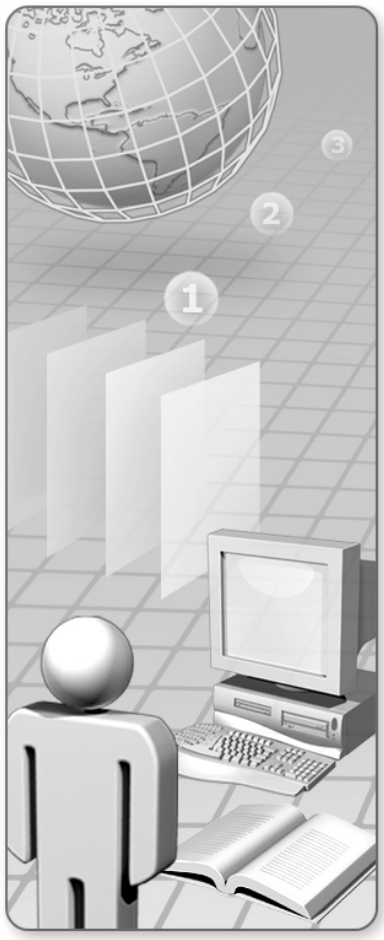
Microsoft

Session 2: Implementing and Administering Windows SharePoint Services 3.0

Contents



Session 2: Implementing and Administering Windows SharePoint Services 3.0

- Deploying Windows SharePoint Services
- Administering Windows SharePoint Services
- Managing Windows SharePoint Services Sites
- Managing Windows SharePoint Services Security
- Upgrading to Windows SharePoint Services 3.0

Overview

Many of the implementation and management tasks in Microsoft® Windows® SharePoint® Services 3.0 are similar to the tasks performed in earlier versions of Windows SharePoint Services. However, the management interface has changed significantly. Also, Windows SharePoint Services includes several important new configuration options.

After completing this session, you will be able to:

- Describe the deployment options for Windows SharePoint Services.
- Administer Windows SharePoint Services.
- Manage Windows SharePoint Services sites.
- Manage Windows SharePoint Services security.
- Describe the options for upgrading to Windows SharePoint Services 3.0.

Deploying Windows SharePoint Services

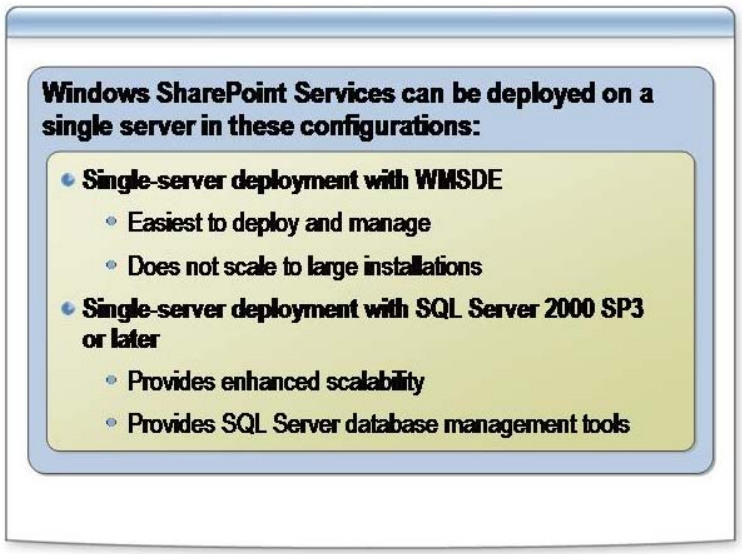
- Single-Server Deployment Options
- Windows SharePoint Services Server Roles
- Web Farm Deployment Options
- Windows SharePoint Services Installation Requirements
- Windows SharePoint Services Installation Process

Windows SharePoint Services is designed to provide SharePoint sites for all organizations, from small businesses that require only a single server running Windows SharePoint Services to very large enterprises that deploy many servers. Windows SharePoint Services can be installed in several deployment scenarios, depending on the organization's requirements for availability and performance.

Specifically, this section will cover:

- Single-server deployment options.
- Windows SharePoint Services server roles.
- Web farm deployment options.
- Windows SharePoint Services installation requirements.
- Windows SharePoint Services installation process.

Single-Server Deployment Options



Windows SharePoint Services can be deployed with all of the services required on a single server. The single-server implementation provides a low-cost and easy-to-manage method of introducing Windows SharePoint Services into an environment. This deployment option is recommended for:

- Small businesses that want to take advantage of Windows SharePoint Services features.
- A team or department within a medium to large organization.

When installing Windows SharePoint Services on a single server, you have two options:

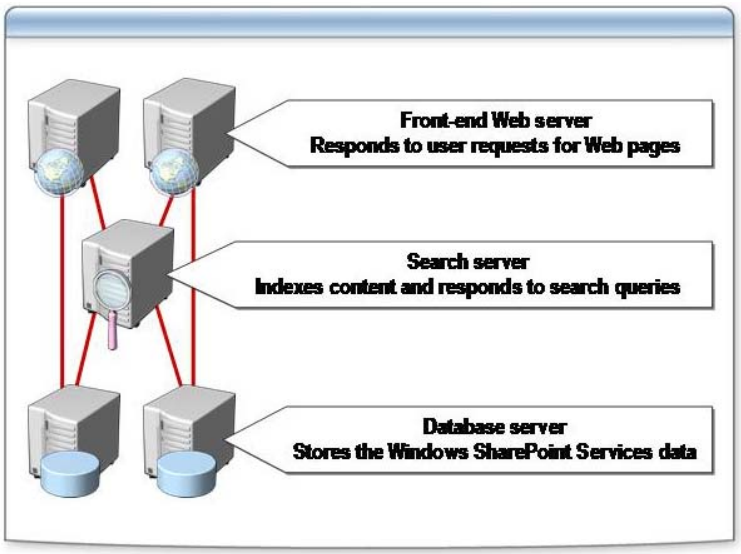
- Single-server deployment with Microsoft SQL Server™ 2000 Desktop Engine (Windows) (WMSDE). In this configuration, a single server runs both Windows SharePoint Services and WMSDE to store Windows SharePoint Services configuration information and site content. This installation option has the following advantages:
  - WMSDE is installed by Windows SharePoint Services setup, so no database configuration is required.
  - It does not require additional server licenses.
  - The data can be migrated to SQL Server after deployment.

  The biggest disadvantage is that this solution does not scale well. WMSDE must run on the same server as Windows SharePoint Services, so you cannot implement multiple servers without first migrating the information to SQL Server.

  Note Unlike earlier versions of Windows SharePoint Services, Windows SharePoint Services 3.0 does not use SQL Server indexing to enable searching. This means that search can be enabled when using WMSDE.

- Single-server deployment with SQL Server. In this configuration, one computer runs Windows SharePoint Services in the Web Server role. The same computer also runs SQL Server 2000 Service Pack 3 (SP3) or later. This installation option has the following advantages:
  - It provides much better scalability.
  - It provides SQL Server administration tools for managing the database.

Windows SharePoint Services Server Roles



The biggest issue with a single-server deployment is that it cannot scale to service a large number of users requesting access to large amounts of data. This limitation means that most organizations that deploy Windows SharePoint Services will require multiple servers. To understand the multiple-server deployment options, you must first understand the Windows SharePoint Services server components.

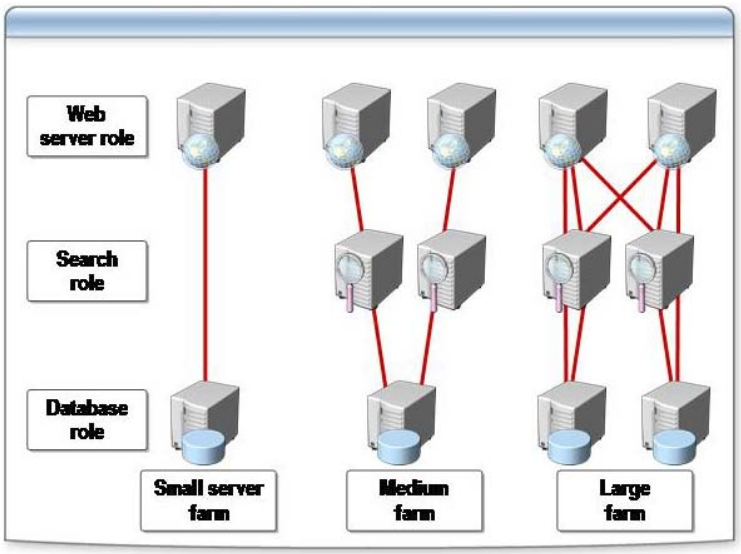
Windows SharePoint Services server components map to three tiers:

- Front-end Web server. This server responds to user requests for Web pages. All front-end Web servers in a farm contain the same configurations. Front-end Web servers can be load balanced using a hardware load balancing device or Windows Network Load Balancing to provide scalability and availability.
- Search server. This server is responsible for indexing the content in Windows SharePoint Services databases and responding to client search queries. This functionality can be deployed on a separate server to dedicate resources to search. With Windows SharePoint Services, search and indexing cannot be separated onto separate servers.
- Database server. This server runs SQL Server and stores the application data. All Windows SharePoint Services databases can live on one database server, or databases can be spread across multiple servers.

In a single-server deployment, all of these server roles run on the same server. However, these roles can also be distributed across multiple physical servers to provide higher performance and availability. For example, you can:

- Deploy the search component on the same server as the front-end Web server component or on the same server as the database component.
- Dedicate a server to operate as the search and index server, adding a middle tier to your farm.
- Add additional search servers and assign each to a dedicated database. Search servers cannot be mirrored or load balanced, so this solution provides multiple points of failure for a very large Windows SharePoint Services installation.
- Add additional front-end Web servers to load balance user requests across multiple front-end Web servers.
- Use SQL Server clustering to provide failover protection for database servers.

Web Farm Deployment Options



For organizations that require a larger Windows SharePoint Services deployment, Windows SharePoint Services 3.0 can also be deployed in the following Web farm configurations:

- Small server farm. In this configuration, one computer runs Windows SharePoint Services, in the Web server role and the search role. A second computer runs SQL Server 2000 SP3 or later. The small-farm implementation takes advantage of at least two servers to:
  - Accommodate a larger number of users.
  - Store a greater amount of data.
  - Increase overall performance.

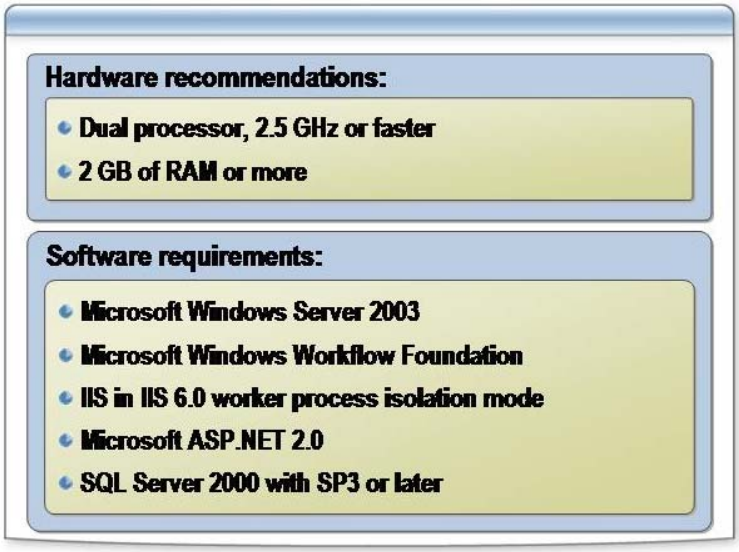
  This implementation is recommended for:
  - Teams or departments with needs that scale beyond the single-server implementation.
  - Organizations that require IT-managed databases.
- Medium farm. In this deployment, servers are deployed in three tiers with one or more front-end Web servers and one or more search servers. The medium farm topology introduces a dedicated server for the search component. The medium farm topology is limited to one dedicated database server. This implementation is recommended for:
  - Scaling beyond use by a single team or department.
  - Improving search and indexing performance.
  - Accommodating a large number of users, compared to the amount of database storage or utilization requirements.
  - Extranet implementations.

- Large farm. This deployment scales the Windows SharePoint Services databases across multiple dedicated servers. The large farm topology incorporates multiple databases residing on separate servers. This topology is recommended for:
  - Scaling across multiple departments within an organization.
  - Maximizing the performance of the database components, and consequently the performance of the entire farm.
  - Storing a large amount of data.
  - Heavily utilized extranet implementations in which database availability is critical.

  The large farm topology integrates a large number of sites and data, which requires a higher degree of coordination across groups to:

  - Anticipate growth patterns.
  - Implement a site hierarchy.
  - Develop a search taxonomy.

Windows SharePoint Services Installation Requirements



Before you install and configure Windows SharePoint Services, you should ensure that your systems meet the hardware and software requirements.

Hardware Recommendations

The recommended hardware for a single-server installation includes 2.5-gigahertz (GHz) dual processors and a minimum of 1 gigabyte (GB) of RAM. However, 2 GB of RAM is recommended for improved performance.

To build server farms, you will need one or more server computers operating in each role. The hardware recommendations for the servers are as follows:

- Web server: 2.5-GHz dual processor, 2 GB RAM
- Database server: 2.0-GHz dual processor, 2 GB RAM

Software Requirements

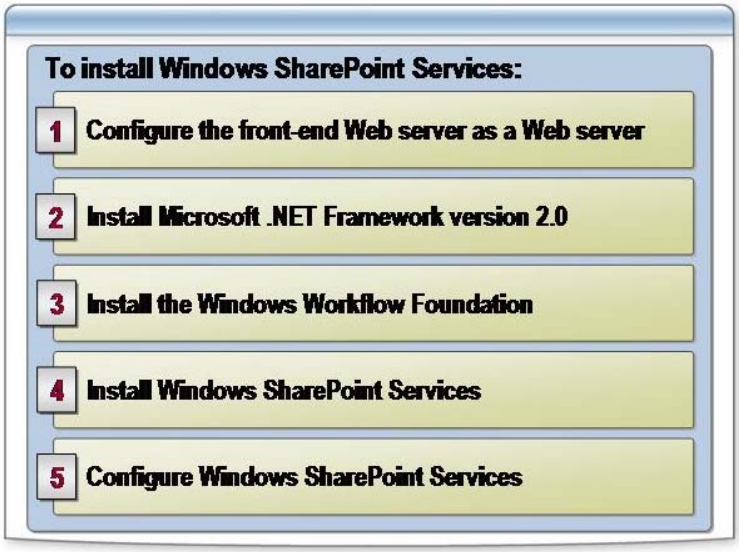
To run Windows SharePoint Services, your servers must meet the following criteria:

- Must be running Microsoft Windows Server™ 2003 (Standard, Enterprise, Datacenter, or Web Edition).
- Must have the Microsoft Windows Workflow Foundation Beta version 1.2 installed.
- Web server must be running Microsoft Internet Information Services (IIS) in IIS 6.0 worker process isolation mode.

- Must be running Microsoft ASP.NET 2.0.
- Must be using the NTFS file system.
- Database computer must be running SQL Server 2000 SP3 or later.

Note SQL Server 2005 is not supported with Windows SharePoint Services 3.0 Beta 1, but it is supported for later releases.

Windows SharePoint Services Installation Process



To install Windows SharePoint Services, complete the following installation process:

1. Configure the server as a Web server. You must configure the server you use as a Web server before you install Windows SharePoint Services. Because IIS is not enabled by default in Windows Server 2003, you must enable and configure IIS on each of the Web server computers in your server farm. IIS must be running in IIS 6.0 worker process isolation mode. By default, all IIS 6.0 installations except servers that have been upgraded from IIS 5.0 are configured to run in IIS 6.0 worker process isolation mode.
2. Install Microsoft .NET Framework version 2.0. Windows SharePoint Services requires version 2.0 of the .NET Framework, so you must install the .NET Framework and enable ASP.NET 2.0 on each of the Web server computers in your server farm.
3. Install the Windows Workflow Foundation. Windows SharePoint Services 3.0 requires the Windows Workflow Foundation to enable workflow.
4. Install Windows SharePoint Services on the Web server. After you have installed prerequisite components, you are ready to install Windows SharePoint Service on your Web server computer.
5. Configure Windows SharePoint Services on the Web server. After the Windows SharePoint Services installation finishes, you must configure Windows SharePoint Services on the server. In a single-server installation, the SharePoint Products and Technologies Configuration Wizard will start after the installation and complete the configuration without user input. If you are deploying Windows SharePoint Services in a Web farm, you must configure the database and authentication settings for the deployment.

Note When you configure Windows SharePoint Services to use a SQL Server database that is on a different server, you must configure an account that is used to connect to the computer running SQL Server. This account must be a member of the local Administrators group and have Security Administrator and Database Creator credentials.

Administering Windows SharePoint Services

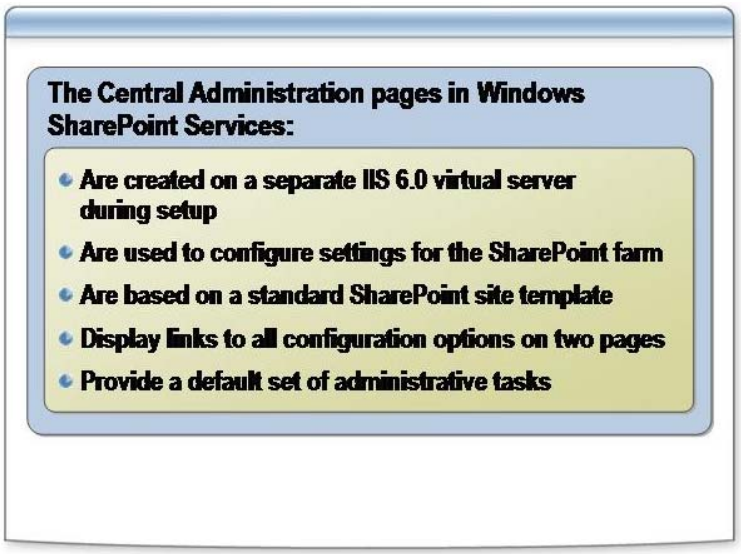
- Central Administration Site Overview
- Windows SharePoint Services Operations Overview
- Backing Up and Restoring Windows SharePoint Services
- Managing Windows SharePoint Services Applications

In many ways, administering a Windows SharePoint Services 3.0 deployment is quite similar to administering earlier versions. However, Windows SharePoint Services includes some new administrative options that correlate to some of the product enhancements. In particular, the user interface used by Windows SharePoint Services administrators has been significantly modified.

Specifically, this section will cover:

- The Central Administration pages.
- Managing Windows SharePoint Services operations.
- Backing up and restoring Windows SharePoint Services sites.
- Managing Windows SharePoint Services applications.

Central Administration Site Overview



Like earlier versions, Windows SharePoint Services 3.0 provides a Central Administration site that can be used to manage settings for the Windows SharePoint Services farm. The Central Administration site is created during Windows SharePoint Services setup and is configured as a separate virtual server in IIS 6.0. The Central Administration pages are accessed by using the administration port for the virtual server that Windows SharePoint Services created during setup.

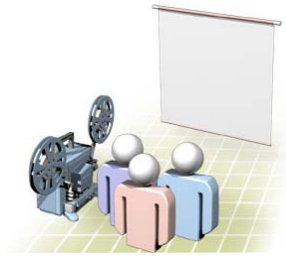
By default, the settings configured on the Central Administration site apply to all servers and SharePoint applications. In some cases, you can change these default settings and specify unique settings for each Windows SharePoint Services application.

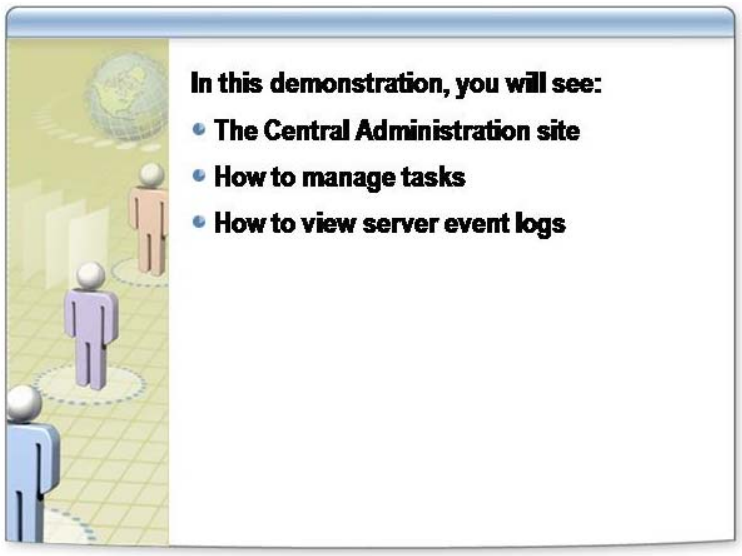
To view the Central Administration pages, you must be a member of the local Administrators group for the server computer or a member of the SharePoint administrators group.

The user interface for the Central Administration site has been redesigned for Windows SharePoint Services. Some of the new features include the following:

- The Central Administration site is now a standard SharePoint site. This makes the site more functional in terms of assigning and managing tasks and searching content.
- The Central Administration pages have three links on the top navigation bar: Home, Operations, and Application Management. Links to all administrative tasks have been grouped on the Operations and Application Management pages.
- The Administrative Tasks list includes a default set of tasks that are created when Windows SharePoint Services is installed. You can use this set of tasks to complete the configuration of the server after deployment. You can add and remove items from this task list, just like you can on any other task list on a SharePoint site.

Demonstration 1: Central Administration Site Overview





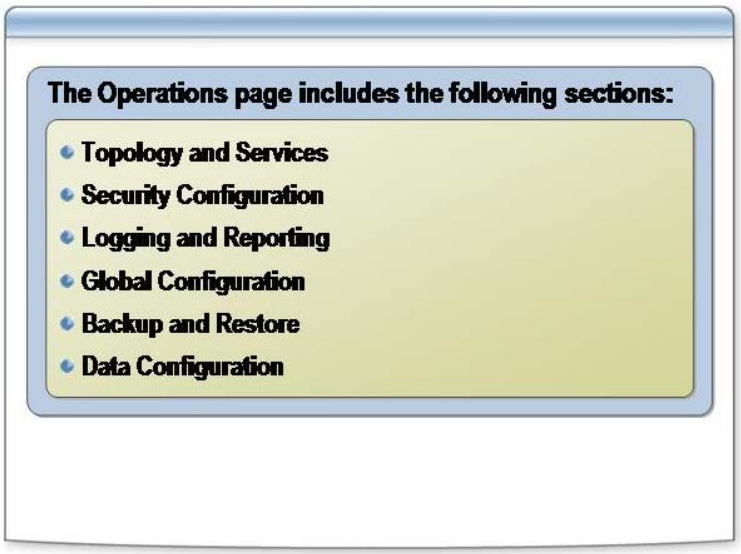
As with earlier versions, Windows SharePoint Services 3.0 provides a Central Administration site that can be used to configure the server and application settings. However, Windows SharePoint Services provides several key improvements to the Central Administration pages.

This demonstration shows an overview of interface changes in the Central Administration pages.

In this demonstration, you will see:

- The Central Administration site.
- How to manage tasks.
- How to view server event logs.

Windows SharePoint Services Operations Overview



The Operations page on the Central Administration site contains links to pages that help you manage your server or server farm, such as changing the server farm topology, specifying which services are running on each server, and changing settings that affect multiple servers or applications.

The Operations page includes the following sections.

Section	Configuration options
Topology and Services	Provides links to view the servers in the Windows SharePoint Services farm, the services running on each server, and the incoming and outgoing e-mail settings.
Security Configuration	Provides links to configure the service accounts in a Windows SharePoint Services farm, information rights management settings, the SharePoint Administration group, and antivirus and blocked file type settings.
Logging and Reporting	Provides links for configuring diagnostic logging and usage analysis processing and viewing the server event logs.
Global Configuration	Provides links for viewing and configuring timer jobs, configuring alternate access mappings, quiescing the farm so that the Windows SharePoint Services servers will not accept connections for long running jobs, and defining quotas.
Backup and Restore	Provides links for backing up and restoring SharePoint sites and for viewing the backup and restore history.
Data Configuration	Provides links for configuring the default database server, and for configuring data retrieval services that can be used to retrieve data from alternate data sources.

Backing Up and Restoring Windows SharePoint Services

The backup and restore tool in Windows SharePoint Services:

- Can back up and restore from the Central Administration site
- Supports user interface and command-line configuration
- Enables backup to a local hard drive or a network location
- Supports both full and incremental backups
- Does not support backup scheduling
- Can back up the farm or an entire site collection only

Windows SharePoint Services provides a backup and restore tool that can be accessed from the Operations page. This tool provides limited functionality, so it is recommended primarily for the single-server or small farm deployment.

The built-in backup and restore tool provides the following advantages:

- It allows the farm administrator to manage the database backup and restore process by means of the Central Administration site.
- It provides user interface and command-line support.
- It enables backup to a local hard drive or a network location so that there is no need for additional hardware.
- It supports both full and incremental backups.

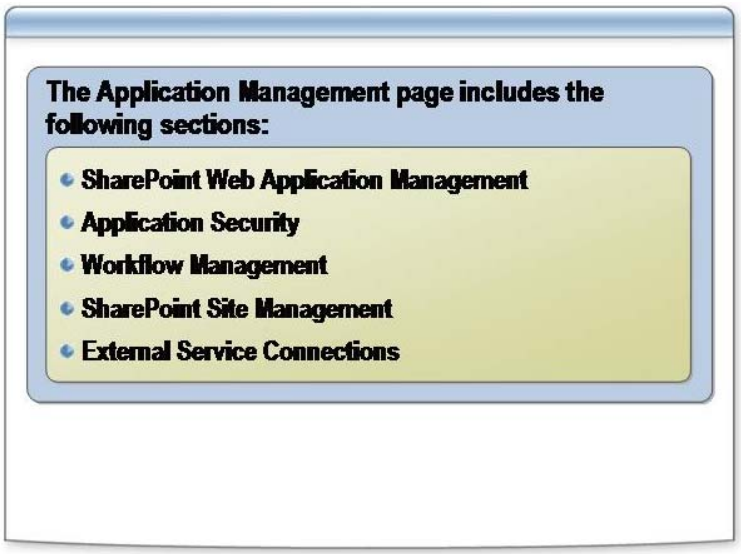
The backup tool has the following limitations:

- It does not provide a scheduling option, so if you want to schedule automatic backups, you must develop a script to call Windows Scheduled Tasks to run the operation.
- It can back up and restore an entire farm or an entire site collection only. You cannot back up or restore subsites or individual pages.

Windows SharePoint Services supports additional backup and restore options, including:

- SQL Server backup and restore. This option is typically used by large organizations with SQL Server expertise.
- Microsoft Office SharePoint Designer backup and restore. With Office SharePoint Designer, you can back up and restore individual subsites.

Managing Windows SharePoint Services Applications



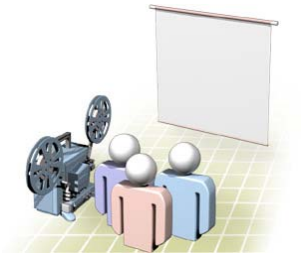
In earlier versions of Windows SharePoint Services, you frequently administer virtual server settings to apply settings to all site collections on that virtual server. In Windows SharePoint Services, you perform many of these same settings on the Application Management page on the Central Administration site. In most cases, Windows SharePoint Services uses the term *application* instead of virtual server.

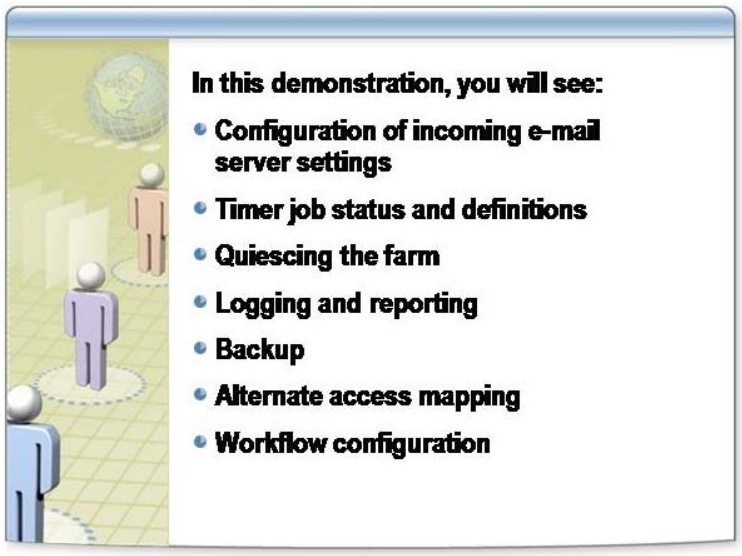
The Application Management page on the Central Administration site contains links to pages that help you configure settings for applications and components that are installed on the server or server farm.

The Application Management page includes the following sections.

Section	Configuration options
SharePoint Web Application Management	Provides links to create or extend Web applications, remove Windows SharePoint Services from IIS Web site, or delete a Web application. Other links include pages to configure alternate access mappings, define managed paths, configure Web application settings, and create or delete content databases.
Application Security	Provides links to configure security for Web Part Pages, self-service site management, and user rights for Web applications; assign security policies for Web applications; and configure authentication providers.
Workflow Management	Provides a link for enabling or disabling workflow for an application.
SharePoint Site Management	Provides links for creating and deleting site collections, configuring site use confirmation and deletion, configuring quota definitions, and configuring site collection administrators.
External Service Connections	Provides links for configuring HTML viewer service and official file connections and document conversions.

Demonstration 2: Managing Windows SharePoint Services





The Operations page on the Windows SharePoint Services Central Administration site includes all of the settings that are applied to the Windows SharePoint Services server or farm. The Application Management page on the Windows SharePoint Services Central Administration site includes all of the settings that are applied to the Windows SharePoint Services applications. In Windows SharePoint Services, the term *application* has replaced the term *virtual server*, so you will see that many of the settings on this page are similar to the virtual server settings in earlier versions of Windows SharePoint Services. This demonstration shows some of the administrative tasks that will be performed on the Operations page and the Application Management page.

In this demonstration, you will see:

- Configuration of incoming e-mail server settings.
- Timer job status and definitions.
- Quiescing the farm.
- Logging and reporting.
- Backup.
- Alternate access mapping.
- Workflow configuration.

Managing Windows SharePoint Services 3.0 Sites

- Windows SharePoint Services Site Definitions
- Windows SharePoint Services Site Templates
- Windows SharePoint Services Web Parts
- Windows SharePoint Services Search

After configuring the farm and application-level settings, the next task for a Windows SharePoint Services administrator is to create and manage SharePoint sites. Windows SharePoint Services 3.0 provides some additional site templates and Web Parts, but the process for creating and managing sites has not changed significantly from earlier versions of Windows SharePoint Services.

Specifically, this section will discuss:

- Windows SharePoint Services site definitions.
- Windows SharePoint Services site templates.
- Windows SharePoint Services Web Parts.
- Windows SharePoint Services search.

Windows SharePoint Services Site Definitions

Site definitions:

- Define the underlying structure for all Web sites
- Are a combination of multiple files stored on a front-end Web server
- Provide flexibility by allowing changes to all sites based on the site definition and by enabling reversion to the original site definition
- Must be created by developers and installed by administrators on the front-end Web server

Windows SharePoint Services uses site definitions to define the underlying structure for all Web sites. A site definition provides the base blueprint for a site, the featured lists, the default navigation structure, and so on.

Each site definition is based on a combination of files that are placed in the *Local_Drive*:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\60\ subdirectory on one or more front-end Web servers during installation of Windows SharePoint Services. Site definition files include core schema XML files, .aspx pages, document template files, and content files.

You can create new site definitions or create sites based on a site definition. One of the advantages of using site definitions to create new sites is that if you change the underlying site definition (for example, by updating a graphic or page), all sites based on site definitions will be updated. You can also restore a site to the original site definition at any time.

Site definitions must be created by developers, and they require administrative permissions to be installed on the front-end Web server.

Windows SharePoint Services Site Templates

Each Windows SharePoint Services site is based on a site template. A site template is a package that contains a set of differences and changes from a base site definition. This package is stored as an .stp file, which is a cabinet file that contains XML files that define the differences. The .stp file can be downloaded from and uploaded to site collections by users with appropriate rights, meaning that .stp files have some measure of portability.

Windows SharePoint Services provides the following templates.

Template name	Description
Team Site	This template creates a site for teams to create, organize, and share information quickly and easily. It includes a document library and basic lists such as Announcements, Calendar, Contacts, and Quick Links.
Blank Site	This template creates a Windows SharePoint Services–enabled Web site with a blank home page. You can add interactive lists or any other Windows SharePoint Services features.
Document Workspace	This template creates a site in which teams can work together on documents. It provides a document library for storing the primary document and supporting files, a Task list for assigning to-do items, and a Links list for resources related to the document.
Basic Meeting Workspace	This template creates a site with all the basics necessary to plan, organize, and track your meeting. It contains the following lists: Objectives, Attendees, Agenda, and Document Library.
Blank Meeting Workspace	This template creates a blank Meeting Workspace site for you to customize based on your requirements.
Decision Meeting Workspace	This template creates a Meeting Workspace site in which to review relevant documents and record decisions. It contains the following lists: Objectives, Attendees, Agenda, Document Library, Tasks, and Decisions.
Social Meeting Workspace	This template creates a planning tool for social occasions, featuring a discussion board and a picture library to post pictures of the event. It contains the following lists and Web Parts: Attendees, Directions, Image/Logo, Things To Bring, Discussions, and Picture Library.

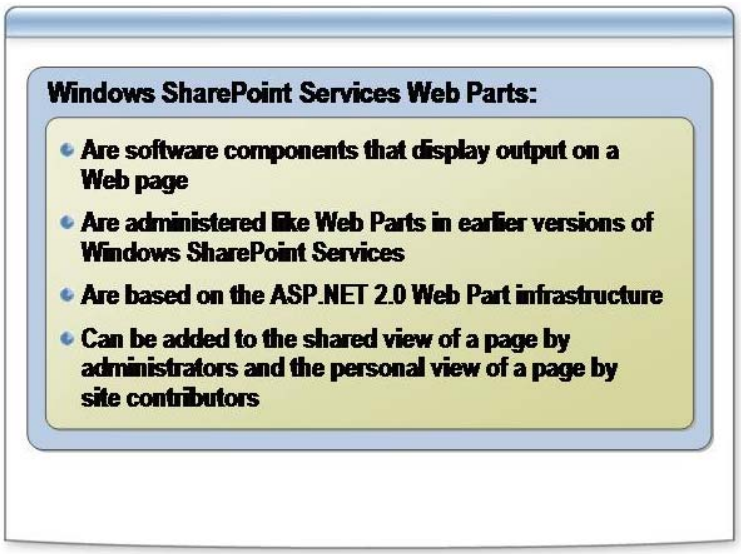
(*continued*)

Template name	Description
Multipage Meeting Workspace	This template creates a site with all the basics necessary to plan, organize, and track your meeting with multiple pages. It contains the following lists: Objectives, Attendees, and Agenda. The template also contains two blank pages for you to customize based on your requirements.
Wiki Site	This template creates a site in which users can quickly and easily add, edit, and link Web pages. Permissions can be set so that anyone who can read pages can edit pages.
Blog	This template creates a site in which users can post information and allow others to comment on it.

You can also create a site based on an existing site template, modify the site to include the components and the appearance that you choose, and then save that site as a template. You can then use that template to create new sites.

User-customized templates are easier to create and install than new site definitions, but they are more limited in scalability and deployability. The user template is portable from one server running Windows SharePoint Services if the underlying site definition exists on the destination server.

Windows SharePoint Services Web Parts



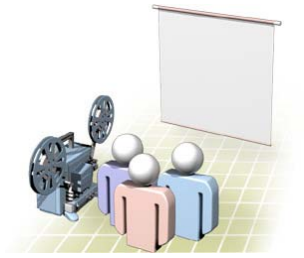
Web Parts are software components that execute in Windows SharePoint Services and display output on a Web page. For example, document libraries and lists are simply Web Parts that provide hyperlinks to content in the SQL Server content database.

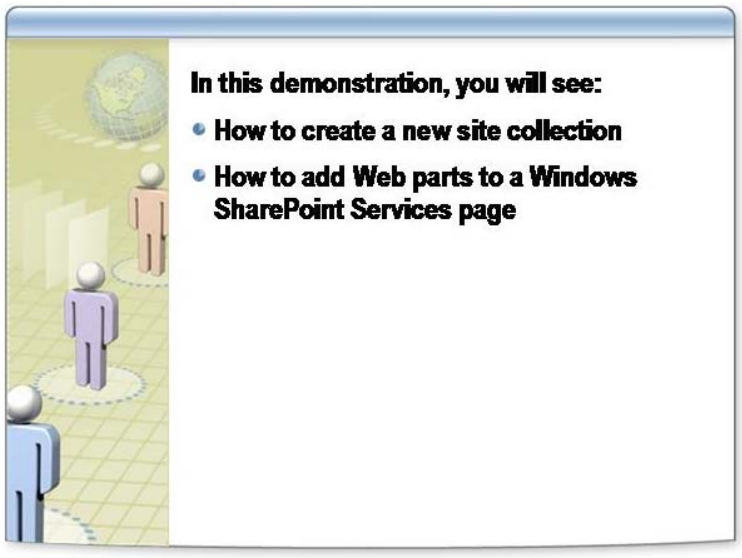
From a Windows SharePoint Services administrator's point of view, the use of Web Parts in Windows SharePoint Services 3.0 has not changed significantly from earlier versions. Administrators can modify a SharePoint site by adding or removing Web Parts.

However, for developers, the Web Part configuration for Windows SharePoint Services 3.0 is different than it is in Windows SharePoint Services 2.0: it has been redesigned and rebuilt to use the new ASP.NET 2.0 Web Part control set, rather than the Web Part infrastructure based on ASP.NET 1.1 that is used in Windows SharePoint Services 2.0.

To add or remove Web Parts, an administrator can edit the shared version of a page on the SharePoint site. When the shared version is modified, all users will see the modified pages. Users with Contributor access to the site can also modify their personal versions of the page. The changes to the personal view are visible only to the individual who made them.

Demonstration 3: Creating and Managing SharePoint Sites





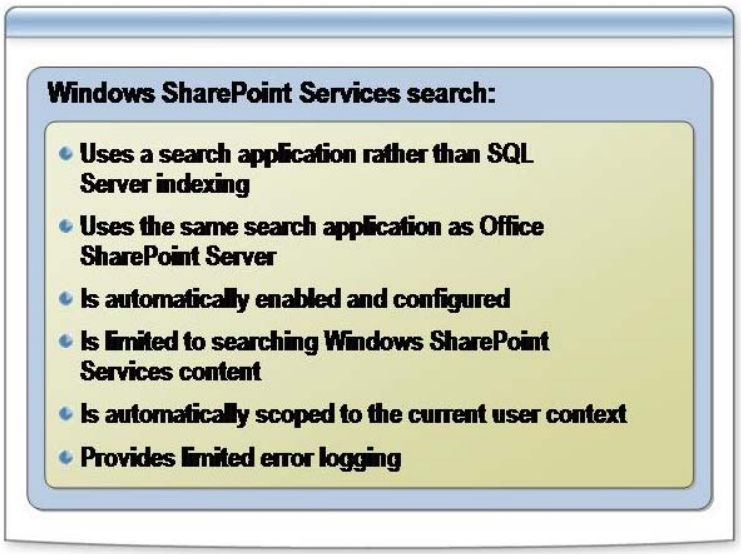
In many ways, creating and managing SharePoint sites has not changed in Windows SharePoint Services 3.0. As a Windows SharePoint Services administrator, you will still create site collections and configure the Web sites for users.

In this demonstration, you will see how to create a site collection in Windows SharePoint Services and how to configure the site home page.

In this demonstration, you will see:

- How to create a new site collection.
- How to add Web Parts to a Windows SharePoint Services page.

Windows SharePoint Services Search



One of the problems experienced by users of earlier versions of Windows SharePoint Services is limited search functionality. This is because earlier versions of Windows SharePoint Services used SQL Server indexing to provide the search functionality.

In Windows SharePoint Services 3.0, search is implemented by using a Windows SharePoint Services search engine that is the same for both Windows SharePoint Services and Microsoft Office SharePoint Server 2007. Search in Windows SharePoint Services provides the following functionality:

- One search application is shared with Office SharePoint Server 2007. This provides a consistent experience for administrators and users across both platforms.
- Search is automatically configured and enabled on Windows SharePoint Services. One content source is automatically created for each virtual server, and indexing is automatically enabled. Content sources are crawled automatically without scheduling. The search configuration cannot be modified.
- The content included in a Windows SharePoint Services search is limited to Windows SharePoint Services content.
- When users initiate a search, the search is automatically scoped to the current context. This means that if you are at a top-level site, all sites in the site collection are included in the search scope. If you are on a subsite or viewing a document library, the search scope includes the content on the subsite or document library only. Users can change the search scope.
- The search application provides limited error logging (credentials, propagation, and hardware failure/data corruption only).

Note Office SharePoint Server significantly enhances the search functionality available in Windows SharePoint Services to include additional content sources, searching for content and people, and searching based on keywords and best bets.

Managing Windows SharePoint Services Security

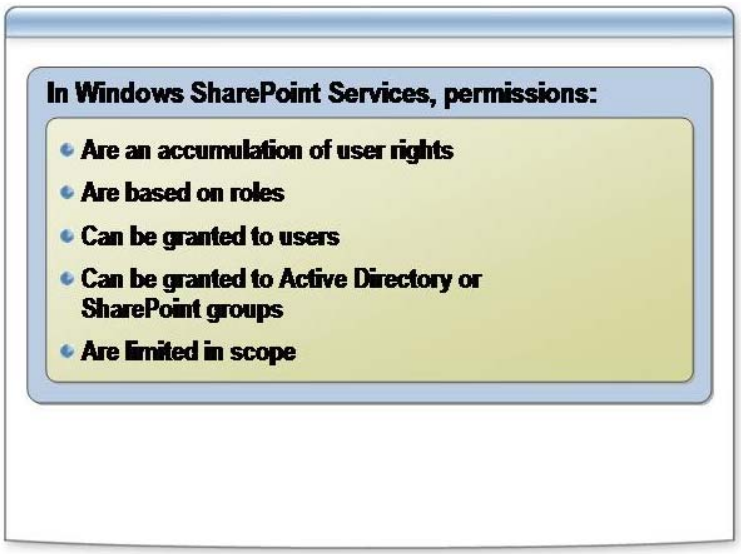
- Windows SharePoint Services Security Overview
- Windows SharePoint Services Authentication Options
- Default Permission Levels
- Default SharePoint Groups Groups
- Managing Permissions and Permission Inheritance
- Application Security Policies
- Windows SharePoint Services Integration with RMS

One of the most important components in deploying Windows SharePoint Services is planning for and configuring security for the SharePoint sites. The SharePoint sites may contain information that is highly confidential and should be accessible to only specified users within the organization. If you make the SharePoint site accessible from the Internet, you must also plan for additional security. This section discusses the security configuration options for Windows SharePoint Services.

Specifically, this section will discuss:

- Windows SharePoint Services Security overview.
- Windows SharePoint Services Authentication options.
- Default permission levels.
- Default SharePoint Groups.
- Managing permissions and permission inheritance.
- Application security policies.
- Windows SharePoint Services integration with RMS.

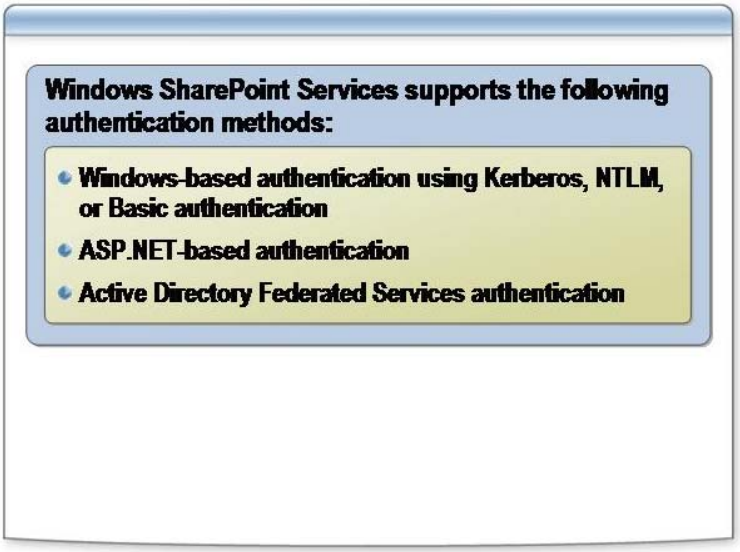
Windows SharePoint Services Security Overview



Before you can plan for Windows SharePoint Services security, you must understand the components that make up the Windows SharePoint Services security model. Regardless of what type of site you are creating, the security and permissions for your site include the following concepts:

- Permissions are an accumulation of user rights. Individual rights grant permission to perform specific actions. For example, the View Items right grants the user the ability to view items in a list. Farm administrators can control which rights are available for the server farm.
- Permissions are based on roles. A role is a pre-defined group of rights that grant users permission to perform related actions. For example, the Read permission role includes the View Items, Open Items, View Pages, and View Versions rights (among others), all of which are needed to read documents, items, and pages on a SharePoint site.
- Permissions can be granted to users. Users can be added and assigned a permission level directly. Users do not have to be part of a group, although it is much easier to manage permissions for groups than for individual users.
- Permissions can be granted to groups. Groups in Windows SharePoint Services can be a Windows security group or a SharePoint group, such as Site Owners, Site Members, and Site Readers. SharePoint groups imply a permission level, but the permission level for any group can be changed as needed.
- Permissions are limited in scope. Users or groups are assigned a permission level for a specific scope such as a site, list, library, folder, or item. By default, permissions for a list, library, folder, or item are inherited from the parent site or parent list or library. But anyone assigned a permission level for a particular scope that includes the Manage Permissions right can change the permissions for that scope. By default, permissions are initially controlled at the site level, with all lists and libraries inheriting the site permissions.

Windows SharePoint Services Authentication Options



To gain access to any content on a SharePoint site that is not configured to allow anonymous access, a user must be authenticated. With earlier versions of Windows SharePoint Services, the only way in which users could be authenticated was through Windows-based authentication. Windows SharePoint Services continues to support Windows-based authentication, but it also provides additional authentication options.

Windows SharePoint Services supports the following authentication options:

- Windows-based authentication using Kerberos protocol, NTLM authentication protocol, or Basic authentication. This authentication option uses the IIS 6.0 authentication methods to enable authentication for users with accounts in an Active Directory domain. In this configuration, IIS 6.0 authenticates the user based on the user name and password.
- ASP.NET-based authentication. The ASP.NET provider model supports custom identity systems. This mode allows Windows SharePoint Services to work with a variety of identity management systems, including Lightweight Directory Access Protocol (LDAP) and lightweight database identity management systems, and to use a variety of authentication methods, such as forms-based authentication and Web single sign-on for Web-based clients.
- Active Directory Federated Services (ADFS). ADFS is a new feature provided with Windows Server 2003 Release 2 that provides token-based authentication between organizations, or between separate Active Directory forests in the same organization. Windows SharePoint Services can be configured to use ADFS to provide authentication for SharePoint sites. ADFS requires persistent cookies, so ADFS integration works only for Web browsers and not for smart clients such as Microsoft Office, unless you first authenticate by using a Web browser.

Default Permission Levels

Site Group	Permission Level
Limited Access	Provides access to a specific list, document library, item, or document, without giving them access to the entire site.
Read	Read-only access to the Web site.
Contribute	Can create and edit items in existing lists and document libraries.
Design	Can create lists and document libraries and edit pages in the Web site.
Full Control	Full control of the scope.

Windows SharePoint Services includes five default permission levels. You can customize the permissions available in these permission levels (except for the Limited Access and Full Control permission levels) or add new permission levels to combine different sets of permissions.

Permission level	Description	Permissions included by default
Limited Access	Designed to be combined with fine-grained permissions to give users access to a specific list, document library, item, or document, without giving them access to the entire site. This permission level allows users to access shared resources on the Web site to access an item within the site. The Limited Access permission level cannot be customized or deleted.	View Form Pages, Browse User Information, Use Remote Interfaces, Open
Read	Allows read-only access to the Web site.	Limited Access permissions, plus: View Items, Open Items, View Versions, Create Alerts, Use Self-Service Site Creation, View Pages
Contribute	Allows users to create and edit items in existing lists and document libraries.	Read permissions, plus: Add Items, Edit Items, Delete Items, Delete Versions, Browse Directories, Edit Own User Info, Manage Personal Views, Add/Remove Private Web Parts, Update Personal Web Parts
Design	Allows users to create lists and document libraries and edit pages on the Web site.	Contribute permissions, plus: Manage Lists, Cancel Check-Out, Approve Items, Add and Customize Pages, Apply Themes and Borders, Apply Style Sheets
Full Control	Gives users full control of the scope.	All permissions

Default SharePoint Groups

Group Name	Default Permission Level
Site name Visitors	Read
Site name Members	Contribute
Site name Owners	Full Control
Site Collection Administrators	Contacts for the site collection with full control of all sites within the site collection; recipients for any administrative alerts
Farm Administrators	Control which users can manage server and server farm settings

With SharePoint groups, you manage sets of users, rather than individual users. SharePoint groups can be made up of many individual users, they can hold a single a Windows security group, or they can be some combination of the two. SharePoint groups confer no specific rights to the site; they are a means of containing a set of users. Depending on the size and complexity of your organization or Web site, or on your preference, you might want to organize your users into several groups, or just a few.

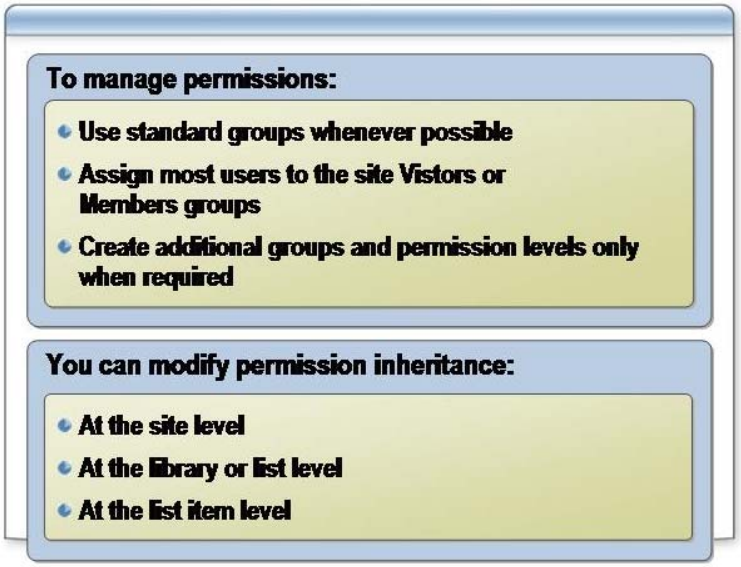
By default, the following SharePoint groups are created for sites in Windows SharePoint Services.

Group name	Default permission level
Site name Visitors	Read
Site name Members	Contribute
Site name Owners	Full Control

In addition, the following special users and groups are available for higher-level administration tasks:

- Site Collection Administrators. One or more users can be identified as Site Collection Administrators (either Primary or Secondary Site Collection Administrators). These users are recorded in the database as the contacts for the site collection, have full control of all sites within the site collection, and are the recipients of any administrative alerts (such as verifying whether the site is still in use). Generally, these users are identified when the site is created, but they can be changed as needed through the Central Administration or Site Settings pages.
- Farm Administrators. The Farm Administrators group is a SharePoint group that controls the users who can manage server and server farm settings. This group eliminates the need to add users to the local Administrators group for the server, or to the SharePoint administrators group that was used in Windows SharePoint Services 2.0. Farm Administrators have no access to site content by default; they must take ownership of the site to view any content. This group is used in Central Administration only and is not available for any sites.

Managing Permissions and Permission Inheritance



When you create your permission structure, it is important to find the balance point between ease of administration and control over specific permissions for individual items. It is also important to follow the principle of least privilege when it comes to authorizing access to the site. To manage permissions:

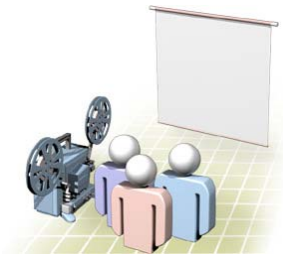
- Begin by using the standard groups (such as Members, Visitors, and Owners) and controlling permissions at the site level for the easiest administration experience.
- Make most users members of the site Visitors or site Members groups. By default, site members can contribute to the site, adding or removing items or documents, but they cannot change the structure of the site or change site settings or appearance.
- Create additional SharePoint groups and permission levels only if you need finer control over the actions that your users can take.

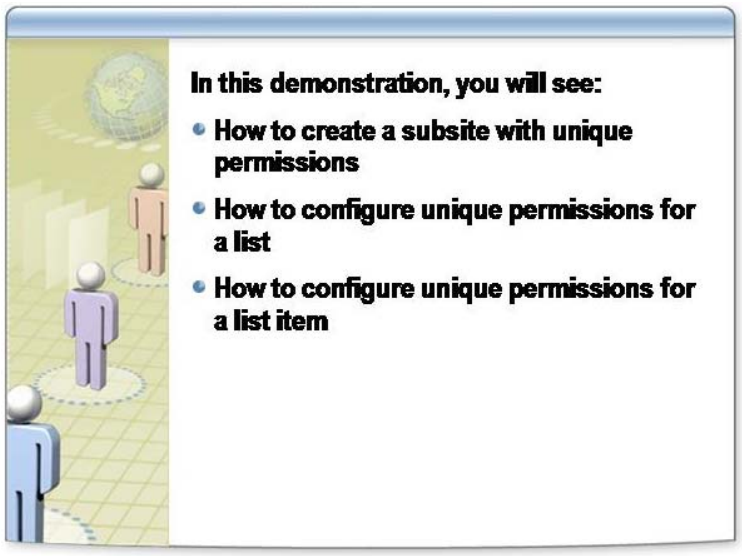
By default, permissions assigned at a site level are automatically inherited by subsites, lists, and libraries, and items within the lists or libraries. You can modify the default inheritance in the following ways:

- When you create a new subsite, you can configure unique permissions for the site. If you choose this option, you will create new site groups for that site. You can also modify permission inheritance at the site level after you create the site.
- You can configure permissions at the list or library level. When you choose to break the link between site permissions and the list or library permissions, you can apply the same permissions as the parent site level, or you can configure entirely new permissions. In either case, any changes that you make to the permissions at the parent site will not be inherited by the list or library.
- You can configure unique permissions at the list item level. The options for configuring these permissions are the same as for configuring list-level permissions.

Caution There is no way to view all of the fine-grained permissions for items within a site. This means that it is difficult to quickly ascertain who has permissions for specific items, and it is also difficult to reset any fine-grained permissions in bulk.

Demonstration 4: Configuring Permissions at the Site, List, and Item Levels



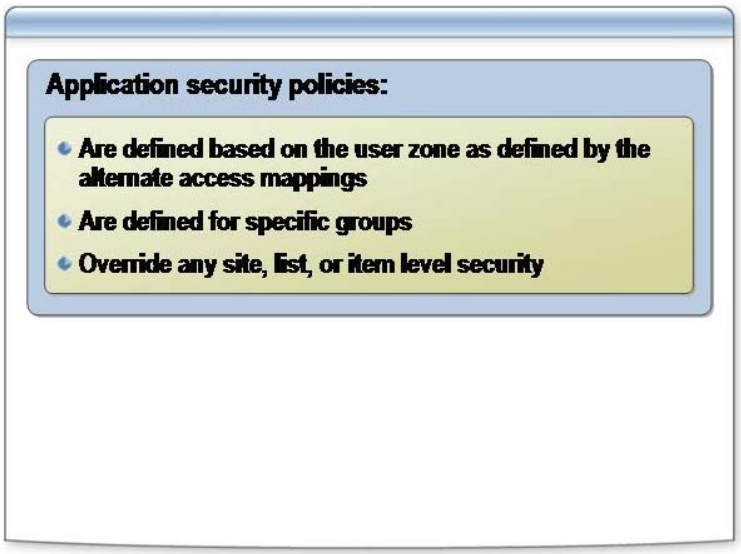


Windows SharePoint Services 3.0 uses many of the same concepts and procedures for assigning permissions that earlier versions used. However, Windows SharePoint Services 3.0 provides some additional features, particularly for item-level security.

In this demonstration, you will see:

- How to create a subsite with unique permissions.
- How to configure unique permissions for a list.
- How to configure unique permissions for a list item.

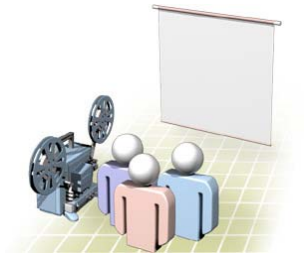
Application Security Policies

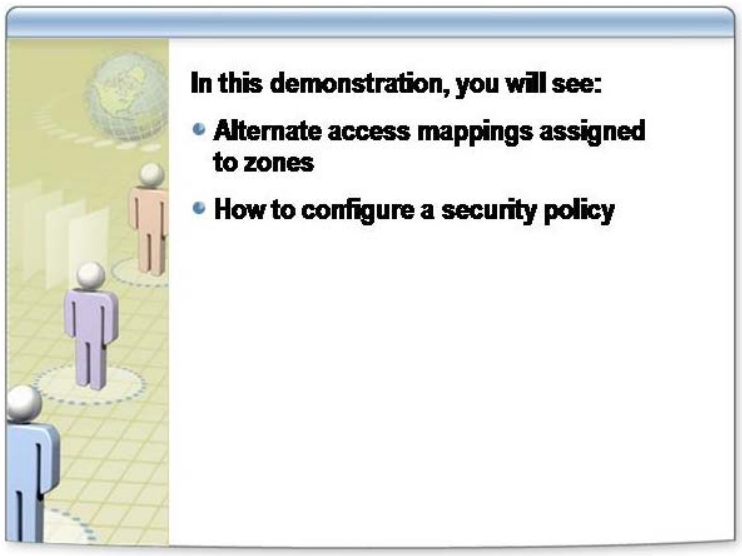


Windows SharePoint Services enables application security policies to provide another way to assign access to a SharePoint site. Application security policies provide the following features:

- The security policies are defined based on the zone from which the user connects to the SharePoint site. When you create a SharePoint application during setup, a Default zone is created. You can configure additional zones by creating alternative access mappings and assigning each mapping to a zone. For example, the URL http://*servername* is assigned to the Default zone. You can create a new access mapping using the URL http://*servername.domainname* and assign that URL to the Internet zone. You can then define different security policies for the Default and Internet zones.
- Security policies are also defined for specific groups. For example, you can configure a security policy that grants an Audit group read access to a SharePoint application. Or you can configure a policy that denies a specific group any access to a SharePoint application. If you want a security policy to apply to all authenticated users, you can create a security policy that will apply the Domain Users group.
- Security polices override any site-level, list-level, or item-level security configured on a Web application. If the security policy grants the Audit group read access to all sites, the members of the Audit group cannot be denied read access at the list or item level. Conversely, if a security policy denies write access to a Web site when any user connects to the site from the Internet zone, a member of the Site Owners group will have read-only access when connecting from that zone.

Demonstration 5: Configuring Security Policies



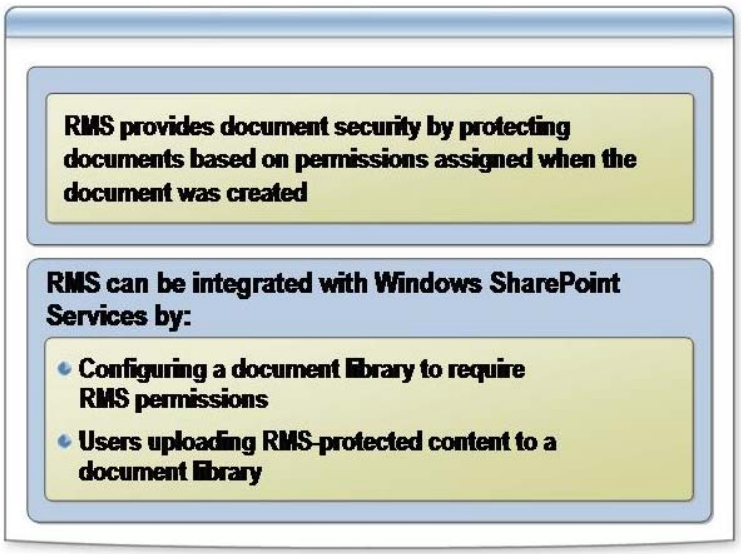


Windows SharePoint Services uses security policies to define the level of access that users have based on the zone from which they access the SharePoint site. With this option, you can configure different permissions for the same user, depending on the URL used by the user to access the Web site.

In this demonstration, you will see:

- Alternate access mappings assigned to zones.
- How to configure a security policy.

Windows SharePoint Services Integration with RMS



Windows SharePoint Services can also be integrated with Microsoft Windows Rights Management Services (RMS) to provide an additional layer of security. RMS is Microsoft's implementation of an information rights management (IRM) solution.

RMS uses an RMS server and RMS client infrastructure to protect documents. When a user creates a document or e-mail message, he or she can assign permissions to that document. These permissions are assigned to the content, and the content is encrypted. When another user tries to open the document, he or she must obtain the credentials required to open the document from the RMS server. If the user has appropriate permissions, he or she can open the document.

RMS can be integrated with Windows SharePoint Services document libraries. Site administrators can elect to protect all downloads from a document library with RMS. When a user attempts to download a file from the library, the server running Windows SharePoint Services verifies that the user has permissions to the given file and issues a license to the user that enables access to the file at the appropriate permission level. The file is then downloaded to the user's computer in an encrypted, rights-managed file format.

The user has access to the file only as long as his or her license remains valid. The site administrator can select one of two ways to determine when the license expires:

- Specify a date on which the file expires. After this date, the user can no longer access the file.
- Specify that the user must renew the license every set number of days. If the user does not connect to the server running Windows SharePoint Services to renew the license each time the specified number of days passes, he or she can no longer access the file.

A user can also upload RMS-protected documents to a Windows SharePoint Services document library. When another user tries to access the protected document, the user permissions are applied just as if the document had been accessed through a file share or as an e-mail attachment.

Additional Information For extensive information about deploying and managing Windows Rights Management Services, see "RMS Overview" at http://www.microsoft.com/resources/documentation/windowsserv/2003/all/rms/en-us/InitExp.mspx.

Upgrading to Windows SharePoint Services 3.0

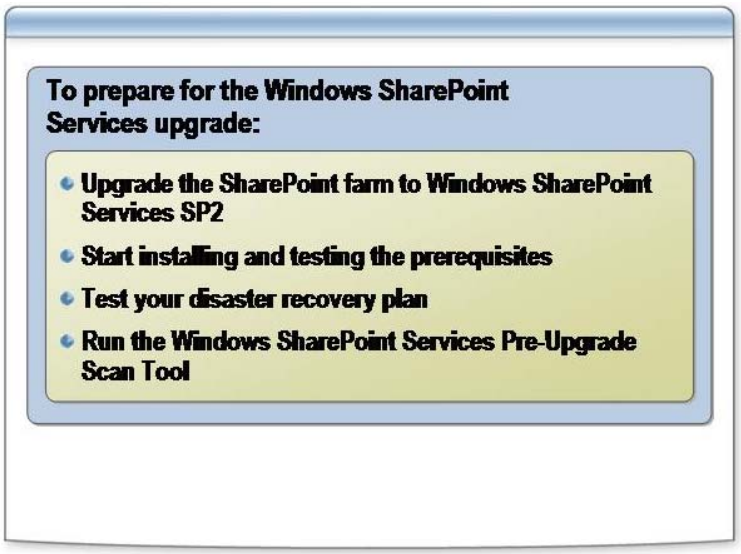
- Preparing to Upgrade to Windows SharePoint Services 3.0
- What Are the Upgrade Options?
- Upgrade Considerations

Windows SharePoint Services 3.0 enables three options for upgrading from earlier versions. As you prepare to upgrade your deployment, you must understand the options available, what is required to prepare for the upgrade, and which upgrade option is the best choice for your organization.

Specifically, this section will discuss:

- What you need to do to prepare for an upgrade.
- The options for upgrading.
- Considerations for choosing the best upgrade option.

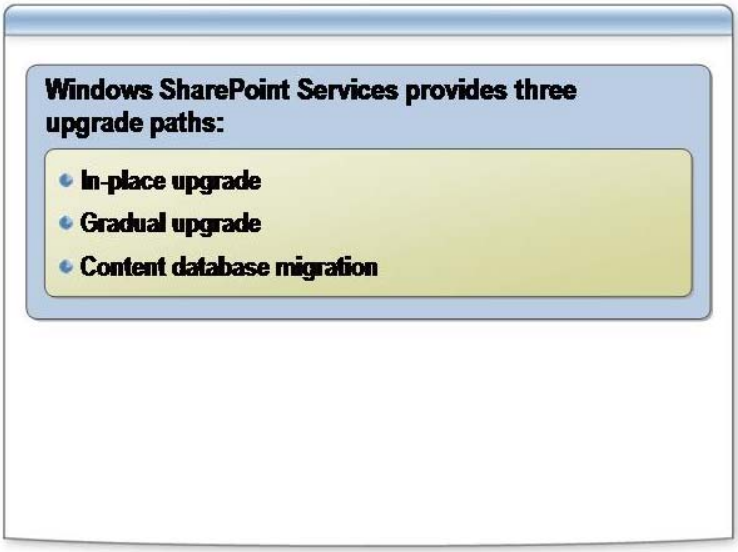
Preparing to Upgrade to Windows SharePoint Services 3.0



Upgrading a Windows SharePoint Services deployment to Windows SharePoint Services 3.0 requires significant planning and preparation. To prepare for the upgrade, you should:

- Upgrade the SharePoint farm to Windows SharePoint Services SP2. This upgrade is required: the farm must be running SP2 before the upgrade process starts.
- Start installing and testing the prerequisites. Windows SharePoint Services 3.0 requires ASP.NET 2.0 and Windows Workflow Foundation. If you have developed custom Web Parts using ASP.NET 1.1, test the Web Parts with ASP.NET 2.0.
- Test your disaster recovery plan. Before starting the upgrade, ensure that you can recover in the event of a disastrous failure. Run a full backup of your Windows SharePoint Services farm and test the recovery process.
- Run the Windows SharePoint Services Pre-Upgrade Scan Tool. This tool reports common issues that you must address, lists all site definitions in use, and updates Windows SharePoint Services lists so that they can be upgraded. This step is required before you can perform an upgrade. The Pre-Upgrade Scan Tool is installed with the product and can also be downloaded from the Microsoft Web site.

What Are the Upgrade Options?



Windows SharePoint Services 3.0 provides three options for upgrading from earlier versions. These options are:

- In-place upgrade. When you perform an in-place upgrade, you install Windows SharePoint Services 3.0 on a server running Windows SharePoint Services 2.0. This process updates existing databases and virtual servers. This option is the easiest upgrade path, but SharePoint sites will not be available during the upgrade. If you have multiple servers running Windows SharePoint Services, you can upgrade the servers sequentially.
- Gradual upgrade. In a gradual upgrade, you install Windows SharePoint Services on the same server that is running Windows SharePoint Services 2.0, but you choose the Gradual Upgrade option during installation. After completing the installation, you can create a new Windows SharePoint Services 3.0 Web application for each site. When you create the new Web applications, a new Windows SharePoint Services 3.0 content database is created for each existing database. When the content is upgraded, the data is moved to the v3 content database and the temporary database is deleted. Then the Windows SharePoint Services 2.0 sites are moved to a new URL created for them, and all client requests are redirected to the Windows SharePoint Services 3.0 sites. At the end of the upgrade process, Windows SharePoint Services 2.0 and Windows SharePoint Services 3.0 are both running and available. When all sites have been upgraded, you can confirm that upgrade is complete and uninstall Windows SharePoint Services 2.0 if you no longer need it.
- Content database migration. In a content database migration, you upgrade the Windows SharePoint Services 2.0 sites into a separate farm. To complete the upgrade, you create a new Windows SharePoint Services 3.0 farm, and then create the required Web applications. Then attach the Windows SharePoint Services 2.0 content to the Windows SharePoint Services 3.0 applications. When you do this, the database content is upgraded to Windows SharePoint Services 3.0.

Upgrade Considerations

Upgrade Approach	Advantages	Disadvantages
In-place	• Easiest upgrade option • Uses existing hardware	• The farm is offline during the upgrade • No option to revert back to V2
Gradual	• Enables a multi-phase upgrade • V2 is available to revert • Uses existing hardware	• Redirect of V2 URL during upgrade may fail for clients • Memory & storage intensive
Content database migration	• V2 is not affected by the migration • Creates a new farm on new hardware	• More complex • Involves many manual steps with a higher risk of error

Each of the upgrade paths to Windows SharePoint Services 3.0 includes some advantages and disadvantages. The following table summarizes these.

Upgrade approach	Advantages	Disadvantages
In-place	• Easiest upgrade option • Uses existing hardware	• The farm is offline during the upgrade • No option to revert back to version 2.0
Gradual	• Enables a multi-phase upgrade • Version 2.0 is available during and after the upgrade to revert • Uses existing hardware	• Redirect of version 2.0 URL during upgrade could fail for clients • Memory and storage intensive
Content database migration	• Version 2.0 is not affected by the migration • Creates a new farm on new hardware	• More complex • Involves many manual steps with a higher risk of error

Session Summary

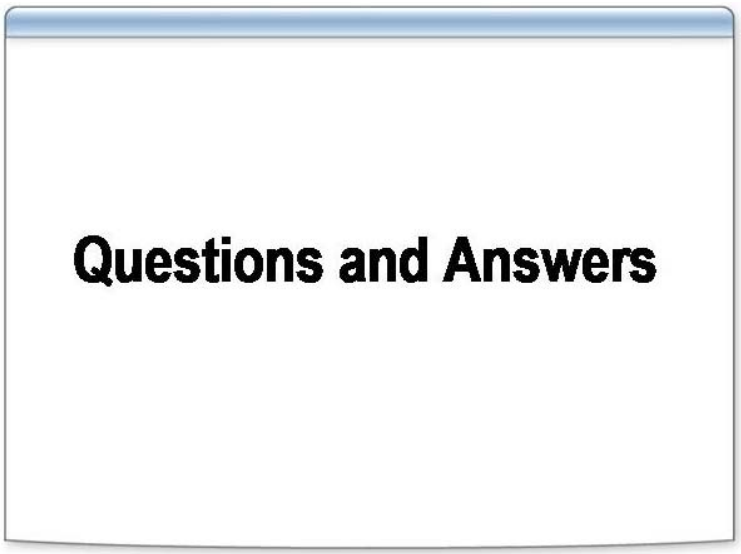
- Deploying Windows SharePoint Services
- Administering Windows SharePoint Services
- Managing Windows SharePoint Services Sites
- Managing Windows SharePoint Services Security
- Upgrading to Windows SharePoint Services 3.0

Many of the Windows SharePoint Services 3.0 implementation and management tasks are similar to the tasks performed in earlier versions. However, the Windows SharePoint Services management interface has changed significantly. Also, Windows SharePoint Services includes several important new configuration options.

In this session, the following topics were discussed:

- Deploying Windows SharePoint Services. This section provided an overview of the deployment options for Windows SharePoint Services. One of the unique options in Windows SharePoint Services is that you can configure the search and indexing role on a separate computer. This section also provided an overview of the requirements and process for installing Windows SharePoint Services.
- Administering Windows SharePoint Services. This section provided an overview of the administrative pages for managing Windows SharePoint Services. The section focused on the Central Administration site and the Operations and Application Management pages, in addition to the new configuration options available in Windows SharePoint Services.
- Managing Windows SharePoint Services sites. This section provided an overview of the process for creating new SharePoint sites and customizing them by adding or removing Web Parts. This section also discussed the new search features available in Windows SharePoint Services.
- Managing Windows SharePoint Services security. This section provided an overview of the security features available in Windows SharePoint Services. It described how to configure security in Windows SharePoint Services, and it emphasized options such as assigning permissions to lists, libraries, and list items, and application security policies.
- Upgrading to Windows SharePoint Services 3.0. This section provided an overview of the upgrade options for upgrading from Windows SharePoint Services 2.0 to Windows SharePoint Services 3.0. The section described what is required to prepare for the upgrade and how to choose an upgrade option.

Questions and Answers



Clinic Evaluation

Your evaluation of this clinic will help Microsoft understand the quality of your learning experience.

Please work with your training provider to access the clinic evaluation form.

Microsoft will keep your answers to this survey private and confidential and will use your responses to improve your future learning experience. Your open and honest feedback is valuable and appreciated.