NetApp
Go further, faster

Technical Report

IIS 7.0 with NetApp Storage Systems

Sureshkumar N, NetApp

August 2009 | TR-3789

NETAPP STORAGE-BASED WEB SERVER

Web servers require back-end storage solutions with high reliability, performance, and manageability. NetApp® storage systems fit this requirement perfectly and serve the purpose flawlessly. Also, file sharing from NetApp storage systems can be done in different ways with different protocols and for different platforms. Web-based file sharing is yet another way to achieve this goal with a Web server installed in between a NetApp storage system and clients. This document discusses NetApp advantages in a Microsoft® IIS 7.0 (Internet Information Services version 7) Web server deployment and Web-based file sharing from NetApp storage.

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

NetApp storage systems provide seamless network file access to clients and support multiple protocols. Server Message Block (SMB), aka Common Internet File System (CIFS), is one of the major protocols supported by NetApp for Windows® file services environments. In Web server deployments, data management is considered a significant part, and storage plays a vital role in serving the data to the server with high reliability and performance. This document explains how NetApp storage systems fit this requirement and what a typical Web server deployment looks like. It also provides some configuration techniques.

In addition, this document talks about Web-based file sharing. Using the CIFS protocol, the user can access files and folders from the CIFS share of the NetApp storage system. Users can map the share to their local system to read, write, and edit/modify the contents of the share if they have the required permission. In Web-based file sharing, the CIFS share can export as a virtual directory and publish through the IIS 7.0 Web server. Users can access the files and folders via browsers, and the contents are read-only.

2 IIS—AN OVERVIEW

IIS is a group of Internet servers (including a Web or Hypertext Transfer Protocol server and a File Transfer Protocol server) with additional capabilities for Microsoft's Windows server operating systems. IIS is Microsoft's entry in the Internet server market that is also addressed by Apache, Sun Microsystems, O'Reilly, and others. With IIS, Microsoft provides a set of programs for building and administering Web sites, a search engine, and support for writing Web-based applications that access databases. Microsoft points out that IIS is tightly integrated with Windows NT® and 2000 servers in a number of ways, resulting in faster Web page serving.

A typical company that buys IIS can create pages for Web sites using Microsoft's Front Page product (with its WYSIWYG user interface). Web developers can use Microsoft's Active Server Page (ASP) technology, which means that applications, including ActiveX controls, can be embedded in Web pages that modify the content sent back to users. Developers can also write programs that filter requests and get the correct Web pages for different users by using Microsoft's Internet Server Application Program Interface (ISAPI). Microsoft claims that ASPs and ISAPI programs run more efficiently than common gateway interface (CGI) and server-side-include (SSI) programs, two current technologies.

Microsoft includes special capabilities for server administrators designed to appeal to Internet service providers (ISPs). It includes a single window (or "console") from which all services can be administered and users can be administered to. It's designed so that you can easily add as snap-ins components that you didn't initially install. The administrative windows can be customized for access by individual customers.

2.1 IIS MANAGER

IIS manager is the configuration interface for the Web server. After IIS 7 installation (for more information on IIS installation, please refer to Appendix B), the IIS manager should be used for all configuration purposes.

To open IIS manager:

Go to Control Panel → Administrative Tools → Internet Information Services (IIS) Manager

Command line shortcut: inetmgr

The window that opens is different from the one in earlier versions of IIS. There are three panels—the Connections panel, the Features panel, and the Actions panel—as shown in Figure 1.

- The Connections panel is on the left side of the IIS manager window. Any IIS-related configuration that includes adding a Web site, a virtual directory, an application pool, etc., starts from this panel. Other Web servers, sites, and applications can also be connected to manage from this panel.

- The center panel, the Features panel, has two types of views: Features view and Content view. Features view shows the options that can be configured for the selected item from the Connections panel. Content view shows the contents that reside in the selected item.

- The Actions panel shows the related actions that are available for the selected item.

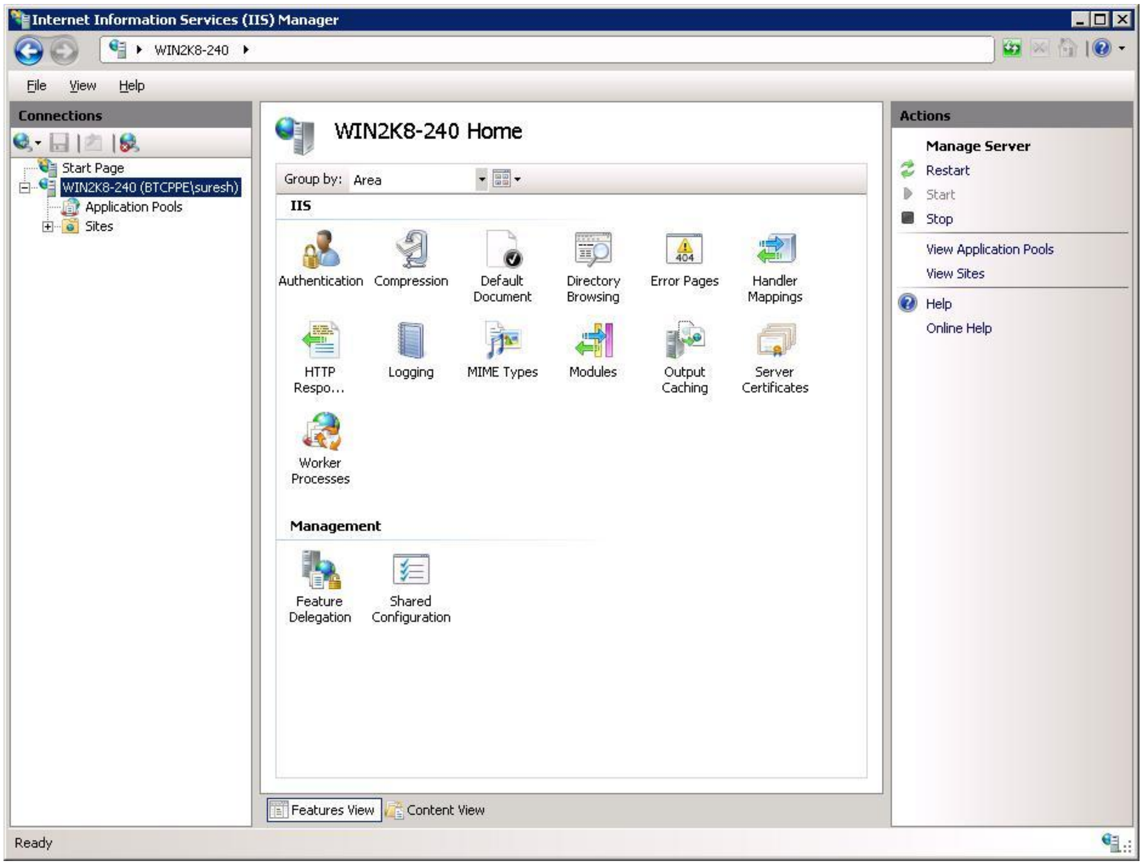


Figure 1) IIS manager.

3 NETAPP STORAGE-BASED WEB SERVER (IIS)

Network file access and file sharing are among the top priority items when it comes to NetApp storage deployment in Windows environments. When a Windows client accesses files from NetApp NAS storage, it uses the CIFS protocol to talk with. This conventional file access and file sharing method has been employed for ages.

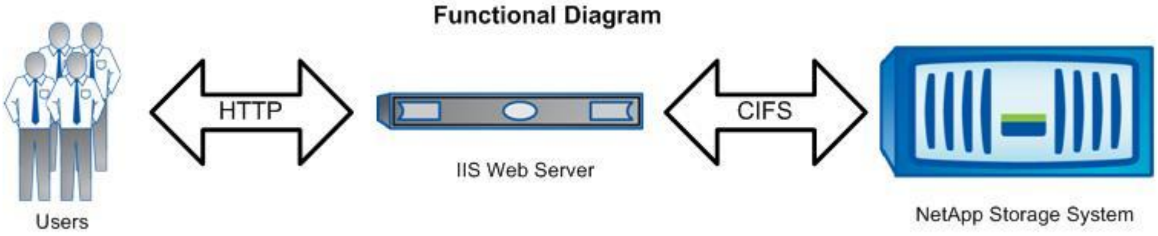


Figure 2) Functional diagram.

In Web-based file sharing, IIS 7 works as a Web front-end server to host the files that need to be shared across the clients. The files hosted are from the NetApp storage system's CIFS share. Users access the required files via a Web browser using HTTP protocol. On the back end, communication between the IIS server and the NetApp storage system takes place in CIFS protocol, as shown in Figure 2.

The CIFS shares that need to be published for file sharing should be configured as virtual directories in the IIS server with the Directory Browsing option enabled. Users can access these shares just by typing the URL of the virtual directory (refer section 4 for more information). The URL contains the IIS server name and the name of the virtual directory, that is, http://<IIS_Server_Name>/<Virtual_Directory_Name>/.

4 THE NETAPP ADVANTAGE

There are several advantages to having NetApp as the back-end storage for the IIS Web server over traditional DAS. Some of the important functionalities are given below.

SMB 2.0

SMB 2.0 is one of the key features in Windows 2008,Vista® and Windows7 operating systems. It is a major revision of the existing SMB 1.0 protocol and it is optimized for performance. The number of commands in SMB 2.0 have been greatly reduced and they are much more handle oriented than those in SMB 1.0. Several enhancements have been introduced to improve WAN access performance, network resiliency, security, data integrity, and server scalability.

Some of the important SMB 2.0 features are:

- *Larger Limits*: File IDs are 64 bit + 64 bit against 16 bit, Message IDs are 64 bit against 16 bit, Tree IDs are 32 bit against 16 bit, and the Security signature is 16 bytes against 8 bytes. As a result, system resources are the limiting factor rather than the protocol.
- *Compounding Operations*: This feature allows related and unrelated requests to be combined into a single transmission request for submission to the underlying transport to reduce network round trips. This improves WAN performance.
- *Durable File Handles*: The server keeps track of open files even after connection drops. This allows an open file to be reestablished after a client connection has been temporarily disconnected.
- *Credit Granting*: This feature limits the number of outstanding requests per connection, which allows the server to balance the number of simultaneous operations a client can have outstanding at any time.
- *Async Messages:* If a request takes an indeterminate amount of time, the server can send an async message to indicate the pending response. Clients can be told that the server is still processing an operation. Connections will not time out because of operations that take a long time to complete. Interim responses are assigned an async ID. The final response is also assigned the same async ID.
- *Packet Signing:* Signing of packets avoids man-in-the-middle attacks. In SMB 2.0, signing is always enabled and packets are signed if either the client or the server says signing is required.

Note: The SMB 2.0 feature is available only in Windows 2008, Windows Vista and Windows 7 and it is implemented in Data ONTAP® 7.3.1. That means that these benefits can be obtained only if the IIS 7.0 Web server is installed in a Windows 2008 (or Vista) server and the NetApp storage system OS is Data ONTAP 7.3.1 or above. Also, the IIS Web server configuration works with pre-7.3.x Data ONTAP versions with 7.3.x CIFS (aka SMB 1.0) but without the above-mentioned advantages.

SNAPSHOT TECHNOLOGY

Compared to competing snapshot technologies, NetApp Snapshot™ offers the advantages of better stability, performance, scalability, user visibility and file recoverability, and storage utilization.

- *Stability:* A NetApp Snapshot copy is read-only, completely static, and incorruptible. As such, it enables organizations to perform consistent backups from a NetApp storage system while applications are running. Administrators do not need to worry about files changing as they are being copied to tape. The result: completely consistent backups, every time.
- *Performance:* Storing a Snapshot copy on a NetApp system has no performance impact. In addition, creating and deleting Snapshot copies have virtually no performance impact. Alternative approaches need to physically relocate data to preserve snapshots, which significantly impacts performance and complicates system administration.
- *Scalability:* NetApp storage volumes support 255 Snapshot copies. Other vendors can permit fewer than 20 online snapshots and some permit as few as 4. The ability to store a large number of low-impact, frequently taken data images increases the likelihood that the desired version of data can be successfully recovered.
- *User Visibility and File Recoverability:* The high performance, scalability, and stability of Snapshot copies mean they provide an ideal online backup for user-driven recovery. A user who overwrites or removes data can find and recover data from hours, days, or weeks in the past and many users recover their own files. Field reports suggest that 80% to 90% of recoveries are single-file recoveries and that 95% take place within one or two weeks of the file being deleted. Snapshot copies are unsurpassed in ease of use and reliability for this application.

- *Storage Utilization*: Two Snapshot copies taken in sequence differ from one another by the blocks added or changed in the time interval between the two. This block-incremental behavior limits associated storage capacity consumption. Some alternative implementations can consume storage volumes rivaling that of an active file system, raising storage capacity requirements.

The products in the NetApp family of data protection solutions use Snapshot as a core technology and have inherited its unique advantages. SnapMirror®, SnapRestore®, SnapManager®, and SnapVault® offer enterprises a range of benefits that competing solutions—not based on NetApp Snapshot—simply cannot match.

SEPARATION OF DATA AND NETWORK

In any storage deployment, data and the network are the two significant parts. It is very important to have the data and the network independent of each other to avoid any single point of failure. NetApp storage system architecture separates these two parts naturally. This enables a high-availability solution on both the data and the network sides.

SHARING DATA ACROSS MULTIPLE IIS 7.0 SERVERS

NetApp storage systems provide an excellent data sharing solution via the CIFS protocol. When multiple Web servers (IIS 7.0) require the same data or different data from the same storage, NetApp serves the requirement flawlessly.

4.1 NETAPP FLEXCLONE AND THE WEB SERVER STAGING AREA

Another important advantage is NetApp FlexClone® technology. NetApp FlexClone provides instant replication of data volumes and data sets as transparent, virtual copies that increase productivity and save storage space without compromising performance.

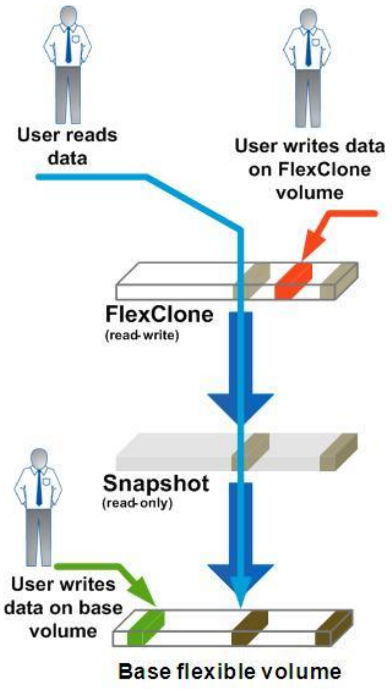


Figure 3) NetApp FlexClone technology.

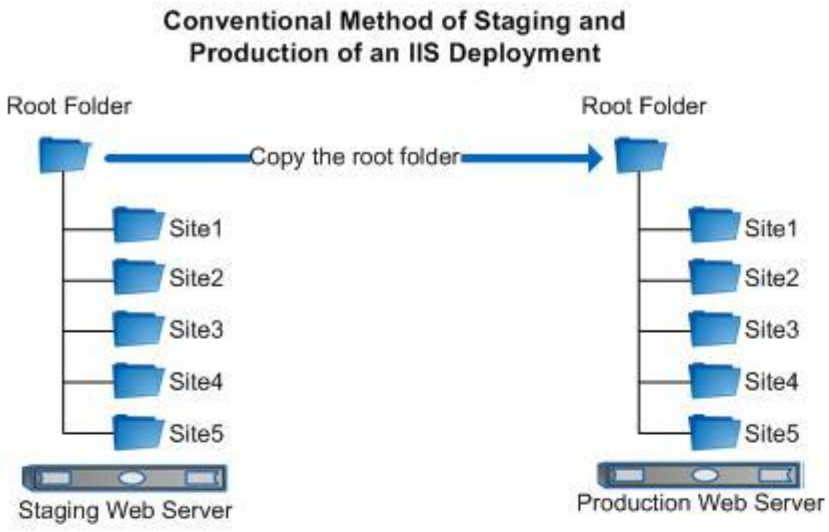
In general, Web server administrators create a staging area to store all the contents that need to be published. These contents are replicated to the Web server for production. This results in more disk space usage (double the time of actual data). With NetApp FlexClone technology, one can take a clone out of the staging area and point the Web server to that clone. This can operate with several Web servers by replicating one content source to several servers, leading to efficient storage utilization by saving storage space and time.

FlexClone technology works as shown in Figure 3. The base flexible volume can be cloned to create a FlexClone volume. The cloning is based on NetApp Snapshot technology. In other words, FlexClone is also a Snapshot copy but it is read-write while a non-FlexClone snapshot is read-only.

CONVENTIONAL METHOD

The conventional method for creating a staging area and production site is a space- and time-consuming process, shown in Figure 4. This process involves the following steps:

1. Create a staging area on the stage server. The staging area is a folder or directory in which the Web files are placed for further review and trial runs. The stage server can be a dedicated Web server or staging can be part of the production Web server. In general, for large-scale Web deployments, a separate staging server is employed.
2. Copy the Web contents to the staging area.
3. Complete the review process and trial runs. Configure the virtual directories pointing to staging folders and publish them for review. Based on review comments, you can modify the contents for final contents.
4. Copy the final contents from staging to production.
5. Publish the contents from the production server.



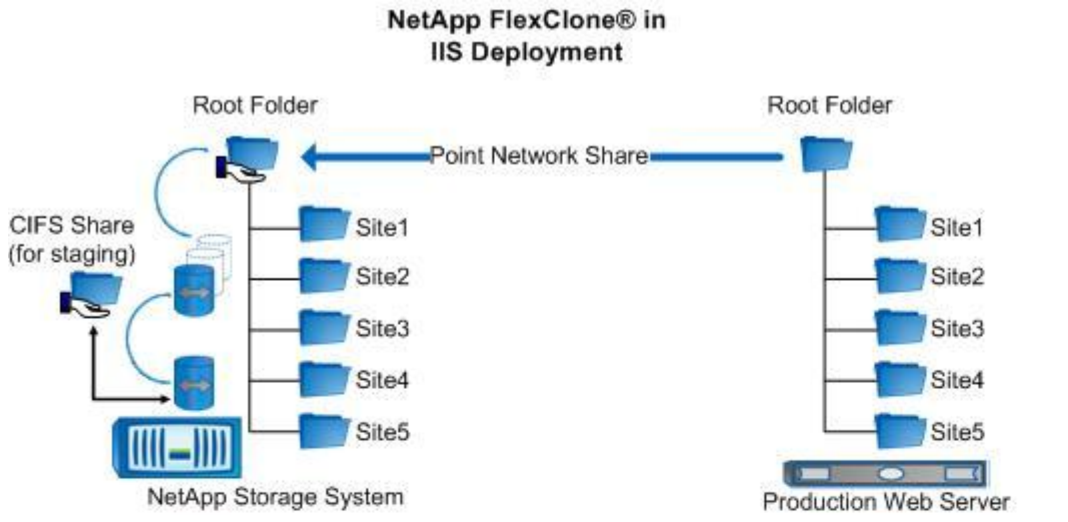
Conventional Method of Staging and Production of an IIS Deployment

- Create a staging area (Root Folder) in Stage Server to keep the web contents
- Complete the review process and trial runs
- Copy the final contents to the Production Server
- Publish the contents

FLEXCLONE IN IIS DEPLOYMENTS

Figure 5 illustrates how FlexClone serves as a production area in an IIS deployment. The base flexible volume forms a staging area for the Web site contents. This can be cloned using FlexClone technology once the reviews and verifications have been completed. By creating a CIFS share on the FlexClone volume and configuring that CIFS share as a virtual directory in the Web server (IIS) you form a production area.

Create a flexible volume separately for Web content; copy the Web content in the newly created volume. This is the staging area for the production site. Create a CIFS share on this volume and configure this CIFS share path as a virtual directory path in the Web server (IIS). Now you have created the stage that serves as a trial run for the production site.



- Create a flexible volume and place the web files. Create a CIFS share and publish it for review. This is the staging area.
- Complete the review process and trial runs and finalize the contents
- Create a FlexClone on that flexible volume and take a CIFS share
- Configure the Production Server pointing the CIFS share
- Publish the contents

Figure 5) NetApp FlexClone in an IIS deployment.

After all the reviews and finalization of the contents, make a FlexClone volume of that volume and create a CIFS share on this. This CIFS share does have production contents. On the IIS server create a virtual directory that points the CIFS share just created for production. Refer to section 6.1 to know more about virtual directory configuration.

Now the staging area resides on the flexible volume and the production data is on the FlexClone volume, which is a virtual entity of the base flexible volume. This minimizes the time, storage space, and effort needed to create another volume, copy the stage area contents to production, and so on.

This is particularly useful in scenarios that involve multiple Web sites. All the sites can be created in different directories under a single flexible volume. The flexible volume can be cloned using FlexClone technology and each directory can be exported as a different CIFS share. Then these CIFS shares can be configured as different virtual directories in the IIS Web server.

5 TYPICAL NETAPP IIS DEPLOYMENT

This section explains some of the important components involved in NetApp IIS deployments. Figure 6 shows an example of how a Web service provider deploys IIS server service while storing the virtual directories in a NetApp storage system. In this illustration, several objects are shown to better understand a typical NetApp setup. It is not in our scope to explain each and every object shown in the topology diagram. Also, this does not represent best practices or a must-have configuration.

The company shown (XYZ Web Services, Inc.) provides Web-oriented services to its customers. It deployed a IIS clustered server for its customer portals and a single-node IIS server for internal use. Both Web servers' data resides in NetApp cluster storage. It is assumed that this is a CIFS-only deployment. The NetApp storage system stores internal home directories of the company's employees, document repository, and customer virtual directories.

The IIS cluster server is responsible for seamless Web activities for customers. The single-node IIS server is employed for many utilities such as an intranet Web server, a customer service portal, transaction processing, and so on. Internal users share files and folders by using a Web-based file-sharing method.

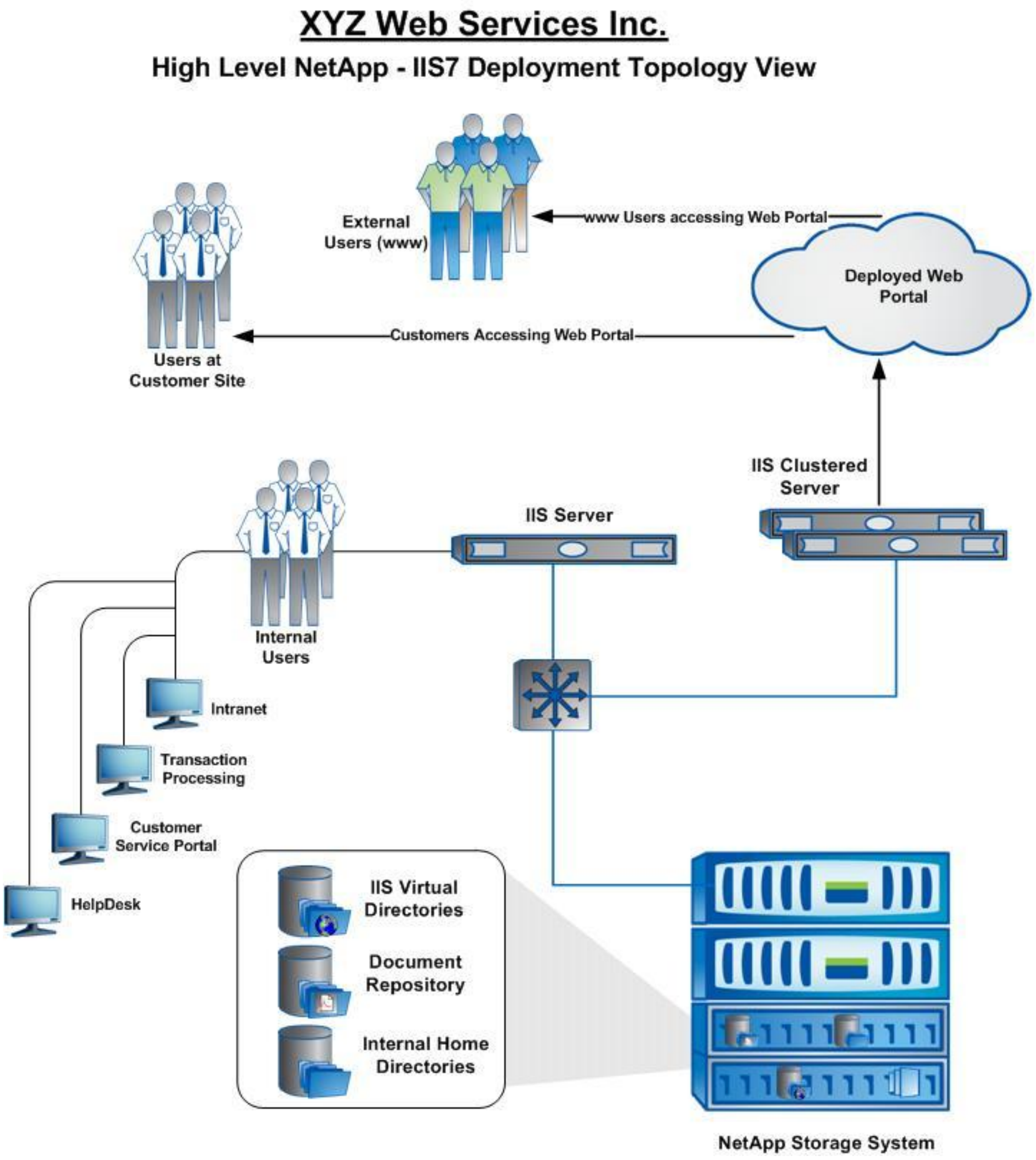


Figure 6) Typical NetApp-based Web server deployment.

6 CONFIGURING WEB-BASED FILE SHARING

This section explains how to configure Web-based file sharing on a NetApp IIS deployment. The CIFS share that needs to be shared over the Web should be configured as a virtual directory on the IIS Web server. The IIS server will publish the virtual directory and the users can access the directory from their browsers using the http protocol.

6.1 CREATING AND PUBLISHING A VIRTUAL DIRECTORY

Step 1

On a CIFS share, create a target directory to host the contents of the Web page or the directory that needs to be shared across. In this example, the target directory has been created as “IIS_test” in default “home” share.

Step 2

From the IIS manager Connections panel, expand the “site” tree. Right-click the ”Default Web Site” and select the “Add Virtual Directory…” option.

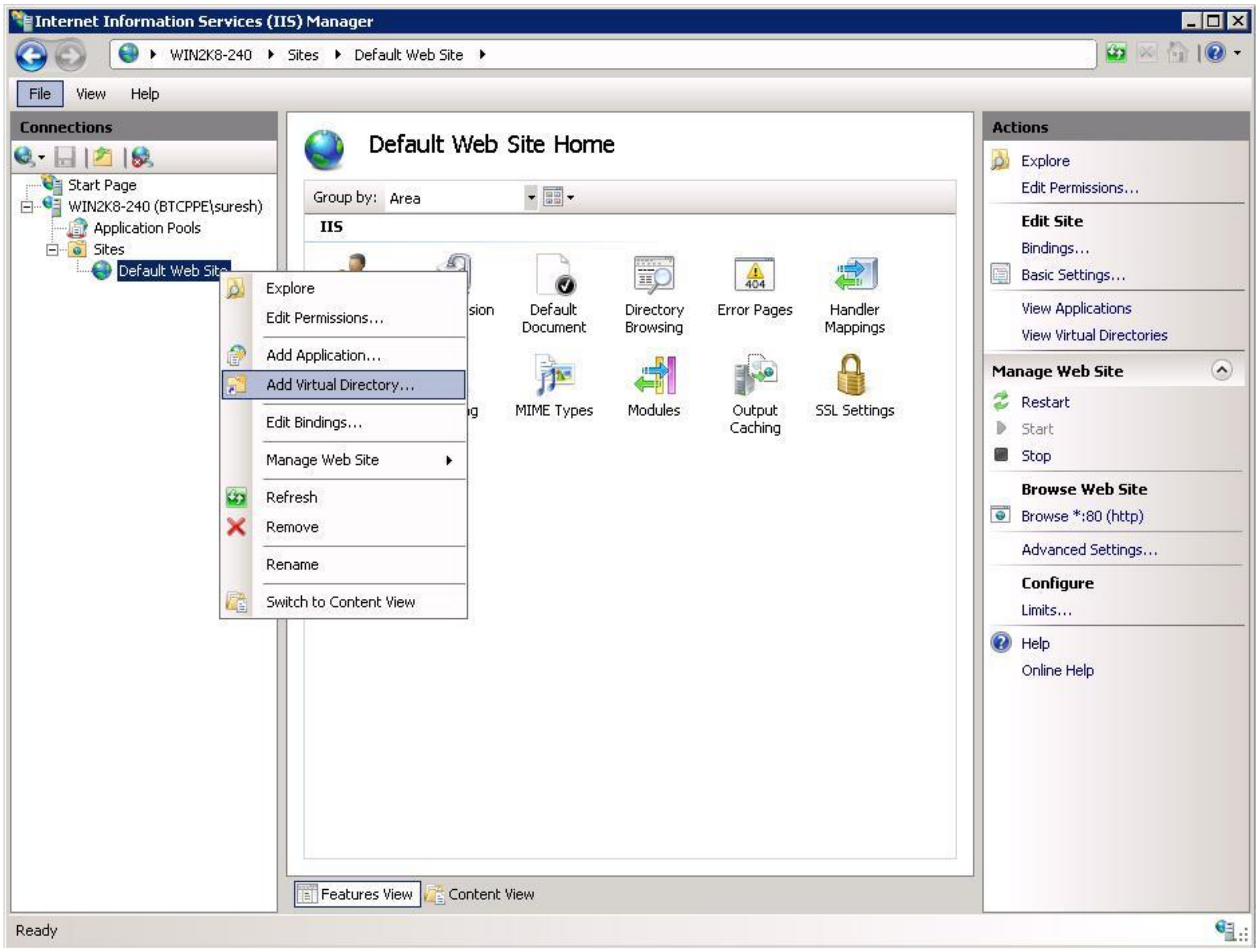


Figure 7) Add virtual directory.

This opens a dialogue box to enter the path and authentication for the virtual directory.

Step 3

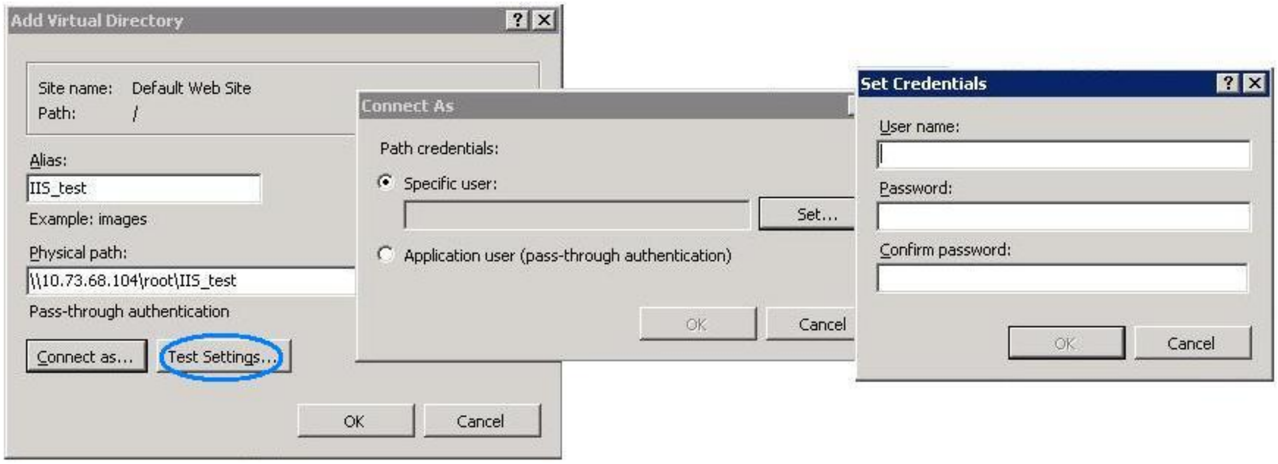
Enter the “Alias” for the site (here it is given as IIS_test) and the path of the directory created in step 1.

Note: *The path should be the UNC name of the appliance directory, not the mapped drive. For instance, if the appliance share and directory name are* ***\\<filer_name>\<share_name>\<dir_name>*** *the share is mapped in the Web server with a drive letter* ***M****. In step 3, the directory should NOT be specified as* ***M:\<dir_name>*** *and it should be* ***\\<filer_name>\<share_name>\<dir_name>.***

Click ”Connect as…” to configure the user credentials.

Step 4

On the “Connect AS” dialogue box, select the “Specific User” option and click the “Set…” button to specify the user credentials. The user should have Full Control permission on this folder.



Site name: Default Web Site
Path: /

Alias: IIS_test

Example: images

Physical path: \\10.73.68.104\root\IIS_test

Pass-through authentication

Path credentials:

● Specific user:

○ Application user (pass-through authentication)

User name:

Password:

Confirm password:

Figure 8) Alias, path, and user credentials.

After configuring this, click on “Test Settings…” to validate the authentication and authorization of the specified user credentials.

The virtual directory has been created and published.

Step 5

To enable directory browsing, on the Features panel select the “Directory Browsing” icon and click “Enable” in the Actions panel. Select the format of the directory listing if required.

The directory listing is now enabled and users can access this directory from their browsers.

6.2 CONFIGURATION BEST PRACTICES

Following are some of the best practices to configure a typical read-only content server deployment.

GENERAL

- To get the SMB 2.0 advantage, Data ONTAP 7.3.1 or above should be used and the Web server operating system should be Windows 2008 or Windows Vista. Enable SMB 2.0 on the storage side; it is enabled by default on the above Windows OSs.
- Create qtrees for different virtual directories. This is to enable the configuration settings to be applied with granularity.
- Duplex mismatches: Make sure that the duplex settings match on the storage, the switch, and the clients.

FOR BEST PERFORMANCE

- *Turn off vscan for read access.* Virus scanning is a performance overhead that results in more storage CPU utilization with increased latency. Also, the deployment is read-only in nature; the possibility of viruses is relatively low because the writes are only from authoring machines rather than from all users. Vscan can be disabled at the CIFS share level, and NetApp advises that you turn off this feature for good performance. To disable virus scanning for the shares when the clients open files for read access, use this command:

cifs shares -change *sharename* **–novscanread**

- *Remove fpolicy.* Fpolicy is another performance overhead for the appliance. Disabling this feature is helpful in boosting storage performance. So try to off-load any fpolicy-related operations from the storage to another appliance.
- *Cifs.max_mpx.* This option controls how many simultaneous operations the storage reports it can process. An "operation" is each I/O the client believes is pending on the storage, including outstanding change notify operations.

This value defaults to 50, but clients such as Windows Terminal Server or IIS may require the number to be increased to avoid errors and performance delays. The approved values for this parameter are 126, 253, and 1,124. The most accurate way to determine which number to use is to measure the RedirectorCurrentCommands statistic on the client with Windows perfmon and to increase the number until Current Commands does not hit the negotiated limit. For more information see Microsoft knowledge base articles Q191370 and Q232890.

This number should only be changed while CIFS is terminated. Only use the approved values to avoid Q232890. This value affects allocations in the clients. Use the smallest value necessary for correct behavior.

FOR GREATEST RELIABILITY

- *Disable 'oplocks'.* In general, CIFS deployments are recommended to turn on Opportunistic locks (oplocks), because this allows a client to request the ability to cache locally the contents and attributes of an open file. This usually results in a dramatic performance gain. In Web server deployments, if oplocks are enabled, a lot of important data being cached on the client can get lost if the network or the power dies. So it is better to turn off oplocks for the qtrees configured for IIS virtual directories. Oplocks can be turned off/on on a qtree, volume, or global basis, without a reboot.

7 FURTHER STUDIES

The following items are a few of the future updates planned for this technical report, but they depend on the field requirement.

- **Performance studies:** To evaluate the performance impact of storage in a Web server environment. This study can be extended to sizing exercises.
- **IIS and Microsoft Hyper-V™:** To evaluate the functionality of virtualizing a IIS Web server using Hyper-V.
- **Dynamic content configuration:** This guide covers the static content configuration part of IIS deployment. Further investigation needs to be done on dynamic content configuration to be included in this doc.
- **Backup:** Studies the options of NetApp backup and management technologies on IIS data.
- **Troubleshooting:** Diagnostics for Web server issues based on NetApp.
- **More best practices:** Configuration tips for the best security and greatest reliability.
- More information on NetApp settings like volume, qtrees, number of snapshots, and so on needs to be included in this report.

APPENDIX A: WHAT IS NEW IN IIS 7.0?

Compared to Microsoft Internet Information Services 6.0, there are a number of improvements in IIS 7.0. Some of these enhancements are related to security and server management while others are geared toward Web developers. Here are some of the new features that matter most to network administrators.

IMPROVED MANAGEMENT INTERFACE

The user interface of IIS manager has been completely redesigned from scratch. One of Microsoft's reasons for doing this was to create a management interface that allows managing Internet Information Services and ASP.NET through a single console. As with most things in Windows Server 2008, IIS 7.0 has been tied into Windows PowerShell, which means that one can perform various management tasks from the command line or through a PowerShell script. Microsoft has also created a new command line tool named APPCMD.EXE that helps automate common management tasks. In doing so, Microsoft has done away with IIS 6.0-style administration scripts.

IMPROVED TROUBLESHOOTING

The troubleshooting mechanism in IIS 7.0 is a lot better than its earlier version. The log file entries that IIS 7.0 produces are much more detailed than those created by IIS 6.0, and they include more status codes. These improvements should help administrators troubleshoot problems much faster.

COMPARTMENTALIZED INSTALLATION

IIS 6.0 did not allow selective component-level installation. Though Windows Server 2003 allows you to pick which IIS 6.0 components you want to install, many of these components are made of subcomponents that cannot be disabled. With Internet Information Services 7.0, Microsoft broke down IIS into dozens of modular components, each of which can be individually enabled or disabled. Figure 2 shows how granular the installation process has become.

SSL—ENCRYPTED FTP

Although IIS has supported Secure Sockets Layer (SSL) encryption for Web sites for many years, for some reason Microsoft never offered the ability to encrypt FTP traffic. In Internet Information Services 7.0, the company has completely rewritten its FTP server module to bring it up to date. Not only does it now support SSL encryption, but it also makes it easy to create FTP publishing points for Web applications, using either an independent authentication method or authentication via Microsoft Active Directory.

DELEGATED ADMINISTRATION

Another cool new feature is something called delegated administration. The basic idea behind this feature is that a single IIS server is capable of hosting multiple Web sites. In the past, if admins could administer one Web site, they could manage every site hosted by the server. Internet Information Services 7.0 allows you to perform delegations so that administrators are limited to managing only specific Web sites or even individual parts of a Web site.

REMOTE ADMINISTRATION

Traditionally, if an administrator wants to manage Internet Information Services, then the tool of choice is usually the IIS manager console. However, IIS 7.0 contains a new remote management tool called Web Management Services (WMSVC) that you can use to manage the server over the Web using HTTPS. Web Management Services is not installed by default; it can be installed by adding the IIS role from the server manager.

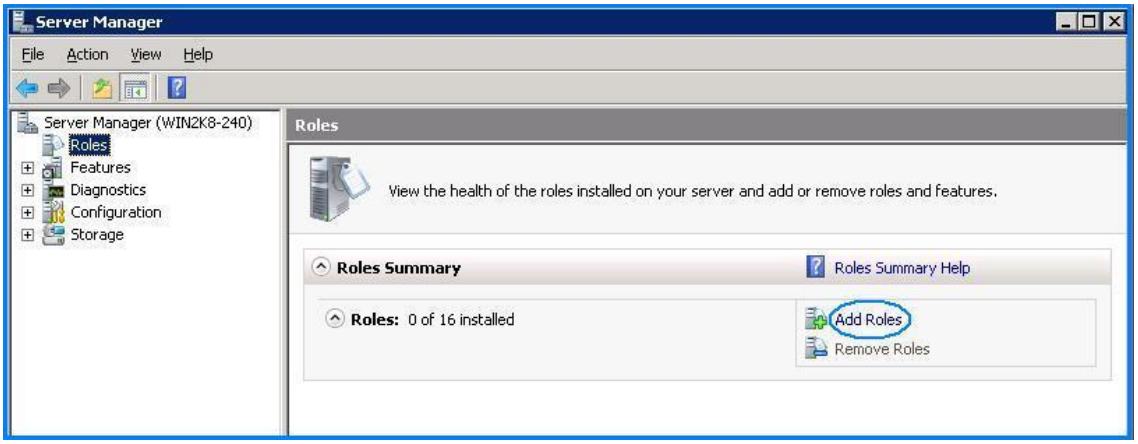
All of these improvements go a long way toward making Internet Information Services 7.0 a lot more secure and easier to manage than IIS 6.0.

APPENDIX B: INSTALLING IIS 7.0 ON A WINDOWS 2008 SERVER

This section explains how to install IIS 7.0 on a Windows 2008 server.

Open Control Panel → Administrative Tools → Server Manager

Command line shortcut: servermanager.msc



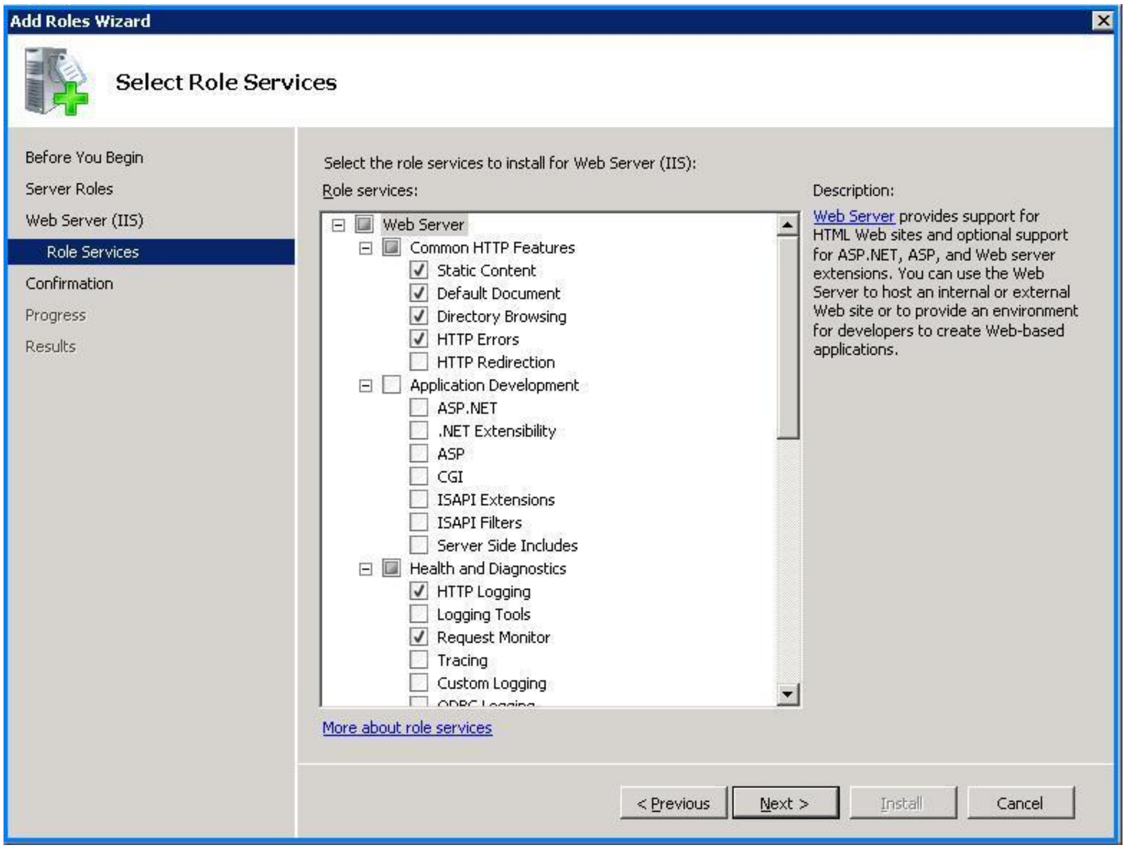
View the health of the roles installed on your server and add or remove roles and features.

Roles: 0 of 16 installed

Figure 9) Server manager.

Click on “Add Roles.” On the next window, select “Web Server (IIS)” from the list of options and click “Next.”

The next window shows the services associated with IIS 7.0. Required services are selected by default; select more services if needed and click “Next.”



Select the role services to install for Web Server (IIS):

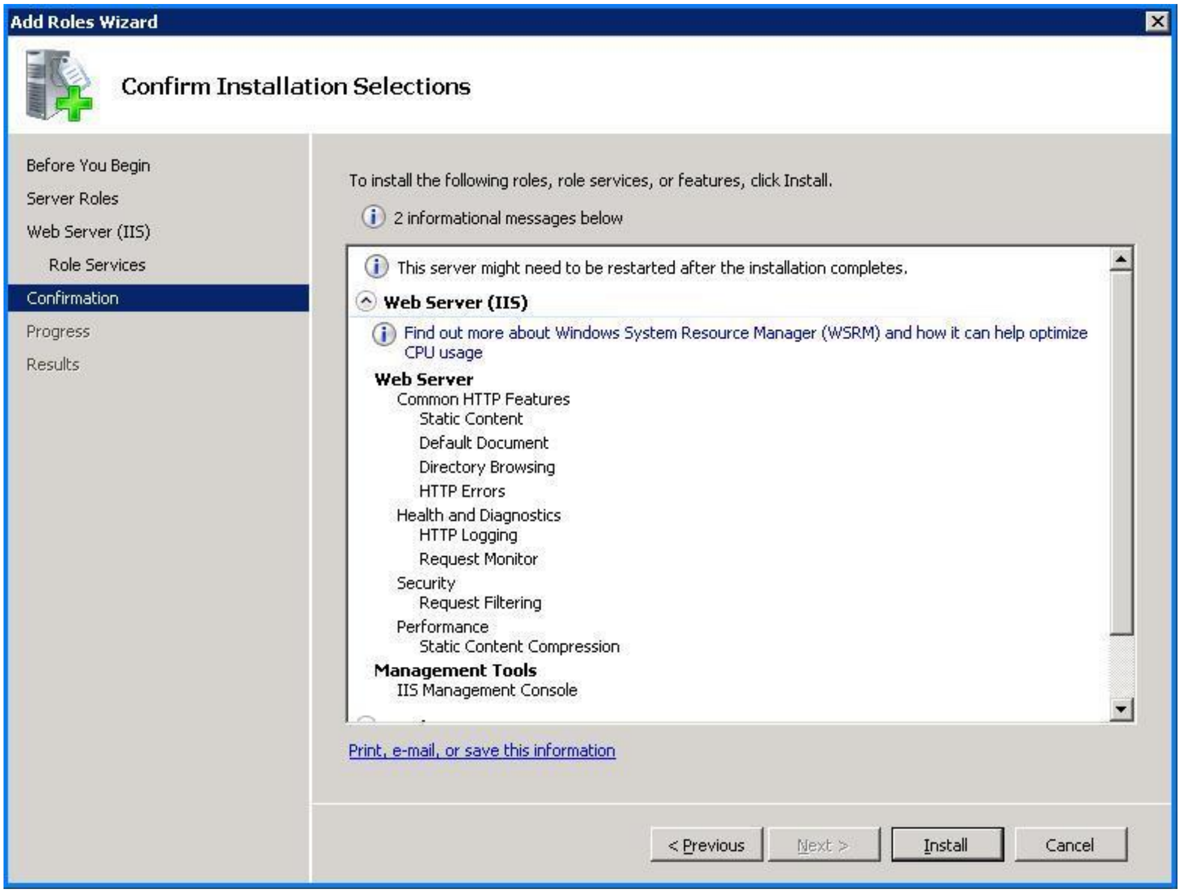
Role services:

- ▣ Web Server
  - ▣ Common HTTP Features
    - ☑ Static Content
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - □ HTTP Redirection
  - □ Application Development
    - □ ASP.NET
    - □ .NET Extensibility
    - □ ASP
    - □ CGI
    - □ ISAPI Extensions
    - □ ISAPI Filters
    - □ Server Side Includes
  - ▣ Health and Diagnostics
    - ☑ HTTP Logging
    - □ Logging Tools
    - ☑ Request Monitor
    - □ Tracing
    - □ Custom Logging
    - □ ODBC Logging

Description:

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

Figure 10) Add roles wizard.



Confirm Installation Selections

To install the following roles, role services, or features, click Install.

2 informational messages below

This server might need to be restarted after the installation completes.

Web Server (IIS)

Find out more about Windows System Resource Manager (WSRM) and how it can help optimize CPU usage

Web Server
- Common HTTP Features
  - Static Content
  - Default Document
  - Directory Browsing
  - HTTP Errors
- Health and Diagnostics
  - HTTP Logging
  - Request Monitor
- Security
  - Request Filtering
- Performance
  - Static Content Compression

Management Tools
- IIS Management Console

Figure 11) Confirm installation services.

The subsequent window shows the selected roles and role services. Click the Install button to continue installation or click the previous button to make changes to the installation.

© Copyright 2009, NetApp, Inc. All rights reserved. No portions of this document may be reproduced without prior written consent of NetApp, Inc. Specifications are subject to change without notice. NetApp, the NetApp logo, Go further, faster, Data ONTAP, FlexClone, SnapManager, SnapMirror, SnapRestore, Snapshot, and SnapVault are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries. Windows, Microsoft, Windows NT, and Vista are registered trademarks and Hyper-V is a trademark of Microsoft Corporation All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. TR-3789