STUDY GUIDE

Microsoft

70-631

TS: Windows SharePoint Services 3.0

Michael W. Krout

ExamForce

About the Author

Michael W. Krout (MCTS, MCSE, MCT) is an IT consultant and trainer with over 21 years of experience with technology. In addition he has owned and operated independent consulting and training firms, serving such prestigious clients as the U.S. Military and the Pentagon. In addition, he has hands-on experience with Microsoft products, dating back to DOS, as a programmer and database engineer, Windows server experience since NT version 3.51 and even Novell and IBM mainframe. These skills, in addition to university level instruction, educational content development and authoring and real world “know-how”, stand as credits to his knowledge and mastery of technical subjects.

Additional Contributor(s)

Brianne Havlik (A+, MCP)

About the Exam

There are six major topic areas that make up this exam:

- Deploy Windows SharePoint Services 3.0 (WSS)
- Monitor Windows SharePoint Services
- Configure Security for Windows SharePoint Services
- Administer Windows SharePoint Services
- Manage Customization
- Configure Network Infrastructure for Windows SharePoint Services

This guide will walk you through all the skills measured by the exam, as published by Microsoft.

Objectives

Chapter 1: Deploy Windows SharePoint Services 3.0 (WSS)

Configure WSS server roles.

Configure WSS topology.

Create WSS namespace.

Upgrade WSS 3.0 from WSS 2.0.

Install WSS.

Chapter 2: Monitor Windows SharePoint Services

Maintain storage performance.

Configure centralized monitoring for WSS.

Configuring performance monitor.

Monitor logs.

Chapter 3: Configure Security for Windows SharePoint Services

Configure Web application authentication.

Configure a Web application for SSL.

Configure NTLM or Kerberos authentication.

Configure roles and site permissions.

Implement access policies.

Manage database permissions.

Configure Information Rights Management (IRM).

Chapter 4: Administer Windows SharePoint Services

Configure site settings.

Manage Central admin.

Administer Windows SharePoint Services by using STSADM.

Configure backup and restore (disaster/recovery).

Chapter 5: Manage Customization

Configure master page.

Customize pages by using SharePoint Designer.

Configure code access security.

Chapter 6: Configure Network Infrastructure for Windows SharePoint Services

Configure names resolution.

Configuring Network Load Balancing (NLB).

Configure WSS to support perimeter network.

Configure Internet Security and Acceleration Server (ISA).

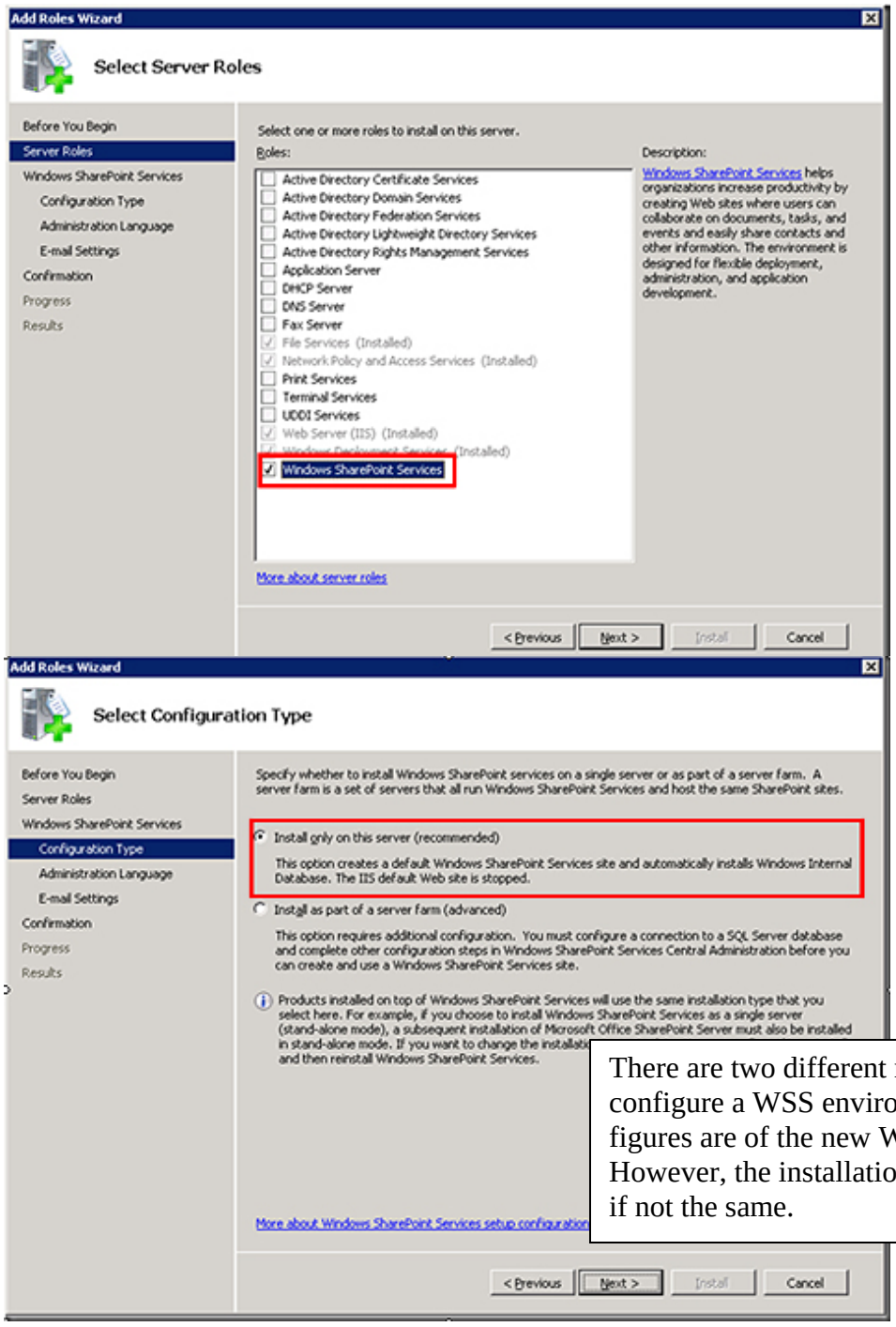
Chapter 1 - Deploy Windows SharePoint Services 3.0 (WSS)

Quick Jump To:

- Chapter 1
- Chapter 2
- Chapter 3
- Chapter 4
- Chapter 5
- Chapter 6

Configure WSS server roles.

There are several ways to configure the WSS Services 3.0. The platform being used designates the process of installing the services. The server may be installed by downloading the WSS 3.0 file for Windows 2003 server platform. The WSS 3.0 is also available as an add on role to the Windows 2008 server.



There are two different roles that can be used to configure a WSS environment. NOTE: These figures are of the new Windows 2008 Servers. However, the installation steps are very similar, if not the same.

Configure WSS topology.

The following are the different types of topologies:

- **Single server**, Windows Microsoft SQL Server™ 2005 Express (SSE) or SQL WSS databases, search service, and Web Front End (WFE) are installed on one server. This is the basic WSS configuration, and it is easy to install and manage. This topology can be scaled to meet the growing demands of an organization. This topology is recommended for:

    - Small businesses that want to take advantage of the WSS features.
    - A single team or department within a medium-to-large organization.
    - In a test environment such as on a VPC to try out the technology before putting it out to production

- **Small farm** When looking at the small farm topology, components are scaled to two tiers. Scaling to a small farm is for when the expected load exceeds the capacity of a single server or to utilize the advantages of using a dedicated SQL Server. For example, there can be two servers, Server A and Server B. Server A contains Web Front End (WFE) and search services. Server B contains SQL WSS databases. A WFE maybe added to handle additional usage. This topology is recommended for:

    - Teams whose needs scale beyond the single-server implementation.
    - Organizations that require IT-managed databases.

- **Medium farm.** When looking at the Medium Farm topology, components are scaled to three tiers and one database. Multiple network load-balanced Web Front End's (WFE)'s handle increasing user demands and accommodate larger volumes of data. SQL can be a single-box or a SQL failover cluster. An example of this would be three servers: Server A, Server B, and Server C. Server A and B contain network load-balanced WFEs and Server C contains SQL Server or SQL cluster WSS databases. This topology is recommended for:

    - Scaling beyond a single team or department.
    - Improving search and indexing performance.
    - Accommodating a large number of users and meeting database storage or utilization requirements.
    - Implementing extranets.

- **Large farm.** The last topology is the Large Farm. Components are scaled to three tiers and multiple dedicated databases. In a large farm, additional network load-balanced Web Front End's (WFE)'s are deployed online when needed to meet the increasing load. The configuration, content, and administration content databases are distributed to separate SQL servers or SQL Server clusters. This deployment can be scaled up as much as needed to meet the load and disk space requirements. For example, there can be three servers: Server A, Server B, and Server C. Server A and B contain network load-balanced Web Front End's (WFE)'s and Server C contains SQL servers or SQL clusters with configuration, content, and administration content databases on separate servers or clusters. This topology is recommended for:

    - Scaling across all departments within an organization.
    - Providing the maximum performance for the database components, and consequently, the performance of the entire farm.
    - Storing a large amount of data as compared to other topologies.
    - Heavily utilized extranet implementations where database availability is critical.

Create WSS namespace.

Windows SharePoint Services, which is available as both a download and also within Windows 2008, is able to be used in different environments. These environments can range from small department sized networks to large enterprise type farms.

The URL namespace in Windows SharePoint Services (3.0) running on Windows 2003 or Windows 2008 is based on the site that is created. There are several types of sites that you can create. These include domain-named sites (http://examforce or http://certs.examforce.com) or subfolder-named sites (http://server/sites/mysite or http://examforce.com/exams/microsoft). Domain-named sites provide the creation of more simple URLs, while subfolder-named sites are typically used to show the hierarchy or sites within an organization. The type of namespace should be determined by the organization's needs.

Once the type of site(s) has been established the namespace configuration must also be decided. Namespace configurations include:

One domain-named site per virtual server

The definition of a virtual server is another web server. When a user accesses a web server they are accessing through a unique IP address. Another characteristic in WSS 3.0 is that the virtual server will have a separate content database. This type of server may be used to support a special purpose.

Multiple subfolder-named sites per virtual server

Another definition for this type of site would be an application. A web application can share the same content database as the virtual server. The difference is that the application will use its own memory space.

One domain-named site and multiple subfolder-named sites per virtual server

This type of configuration uses the same content database but has several applications housed on the virtual server.

Two virtual servers hosting the same content

In this scenario, the same content databases are shared between in intranet and the extranet. The difference is that there are different settings on the underlying IIS server.

Multiple domain-named sites per virtual server

In this scenario, there are several Web servers with different URL's pointing to the web sites. The content databases may be different or they can be the same.

Upgrade WSS 3.0 from WSS 2.0.

There are three methods available when upgrading an existing Windows SharePoint Server implementation. These include: in-place, gradual or by doing a database migration. The easiest of the upgrades is the in-place upgrade which may be used with all versions of Windows SharePoint Server.

A gradual upgrade would be used if an organization is retraining its staff on the new changes and planning for the new implementation. When performing an in-place and gradual upgrade this done on the same hardware. When completing a migration the content is moved from one server to another.

In-place upgrade:

- Current version is overwritten by the new version.
- The information that was on the server is replaced by the newer version.
- During the upgrade clients will not be able to connect to the server or the server farm depending on what is being updated.
- The URL's that clients use do not change.

Gradual upgrade:

- During this type of upgrade the information is replaced only when the administrator deems it necessary to do so.
- Clients can still access the site during this type of upgrade.
- The only impact on the environment is that users that need access to the sites that are being upgraded may see some unavailability.
- Once the upgrade has finished the URL's are pointed to the new content sites.

Database Migration:

- This is fundamentally the same as an in-place upgrade, except the process is performed on a copy of the content.
- The content databases are added to a new server or server farm.
- Once the databases are attached to the server or server farm an in-place upgrade takes place.

Install WSS.

This information applies to Microsoft Windows Server 2003. When using Windows Server 2008 environment, the steps to install and configure Internet Information Services (IIS), the Microsoft .NET Framework version 3.0, and Windows SharePoint Services 3.0 vary.

It is possible to easily and quickly publish a SharePoint site by deploying Windows SharePoint Services 3.0 on a single server. A stand-alone configuration is useful for evaluating Windows SharePoint Services 3.0 features and capabilities such as collaboration, document management, and search. It is also useful when deploying a small number of Web sites to minimize administrative cost.

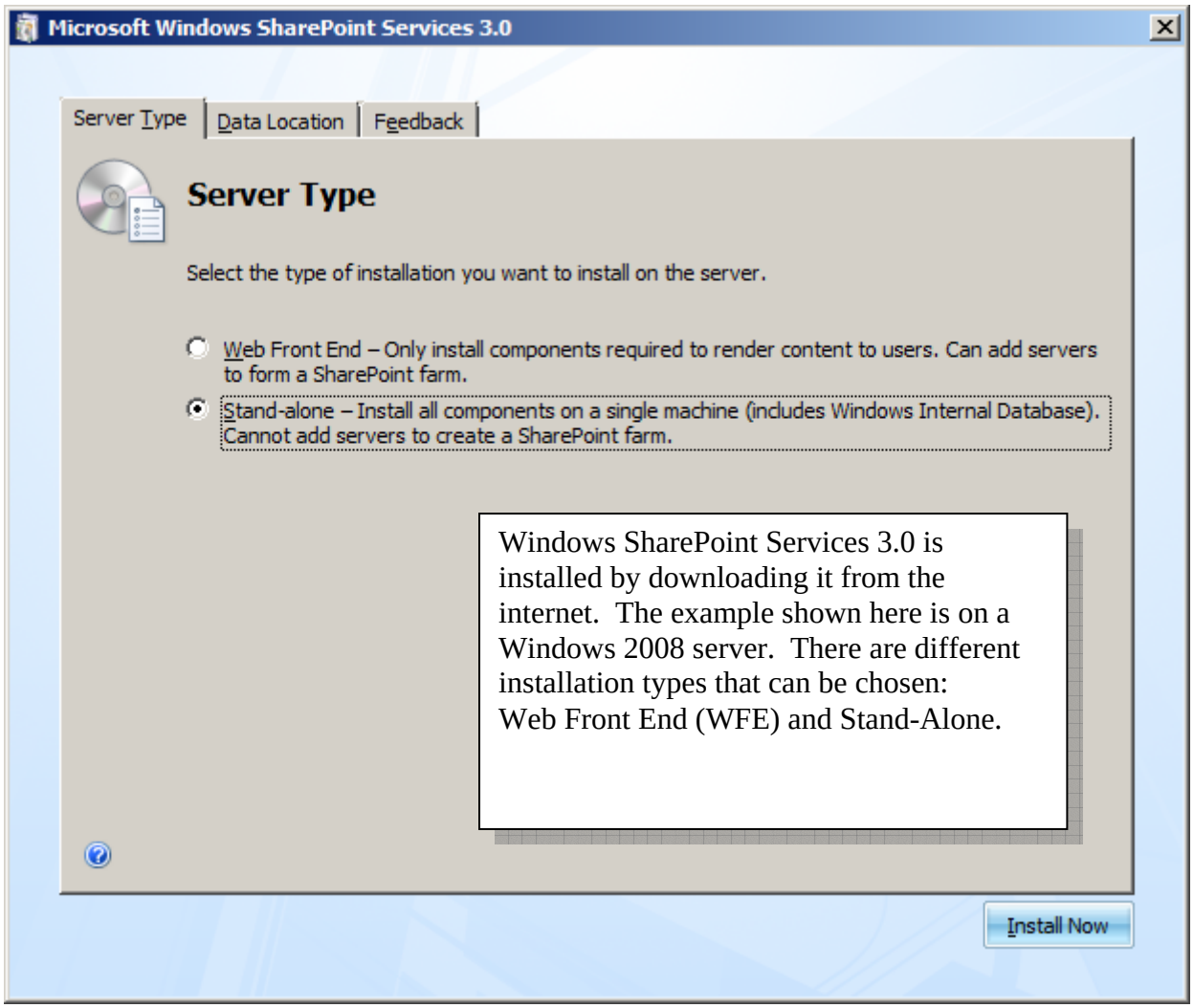
When deploying Windows SharePoint Services 3.0 on a single server using the default settings, the Setup program automatically installs the Windows internal Database and uses it to create the configuration database and content database for your SharePoint sites. This uses SQL Server technology as a relational data store for Windows roles and features only, such as Windows SharePoint Services, Active Directory Rights Management Services, UDDI Services, Windows Server Update Services, and Windows System Resources Manager. Additionally, Setup installs the SharePoint Central Administration Web site and creates the first SharePoint site collection and site.

Before installing and configuring SharePoint Services 3.0, be sure that any servers meet the required hardware and software minimums.

Component	Minimum	Recommended
Processor	2.5 gigahertz (GHz)	Dual processors that are each 3 GHz or faster
RAM	1 gigabyte (GB)	2 GB
Disk	NTFS file system–formatted partition with a minimum of 3 GB of free space	NTFS file system–formatted partition with 3 GB of free space plus adequate free space for your Web sites
Drive	DVD drive	DVD drive or the source copied to a local or network-accessible drive
Display	1024 × 768	1024 × 768 or higher resolution monitor
Network	56 kilobits per second (Kbps) connection between client computers and server	56 Kbps or faster connection between client computers and server

These are the steps required to install WSS 3.0:

1. Configure a server as a web server
2. Install the Microsoft .Net 3.0 Framework
3. Enable ASP.Net 2.0
4. Install and configure Windows SharePoint Services 3.0 with Windows Internal Database
5. Post Install Tasks
    a. Configure incoming e-mail settings
    b. Configure outgoing e-mail settings
    c. Configure antivirus protection settings



Windows SharePoint Services 3.0 is installed by downloading it from the internet. The example shown here is on a Windows 2008 server. There are different installation types that can be chosen: Web Front End (WFE) and Stand-Alone.

Chapter 2 - Monitor Windows SharePoint Services

Quick Jump To:

- Chapter 1
- Chapter 2
- Chapter 3
- Chapter 4
- Chapter 5
- Chapter 6

Maintain storage performance.

One issue developers encountered with WSS 2.0 was that several features supported with document libraries were not supported with lists. This included versioning and events. However, with WSS 3.0 these features are now supported in addition to several new features such as exposing data though automatic RSS feeds. Another new feature introduced is column-indexing, which alleviates performance issues. It is possible to add an index to any column on a document library or list settings page. While this does not create a physical index in SQL it creates a table with the ID of the item and the value of the indexed column. This is then used to improve performance or return data, especially when a filter is used. WSS 3.0 also enables developers to have more control over field rendering and validation by using new extensible field types. These fields can be created using Visual Basic or C#. Extensible field types can use ASP.NET user controls.

Another advancement in WSS 3.0 are custom site columns, which are a reusable definition that can be applied across several lists. They define the name for a column, its field type, and its various characteristics such as default value, formatting, and validation. Custom site columns can be used to define the structure of user-defined lists. Updating the site column in one place will affect every other list where the column has been used. By defining a site column at the top level of a site it is inherited to all child sites. Site columns also provide the ability to more easily perform field lookups across sites.

WSS 3.0 introduces a powerful new storage mechanism called content types, which is a flexible and reusable WSS type that defines the shape and behavior for an item.

Configure centralized monitoring for WSS.

One of the utilities that we can use is Microsoft Operations Management (MOM) 2005, and the Microsoft Office SharePoint Server 2007 Management pack. The MOS 2007 Management pack assists in detecting bottlenecks with in the server. It can be used to detect abnormalities in the server and detect things before they happen. This will allow the creation of a proactive stance on server monitoring, and allows administrators to take preventative and corrective action to problems not only when they occur and but beforehand.

Configuring performance monitor.

The best way to monitor WSS 3.0 is by using the Microsoft Operations Manager 2007. This utility has predefined settings for all of the resources that are going to be used by the WSS 3.0 server. Remember that this is actually using a web server. The four subsystems include:

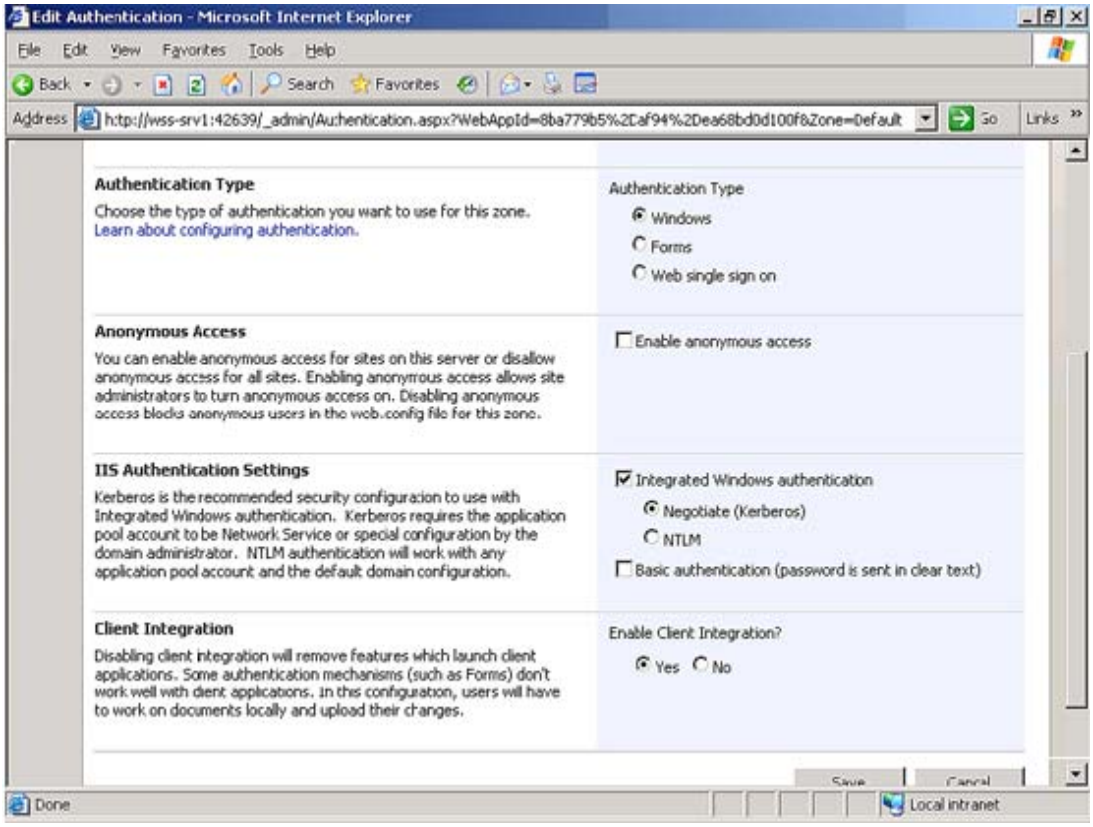
1. Memory
2. Disk Subsystem – remember to measure the physical disk and not the logical
3. Network
4. CPU

Monitor logs.

Monitoring logs allows administrators to access the performance of a server. By evaluating the Application log it is possible to study the trends that are taking place on the server. The best way to monitor logs is by centralizing access to the logs. This can be implementing by the Microsoft Operations Manager (MOM) 2007 along with the WSS management pack. This will allow easy control of what is seen on the logs and provide repair of any malfunctioning parts of the WSS environment.

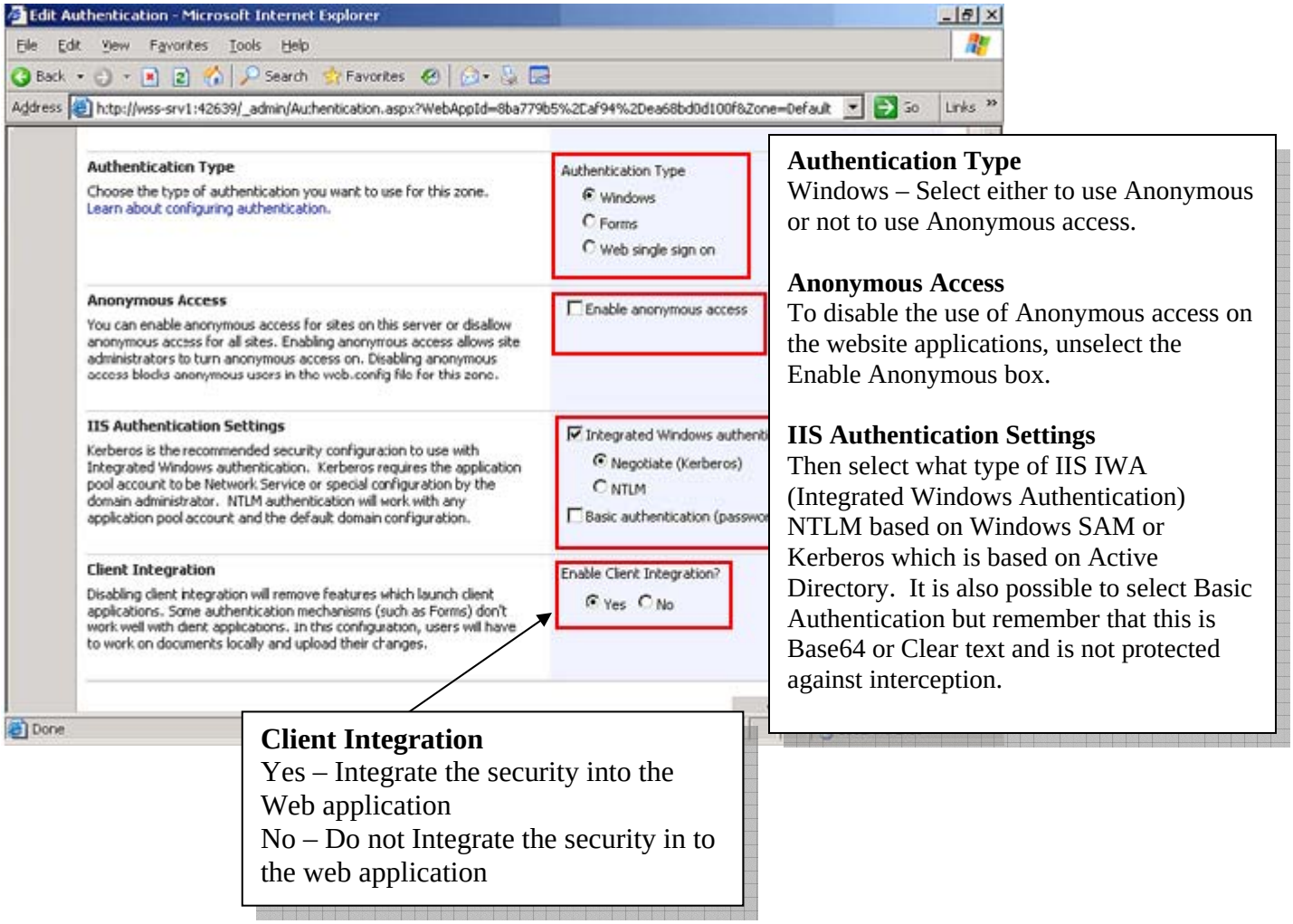
Chapter 3 - Configure Security for Windows SharePoint Services

Configure Web application authentication.



The following are example steps for configuring authentication:

1. Navigate to the Authentication Providers page.
2. Click Application Management.
3. In the Application Security section click Authentication providers.
4. This will bring up the Authentication Providers page. Click the zone name that you want to configure.
5. On the edit Authentication Page click one of the following:



Authentication Type
Windows – Select either to use Anonymous or not to use Anonymous access.

Anonymous Access
To disable the use of Anonymous access on the website applications, unselect the Enable Anonymous box.

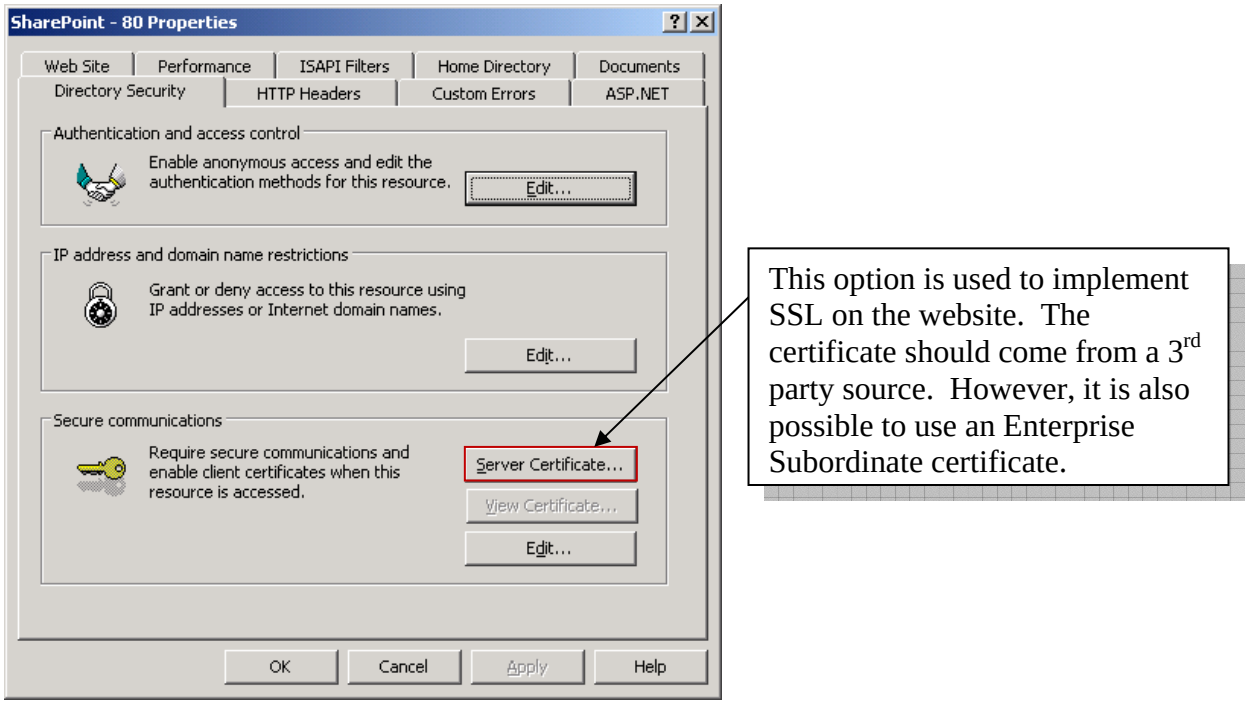
IIS Authentication Settings
Then select what type of IIS IWA (Integrated Windows Authentication) NTLM based on Windows SAM or Kerberos which is based on Active Directory. It is also possible to select Basic Authentication but remember that this is Base64 or Clear text and is not protected against interception.

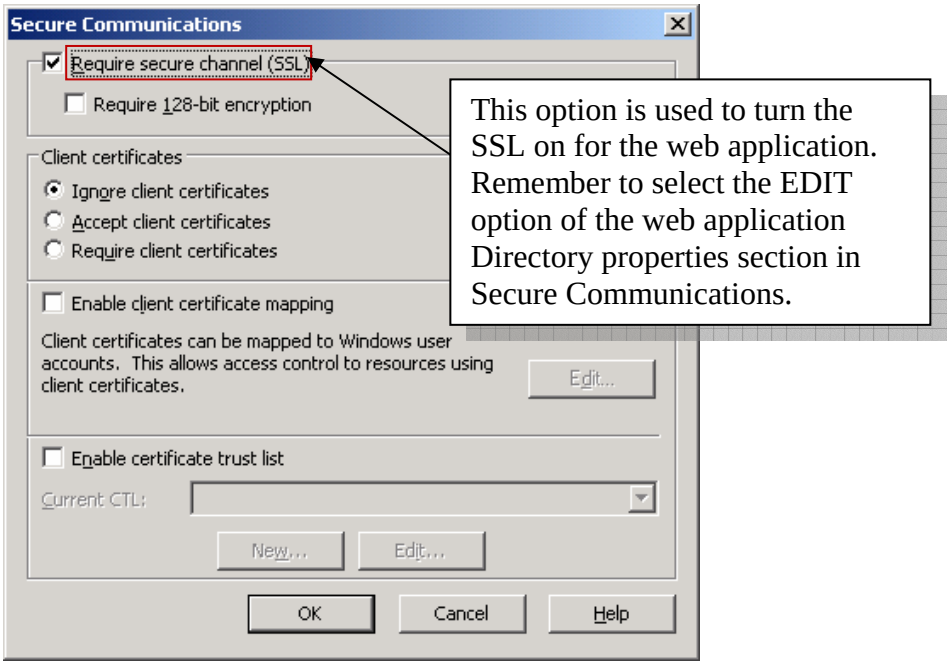
Client Integration
Yes – Integrate the security into the Web application
No – Do not Integrate the security in to the web application

Configure a Web application for SSL.

SSL (Secure Socket Layer) is used to protect a website. Using SSL will protect the transmission of information over the internet. SSL uses a two step encryption process. One key is used to encrypt data and is known as the Public Key. The other key is used to decrypt data and is known as the private or secret key. This key is only available to the person or entity that is receiving the information. This can implemented this on both websites and email messages. The port that is associated with the SSL protocol for HTTP is HTTPS or 443.

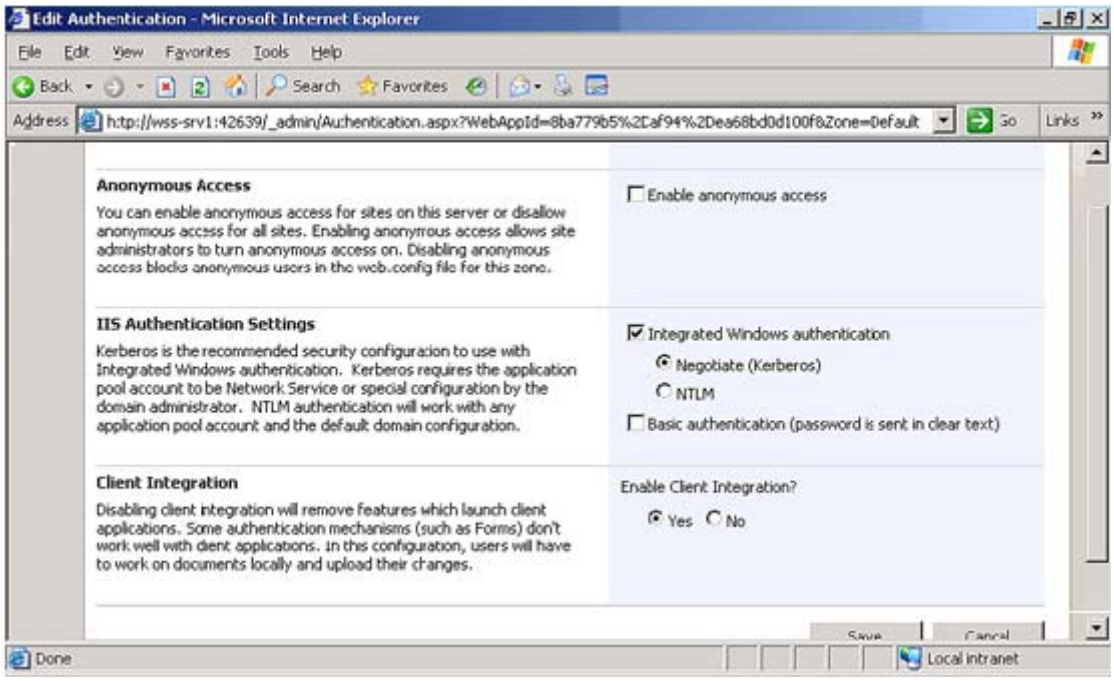
To implement SSL for a web application the first step is to first secure the web server. The Internet Information Systems (IIS) Management tool is used to accomplish this task.





Once a server certificate has been implemented, it is possible to do the same for the applications that should be protected with SSL. From that point forward clients will access the web application by using https (port 443).

Configure NTLM or Kerberos authentication.



Microsoft Windows Integrated Authentication supports the following two protocols that provide challenge/response authentication:

- NTLM

  NTLM or NT LAN Manager is a protocol that is used with the SAM (Security Account Manager) and deals with encrypting passwords and usernames over the network. This type of network is NT based, not Active Directory based which uses Kerberos.

- Kerberos

  The Kerberos protocol is based on a ticketing system. Kerberos works by having a KDC (Key Distribution Center). The KDC is responsible for handing out authorizations. These authorizations are referred to as tickets. Tickets give clients access to resources. Access is granted based on the DACL ((Discretionary Access Control List) which can be thought of as similar to a guest list. The KDC within a Windows 2000 or above network is the DC (Domain Controller).

Configure roles and site permissions.

The security of the WSS 3.0 environment is similar to Microsoft SQL Server©. Microsoft SQL Server© uses role based authentication method for securing the database. Roles work the same as groups within the Windows environment. However, WSS 3.0 works slightly different from SQL Server. WSS 3.0 is based on a two-tier administrative model which allows the centralization of configuration and management tasks. With this model it is possible to delegate administration and assign it to the appropriate users or groups within an organization. By being part of a role a user inherits the rights of that role. More efficient control of the environment is accomplished by assigning the roles within each tier.

The two tiers are featured below:

- Tier 1: Farm-level administrators
    - Administrators in this tier are top-level administrators and have overall permissions for all servers in the server farm. Members of this role also inherit these privileges.
- Tier 2: Site collection administrators
    - Members of this role have Full control permissions on their sites.

WSS 3.0 Tiered administration enables roles to be assigned to many different groups within the operating environment. When dealing with delegating keep in mind the type of administration model that is being used:

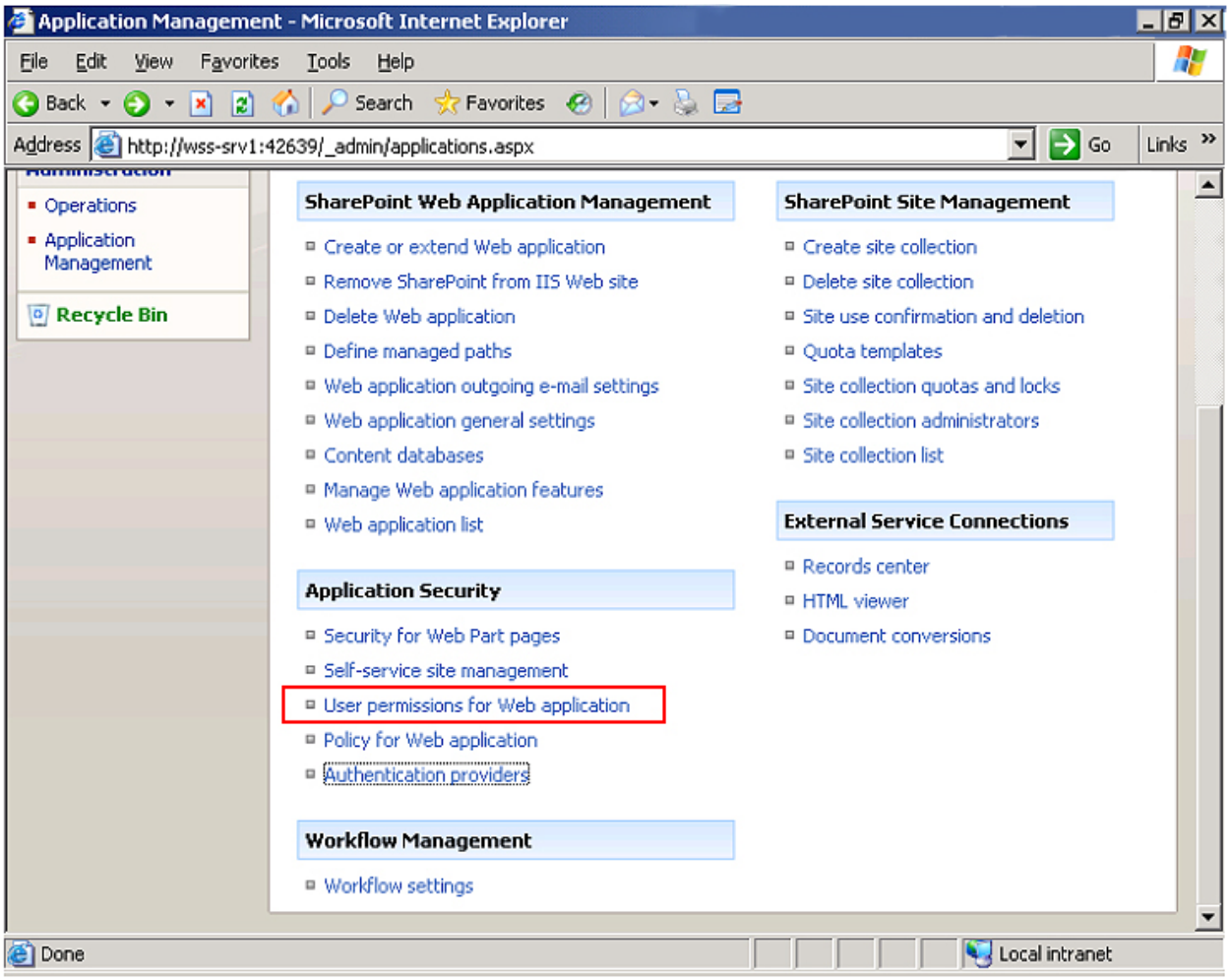
- Centralized – Keep everything tightly controlled by a few key people.
- Decentralized – This is used in a departmental type of environment.

Implement access policies.

When implementing policies there are five elements to keep in mind:

Individual user permissions

What is granted to the individual? Controlling what individuals can do within the site is accomplished by modifying the permissions through Application Management and the Application Security Section.



Permission Level

These are the predefined set of permissions:

- Limited Access
- Read
- Contribute
- Design
- Full Control

User

The user is the person or entity requesting access to resources. For a user to have access to the environment they must have a user account and password.

Group

A group is a collection of users that have similar responsibilities. Permissions should be applied to a group instead of a user. You can use the acronym AGLP (Account Globals Locals Permissions). Put a user account into a group and assign permissions to the group.

Securable Object

This can be a web site or resource. If the object needs to be protected then the object is known as securable.

WSS 3.0 has five permission levels by default. It is possible customize the permissions available in these permission levels (except for the Limited Access and Full Control permission levels). It is also possible to create new permission levels that contain specific permissions based on specific organizational needs. Below lists the details regarding the five default permission levels:

Permission level	Description	Permissions included by default
Limited Access	Gives user access to areas that such as documents etc.	View Application Pages, Browse User Information, Use Remote Interfaces, Use Client Integration Features, Open
Read	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	Can create and edit items in existing lists and document libraries.	Read permissions plus: Add Items, Edit Items, Delete Items, Delete Versions, Browse Directories, Edit Personal User Information, Manage Personal Views, Add/Remove Personal Web Parts, Update Personal Web Parts
Design	Can create lists and document libraries and edit pages in the Web site.	Contribute permissions plus: Manage Lists, Override Check Out, Approve Items, Add and Customize Pages, Apply Themes and Borders, Apply Style Sheets
Full Control	Full control of the scope.	All permissions

Manage database permissions.

WSS 3.0 uses SQL Server 2005. To modify Database permissions use the SQL Server 2005 management tools.

Configure Information Rights Management (IRM).

Piracy has been a big debate among recording artists and regarding the production of electronic media. To protect against illegal access or use of this material, Microsoft has implemented the Information Rights Management Server. This server enables companies to protect and limit the actions that user can take on files that clients have downloaded from their WSS 3.0 lists or libraries. Information Rights Management (IRM) encrypts the downloaded information and controls who can access the information. When users located on the allowed list attempt to download information programs such as Windows Media Services will be accessed to decrypt the information for use. If protected information is accessed without authorization the connection will be blocked from access.

IRM can be used on WSS 3.0 to protect information from being accessed through lists and libraries within WSS 3.0. You can apply this to part of a library or to the whole library. When information is added to the library, this information will be protected by default.

IRM provides the following benefits:

- Prevents unauthorized copying, modifying, printing, faxing or copying and pasting of protected information.
- Prevents copying using Print Screen.
- Prevents sending protected information through email.
- Sets a time limit on the amount of time information can be used
- Enforces policies that are set by the organization regarding the use of protected information

IRM cannot protect in the following circumstances

- Attack from malicious code such as Trojan Horses, Viruses, Adware/Spyware
- Manual copying of information and retyping of information
- Photos that are displayed on the screen
- Information captured using a 3rd Party utility such as ClipIt

Chapter 4 - Administer Windows SharePoint Services

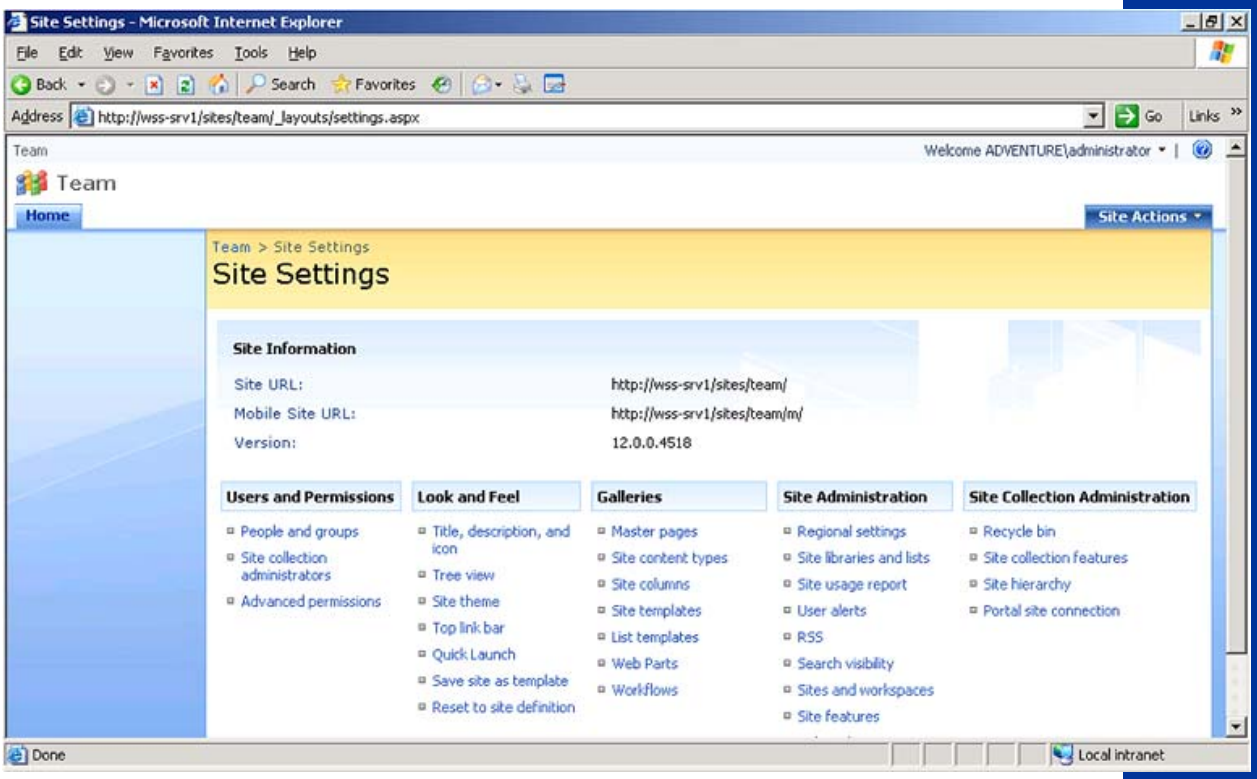
Quick Jump To:

- Chapter 1
- Chapter 2
- Chapter 3
- Chapter 4
- Chapter 5
- Chapter 6

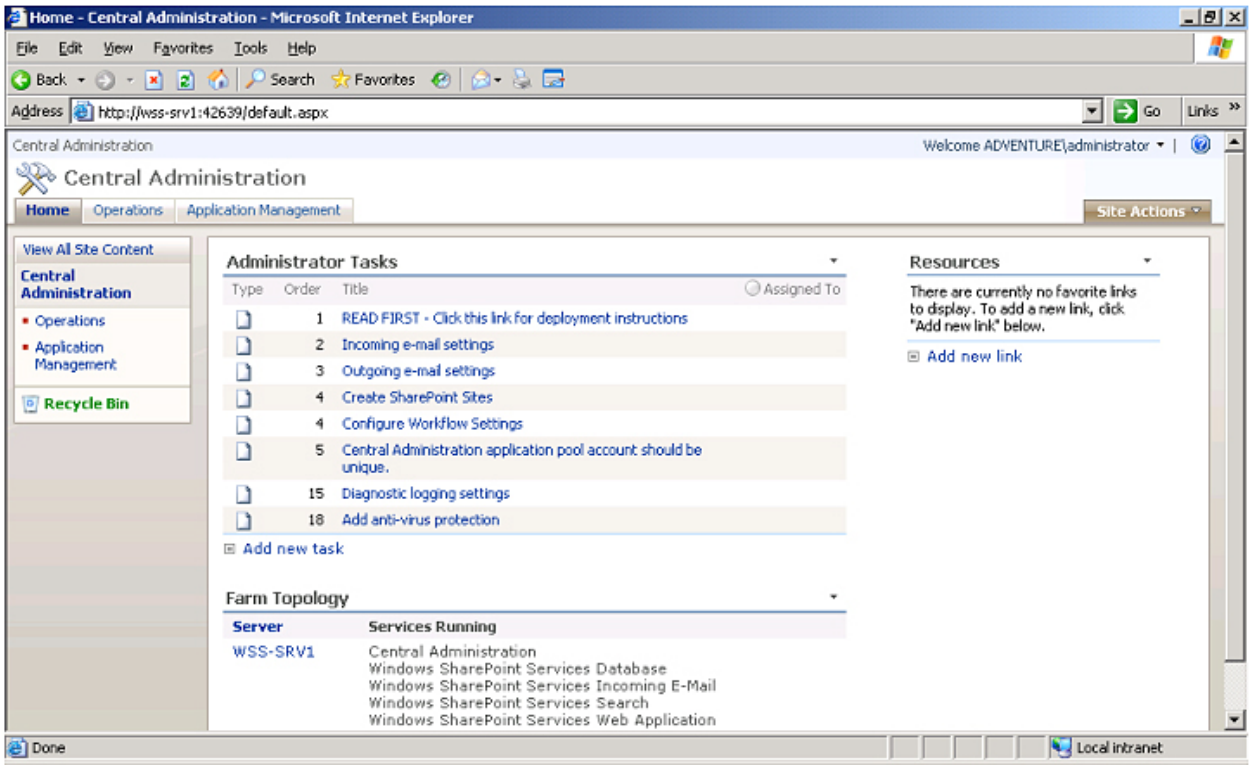
Configure site settings.

All of the settings for the sites are located under the site settings option. As shown in the image below, there are many settings that can be configured:

- Users and Permissions
- Look and Feel
- Galleries
- Site Administration
- Site Collection Administration



Manage Central admin.



The Central Administration page allows the management of all aspects of the WSS 3.0 environment. There are two sections:

- Operations
  - Topology and Services
  - Security Configuration
  - Logging and Reporting
  - Global Configuration
  - Backup and Restore
  - Data Configuration
- Application Administration
  - SharePoint Web Application Management
  - Application Security
  - Workflow Management
  - SharePoint Site Management
  - External Service Connections

Administer Windows SharePoint Services by using STSADM.

Stsadm is the command line tool included in Windows SharePoint Services 3.0. This tool allows for the administration of Windows SharePoint Services servers and sites. Please note the tool can be found here:

- 32-bit versions of Windows Server 2003
  - %PROGRAMFILES%\common files\microsoft shared\web server extensions\12\bin
- x64-based versions of Windows Server 2003
  - %drive%\program files (x86)\common files\microsoft shared\web server extensions\12\bin

Local administration privileges are required to utilize the Stsadm tool.

A primary benefit to using the Stsadm command line tool is that Windows SharePoint Services 3.0 administration tasks can be somewhat automated by using batch files or scripts. Additionally, some tasks (e.g. changing the administration port) are not available using the Central Administration site. Also, the interface Stsadm provides has a more logical flow while giving all the functionality of the Central Administration site. There is, of course, much more depth to this utility, but for now keep in mind that certain operations and certain parameters are only available via the Stsadm command-line tool.

Configure backup and restore (disaster/recovery).

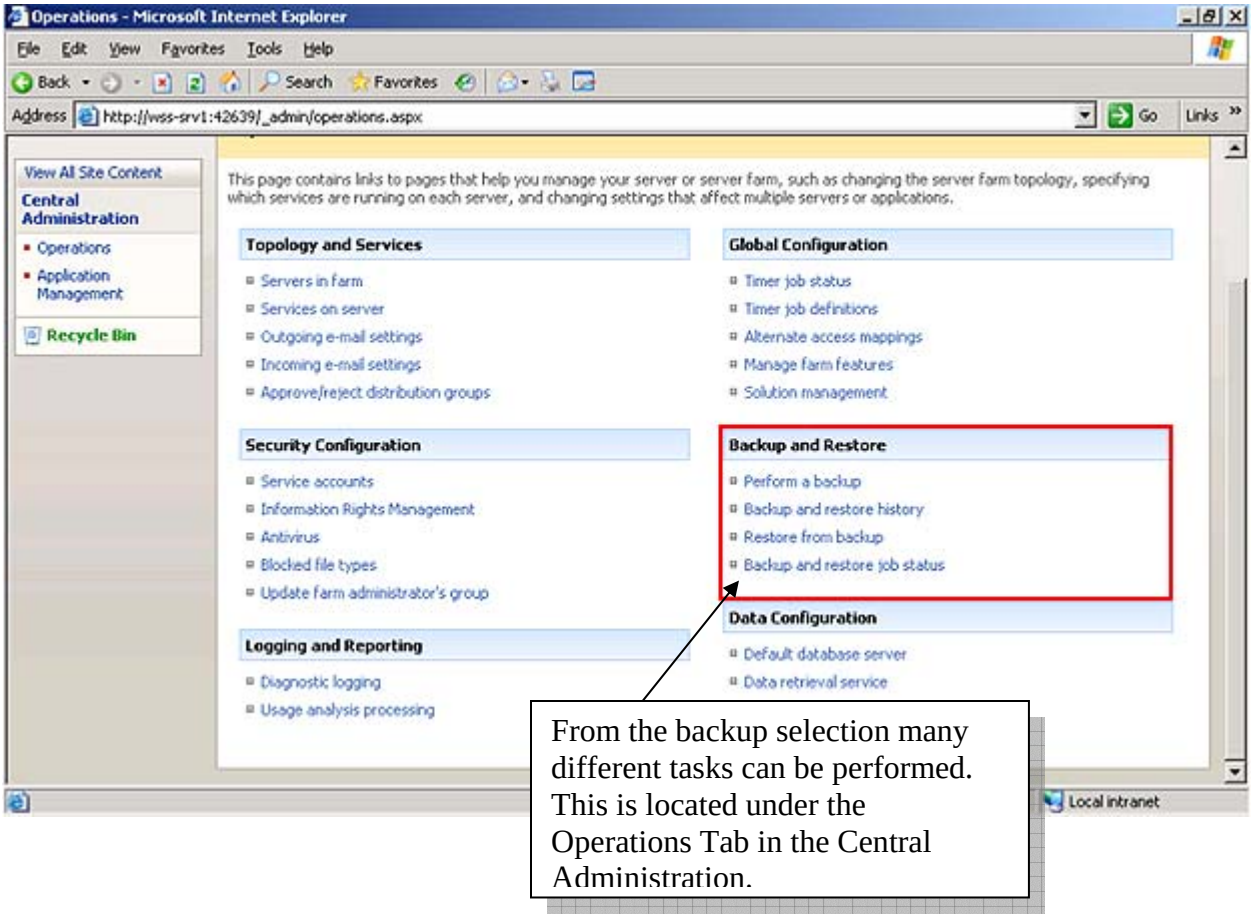
Backing up a server or hard drive is making an exact copy of the information and then storing it someplace else. In Windows, we use the built in Backup utility or a third party backup utility. When backup strategies are used correctly it is possible to recover from:

- Media Failure
- User Errors (Problem Between Keyboard and Chair)
- Hardware problems (Hard Drive)
- Natural Disasters (Katrina – New Orleans)

When doing backups it is important that the backups are readily available in case of an unexpected occurrence. Keep one copy of the backup on site and another off site.

WSS 3.0 has a slightly different strategy for backup. These are performed on sites, sub-sites, and files:

- Backup WSS 3.0 using the built-in tools. The built-in tools will allows back up of the content database which is located on the SQL Server.
- Use the Windows SharePoint Central Administration Site or Stsadm command line utility.
- Central Administration is used to backup WSS 3.0.



From the backup selection many different tasks can be performed. This is located under the Operations Tab in the Central Administration.

Back up Windows SharePoint Services 3.0 by using SQL Server Tools

When selecting a backup strategy for WSS 3.0 content databases use the utilities in Central Administration but also use the SQL Server 2000 or SQL Server 2005. You must be running SQL Server 2000 or 2005 and not the Express Edition or Windows Internal Database. Keep in mind that you must be part of the Administrators group on the SQL Server. When using SQL Server 2000 or SQL Server 2005 it is also possible to use options such as mirroring and log shipping.

Volume Shadow Copy Service (VSS)

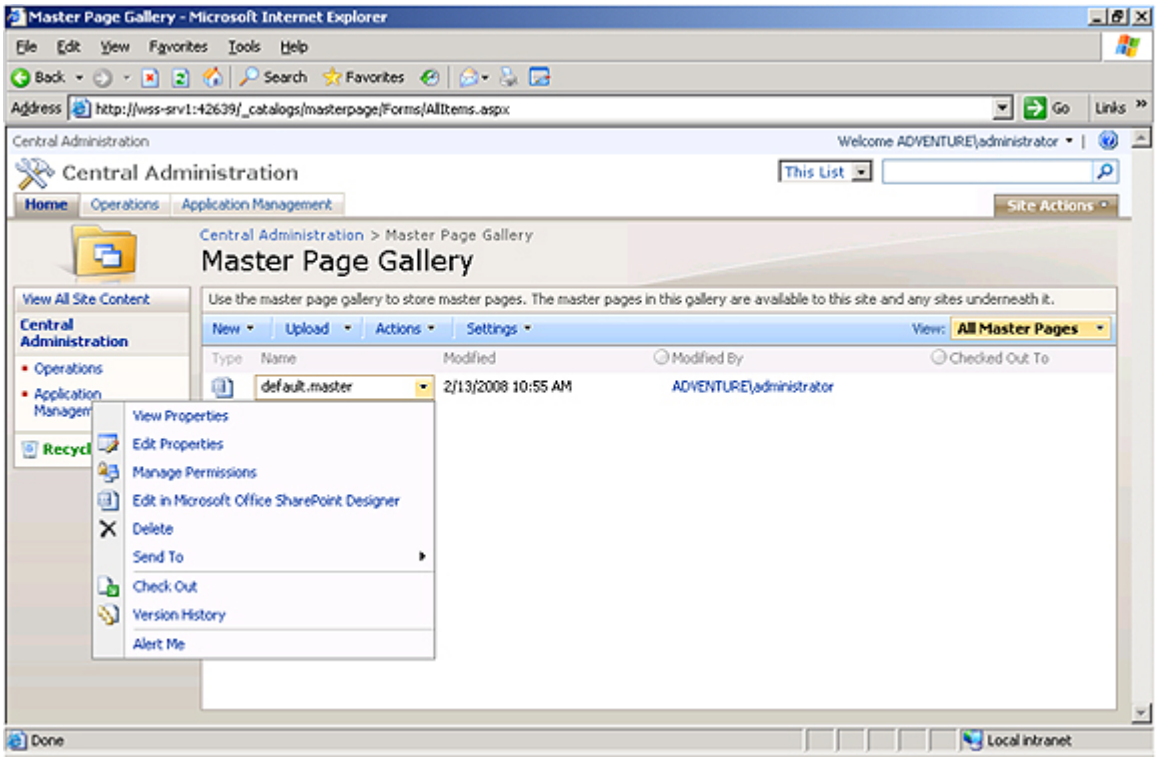
Windows Volume Shadow Copy Services (VSS) is used extensively in Windows Server 2003 or Windows 2008. With this technology it allows roll back to a previous version of a snap-shot. This is useful for recovering overwritten files and applications. The WSS 3.0 server has a new service called SharePoint Service VSS writer. This service enables Windows SharePoint server to provide VSS backups.

Chapter 5 - Manage Customization

Quick Jump To:

- Chapter 1
- Chapter 2
- Chapter 3
- Chapter 4
- Chapter 5
- Chapter 6

Configure master page.



When a Master Page is created it designs the layout for all pages created from that point forward. A master page is designed using the Microsoft Office SharePoint Designer. This utility produces the layout of the Master page with the graphics that will be included in all future pages. It is possible to include anything in a Master page such as links and logos. When creating a new page the page will have all of this information on it by default.

Customize pages by using SharePoint Designer.

The Office SharePoint Designer is a design tool that allows the creation and management of SharePoint sites.

- Design SharePoint sites tailored to the needs of client computers.
- Build application and solutions quicker.
- Leverage the ASP.Net platform and Microsoft Visual Studio 2005 to create controls and workflows.

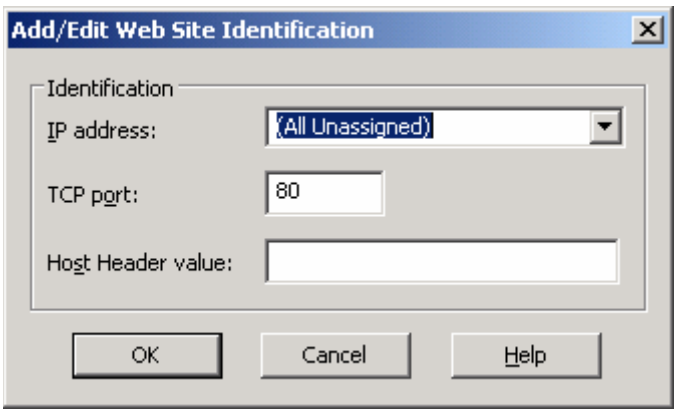
Configure code access security.

When a Web Part is created using Visual Studio 2005 Extensions for Windows SharePoint Services 3.0, the .NET assembly is kept in the global assembly cache. Through the development of the Web Part full access is available to the Web Service so there is no problem with security. However, this will only work if the Web Part is deployed in the global assembly cache by the administrator. If it shows up in other areas the security uses the web.config file which will determine what security mechanism is to be used in that session.

Chapter 6 - Configure Network Infrastructure for Windows SharePoint Services

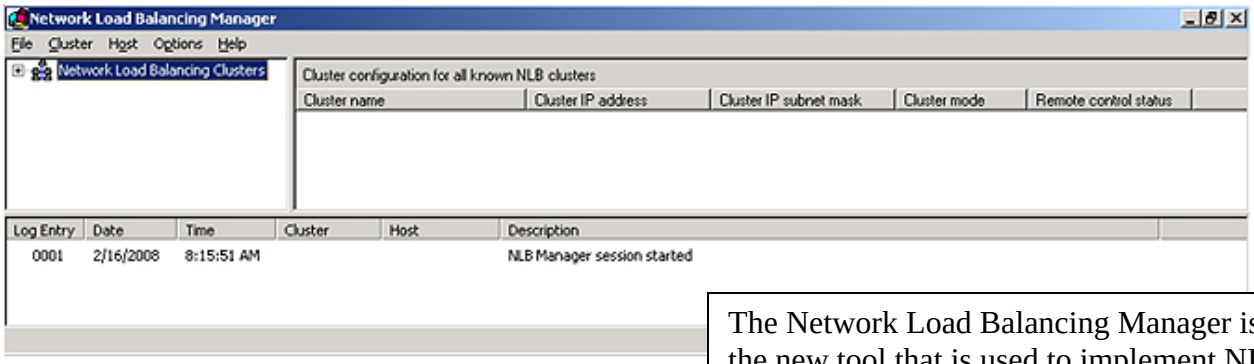
Configure names resolution.

Several applications may be located on the same server by having multiple Host-headers. Host-headers are names such as www which represent the application that trying to be accessed. It is possible to associate any type of name with an A record which will allow the application to be used with a Host Header.



Configuring Network Load Balancing (NLB).

To provide redundancy of web servers we can use a technology called Network Load Balancing (NLB). Network Load Balancing allows us to set up an environment to provide failover when a node (server) is not available. It also load balances client traffic based on a mathematical algorithm which calculates where to send client traffic. This is used on servers such as Web, Client Access Servers in Exchange 2007, VPN networking, Streaming Media Servers, Terminal Services and Proxies (ISA).



The Network Load Balancing Manager is the new tool that is used to implement NLB clusters. In a few steps, it is possible to have the cluster ready to except connections from the clients.

Once the cluster has been configured, when clients contact the cluster the client load will be balanced among the servers. Also, the NLB cluster provides redundancy for the applications that being installed into the environment. Remember, it is critical to have the exact same information on each of the servers for this to work.

Configure WSS to support perimeter network.

A perimeter network is a network that is not connected to the main network. It is usually described as being in a DMZ (Demilitarized Zone). It has the following traits:

- All information and hardware reside in the perimeter network.
- Server farm roles can be separated and infrastructure across multiple layers.
- Each layer can be further separated using routers or firewalls.
- Traffic can be redirected from the internet to an ISA server and then direct it from there to the destination increasing security.

Advantages

- Content is isolated to one server (extranet) which decreases maintenance and simplifies sharing.
- Client access is contained to the extranet.
- If the Extranet is compromised then the internal network is safe.
- A separate Active Directory keeps from affecting internal or corporate directory.

Disadvantages

Requires additional hardware and infrastructure.

Configure Internet Security and Acceleration Server (ISA).

The ISA server can be installed in the network to act as a software firewall. ISA Server 2006 is an integrated edge security gateway that helps protect IT environments from Internet-based threats while providing users fast and secure remote access to applications and data. ISA Server 2006 is available in two versions: standard edition and enterprise edition. With ISA server it is possible to configure the ISA server to publish the SharePoint Server. This will provide an extra layer of protection. Clients from the outside will not have direct access to the SharePoint server environment but will go through the intermediary security of the ISA server.