logs`
`DB2.log`	Contains information about the installation and uninstallation commands. Return codes can be retrieved from this log file, but not for DB2. If installation or uninstallation completed, the executePackage or remove-package scripts for a component are available.	`coi/plan/install` or `coi/plan/uninstall`
Administration Center installation log files	Installation log files. Review these log files if the Administration Center installation or uninstallation fails. For log information about additional Administration Center components, see the *Problem Determination Guide*.	• `coi/plan/install/logs` • `coi/plan/install/MachinePlan_host_name/ 00001_eWAS` • `coi/plan/install/MachinePlan_host_name/ 00002_TIP` • `coi/plan/install/MachinePlan_host_name/ 00003_TSM_AdminCenter` or • `install_root/_uninst/plan/install/ MachinePlan_host_name/00001_eWAS` • `install_root/_uninst/plan/install/ MachinePlan_host_name/00002_TIP` • `install_root/_uninst/plan/install/ MachinePlan_host_name/00003_TSM_AdminCenter`

Tip: Some of the exit codes for a silent installation might be different than the exit codes for a GUI or console installation. For example, an exit code of 1 for a silent installation means that the installation completed successfully without warnings or errors. However, for a GUI or console installation, an exit code of 1 means that the installation completed, but that one or more of the actions from the installation sequence caused a warning or non-fatal error. See the *Problem Determination Guide* for the latest information.

Table 41. InstallAnywhere exit codes

Code	Description
0	Success: The installation completed successfully without any warnings or errors.
1	The installation completed successfully, but one or more of the actions from the installation sequence caused a warning or a non-fatal error.
-1	One or more of the actions from the installation sequence caused an unrecoverable error.
1000	The installation was canceled by the user.
1001	The installation includes an invalid command-line option.
2000	Unhandled error.
2001	The installation failed the authorization check, might indicate an expired version.
2002	The installation failed a rules check. A rule placed on the installer itself failed.
2003	An unresolved dependency in silent mode caused the installer to exit.
2004	The installation failed because not enough disk space was detected during the execution of the Install action.
2006	The installation failed because it was launched in a UI mode that is not supported by this installer.
3000	Unhandled error specific to a launcher.
3001	The installation failed due to an error specific to the lax.main.class property.
3002	The installation failed due to an error specific to the lax.main.method property.
3003	The installation was unable to access the method specified in the lax.main.method property.
3004	The installation failed due to an exception error caused by the lax.main.method property.
3005	The installation failed because no value was assigned to the lax.application.name property.
3006	The installation was unable to access the value assigned to the lax.nl.java.launcher.main.class property.
3007	The installation failed due to an error specific to the lax.nl.java.launcher.main.class property.
3008	The installation failed due to an error specific to the lax.nl.java.launcher.main.method property.
3009	The installation was unable to access the method specified in the lax.nl.launcher.java.main.method property.
4000	A component to start Java could not be found at the directory specified by the java.home system property.
4001	An incorrect path to the installer jar caused the relauncher to launch incorrectly.

Appendix B. Accessibility features for the Tivoli Storage Manager product family

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

The following list includes the major accessibility features in the Tivoli Storage Manager family of products:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

If you install the IBM Tivoli Storage Manager Operations Center in console mode, the installation is fully accessible.

The accessibility features of the Operations Center are fully supported only in the Mozilla Firefox browser that is running on a Windows system.

The Tivoli Storage Manager Information Center, and its related publications, are accessibility-enabled. For information about the accessibility features of the information center, see the following topic: http://pic.dhe.ibm.com/infocenter/tsminfo/v6r3/topic/com.ibm.help.ic.doc/iehs36_accessibility.html.

Keyboard navigation

On Windows, the Tivoli Storage Manager product family follows Microsoft conventions for all keyboard navigation and access. Drag and Drop support is managed by using the Microsoft Windows Accessibility option known as *MouseKeys*. For more information about MouseKeys and other Windows accessibility options, see the Windows online help, citing the keyword "MouseKeys".

On other operating systems, these products follow the operating-system conventions for keyboard navigation and access.

Vendor software

The Tivoli Storage Manager product family includes certain vendor software that is not covered under the IBM license agreement. IBM makes no representation about the accessibility features of these products. Contact the vendor for the accessibility information about its products.

IBM and accessibility

See the IBM Human Ability and Accessibility Center (http://www.ibm.com/able) for information about the commitment that IBM has to accessibility.

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 grant 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 character set (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 may 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 want 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
2Z4A/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 information 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 measurements 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.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample

programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and 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 and Itanium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Glossary

A glossary is available with terms and definitions for the IBM Tivoli Storage Manager family of products.

You can view the glossary in the Tivoli Storage Manager information center at http://pic.dhe.ibm.com/infocenter/tsminfo/v6r3.

To view glossaries for other IBM products, see http://www.ibm.com/software/globalization/terminology/.

Index

Special characters

(TLS) Transport Layer Security   58

A

access rights
   configuration for deployment engine
      UNIX operating systems   62
accessibility features   225
activating
   server
      AIX, HP-UX, Linux, Solaris   63
active log
   space requirements   19
adding the agent to the agent depot   140
Administration Center
   ASCII
      language   201, 202
   backward compatibility   213
   configuring server   45, 49
   console installation wizard   201, 202
   default port   201, 202
   DISPLAY   201, 202
   estimating requirements   190
   I/O throughput   191
   installation   201, 202
   installation log   201, 202
   installing   201, 202
   Java   192
   Java heap memory size   194
   Java heap size   192
   languages
      set   201, 202
   LD_LIBRARY_PATH_64   201, 202
   location   196
   memory usage   192
   non-ASCII
      language   201, 202
   number of administrators   191
   overview   189
   port   201, 202
   post-installation tasks   204
   prerequisite checker   12, 200
   processing capacity   191
   processing memory   192
   secure port   201, 202
   SELINUX   201, 202
   server connection to   217
   system requirements   190
   Tivoli Storage Manager installation   208
   uninstalling   208, 211
   upgrading   213, 214
   verifying   208
   verifying prerequisites   12, 200
   worksheet   197
Administration Center, configuration wizard   52
Administration Centerreporting   134, 154
administrative commands
   HALT   67
   REGISTER LICENSE   68

administrator ID   178
administrator password   178
agent
   Tivoli Monitoring for Tivoli Storage Manager, installing on
      existing server   136
agents
   Tivoli Monitoring for Tivoli Storage Manager,
      installing   135
alerts
   email alerts   180
   sending and receiving by email   180
API   50, 59
API configuration   50, 59
archive failover log space
   description   30
archive log
   space requirements   19
archive log directory   48
ASCII
   language   37, 38
Asian fonts   184
automatic starting, server   66

B

BACKUP DB command   50, 59
backup-archive client
   installable package   viii
backups
   database   68

C

capacity planning
   database space requirements
      estimates based on number of files   15
      estimates based storage pool capacity   18
      starting size   15
   recovery log space requirements
      active and archive logs   19
      active log mirror   30
   Tivoli Monitoring for Tivoli Storage Manager   115
Chinese fonts   184
client nodes
   reverting to previous server version
      data affected   95
client options
   for shared memory communications   57
clustered environment
   upgrading
      server   94
   upgrading server on Linux
      V6 to V6.3 or later   94
commands
   administrative, SET DBRECOVERY   68
   DSMSERV FORMAT   59
commands, administrative
   HALT   67
   REGISTER LICENSE   68

IBM®