Edmonds Community College

Web Server Technology and Security

This book documents the Windows Server 2008 utilizing Internet Information Systems (IIS) 7.0, which covers detailed information about the server, including the documentation of processes and procedures that apply to the server.

Doug Vickers

Winter, 2011

Contents

Hardware Specifications:

Virtual Server Windows Server – Enterprise

Name - dvickers

Workgroup - WORKGROUP

Processor - Intel Xeon W3530 @ 2.80 GHz (2 processors)

RAM - 1.00 GB

Hard Drive - 40 GB

VMware Virtual S SCSI Disk Drive

Floppy Disk Drive

VMware IDE CDR 10 ATA DVD/CD ROM drive

Host HP Z400 Workstation

Name - EDCC-C19CWOZI7D

Domain – sandbox.edcc.edu

Processor - Intel Xeon W3530 @ 2.80 GHz (2 processors)

RAM – 8.00 GB

Hard Drive – 500 GB

Hitachi HDS721050CLA362 Disk drive

Hp DVD A DH16AAL DVD/CD-ROM drive

Warranty

Software Specifications:

Virtual Server Web Server (IIS 7 Professional)

Common HTTP Features

Static Content

Default Document

Directory Browsing

HTTP errors

HTTP redirection

Application Development

ASP.NET

.NET Extensibility

ASP

CGI

ISAPI Extensions

Server Side includes

Health and Diagnostics

HTTP Logging

Request Monitor

Security

Request Filtering

Performance

Static Content Compression

Dynamic Content Compression

Management Tools

- IIS Management Console
- IIS Management Scripts and Tools
- Management Service
- IIS 6 Management Compatibility

IIS 6 Metabase Compatibility

IIS 6 Management Console

FTP Publishing service

FTP Server

FTP Management Console

.NET Framework 3.0 Features

.NET Framework 3.0

XPS Viewer

Remote Server Administration Tools

Role Administration Tools

Web server (IIS) tools

Feature Administration Tools

SMTP Server Tools

SMTP Server

Windows process Activation Service

Process Model

.NET Environment

Configuration APIs

Internet Explorer

Microsoft Baseline Security Analyzer 2.2

Windows Server 2008 Enterprise – Service Pack 2

COMODO Antivirus

Windows Marketplace

PHP 5

Novasoft testing Master

Weblog Expert

SQL Server Express

Security Features

Accounts:

Name:	Full Name:		Description:
doug vickers	doug vickers	Enabled	Server Administrator (password – Pa55word)
mbaker	marti baker	Enabled	Server Administrator
Administrator		Disabled	Built in account for computer/domain
bojdDev	John Smith	Enabled	BOJD Site Aadministrator
defaultAdmin	James Jones	Enabled	Default Site Administrator
Guest		Disabled	Built in account for guest to IIS
IUSR_DVICKERS	Internet Guest	Enabled	Built in account for anonymous to IIS

Security:

Limited Access per above

Comodo Anti-virus software installed

Microsoft Baseline Security Analyzer 2.2 installed)(latest report)

Windows updates done weekly

Client Assurance Agreement

Update Log

Date	Type of Update	Reason
Installation date: 1/19/2011 7:10 PM	Important	Security Update for Windows Server 2008 x64 Edition (KB2124261) Installation status: Successful A security issue has been identified that could allow an unauthenticated remote attacker to compromise your system and gain control over it. You can help protect your system by installing this update from Microsoft. After you install this update, you may have to restart your system.
Installation date: 1/19/2011 7:11 PM	Important	Security Update for Windows Server 2008 x64 Edition (KB982666) Installation status: Successful A security issue has been identified that could allow an authenticated remote attacker to compromise your system and gain control over it. You can help protect your system by installing this update from Microsoft. After you install this update, you may have to restart your system.
Installation date: 1/19/2011 7:11 PM	Important	Security Update for Windows Server 2008 x64 Edition (KB2419640) Installation status: Successful A security issue has been identified that could allow an unauthenticated remote attacker to compromise your system and gain control over it. You can help protect your system by installing this update from Microsoft. After you install this update, you may have to restart your system.
Installation date: 1/19/2011 7:11 PM	Important	Security Update for Windows Server 2008 x64 Edition (KB975254) Installation status: Successful A security issue has been identified that could allow an authenticated remote attacker to compromise your system and gain control over it. You can help protect your system by installing this update from Microsoft. After you install this update, you may have to restart your system.
Installation date: 1/19/2011 7:11 PM	Important	Windows Malicious Software Removal Tool x64 - January 2011 (KB890830) Installation status: Successful After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including

		Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.
Installation date: 2/2/2011 6:22 PM	Important	Security Update for Windows Server 2008 x64 Edition (KB976323) Installation status: Successful A security issue has been identified that could allow an unauthenticated remote attacker to cause the affected application to stop responding. You can help protect your system by installing this update from Microsoft. After you install this update, you may have to restart your system.
Installation date: 2/9/2011 8:13 PM	Important	Security Update for Windows Server 2008 x64 Edition (KB2483185) Installation status: Successful A security issue has been identified that could allow an unauthenticated remote attacker to compromise your system and gain control over it. You can help protect your system by installing this update from Microsoft. After you install this update, you may have to restart your system.
Installation date: 2/9/2011 8:14 PM	Important	Cumulative Security Update for Internet Explorer 8 for Windows Server 2008 x64 Edition (KB2482017) Installation status: Successful Security issues have been identified that could allow an attacker to compromise a system that is running Microsoft Internet Explorer and gain control over it. Help protect your system by installing this update from Microsoft. After you install this item, you may have to restart your computer.
Installation date: 2/9/2011 8:14 PM	Important	Security Update for Windows Server 2008 x64 Edition (KB2393802) Installation status: Successful A security issue has been identified that could allow an authenticated local attacker to compromise your system and gain control over it. You can help protect your system by installing this

		update from Microsoft. After you install this update, you may have to restart your system.
Installation date: 2/9/2011 8:14 PM	Important	Security Update for Windows Server 2008 x64 Edition (KB2485376) Installation status: Successful A security issue has been identified that could allow an unauthenticated remote attacker to compromise your system and gain control over it. You can help protect your system by installing this update from Microsoft. After you install this update, you may have to restart your system.
Installation date: 2/9/2011 8:15 PM	Important	Windows Malicious Software Removal Tool x64 - February 2011 (KB890830) Installation status: Successful After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.
Installation date: 2/9/2011 8:16 PM	Important	Security Update for Windows Server 2008 x64 Edition (KB2479628) Installation status: Successful A security issue has been identified that could allow an authenticated local attacker to compromise your system and gain control over it. You can help protect your system by installing this update from Microsoft. After you install this update, you may have to restart your system.
Installation date: 2/24/2011 4:05 PM	Important	Update for Windows Server 2008 x64 Edition (KB971029) Installation status: Successful

		Install this update to restrict AutoRun entries in the AutoPlay dialog to only CD and DVD drives. After you install this item, you may have to restart your computer.

More information:

http://support.microsoft.com/kb/971029

Help and Support:

http://support.microsoft.com

Web Site Documentation

Company:	Doug Vickers
Decision Authority:	Tom Baldwin Phone: 425-555-1111
Billing Authority:	Sally Smith Phone: 425-555-1212
Development Authority:	John Jones Phone: 425-555-1122
IP Address:	10-1-13-101
Primary domain:	www.dougVickers.com
Application Pool:	dougVickersAppPool
Secondary domain(s):	
Application Pool:	n/a
Domain Renewal Date:	12/15/2012

Software needed:	Internet Explorer, Microsoft Baseline Security Analyzer 2.2, Windows Server 2008 Enterprise – Service Pack 2, COMODO Antivirus, Windows Marketplace, PHP 5, Novasoft testing Master, Weblog Expert, SQL Server Express
Other configurations notes:	odbc, smtp, parent paths enabled
Mime Types allowed:	MIME Types
TSL / SSL Required?	__ Yes _X_ No If yes Certificate Authority: Renewal period: Renewal date:
Backup Assurance:	__ Hourly _X_ Daily __ Weekly
Support Response:	Contact John Jones
Access Accounts:	FTP Accounts: n/a User name: Password: Configuration Accounts: User name: Password:
Company:	Business Outreach Job Development
Decision Authority:	Tom Baldwin Phone: 425-555-1111
Billing Authority:	Sally Smith Phone: 425-555-1212
Development Authority:	John Jones Phone: 425-555-1122
IP Address:	10-1-13-101
Primary domain:	www.dcvbojd.com
Application Pool:	cacAppPool
Secondary domain(s):	n/a
Application Pool:	n/a
Domain Renewal Date:	12/15/2012

Software needed:	Internet Explorer, Microsoft Baseline Security Analyzer 2.2, Windows Server 2008 Enterprise – Service Pack 2, COMODO Antivirus, Windows Marketplace, PHP 5, Novasoft testing Master, Weblog Expert, SQL Server Express
Other configurations notes:	Odbc, smtp, parent paths enabled
Mime Types allowed:	MIME Types
TSL / SSL Required?	__ Yes _X_ No If yes Certificate Authority: Renewal period: Renewal date:
Backup Assurance:	__ Hourly _X_ Daily __ Weekly
Support Response:	Contact John Jones
Access Accounts:	FTP Accounts: n/a User name: Password: Configuration Accounts: User name: Password:

Company:	My Grill
Decision Authority:	Tom Baldwin Phone: 425-555-1111
Billing Authority:	Sally Smith Phone: 425-555-1212
Development Authority:	John Jones Phone: 425-555-1122
IP Address:	10-1-13-101
Primary domain:	www.dcvmyGrill.com
Application Pool:	myGrill.com
Secondary domain(s):	dcvadmin.myGrill.com

Application Pool:	n/a
Domain Renewal Date:	12/15/2012
Software needed:	Internet Explorer, Microsoft Baseline Security Analyzer 2.2, Windows Server 2008 Enterprise – Service Pack 2, COMODO Antivirus, Windows Marketplace, PHP 5, Novasoft testing Master, Weblog Expert, SQL Server Express
Other configurations notes:	Odbc, smtp, parent paths enabled
Mime Types allowed:	MIME Types
TSL / SSL Required?	__ Yes _X_ No If yes Certificate Authority: Renewal period: Renewal date:
Backup Assurance:	__ Hourly _X_ Daily __ Weekly
Support Response:	Contact John Jones
Access Accounts:	FTP Accounts: n/a User name: Password: Configuration Accounts: User name: Password:

Change Request

Desired State			
Change Recommendation			
e	Priority	Services Affected	Impact
ks	Likelihood x Impact (1 - 5)	Mitigation	
ıer:		Technical Lead:	
ager:		Business Liaison:	

Add a New Web Site

IIS Manager presents the administrator with a GUI interface that allows the creation of a web site by following these steps:

Start IIS Manager by clicking Start ⇛ Run, entering **inetmgr**, and then pressing Enter.

Select the server to administer (your machine name). Expand the server by clicking on the +. Click the Sites icon, and then select Add Web Site from the Actions pane or by right-clicking the Sites icon. This will present the Add Web Site dialog, as shown in Figure 6-2.

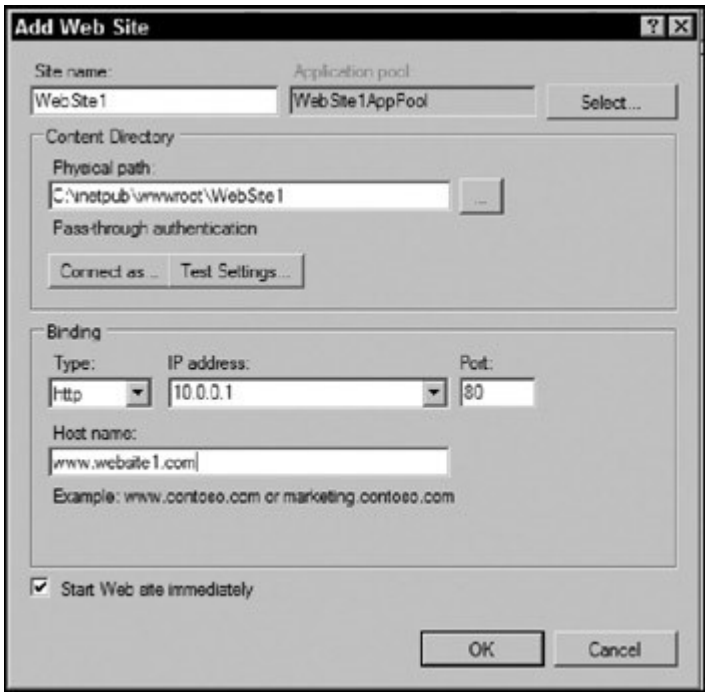


Figure 6-2

Enter a web-site name; use your full name, without any prefix or any spaces. This name should include **NO SPACES**! Use camel case to help with readability: ie: martiBaker.

Select the application pool for your site, DefaultAppPool.

Click the start button, select computer, navigate to c:\inetpub\wwwroot. Create a folder in this location. Name this folder “yourName”, where yourName is your full name with no spaces.

Set the path to the web-site files. Browse to the folder that you just created in c:\inetpub\wwwroot\yourName. Click OK.

Click “Test Settings”. You will see a warning on “Authorization”, there is no need to change this setting at this time. Click Close.

Enter binding details. Set this to HTTP.

Next, select the IP address to bind the site to; use the IP address of your machine.

Verify the port setting is 80.

Enter the Host name: www.yourpame.com.

Note: A host header entry is required if you are going to host multiple web-site domains on the same IP address. When first creating the site, enter your domain to get started, and you can later add additional domains as required. There are some requirements when using host headers that are inherent to the HTTP v1.1 specification (which defined host headers). These requirements are discussed below in this lab.

Click OK.

Click on your newly made site and click Start.

You can now browse to your site by its domain name, provided the DNS is correctly configured. Figure 6-3 shows WebSite1 in the Sites menu.

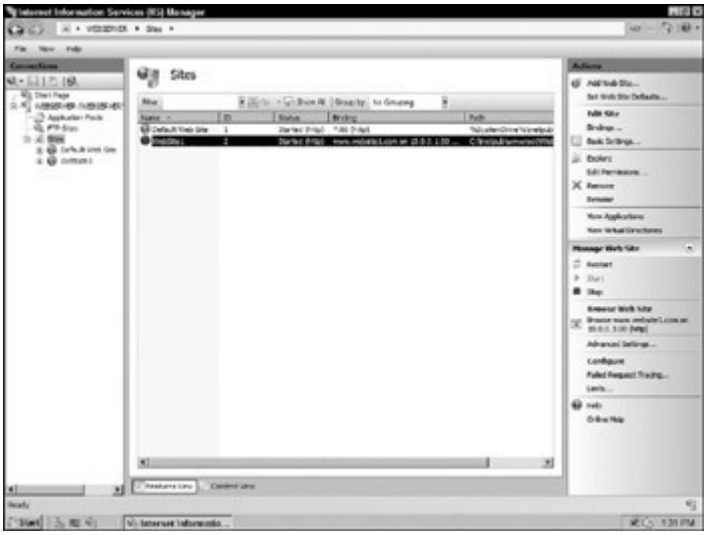


Figure 6-3

To start modifying the site configuration, simply click the site's name under the Sites list and you will be presented with the Features view, which gives you access to alter the configuration. The Content view shows the web-site files that are in the root directory of the site

Add a New Application Pool

It is a good practice to create a new application pool for each site, especially when you are hosting more than one web site on the same server. This will ensure that each web application runs inside its own process such that if an application causes a failure, it does not affect any other sites. Further information on application pools is available in Chapter 8, "Web Application Pool Administration." The Add Web Site tool in IIS Manager will automatically create a new application pool and map the site to it. If you chose not to create a new application pool when you created the site, or if you imported the site through a different method, you may need to manually create an application pool.

To create the new application pool, follow these steps:

Open IIS Manager, if it is not already open. (Start ⇛ Run, enter **inetmgr**, and press Enter.)

Select Application Pools under the server name from the Connections pane, and then select Add Application Pool from the Actions pane or right-click the Application Pools icon. This will present the Add Application Pools dialog. Figure 6-4 shows the Add Application Pool tool.

Figure 6-4

Set the name to something that is relevant — in this case, yourNameAppPool. (It might seem redundant to add AppPool to the end of the name; however, it does help for easing confusion with novice or other administrators.)

Select the .NET Framework version for the application pool to default to.

Select the Managed Pipeline Mode. For this site, we are going to use Integrated, which is the default setting. By default, the application pool will be created to run with the NetworkService identity.

Verify that the Start application pool immediately is checked, and click OK.

Now you can assign the new application pool to your site. To do this, select your web site under the server pane, then right-click or select View Applications from the Actions pane.

The View Applications, Select Application Defaults in the Actions area.

Click the Select button. In the drop down list select the yourNameAppPool. Click OK

Click OK again.

As soon as you click OK, the application is moved to the new application pool, which is then recycled. Be wary of this in production environment, lest you receive any unexpected results.

Add an ODBC Connection

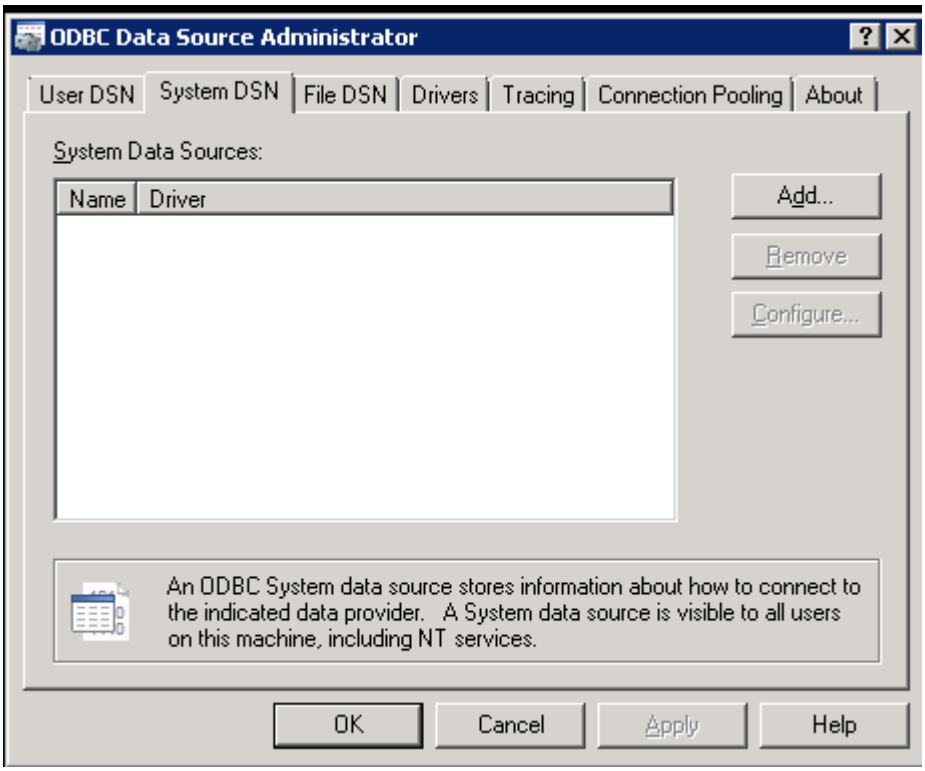
ODBC (Open database Connectivity) is a technology used by many Web applications. You will be creating an ODBC connection for myGrill.com. ODBC allows the web developer to establish a simple connection to a database and reuse that connection by referencing the name given to the connection.

Click on Start

In the Start Search box type **c:\windows\sysWOW64\odbcad32.exe, click** on odbcad32.exe when available from the list.

When the User Account Control dialog box appears, click Continue

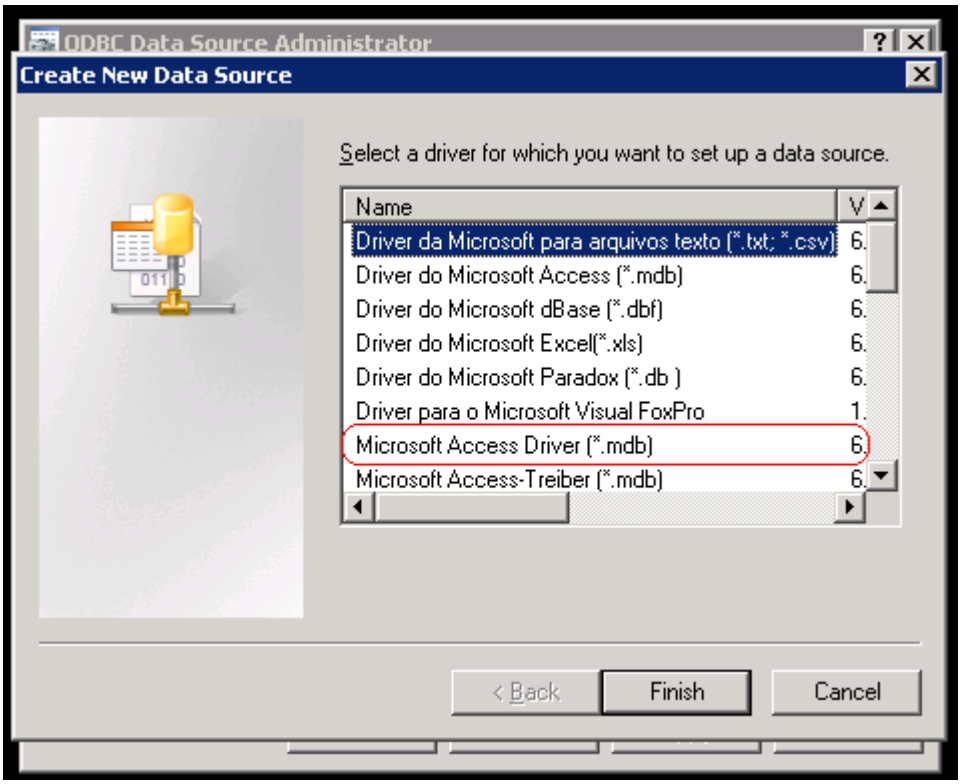
The ODBC Data Source Administrator dialog box will open



Select the **System DSN tab**

Click **Add**

Select **Microsoft Access Driver (.mdb)**



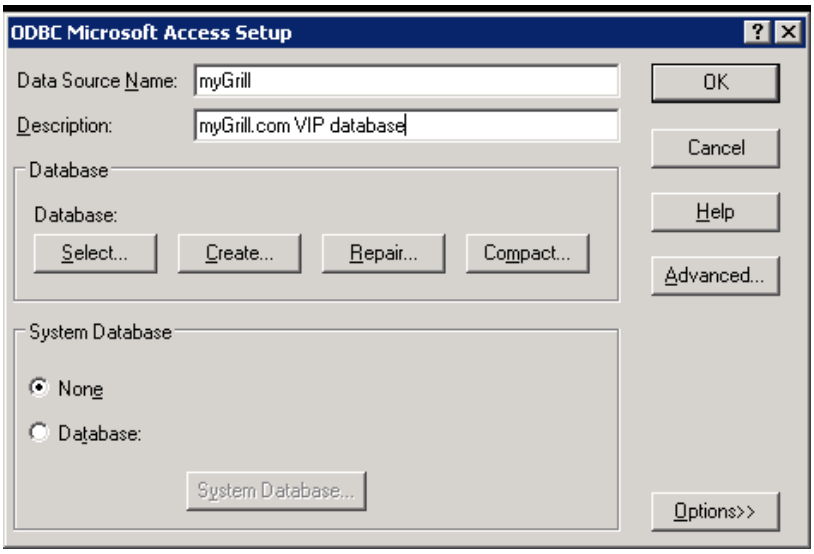
Click **Finish**

The ODBC Microsoft Access Setup dialog box will open

As an example, complete the following information:

Data Source Name: myGrill

Description: myGrill.com VIP database



Click **Select**

Navigate to and select: **c:\inetpub\wwwroot\myGrill.com\database\grill.mdb**

Click **OK**

Click **OK**

Click **OK**

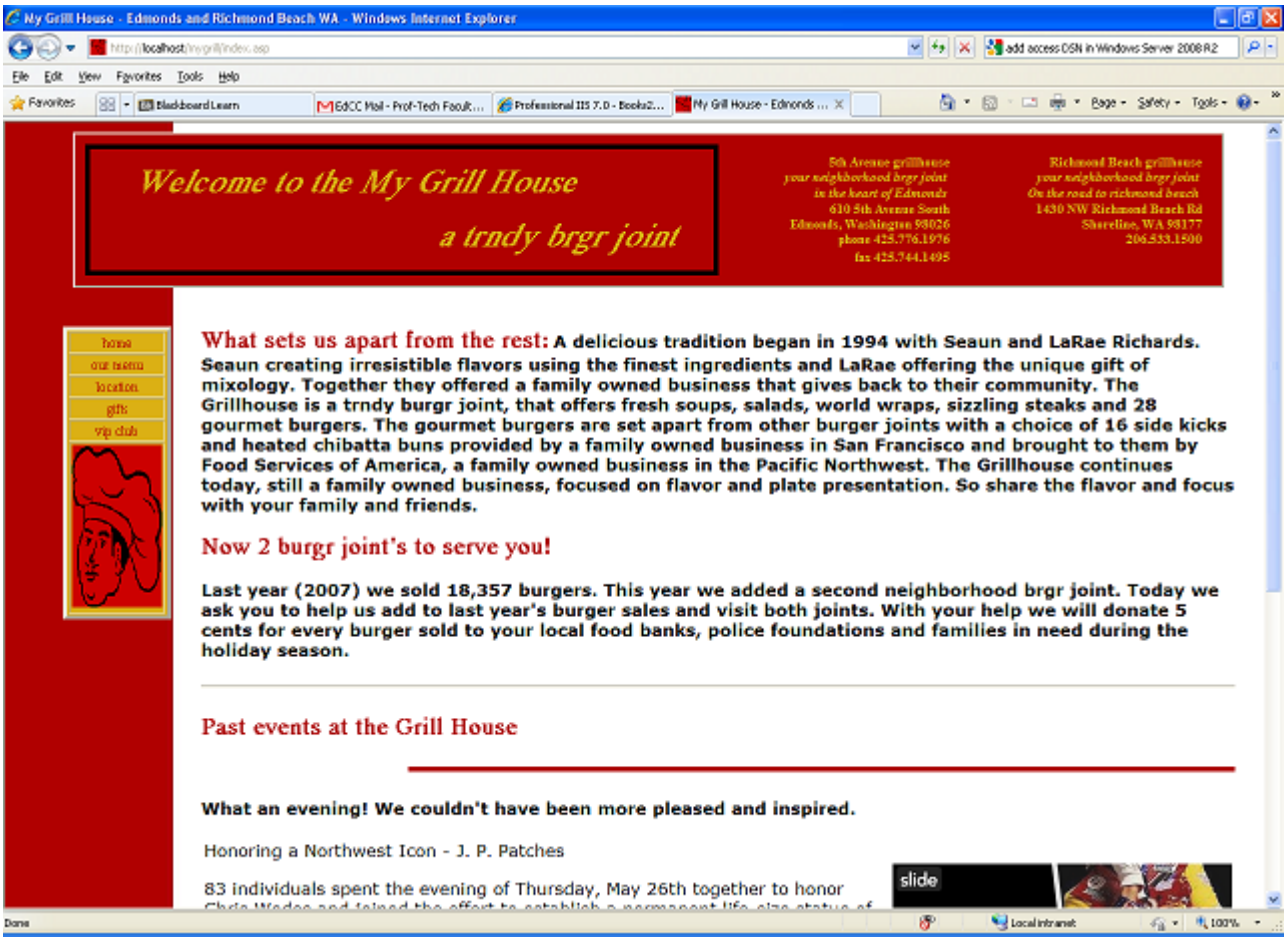
Verify that myGrill.com is working

Open Internet Explorer

Type the URL: http://localhost/mygrill.com/index.asp

You should see the following screen if myGrill.com is working correctly:

Windows IIS 7.0--EdCC



Create, Request, and Install TSL / SSL Certificates

TSL and its successor SSL are means of encrypting traffic (packets filled with information) across the WWW. Pages that request personal information should be accessed through encrypted pages. These include, but not restricted to:

Any personal information

User IDs

Passwords

Credit card numbers

Bank accounts

If you are at a site, and are asked for this type of information and are not on a page URI beginning with https:// you should verify that the form is sending the information encrypted before hitting submit.

FYI: you do not need to do this but you should be aware of how to do this as a savvy web user.

To verify that your information is being encrypted:

When asked for personal information

Look to see that the URL address includes: https:// at the beginning

If not, right click on the page and select View Source or View Page Source

Click on edit and search for the value of "**<form**"

Verify that the action attribute of the form element includes the value https://

Certificate Authorities

As you surf the web, you will run into certificates of authority and will at times accept these certificates. CA or Certificate Authorities are stored in your computer. These certificates often tell your browser to trust or un-trust a web site.

Viewing current CA's on your Web Server

To view a list of installed trusted CAs:

Click Start → Run, enter mmc.exe, and then press [Enter].

Choose File → Add/Remove Snapin.

Scroll through the list of Snapins and Select Certificates and click Add.

A prompt will appear offering a selection of the current user's account, a nominated service account, or the machine's account. Select Computer Account, click Next

Select Local Machine. Click Finish

Click OK to exit the Add/Remove Snapin dialog.

Expand the Trusted Root Certification Authorities node, and click on Certificates to view a list of installed trusted root CAs, as shown in Figure 15-1.

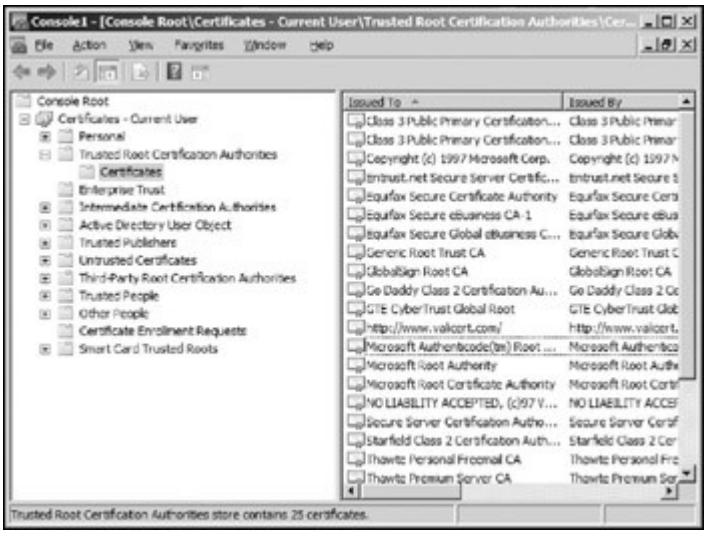


Figure 15-1

Close MMC

About Certificate Authorities

When establishing pages that should be viewed through encryption, you need to install a certificate on your Web server. This is a process that happens often in Web administration. Most ISP offer the services of getting a certificate for you site from a respected certificate authority. The two most trusted certificate authorities (IMHO) are:

VeriSign

GoDaddy.com

Prices vary greatly depending on the type of certificate that you purchase.

In this lab, we are going to create a self-signing certificate authority. While this is good practice, if you are actually running a web site or server for live production of a web site where you are collecting information from your users, you should consider purchasing a Certificate from a respected CA.

Generate a self-signed Certificate

Creating a server level certificate

Open IIS Manager (inetmgr)

Click Continue if requested

Click on your machine name:

Double click Server Certificates

In the Actions Pane, click on "Create Self-Signed Certificate"

Create a friendly name for the certificate – this is a reference name and can be anything that will identify what the certificate is. I would use something like "Server self-signed certificate"

Click OK

The certificate is now listed in your list of server certificates

Applying a certificate for use.

Expand the sites node in IIS Manager

Expand the myGrill.com node

In the Actions pane, click on bindings

Click the Add button

In the Types drop down list, select https

In the IP Address list, select 10.1.13.1XX (Your IP address)

In the SSL Certificate drop down list, select the certificate you created in step 4a Creating a server level certificate.

Click the View button

On the general tab, verify that the certificate is:

Issued to: (your machine name)

Issued by: (your machine name)

Click OK

Click OK

Click Close

Expand the admin folder node (note: you must have downloaded and replaced adminheader.inc from Blackboard for this to work)

Click on the myGrillAdmin folder with the application pool icon

Under the IIS area of features, double click SSL Settings

Click the checkbox “Require SSL”

Click Apply

The result of this setting is that the files within the admin folder will no longer be accepted unless the user agent (browser) is using an https: connection

Restart your server

Click Start →the right arrow icon →Restart

It is possible that you may need to create the admin folder as a virtual application

Right click on the admin folder of mygrill.com

Select Convert to an Application

From the dropdown list select Application myGrillAdminPool

Click the Select button

For alias type “admin”

Browse for the physical path: c:\inetpub\wwwroot\mygrill.com\admin

Click OK

Creating a virtual directory for the admin folder in mygrill.com

Right click on the admin folder

Select Add virtual directory

Alias: admin

Browse for the physical path: c:\inetpub\wwwroot\mygrill.com\admin

Click OK

Test your new settings

From IIS Manager Open Internet Explorer

Type in the URL: http://10.1.13.1XX/mygrill.com (where 1XX represents your IP address)

This page should still display without a problem

Navigate to a couple of pages at this level (the public level set for anonymous browsing)

Type in the URL: http://10.1.13.1XX/admin

The page should no longer display for you under http:// protocol You should receive a 403.4 error

Type in the URL: https://10.1.13.1XX/admin

When asked if you want to continue over a secure connection click yes

The page should now display again

Backing Up Your Virtual Server—Snapshot and Copy

Backup copies are to be done weekly

Snapshots are to be done any time a new process is to be implemented

Creating a VMWare Snapshot

Using remote desktop, login to your Windows 2008 R2 Server

Navigate to c:\inetpub\wwwroot\mygrill.com

To protect yourself during this lab we will be doing one more step

Right click on mygrill.com and select copy

Click on Documents

Right click in the right pane of Explorer and select paste; this process should take about 2 minutes

Log out of your Windows 2008 R2 Server

From your Windows 7 host machine

Double click your VMWare desktop icon

Click on your 225 Server 2008 R2 server

If needed start your server

In the Commands portion of the VMWare Web Access console

Click on “Take Snapshot”

If requested to replace an existing snapshot, click yes

The Snapshot process should take approximately 5 minutes

Making a drastic change to your server structure (ooops)

Using remote desktop, login to your Windows 2008 R2 virtual server

Right click on Start and select Explore

Navigate to c:\inetpub\wwwroot\mygrill.com

Right click on mygrill.com and select Delete

Click Yes

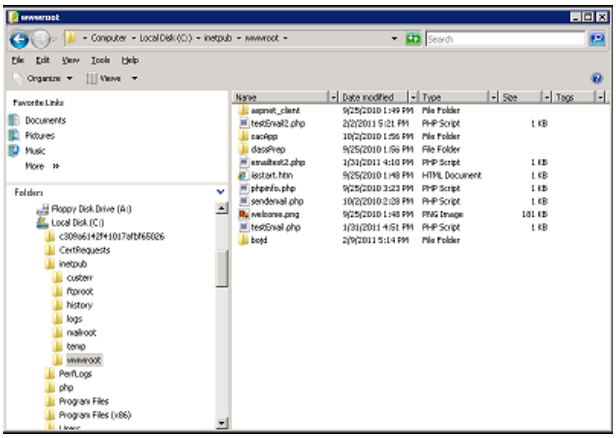
When asked to confirm this, select Continue

When asked to confirm this, select Continue

Ooops! – your really didn't want to delete this web site!

To assure that you have completed this step, please paste a screen capture of your virtual server directory structure showing wwwroot and all sub folders here:

Example: (be sure to resize this in a manner that will allow the full screen to fit and be readable)



Log off of your Windows 2008 R2 virtual server

Restoring your Snapshot

Return to your Windows 7 host machine and the VMWare Web Access console

In the Commands area, click on Revert to Snapshot

When requested to confirm reverting to the Snapshot, Select Yes

This process should take less than one minute

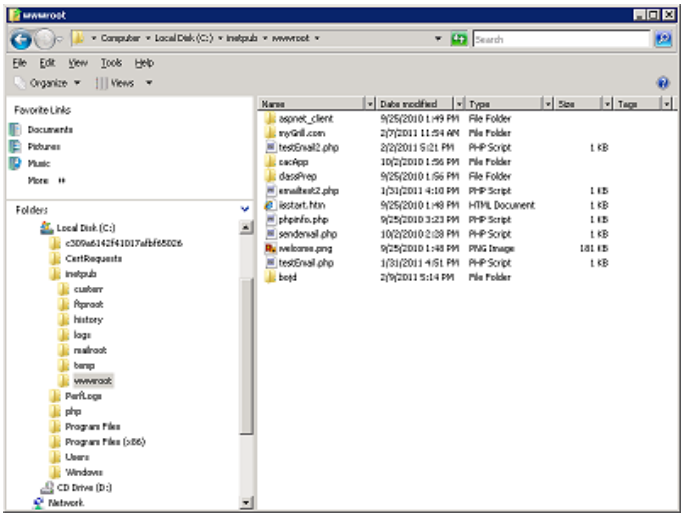
Verify the restoration of your file structure

Using remote desktop, login to your Windows 2008 R2 virtual server

Navigate to c:\inetpub\wwwroot and verify that mygrill.com has been returned to your directory structure.

Create a screen capture showing that myGrill.com has been returned to your file structure

Example: (be sure to resize this in a manner that will allow the full screen to fit and be readable)



Now that was painless!

Using Copy to Backup Your Virtual Server

While taking snapshots are a great interim backup method, there are hardware and software failures that could make snapshots unavailable for recovery. You should systematically create actual copies of your virtual servers on secondary storage devices.

In this lab, we are going to simulate creating a copy of your virtual server to a secondary storage device.

If needed, log off your Windows 2008 R2 virtual server

Return to your Windows 7 Host machine and the and the VMWare Web Access console

These steps are very important. PLEASE be careful as you do them.

In the Commands area of your VMWare Web Access console, click Configure VM

On the General tab: identify and write down the Working Directory name of your virtual server
Example: [standard] 225 Server 2008 R2
Your virtual server: _____

Click OK

Open Windows Explorer

Navigate to c:\Virtual Machines

Locate the folder named the same as the Working Directory specified above

Right click on the Working Directory and select Copy

Click on your Documents folder in Windows Explorer

Right click in the Document Library pane and select Paste

This process should take approximately one hour.

You have now created a backup "copy" of your virtual server.

At any time you could simply copy your virtual server back to its original location and be ready to fly!

Labs

Lab 1– Starting up

Lab 2– Installing IIS

lab 3– working with administration tools

lab 4– Application pool administration

lab 5– Remote administration

lab 5 supplement– Remote administration

lab 6– Configuring FTP services

lab 7– SMTP

lab 7 supplement– adding a printer

lab 8—Baseline Analizer

lab 9– NTFS and URL authentication

lab 10– SSL / TSL

lab 10 supplemental– Setting default files

lab 11– Submitting a request to a certificate authority

lab 11 supplemental– Updating your host file

lab 11 supplemental2– Installing SQL Server Express

Lab 12– Backing up virtual servers

Lab 12 supplement– Installing anti-virus software

lab 13– Installing PHP and MySQL

lab 14– Management

lab 14 supplemental– Configuring MIME types

lab 15-- Monitoring

HP Warranty

Introduction

Service Announcement 2080E_25 supersedes Service Announcement 2080E_24. The changes include the following released products:

■ Addition of all products announced since Revision 24.

HP Warranty Information

This document contains warranty information for HP products, including Compaq, Digital and Tandem branded products.

Note: Some products detailed are normally only supported directly by the HP Customer Services organisation. This document provides summary information. Please refer to the warranty statement shipped with product for a detailed explanation of the warranty terms associated with a particular product.

Limited warranty

This Limited Warranty applies only to HP-branded and Compaq-branded hardware products (collectively referred to in this document as “HP Hardware Products”) sold by or leased from Hewlett-Packard Company, its worldwide subsidiaries, affiliates, authorized resellers, or country distributors (collectively referred to in this Limited Warranty as “HP”) with this Limited Warranty. The term “HP Hardware Product” is limited to the hardware components and required firmware. The term “HP Hardware Product” DOES NOT include any software applications or programs; non-HP products or non-HP branded peripherals. All non-HP products or non-HP branded peripherals external to the HP Hardware Product— such as external storage subsystems, displays, printers and other peripherals—are provided “AS IS” without HP warranty. However, non-HP manufacturers and suppliers, or publishers may provide their own warranties directly.

HP guarantees that the HP Hardware Products that you have purchased or leased from HP are free from defects in materials or workmanship under normal use during the Limited Warranty Period. The Limited Warranty Period starts on the date of purchase or lease from HP. Your dated sales or delivery receipt, showing the date of purchase or lease of the product, is your proof of the purchase or lease date. You may be required to provide proof of purchase or lease as a condition of receiving warranty service. You are entitled to hardware warranty service according to the terms and conditions of this document if a repair to your HP Hardware Product is required within the Limited Warranty Period.

During the Limited Warranty Period, HP will, at its discretion, repair or replace any defective component. All component parts or hardware products removed under this Limited Warranty become the property of HP. In the unlikely event that your HP Hardware Product has recurring failures, HP, at its sole discretion, may elect to provide you with (a) a replacement unit of HP’s choosing that is the same or equivalent to your HP Hardware Product in performance or (b) to give you a refund of your purchase price or lease payments (less interest) instead of a replacement. This is your exclusive remedy for defective products.

It is mandatory that the unit product number and serial number be made available when requesting a warranty service event. Failure to do so may result in the event being deemed out of warranty by HP or, HP's Authorised Service Providers, and therefore chargeable to the requester.

Unless otherwise stated, and to the extent permitted by local law, new HP Hardware Products may be manufactured using new materials or new and used materials equivalent to new in performance and reliability. HP may repair or replace HP Hardware Products (a) with new or previously used products or parts equivalent to new in performance and reliability, or (b) with equivalent products to an original product that has been discontinued. Replacement parts are warranted to be free from defects in material or workmanship for ninety (90) days or, for the remainder of the Limited Warranty Period of the HP Hardware Product they are replacing or in which they are installed, whichever is longer.

Notes:

■Products external to the system processor (CPU) box, such as external storage subsystems, printers and other peripherals, are covered by the applicable warranty for those products or options.

■An effective repair does not necessarily require the replacement of a defective part. For example, cleaning the heads of a floppy drive or updating revision levels of ROM BIOS on a PCA board are activities that in many instances deliver an effective repair.

■BIOS/Firmware upgrades are not covered under the basic warranty Terms & Conditions. Firmware that is an integral part of the option hardware board is not automatically upgraded when new versions of firmware are released.

Where a specific hardware product problem is found to be caused by a superseded BIOS/firmware revision on an HP component, HP will either bring the firmware up to the latest revision, by exchanging the affected component under warranty, or will recommend that the customer upgrade the firmware using Flash-ROM where appropriate. It is essentially the responsibility of the customer to:

1.Ensure that their software is compatible with the latest BIOS/firmware revision.

2.Upgrade their firmware to keep it synchronised with the new software releases.

■HP fully understands the concerns raised by customers with regards to the security of any data which may be contained on a hard disk being sent for repair. HP's procedures for handling these items start by acknowledging that all such disks may contain sensitive business or technological information and that all appropriate security is in place to safeguard that information.

1.The procedure for handling returned units is as follows:

2.The documents accompanying a returned item, record the Authorised Service Provider name and ID number, the serial number of the machine it was removed from and a description of the fault.

3.Using the first two pieces of information for warranty verification only, the unit is then transferred to HP in Scotland, where it is mixed with units from all over Europe, Middle East and Africa for return to the repair vendor.

4.The repair of the item in no way depends on HP's ability to read any user data contained on the disk.

5.During the testing/repair cycle, the disks will have a destructive pattern written onto them that will erase all previously held user data.

6.If the media is damaged, it is removed and scrapped.

Note: HP does not support the use of degaussers to erase data on the disks. Doing so will invalidate the warranty as the degaussing will also erase other data on the disk which is required to format the disk and ensure it operates appropriately, for example sector alignment data, error correction logic, bad sector files and the geometry of the drive.

Even with the above processes, customers may still be reluctant to return defective disks due to confidential data contained on the disks. Customers who wish to retain the original disk will be required to purchase a replacement disk to affect the repair or, purchase the "Defective Material Retention" service offer.

■All marking and/or branding of HP products must be removable. If the marked or branded product can not be refurbished by HP for use (eg. the branding or tagging removed), then the customer may require to purchase a replacement part or unit. Where marking and/or branding cannot be removed, then the Part credit element of a service event may not be paid.

Exclusions HP does not guarantee that the operation of this product will be uninterrupted or error-free. HP is not responsible for damage that occurs as a result of your failure to follow the instructions intended for the HP hardware product.

This Limited Warranty does not apply to expendable or consumable parts and does not extend to any product from which:

The serial number has been removed, damaged or rendered defective;

(a) as a result of accident, misuse, abuse, contamination, improper or inadequate maintenance or calibration or other external causes;

(b) by operation outside the usage parameters stated in the user documentation that shipped with the product(including burned monitor screens and incorrect input voltage);

(c) by software, interfacing, parts or supplies not supplied by HP

(d) improper site preparation or maintenance

(e) virus infection

(f) loss or damage in transit

(g) by modification or service by anyone other than

(i) HP

(ii) an HP authorized service provider

(iii) your own installation of end-user replaceable HP or HP approved parts if available for your product in the servicing country or region.

HP IS NOT RESPONSIBLE FOR DAMAGE TO OR LOSS OF ANY PROGRAMS, DATA, OR REMOVABLE STORAGE MEDIA. HP IS NOT RESPONSIBLE FOR THE RESTORATION OR REINSTALLATION OF ANY PROGRAMS OR DATA OTHER THAN SOFTWARE INSTALLED BY HP WHEN THE PRODUCT IS MANUFACTURED.

Before returning any unit for service, be sure to back up data and remove any confidential, proprietary, or personal information.

HP is not responsible for any interoperability or compatibility issues that may arise when (1) products, software, or options not supported by HP are used; (2) configurations not supported by HP are used; (3) parts intended for one system are installed in another system of different make or model.

Limitation of liability

If the HP hardware product fails to work as warranted above, HP's maximum liability under the limited warranty is expressly limited to the lesser of the price paid for the product or the cost of repair or replacement of any hardware components that malfunction in conditions of normal use. Except as indicated above, in no event will HP be liable for any damages caused by the product or the failure of the product or perform, including any lost profits or savings, business interruption, loss of use or any other commercial or economic loss of any kind, or special, incremental, or consequential damages. HP is not liable for any claim made by a third party or made by you for the third party. This limitation of liability applies whether damages are sought, or a claim made, under this limited warranty or as a tort claim (including negligence and strict product liability), a contract claim or any other claim. This limitation in liability cannot be waivered or amended by any person. This limitation of liability will be effective even if you have advised HP, or an authorized representative of HP, of the possibility of any such damages or even if such possibility were reasonably foreseeable. This limitation of liability, however, will not apply to claims for personal injury.

This limited liability gives specific legal rights. You may also have other rights that may vary from state to state or from county to country. You are advised to consult applicable state or country laws for a full determination of rights.

If HP determines that damage/failure that exists is not covered by the warranty -- i.e. failure of Non-HP memory or options etc. -- the end user will be contacted to determine whether such damage/failure should be repaired for a charge or whether the Product should be returned to the end user as received. All associated transportation and handling costs are charged to the customer.

HP's warranty obligation extends only to products, options, and parts manufactured or distributed by HP, Compaq, Digital or Tandem under their respective brand names.

HP in this statement is the sales subsidiary of Hewlett Packard Corporation in the country where the claim is first raised; if no subsidiary exists in the country, it is Hewlett Packard Corporation GmbH in Munich, Germany.

Customer responsibilities

To enable HP to provide the best possible support and service during the Limited Warranty Period, you will be required to:

■Maintain a proper and adequate environment, and use the HP Hardware Product in accordance with the instructions furnished.

■Verify configurations, load most recent firmware, install software patches, run HP diagnostics and utilities, and implement temporary procedures or workarounds provided by HP while HP works on permanent solutions.

■Allow HP to keep resident on your systems or sites certain system and network diagnosis and maintenance tools to facilitate the performance of warranty support (collectively referred to as “Proprietary Service Tools”); Proprietary Service Tools are and remain the sole and exclusive property of HP. Additionally, you will:

- Use the Proprietary Service Tools only during the applicable warranty period and only as allowed by HP

- Install, maintain, and support Proprietary Service Tools, including any required updates and patches

- Provide remote connectivity through an HP-approved communications line, if required

- Assist HP in running the Proprietary Service Tools

- Use the electronic data transfer capability to inform HP of events identified by the software

- Purchase HP-specified remote connection hardware for systems with remote diagnosis service, if required

- Return the Proprietary Service Tools or allow HP to remove these Proprietary Service Tools upon termination of warranty support

- Not sell, transfer, assign, pledge, or in any way encumber or convey the Proprietary Service Tools

In some cases, HP may require additional software such as drivers and agents to be loaded on your system in order to take advantage of these support solutions and capabilities.

■Use HP remote support solutions where applicable. HP strongly encourages you to use available support technologies provided by HP. If you choose not to deploy available remote support capabilities, you may incur additional costs due to increased support resource requirements.

■Cooperate with HP in attempting to resolve the problem over the telephone. This may involve performing routine diagnostic procedures, installing additional software updates or patches, removing third-party options, and/or substituting options.

■Make periodic backup copies of your files, data, or programs stored on your hard drive or other storage devices as a precaution against possible failures, alteration, or loss. Before returning any HP Hardware Product for warranty support, back up your files, data, and programs, and remove any confidential, proprietary, or personal information.

■Maintain a procedure to reconstruct your lost or altered files, data, or programs that is not dependent on the HP Hardware Product under warranty support.

■Notify HP if you use HP Hardware Products in an environment that poses a potential health or safety hazard to HP employees or subcontractors. HP may require you to maintain such products under HP supervision and may postpone warranty service until you remedy such hazards.

■Perform additional tasks as defined within each type of warranty service listed below and any other actions that HP may reasonably request in order to best perform the warranty support.

Types of hardware warranty service

Listed below are the types of warranty services that may be applicable to the HP Hardware Product you have purchased. For more details, refer to the "Limited warranty period" section.

Customer self repair

HP products are designed with many Customer Self Repair (CSR) parts to minimize repair time and allow for greater flexibility in performing defective parts replacement. If during the diagnosis period, HP identifies that the repair can be accomplished by the use of a CSR part, HP will ship that part directly to you for replacement. There are two categories of CSR parts:

■Parts for which customer self repair is mandatory. If you request HP to replace these parts, you will be charged for the travel and labor costs of this service.

■Parts for which customer self repair is optional. These parts are also designed for customer self repair. If, however, you require that HP replace them for you, this may be done at no additional charge under the type of warranty service designated for your product.

Based on availability and where geography permits, CSR parts will be shipped for next business day delivery. Same-day or four-hour delivery may be offered at an additional charge where geography permits. If assistance is required, you can call the HP Technical Support Center and a technician will help you over the phone. HP specifies in the materials shipped with a replacement CSR part whether a defective part must be returned to HP. In cases where it is required to return the defective part to HP, you must ship the defective part back to HP within a defined period of time, normally five (5) business days. The defective part must be returned with the associated documentation in the provided shipping material. Failure to return the defective part may result in HP billing you for the replacement. With a customer self repair, HP will pay all shipping and part return costs and determine the courier/carrier to be used.

Parts only warranty service: Your HP Limited Warranty may include a parts only warranty service. Under the terms of parts only service, HP will provide replacement parts free of charge. If HP carries out the repair, labor and logistics costs are at your expense.

Advanced unit replacement warranty service

Your HP Limited Warranty may include an advanced unit replacement warranty service. Under the terms of the advanced unit replacement warranty service, HP will ship a replacement unit directly to you if the HP Hardware Product you purchased is diagnosed as defective. On receiving the replacement unit, you will be required to return the defective unit back to HP, in the packaging that arrives with the replacement unit, within a defined period of time, normally five (5) days. HP will incur all shipping and insurance costs to return the defective unit to HP. Failure to return the defective unit may result in HP billing you for the replacement unit.

Pick up and return warranty service

Your HP Limited Warranty may include a pick up and return warranty service. Under the terms of pick up and return service, HP will pick up the defective unit from your location, repair it, and return it to your location. HP will incur all repair, logistics, and insurance costs for this type of service.

Mail-in warranty service

Your HP Limited Warranty may include a mail-in warranty service. Under the terms of mail-in service, you will be required to ship your HP Hardware Product to an authorized service location for warranty repair. You must prepay any shipping charges, taxes, or duties associated with transportation of the product to the repair location. In addition, you are responsible for insuring any product you ship, and you assume risk of loss during shipping. HP will return the repaired product to you and incur all logistics and insurance costs to return the product to you.

Carry-in warranty service

Your HP Limited Warranty may include a carry-in warranty service. Under the terms of carry-in service, you will be required to deliver your HP Hardware Product to an authorized service location for warranty repair. You must prepay any shipping charges, taxes, or duties associated with transportation of the product to and from the service location. In addition, you are responsible for insuring any product shipped or returned to an authorized service location, and you assume risk of loss during shipping.

On-site warranty service

Your HP Limited Warranty may include an on-site warranty service. Under the terms of on-site service, HP may, at its sole discretion, determine if a defect can be repaired:

■Remotely

■By the use of a CSR part

■By a service call at the location of the defective unit

If HP ultimately determines that an on-site service call is required to repair a defect, the call will be scheduled during standard office hours unless otherwise stated for the HP Hardware Product you purchased. Standard office hours are typically 08:00 to 17:00, Monday through Friday, but may vary with local business practices. If

the location of the defective unit is outside the customary service zone (typically 50km), response times may be longer or there may be additional charges. To locate the nearest HP authorized service provider, refer to the HP website at www.hp.com/support.

In order to receive on-site support, you must:

■Have a representative present when HP provides warranty services at your site

■Notify HP if products are being used in an environment which poses a potential health or safety hazard to HP employees or subcontractors

■Subject to its reasonable security requirements, provide HP with sufficient, free, and safe access to and use of all facilities, information, and systems determined necessary by HP to provide timely support

■Ensure that all manufacturers labels (such as serial numbers) are in place, accessible, and legible

■Maintain an environment consistent with product specifications and supported configurations

Listed below are the types of warranty services that may be applicable to the HP Hardware Product you have purchased. For more details, refer to the "Limited warranty period" section.

Options limited warranty

The Limited Warranty terms and conditions for most HP-branded options (HP Options) are as set forth in the Limited Warranty applicable to the HP Option and are included in the HP Option product packaging. If your HP Option is installed in an HP Hardware Product, HP may provide warranty service for either the period specified in the warranty documents (HP Option Limited Warranty Period) that shipped with the HP Option or for the remaining warranty period of the HP Hardware Product in which the HP Option is being installed, whichever period is the longer unless stated otherwise in the "Limited warranty period" section. In all cases, the warranty period of the HP Option will not exceed three (3) years from the date you purchased the HP Option. The HP Option Limited Warranty Period starts from the date of purchase from HP or an HP authorized reseller. Your dated sales or delivery receipt, showing the date of purchase of the HP Option, is your warranty start date. See your HP Option Limited Warranty for more details. Non-HP options are provided "AS IS". However, non-HP manufacturers and suppliers may provide warranties directly to you.

Spare parts

All HP spare parts (see Notes 1 and 2 below) that are used to replace defective parts in a HP product are entitled to:

•the remaining service period of the product in which it is installed; or

•90 days parts replacement warranty, whichever is greater.

This may include free on-site repair if the HP product is entitled to on-site warranty. See Table - Warranty Services Table.

NOTE 1: The replacement spare part must be a genuine HP spare part.

NOTE 2: This does not include Spare Rechargeable Battery Packs, Spare Compaq Netelligent Products and Network Interface Cards, Microcom Integrated Access Devices, and Compaq External Modems (see below).

Spare Compaq Rechargeable Battery Packs are entitled to a 12 month Parts-only Warranty. Spare Compaq Netelligent, Compaq External Modems and Microcom Integrated Access Products are entitled to the remaining warranty of the replaced product as shown in Table. They do not adopt the remaining service period of the product to which they are connected and or any warranty services to which the product is entitled (this/which may include free on-site repair). Spare Netelligent Network Interface Cards receive lifetime Parts-only Warranty.

NOTE: Spare Part, provided that the replacement part is a genuine HP spare part, purchased to repair ''Out of Warranty'' machines are entitled to 90 days parts-only warranty from date of sale of the spare part to the End User. It is a requirement that an End User Proof of Purchase is provided when claiming spare part warranty. Validation of the spare part warranty will be made against this Proof of Purchase. This may be dependent on local country legislation.

Software limited warranty

Except as provide in the applicable software end-user license or program license agreement, or if otherwise provided under local law, software products, including any software products, freeware (as defined below) or operating systems preinstalled by HP are provided “AS IS” and with all faults, and HP hereby disclaims all other warrantyies and conditions, either express, implied, or statutory, including, but not limited to, warranties of title and non-infringement, any implied warranties, dutues or conditions of merchantability, of fitness for a particular purpose, and lack of viruses.

Some states/jurisdictions do not allow exclusion of implied warranties or limitations on the duration of implied warranties, so the above disclaimer may not apply to you in its entirety. To the maximum permitted by applicable law, in no event shall HP or its suppliers be liable for any special, incidental, indirect, or consequential damages whatsoever (including, but not limited to, damages for loss of profits or confidential or other information, for business interruption, for personal injury, for loss of privacy arising out of or in any way related to the use or inability to use the software product, even if HP or any supplier has been advised of the potential of such damages and even if the remedy fails of its essential purpose.. Some states/jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

HP's only warranty obligations with respect to software distributed by HP under the HP brand name are set forth in the applicable end-user license or program license agreement provided with that software. If the removable media on which HP distributes the software proves to be defective in materials or workmanship

within ninety (90) days of purchase, your sole remedy shall be to return the removable media to HP for replacement. For blank tape removable media please refer to the following website: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=lpg50101

It is your responsibility to contact non-HP manufacturers or suppliers for their warranty support.

Freeware operating systems and applications

HP does not provide support for software provided under public license by third parties, including operating systems or applications ("Freeware"). Support for Freeware provided with HP Hardware Products is provided by the Freeware vendor. Please refer to the Freeware operating system or other Freeware application support statement included with your HP Hardware ProductNote:If the removable media on which HP distributes the software proves to be defective in materials or workmanship within ninety (90) days of purchase, the sole remedy shall be to return the removable media to HP for replacement. For blank tape removable media please refer to the following web site.

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=lpg50101

Support for initial setup

Electronic or telephone support for initial setup is available from HP for ninety (90) days from date of purchase. See “Contacting HP” for online resources and telephone support.

Support includes:

■Answering installation questions (how-to, first steps, and prerequisites)

■Setting up and configuring software and options supplied or purchased with HP Hardware Products (how-to and first steps)

■Interpreting system error messages

■Isolating system problems

■Obtaining support pack information or updates for software purchased or supplied with HP Hardware Products

Support does NOT include assistance with:

■Generating or diagnosing user-generated programs or source codes

■Installation of non-HP products

■System optimization, customization, and network configuration.

Limited warranty transfer to another country

Under the HP Global Limited Warranty program, products may be purchased in one country/region and transferred to another country/region, where HP or its authorized service providers offer warranty service for the same product model number without voiding the warranty. Warranty terms, service availability, and service response times may vary from country to country or region to region. Standard warranty service response time is subject to change due to local parts availability. When the product has been transferred to another country it will be entitled to the same warranty as if the product had been purchased in the country to which it has been transferred.

HP is not responsible for any tariffs or duties that may be incurred in transferring the products. Transfer of the products may be covered by export controls issued by the United States or other governments.

HP's Warranty Service Delivery Methods.

HP delivers warranty service on HP products via several delivery methods. Warranty service is provided during normal business hours, excluding local holidays, and is based on commercially reasonable efforts by HP or an HP Service Provider. Unless otherwise stated, all responses are measured from the time the customer calls HP or until HP has established a mutually acceptable time for support to be performed.

The definitions of HP's Warranty Service Delivery methods are detailed below:

On site Same Business Day: HP aims to ensure that a customer problem will be responded to within 4 hours, following the end users first notification of equipment failure. Unless otherwise stated, all responses are measured from the time the customer calls, or a mutually acceptable time for support to be performed has been established, or HP has begun to provide support or remote diagnostics. This is available on a 24 hour x 7 day basis with a work through until resolution of the problem.

On site One Business Day: HP aims to ensure that the product will be operational by the end of the next business day following the end users first notification of equipment failure. Unless otherwise stated, all responses are measured from the time the customer calls, or a mutually acceptable time for support to be performed has been established, or HP has begun to provide support or remote diagnostics.

For example: Customer reports the failure of a Systems product at any time during business hours on Monday, the product will be fixed by the end of business day on Tuesday.

On site Two Business Day: HP aims to ensure that the product will be operational by the end of the second business day following the end users first notification of equipment failure. Unless otherwise stated, all responses are measured from the time the customer calls, or a mutually acceptable time for support to be performed has been established, or HP has begun to provide support or remote diagnostics.

For example: Customer reports the failure of a Business Desktop product at any time during business hours on Monday, the product will be fixed by the end of business day on Wednesday.

Carry-in Two Business Day: HP aims to ensure that the product will be operational and available to the end user within two business days following arrival of the faulty equipment at the service providers workshop location.

For example: Customer delivers a faulty product to a carry-in repair centre at any time during business hours on Monday, the product will be available for collection by the end of business day on Wednesday.

Carry-in Five Business Day: HP aims to ensure that the product will be operational and available to the end user within five business days following arrival of the faulty equipment at the service provider's workshop location.

For example: Customer delivers a faulty product to a carry-in repair centre at any time during business hours on Monday, the product will be available for collection by the end of business day on the following Monday.

Mail-in Five Business Day: HP aims to ensure that the product will be operational and returned to the end user within five business days following arrival of the faulty equipment at a HP Service Centre for repair.

For example: Customer delivers a faulty product to a Mail-in centre at any time during business hours on Monday, the product will be returned to the customer by the end of business day on Tuesday of the following week.

Pick Up & Return Two Business Day: HP aims to ensure that the product will be operational and returned to the end user within two business days following the pick up of the faulty equipment from the customer.

For example: HP or an HP Service Provider pick up the defective unit from the customer any time during business hours on Monday, the product will be delivered back to the customer by the end of business day on Wednesday.

Pick Up & Return Five Business Day: HP aims to ensure that the product will be operational and returned to the end user within five business days following the pick up of the faulty equipment from the customer..

For example: HP or an HP Service Provider pick up the defective unit from the customer any time during business hours on Monday, the product will be delivered back to the customer by the end of business day on Friday.

HP Care Pack Services Information

HP also offers extended/upgraded services under the name of Care Pack. A wide range of Care pack services is available to cover most current HP products. It is the customer's responsibility to register each Care pack with HP so that the related hardware is automatically allocated the correct extended/upgraded service by the EMEA service management system. Refer to the following site for more details.

http://h41111.www4.hp.com/hps/carepack/uk/en/index.html

HP Care Pack Services Information

Requirements

HP Warranty Services

The following Warranty Services tables provide a general summary of the warranty offerings for HP products. The warranty documents provided with the goods at time of sale provide details of the actual warranty terms. Please refer to the notes at the end of the table for clarification of terminology, delivery methods and additional information.

Key to Warranty

Please refer to the Warranty methods section above for an explanation of terms.

SBD = Onsite Same business day,

1BD = Onsite One business day,

2BD = Onsite second business day,

5BD = Onsite fifth business day,

PuR = Pick Up and Return,

POW = parts only warranty.

back

CLIENT ASSURANCE AGREEMENT

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE YOU AGREE TO THESE TERMS. IF YOU ARE ACTING ON BEHALF OF AN ENTITY, THEN YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO ENTER INTO THIS AGREEMENT ON BEHALF OF THAT ENTITY. IF YOU DO NOT AGREE TO THESE TERMS, YOU WILL CONTINUE TO BE ABLE TO USE THE COVERED SOFTWARE TO THE EXTENT PERMITTED BY OTHER AGREEMENTS WITH CDS; HOWEVER, YOU WILL NOT BE COVERED UNDER CDS'S OPEN SOURCE ASSURANCE PROGRAM AS PROVIDED HEREIN.

This Open Source Assurance Agreement ("Agreement") is between Client (defined below) and Cheetah Delivery Services., a Washington corporation, with a principal place of business of 20000 68th Ave W, Lynnwood, WA, U.S.A. (“CDS”). Client is the entity represented by the authorized individual that accepts this Agreement. The effective date of this Agreement ("Effective Date") is the date that the authorized individual accepted this Agreement on behalf of Client.

1. Open Source Assurance Program

If an unaffiliated third party initiates a legal action against Client alleging that Client's use of Covered Software directly infringes the third party's copyrights, patents or trademarks, or misappropriates the third party's trade secret rights ("Third Party Rights") (such action, a "Claim") and Client has complied with the terms of this Agreement and the Support Agreement(s), then:

Subject to the other terms in this Agreement, CDS will (i) defend Client against the Claim and (ii) pay costs, damages and/or attorneys fees that are included in a final judgment against Client (without right of appeal) or in a settlement approved by CDS that are attributable to Client's use of the Covered Software; and

If Client's use of Covered Software is found by a court to infringe Third Party Rights (or CDS believes that such a finding is likely), then CDS will, at its expense and option: (i) obtain the rights necessary for Client to continue to use the Covered Software consistent with the Support Agreement(s); (ii) modify the Covered Software so that it is non-infringing; or (iii) replace the infringing portion of the Covered Software with non-infringing code of similar functionality (subsections (i), (ii) and (iii) are the "IP Resolutions"); provided that if none of the IP Resolutions is available on a basis that CDS finds commercially reasonable, then CDS may terminate the Support Agreement(s) without further liability under this paragraph, and, if Client then returns the Covered Software that is subject to the Claim, CDS will refund any prepaid subscription fees related to Covered Software.

As conditions precedent to CDS's obligations to Client under this Section 1, Client must comply with the following conditions. Client must (i) be current in the payment of all applicable fees prior to a Claim or threatened Claim; (ii) notify CDS promptly, but in no event later than ten (10) days of receipt of any Claim for which relief is sought under this Agreement (including evidence of the Claim brought); (iii) provide CDS with the right to control and conduct the defense of the Claim with counsel of its choice and to settle such Claim at CDS's sole discretion; and (iv) cooperate with CDS in the defense of the Claim. Notwithstanding the foregoing, CDS will have no obligations under Section 1 with regard to any Claim that is based upon (I) a modification of Covered Software made by Client (other than at CDS's written direction); (II) CDS's compliance with any designs, specifications or instructions provided by Client; (III) use of the Covered Software in combination with products, data or business methods not provided by CDS, if the infringement or misappropriation would not have occurred without the combined use; (IV) facts or circumstances constituting a breach of any Support Agreement; (V) use of any release of the Covered Software if, as of the date of a Claim or threatened Claim, the infringement or misappropriation would not have occurred through use of a more recent release of the Covered Software; (VI) any use of the Covered Software by Client other than for Client's internal use (such use not to include web hosting services, managed services, Internet service provider (ISP) services or similar uses); (VII) use by Client after notice by CDS to discontinue use of all or a portion of the Covered Software; or (VIII) a Client's claim or lawsuit against a third party.

2. Term, Warranties, Governing Law

The term of this Agreement will begin on the Effective Date and will terminate upon the expiration or termination of Client's Support Agreement(s); provided that if CDS updates or amends its Open Source Assurance program, (i) this Agreement will apply only until the end of the current annual subscription period

for any active Client Subscriptions and (ii) Client will have the opportunity, if it so elects, to participate in the updated or amended Open Source Assurance program for any additional Subscriptions or renewal Subscriptions. If this Agreement is terminated for any reason, Sections 2 - 5 will survive termination. No express or implied warranties by CDS or its affiliates are created as a result of this Agreement.

THE VALIDITY, INTERPRETATION AND ENFORCEMENT OF THIS AGREEMENT WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE UNITED STATES AND OF THE STATE OF NEW YORK WITHOUT GIVING EFFECT TO THE CONFLICTS OF LAWS PROVISIONS THEREOF OR THE UNITED NATIONS CONVENTION ON CONTRACTS FOR THE INTERNATIONAL SALE OF GOODS. ALL DISPUTES ARISING OUT OF OR RELATING TO THIS AGREEMENT WILL BE SUBMITTED TO THE EXCLUSIVE JURISDICTION OF THE STATE OR FEDERAL COURTS OF COMPETENT JURISDICTION LOCATED IN RALEIGH, NORTH CAROLINA, U.S.A. AND EACH PARTY IRREVOCABLY CONSENTS TO PERSONAL JURISDICTION IN SUCH COURTS AND WAIVES ALL OBJECTIONS TO THIS VENUE.

In the event the Uniform Computer Information Transactions Act (UCITA) or any similar federal or state laws or regulations are enacted, it will not apply to this Agreement, and the governing law will remain as if such law or regulation had not been enacted.

3. Limitations on Liability

CDS will not be obligated to pay any amounts in connection with a Claim related to any period of time during which Client does not have active, fully-paid Subscriptions related to the Covered Software. CDS will have no obligation to Client under this Agreement if, as of the Effective Date, Client has received notice of allegations of infringement or is engaged in litigation concerning the subject matter of what would otherwise be a Claim under this Agreement or with respect to a product substantially similar to the Covered Software.

IT IS CDS'S INTENT TO PROVIDE CLIENT A SET OF PROTECTIONS UNDER THIS AGREEMENT RELATED TO CLAIMS (AS DEFINED ABOVE). IT IS NOT, HOWEVER, CDS'S INTENT TO EXPAND CDS'S TOTAL LIABILITY TO CLIENT IN EXCESS OF THE LIABILITY LIMITATIONS SET FORTH UNDER EXISTING SUPPORT AGREEMENT(S) WITH CLIENT. IN THIS REGARD, CDS'S AND ITS AFFILIATES' AGGREGATE AND CUMULATIVE LIABILTY UNDER BOTH THIS AGREEMENT AND THE SUPPORT AGREEMENT(S) SHALL BE SUBJECT TO THE LIMITATIONS OF LIABILITY CONTAINED IN THE SUPPORT AGREEMENT(S) IN EFFECT AS OF THE DATE OF A CLAIM; PROVIDED, HOWEVER, IN NO EVENT WILL CDS'S AND ITS AFFILIATES' AGGREGATE AND CUMULATIVE LIABILITY TO CLIENT ARISING OUT OF OR RELATING TO ANY AND ALL CLAIMS UNDER THIS AGREEMENT EXCEED THE TOTAL FEES PAID TO CDS IN RESPECT OF CLIENT'S PURCHASES OF SUBSCRIPTIONS (DIRECTLY OR INDIRECTLY FROM A CDS RESELLER) DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE FIRST EVENT GIVING RISE TO LIABILITY FOR CDS FOR CLAIMS UNDER THIS AGREEMENT. NOTWITHSTANDING ANYTHING TO THE

CONTRARY CONTAINED IN THIS AGREEMENT OR THE SUPPORT AGREEMENT(S), IN NO EVENT WILL CDS OR ITS AFFILIATES BE LIABLE TO CLIENT OR ITS AFFILIATES FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, INDIRECT, EXEMPLARY OR PUNITIVE DAMAGES, WHETHER ARISING IN TORT, CONTRACT, OR OTHERWISE; OR FOR ANY DAMAGES ARISING OUT OF OR IN CONNECTION WITH ANY MALFUNCTIONS, DELAYS, LOSS OF DATA, LOST PROFITS, LOST SAVINGS, INTERRUPTION OF SERVICE, LOSS OF BUSINESS OR ANTICIPATORY PROFITS, EVEN IF CDS OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This Agreement sets forth Client's exclusive remedies and CDS's sole obligations for claims arising from or related to copyrights, patents, trademarks and trade secrets and supersedes any other CDS obligation related to the subject matter of this Agreement (including, but not limited to, indemnification, breach of warranty, and/or breach of contract under the Support Agreement(s) or otherwise). For the avoidance of doubt, the terms of Section 1 above shall apply in the place of, and the Client expressly waives any rights and releases CDS from, any obligations under the terms of any other warranties or terms relating to intellectual property rights or remedies, including without limitation Open Source Assurance terms or conditions that may be included in the Support Agreement(s). If there are any other applicable indemnity coverage or remedies available to Client related to intellectual property infringement, Client agrees that the total of all benefits payable under all such provisions will not exceed the total damages, costs, and expenses incurred by Client, and that CDS will pay only its proportional share of such total damages, costs, and expenses, subject to the immediately preceding paragraph above.

4. Covered Software, Covered Systems, Subscription

The "Covered Software" is CDS Enterprise Linux and other CDS branded software programs (including modifications and enhancements) generally released to its customers by CDS and/or its subsidiaries that Client installs or executes on Covered Systems, where "Covered Systems" are those computer systems on which Client has an active Subscription at the time of the Claim or threatened Claim. A "Subscription" is a services subscription purchased from CDS and/or its affiliates or a CDS reseller that entitles Client to receive CDS Services and that has been activated in RHN (see http://www.redhat.com/rhel/details/howtoactivate/ for information on activation). Covered Software does not include the Third Party Programs or the Excluded Programs, in each case, listed at www.redhat.com/licenses.

5. Miscellaneous

(i) Notices must be in English, in writing, and will be deemed given when delivered by hand or five (5) days after being sent using a method that provides for positive confirmation of delivery to Client at the address indicated on Client's CDS Network account registration form or to CDS at: CDS, Inc., Attention: General Counsel, 1801 Varsity Drive, Raleigh, North Carolina 27606, U.S.A.; Facsimile: (919) 754-3704. (ii) This Agreement is binding on the parties to this Agreement, and nothing in this Agreement confers upon any other person or entity any right, benefit or remedy of any nature whatsoever. This Agreement is assignable by either party only with the other party's prior written consent; provided that CDS may assign this Agreement to an affiliate or pursuant to a

merger or a sale of all or substantially all of its assets or stock without the prior approval of Client. (iii) The delay or failure of either party to exercise any rights hereunder will not constitute or be deemed a waiver or forfeiture of such rights. No waiver will be valid unless in writing and signed by an authorized representative of the party against whom such waiver is sought to be enforced. (iv) This Agreement represents the final, complete and exclusive statement of the agreement between the parties with respect to the subject matter of this Agreement, and all prior written agreements and all prior and contemporaneous oral agreements with respect to the subject matter of this Agreement are merged herein. If any provision of this Agreement is held invalid or unenforceable for any reason, this Agreement will be deemed invalid in its entirety. Except as set forth in Section 2 above, this Agreement may not be amended, supplemented or modified except by a written instrument signed by the parties hereto, which instrument makes specific reference to this Agreement.

* Found at http://www.redhat.com/legal/open_source_assurance_agreement.html

back

MIME Types

.3dm	x-world/x-3dmf
.3dmf	x-world/x-3dmf
.a	application/octet-stream
.aab	application/x-authorware-bin
.aam	application/x-authorware-map
.aas	application/x-authorware-seg
.abc	text/vnd.abc
.acgi	text/html
.afl	video/animaflex
.ai	application/postscript
.aif	audio/aiff
.aif	audio/x-aiff
.aifc	audio/aiff
.aifc	audio/x-aiff
.aiff	audio/aiff
.aiff	audio/x-aiff
.aim	application/x-aim
.aip	text/x-audiosoft-intra
.ani	application/x-navi-animation
.aos	application/x-nokia-9000-communicator-add-on-software
.aps	application/mime
.arc	application/octet-stream
.arj	application/arj
.arj	application/octet-stream
.art	image/x-jg
.asf	video/x-ms-asf
.asm	text/x-asm
.asp	text/asp
.asx	application/x-mplayer2
.asx	video/x-ms-asf
.asx	video/x-ms-asf-plugin
.au	audio/basic
.au	audio/x-au
.avi	application/x-troff-msvideo
.avi	video/avi
.avi	video/msvideo
.avi	video/x-msvideo
.avs	video/avs-video
.bcpio	application/x-bcpio
.bin	application/mac-binary
.bin	application/macbinary
.bin	application/octet-stream
.bin	application/x-binary
.bin	application/x-macbinary
.bm	image/bmp
.bmp	image/bmp

.bmp image/x-windows-bmp

.boo application/book

.book application/book

.boz application/x-bzip2

.bsh application/x-bsh

.bz application/x-bzip

.bz2 application/x-bzip2

.c text/plain

.c text/x-c

.c++ text/plain

.cat application/vnd.ms-pki.seccat

.cc text/plain

.cc text/x-c

.ccad application/clariscad

.cco application/x-cocoa

.cdf application/cdf

.cdf application/x-cdf

.cdf application/x-netcdf

.cer application/pkix-cert

.cer application/x-x509-ca-cert

.cha application/x-chat

.chat application/x-chat

.class application/java

.class application/java-byte-code

.class application/x-java-class

.com application/octet-stream

.com text/plain

.conf text/plain

.cpio application/x-cpio

.cpp text/x-c

.cpt application/mac-compactpro

.cpt application/x-compactpro

.cpt application/x-cpt

.crl application/pkcs-crl

.crl application/pkix-crl

.crt application/pkix-cert

.crt application/x-x509-ca-cert

.crt application/x-x509-user-cert

.csh application/x-csh

.csh text/x-script.csh

.css application/x-pointplus

.css text/css

.cxx text/plain

.dcr application/x-director

.deepv application/x-deepv

.def text/plain

.der application/x-x509-ca-cert

.dif video/x-dv

.dir application/x-director

.dl video/dl

.dl video/x-dl

.doc application/msword

.dot application/msword

.dp application/commonground

.drw application/drafting

.dump application/octet-stream

.dv video/x-dv

.dvi application/x-dvi

.dwf drawing/x-dwf (old)

.dwf model/vnd.dwf

.dwg application/acad

.dwg image/vnd.dwg

.dwg image/x-dwg

.dxf application/dxf

.dxf image/vnd.dwg

.dxf image/x-dwg

.dxr application/x-director

.el text/x-script.elisp

.elc application/x-bytecode.elisp (compiled elisp)

.elc application/x-elc

.env application/x-envoy

.eps application/postscript

.es application/x-esrehber

.etx text/x-setext

.evy application/envoy

.evy application/x-envoy

.exe application/octet-stream

.f text/plain

.f text/x-fortran

.f77 text/x-fortran

.f90 text/plain

.f90 text/x-fortran

.fdf application/vnd.fdf

.fif application/fractals

.fif	image/fif
.fli	video/fli
.fli	video/x-fli
.flo	image/florian
.flx	text/vnd.fmi.flexstor
.fmf	video/x-atomic3d-feature
.for	text/plain
.for	text/x-fortran
.fpx	image/vnd.fpx
.fpx	image/vnd.net-fpx
.frl	application/freeloader
.funk	audio/make
.g	text/plain
.g3	image/g3fax
.gif	image/gif
.gl	video/gl
.gl	video/x-gl
.gsd	audio/x-gsm
.gsm	audio/x-gsm
.gsp	application/x-gsp
.gss	application/x-gss
.gtar	application/x-gtar
.gz	application/x-compressed
.gz	application/x-gzip
.gzip	application/x-gzip
.gzip	multipart/x-gzip
.h	text/plain
.h	text/x-h
.hdf	application/x-hdf
.help	application/x-helpfile
.hgl	application/vnd.hp-hpgl
.hh	text/plain
.hh	text/x-h
.hlb	text/x-script
.hlp	application/hlp
.hlp	application/x-helpfile
.hlp	application/x-winhelp
.hpg	application/vnd.hp-hpgl
.hpgl	application/vnd.hp-hpgl
.hqx	application/binhex
.hqx	application/binhex4
.hqx	application/mac-binhex
.hqx	application/mac-binhex40
.hqx	application/x-binhex40
.hqx	application/x-mac-binhex40
.hta	application/hta
.htc	text/x-component
.htm	text/html
.html	text/html
.htmls	text/html
.htt	text/webviewhtml
.htx	text/html
.ice	x-conference/x-cooltalk
.ico	image/x-icon
.idc	text/plain
.ief	image/ief
.iefs	image/ief
.iges	application/iges
.iges	model/iges
.igs	application/iges
.igs	model/iges
.ima	application/x-ima
.imap	application/x-httpd-imap
.inf	application/inf
.ins	application/x-internett-signup
.ip	application/x-ip2
.isu	video/x-isvideo
.it	audio/it
.iv	application/x-inventor
.ivr	i-world/i-vrml
.ivy	application/x-livescreen
.jam	audio/x-jam
.jav	text/plain
.jav	text/x-java-source
.java	text/plain
.java	text/x-java-source
.jcm	application/x-java-commerce
.jfif	image/jpeg
.jfif	image/pjpeg
.jfif-tbnl	image/jpeg
.jpe	image/jpeg
.jpe	image/pjpeg
.jpeg	image/jpeg
.jpeg	image/pjpeg
.jpg	image/jpeg
.jpg	image/pjpeg
.jps	image/x-jps

.js	application/x-javascript
.jut	image/jutvision
.kar	audio/midi
.kar	music/x-karaoke
.ksh	application/x-ksh
.ksh	text/x-script.ksh
.la	audio/nspaudio
.la	audio/x-nspaudio
.lam	audio/x-liveaudio
.latex	application/x-latex
.lha	application/lha
.lha	application/octet-stream
.lha	application/x-lha
.lhx	application/octet-stream
.list	text/plain
.lma	audio/nspaudio
.lma	audio/x-nspaudio
.log	text/plain
.lsp	application/x-lisp
.lsp	text/x-script.lisp
.lst	text/plain
.lsx	text/x-la-asf
.ltx	application/x-latex
.lzh	application/octet-stream
.lzh	application/x-lzh
.lzx	application/lzx
.lzx	application/octet-stream
.lzx	application/x-lzx
.m	text/plain
.m	text/x-m
.m1v	video/mpeg
.m2a	audio/mpeg
.m2v	video/mpeg
.m3u	audio/x-mpequrl
.man	application/x-troff-man
.map	application/x-navimap
.mar	text/plain
.mbd	application/mbedlet
.mc$	application/x-magic-cap-package-1.0
.mcd	application/mcad
.mcd	application/x-mathcad
.mcf	image/vasa
.mcf	text/mcf
.mcp	application/netmc
.me	application/x-troff-me
.mht	message/rfc822
.mhtml	message/rfc822
.mid	application/x-midi
.mid	audio/midi
.mid	audio/x-mid
.mid	audio/x-midi
.mid	music/crescendo
.mid	x-music/x-midi
.midi	application/x-midi
.midi	audio/midi
.midi	audio/x-mid
.midi	audio/x-midi
.midi	music/crescendo
.midi	x-music/x-midi
.mif	application/x-frame
.mif	application/x-mif
.mime	message/rfc822
.mime	www/mime
.mjf	audio/x-vnd.audioexplosion.mjuicemediafile
.mjpg	video/x-motion-jpeg
.mm	application/base64
.mm	application/x-meme
.mme	application/base64
.mod	audio/mod
.mod	audio/x-mod
.moov	video/quicktime
.mov	video/quicktime
.movie	video/x-sgi-movie
.mp2	audio/mpeg
.mp2	audio/x-mpeg
.mp2	video/mpeg
.mp2	video/x-mpeg
.mp2	video/x-mpeq2a
.mp3	audio/mpeg3
.mp3	audio/x-mpeg-3
.mp3	video/mpeg
.mp3	video/x-mpeg
.mpa	audio/mpeg
.mpa	video/mpeg
.mpc	application/x-project
.mpe	video/mpeg
.mpeg	video/mpeg

.mpg audio/mpeg

.mpg video/mpeg

.mpga audio/mpeg

.mpp application/vnd.ms-project

.mpt application/x-project

.mpv application/x-project

.mpx application/x-project

.mrc application/marc

.ms application/x-troff-ms

.mv video/x-sgi-movie

.my audio/make

.mzz application/x-vnd.audioexplosion.mzz

.nap image/naplps

.naplps image/naplps

.nc application/x-netcdf

.ncm application/vnd.nokia.configuration-message

.nif image/x-niff

.niff image/x-niff

.nix application/x-mix-transfer

.nsc application/x-conference

.nvd application/x-navidoc

.o application/octet-stream

.oda application/oda

.omc application/x-omc

.omcd application/x-omcdatamaker

.omcr application/x-omcregerator

.p text/x-pascal

.p10 application/pkcs10

.p10 application/x-pkcs10

.p12 application/pkcs-12

.p12 application/x-pkcs12

.p7a application/x-pkcs7-signature

.p7c application/pkcs7-mime

.p7c application/x-pkcs7-mime

.p7m application/pkcs7-mime

.p7m application/x-pkcs7-mime

.p7r application/x-pkcs7-certreqresp

.p7s application/pkcs7-signature

.part application/pro_eng

.pas text/pascal

.pbm image/x-portable-bitmap

.pcl application/vnd.hp-pcl

.pcl application/x-pcl

.pct image/x-pict

.pcx image/x-pcx

.pdb chemical/x-pdb

.pdf application/pdf

.pfunk audio/make

.pfunk audio/make.my.funk

.pgm image/x-portable-graymap

.pgm image/x-portable-greymap

.pic image/pict

.pict image/pict

.pkg application/x-newton-compatible-pkg

.pko application/vnd.ms-pki.pko

.pl text/plain

.pl text/x-script.perl

.plx application/x-pixclscript

.pm image/x-xpixmap

.pm text/x-script.perl-module

.pm4 application/x-pagemaker

.pm5 application/x-pagemaker

.png image/png

.pnm application/x-portable-anymap

.pnm image/x-portable-anymap

.pot application/mspowerpoint

.pot application/vnd.ms-powerpoint

.pov model/x-pov

.ppa application/vnd.ms-powerpoint

.ppm image/x-portable-pixmap

.pps application/mspowerpoint

.pps application/vnd.ms-powerpoint

.ppt application/mspowerpoint

.ppt application/powerpoint

.ppt application/vnd.ms-powerpoint

.ppt application/x-mspowerpoint

.ppz application/mspowerpoint

.pre application/x-freelance

.prt	application/pro_eng
.ps	application/postscript
.psd	application/octet-stream
.pvu	paleovu/x-pv
.pwz	application/vnd.ms-powerpoint
.py	text/x-script.phyton
.pyc	applicaiton/x-bytecode.python
.qcp	audio/vnd.qcelp
.qd3	x-world/x-3dmf
.qd3d	x-world/x-3dmf
.qif	image/x-quicktime
.qt	video/quicktime
.qtc	video/x-qtc
.qti	image/x-quicktime
.qtif	image/x-quicktime
.ra	audio/x-pn-realaudio
.ra	audio/x-pn-realaudio-plugin
.ra	audio/x-realaudio
.ram	audio/x-pn-realaudio
.ras	application/x-cmu-raster
.ras	image/cmu-raster
.ras	image/x-cmu-raster
.rast	image/cmu-raster
.rexx	text/x-script.rexx
.rf	image/vnd.rn-realflash
.rgb	image/x-rgb
.rm	application/vnd.rn-realmedia
.rm	audio/x-pn-realaudio
.rmi	audio/mid
.rmm	audio/x-pn-realaudio
.rmp	audio/x-pn-realaudio
.rmp	audio/x-pn-realaudio-plugin
.rng	application/ringing-tones
.rng	application/vnd.nokia.ringing-tone
.rnx	application/vnd.rn-realplayer
.roff	application/x-troff
.rp	image/vnd.rn-realpix
.rpm	audio/x-pn-realaudio-plugin
.rt	text/richtext
.rt	text/vnd.rn-realtext
.rtf	application/rtf
.rtf	application/x-rtf
.rtf	text/richtext
.rtx	application/rtf
.rtx	text/richtext
.rv	video/vnd.rn-realvideo
.s	text/x-asm
.s3m	audio/s3m
.saveme	application/octet-stream
.sbk	application/x-tbook
.scm	application/x-lotusscreencam
.scm	text/x-script.guile
.scm	text/x-script.scheme
.scm	video/x-scm
.sdml	text/plain
.sdp	application/sdp
.sdp	application/x-sdp
.sdr	application/sounder
.sea	application/sea
.sea	application/x-sea
.set	application/set
.sgm	text/sgml
.sgm	text/x-sgml
.sgml	text/sgml
.sgml	text/x-sgml
.sh	application/x-bsh
.sh	application/x-sh
.sh	application/x-shar
.sh	text/x-script.sh
.shar	application/x-bsh
.shar	application/x-shar
.shtml	text/html
.shtml	text/x-server-parsed-html
.sid	audio/x-psid
.sit	application/x-sit
.sit	application/x-stuffit
.skd	application/x-koan
.skm	application/x-koan
.skp	application/x-koan
.skt	application/x-koan
.sl	application/x-seelogo
.smi	application/smil
.smil	application/smil

.snd	audio/basic
.snd	audio/x-adpcm
.sol	application/solids
.spc	application/x-pkcs7-certificates
.spc	text/x-speech
.spl	application/futuresplash
.spr	application/x-sprite
.sprite	application/x-sprite
.src	application/x-wais-source
.ssi	text/x-server-parsed-html
.ssm	application/streamingmedia
.sst	application/vnd.ms-pki.certstore
.step	application/step
.stl	application/sla
.stl	application/vnd.ms-pki.stl
.stl	application/x-navistyle
.stp	application/step
.sv4cpio	application/x-sv4cpio
.sv4crc	application/x-sv4crc
.svf	image/vnd.dwg
.svf	image/x-dwg
.svr	application/x-world
.svr	x-world/x-svr
.swf	application/x-shockwave-flash
.t	application/x-troff
.talk	text/x-speech
.tar	application/x-tar
.tbk	application/toolbook
.tbk	application/x-tbook
.tcl	application/x-tcl
.tcl	text/x-script.tcl
.tcsh	text/x-script.tcsh
.tex	application/x-tex
.texi	application/x-texinfo
.texinfo	application/x-texinfo
.text	application/plain
.text	text/plain
.tgz	application/gnutar
.tgz	application/x-compressed
.tif	image/tiff
.tif	image/x-tiff
.tiff	image/tiff
.tiff	image/x-tiff
.tr	application/x-troff
.tsi	audio/tsp-audio
.tsp	application/dsptype
.tsp	audio/tsplayer
.tsv	text/tab-separated-values
.turbot	image/florian
.txt	text/plain
.uil	text/x-uil
.uni	text/uri-list
.unis	text/uri-list
.unv	application/i-deas
.uri	text/uri-list
.uris	text/uri-list
.ustar	application/x-ustar
.ustar	multipart/x-ustar
.uu	application/octet-stream
.uu	text/x-uuencode
.uue	text/x-uuencode
.vcd	application/x-cdlink
.vcs	text/x-vcalendar
.vda	application/vda
.vdo	video/vdo
.vew	application/groupwise
.viv	video/vivo
.viv	video/vnd.vivo
.vivo	video/vivo
.vivo	video/vnd.vivo
.vmd	application/vocaltec-media-desc
.vmf	application/vocaltec-media-file
.voc	audio/voc
.voc	audio/x-voc
.vos	video/vosaic
.vox	audio/voxware
.vqe	audio/x-twinvq-plugin
.vqf	audio/x-twinvq
.vql	audio/x-twinvq-plugin
.vrml	application/x-vrml
.vrml	model/vrml
.vrml	x-world/x-vrml
.vrt	x-world/x-vrt
.vsd	application/x-visio
.vst	application/x-visio

.vsw	application/x-visio
.w60	application/wordperfect6.0
.w61	application/wordperfect6.1
.w6w	application/msword
.wav	audio/wav
.wav	audio/x-wav
.wb1	application/x-qpro
.wbmp	image/vnd.wap.wbmp
.web	application/vnd.xara
.wiz	application/msword
.wk1	application/x-123
.wmf	windows/metafile
.wml	text/vnd.wap.wml
.wmlc	application/vnd.wap.wmlc
.wmls	text/vnd.wap.wmlscript
.wmlsc	application/vnd.wap.wmlscriptc
.word	application/msword
.wp	application/wordperfect
.wp5	application/wordperfect
.wp5	application/wordperfect6.0
.wp6	application/wordperfect
.wpd	application/wordperfect
.wpd	application/x-wpwin
.wq1	application/x-lotus
.wri	application/mswrite
.wri	application/x-wri
.wrl	application/x-world
.wrl	model/vrml
.wrl	x-world/x-vrml
.wrz	model/vrml
.wrz	x-world/x-vrml
.wsc	text/scriplet
.wsrc	application/x-wais-source
.wtk	application/x-wintalk
.xbm	image/x-xbitmap
.xbm	image/x-xbm
.xbm	image/xbm
.xdr	video/x-amt-demorun
.xgz	xgl/drawing
.xif	image/vnd.xiff
.xl	application/excel
.xla	application/excel
.xla	application/x-excel
.xla	application/x-msexcel
.xlb	application/excel
.xlb	application/vnd.ms-excel
.xlb	application/x-excel
.xlc	application/excel
.xlc	application/vnd.ms-excel
.xlc	application/x-excel
.xld	application/excel
.xld	application/x-excel
.xlk	application/excel
.xlk	application/x-excel
.xll	application/excel
.xll	application/vnd.ms-excel
.xll	application/x-excel
.xlm	application/excel
.xlm	application/vnd.ms-excel
.xlm	application/x-excel
.xls	application/excel
.xls	application/vnd.ms-excel
.xls	application/x-excel
.xls	application/x-msexcel
.xlt	application/excel
.xlt	application/x-excel
.xlv	application/excel
.xlv	application/x-excel
.xlw	application/excel
.xlw	application/vnd.ms-excel
.xlw	application/x-excel
.xlw	application/x-msexcel
.xm	audio/xm
.xml	application/xml
.xml	text/xml
.xmz	xgl/movie
.xpix	application/x-vnd.ls-xpix
.xpm	image/x-xpixmap
.xpm	image/xpm
.x-png	image/png
.xsr	video/x-amt-showrun
.xwd	image/x-xwd
.xwd	image/x-xwindowdump
.xyz	chemical/x-pdb
.z	application/x-compress

.z	application/x-compressed			.zoo	application/octet-stream
.zip	application/x-compressed	.zip	application/zip	.zsh	text/x-script.zsh
.zip	application/x-zip-compressed	.zip	multipart/x-zip		

back

Lab 1

Welcome to CIS 225 – Web Server Technology and Security – January 3rd, 2011

To log in the student sandbox

User name: the first letter of your first name, your full last name (if you name contains a hyphen, do not use it).

Password: Password01 (you will be required to change it as soon as you login in).

Once you are logged into the Sandbox, please log into Blackboard.

Select CIS 225 from your list of classes.

Click on the Elluminate link provided in the Announcements area of the virtual classroom

Enter your full name

Virtual Server Access:

The following instructions are written for Internet Explorer, please use IE for tonight. If you choose to use another browser, you will be responsible for setting the options below correctly.

Try to connect to https://vserver.sandbox.edcc.edu:8333/

If it is not available:

Connect to https://71.121.242.69:8333

Click Continue to this website (not recommended).

Log in to the VMware server using your sandbox log in and password

Skip to Starting your virtual server below.

If it is available: (You will need to do this once the DNS server entry is completed by the College)

Go to https://vserver.sandbox.edcc.edu:8333/

At any time if you should get a warning box “This website wants to run the following add-on: ‘VMware Remote Console Plug-in…’, click and choose “Run Add-on”

Choose “Continue to this website (not recommended).”

Go to Tools --> Internet Options --> Security (tab) --> Click on Trusted Sites, click on “Sites” button, click “add” button to add the https://vserver.sandbox.edcc.edu:8333/ to the trusted web sites

Go through “Close,Ok” to close all the dialog boxes.

Close your browser and reopen it

https://vserver.sandbox.edcc.edu:8333/

Choose “Continue to this website (not recommended).”

Click “Yes” on the dialog box “The current webpage is trying to open a site in your trusted...”

Click on “Certificate Error” in the URL field.

Click on “View certificates”

Click on “Install Certificate”

Click Next

Choose “Place certificate…”

Click Browse

Choose “Trusted Root Certificate Authorities”

Click “OK”

Click Next, finish

Click “YES”

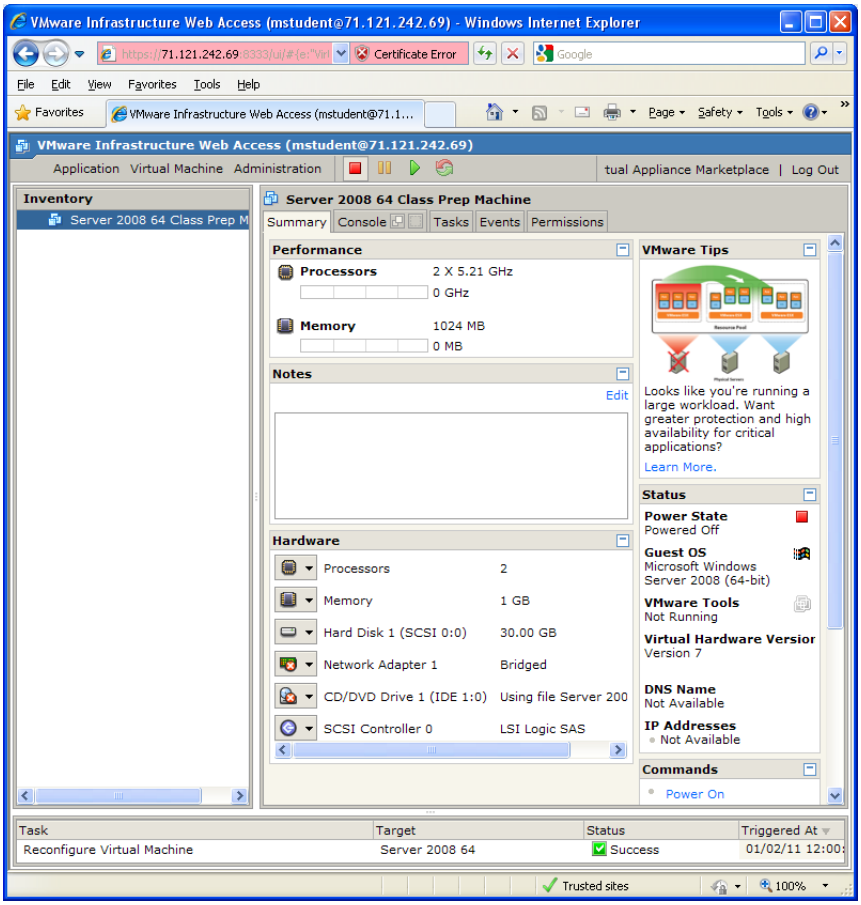
Click through “OK, OK”

Close your browser and reopen it

https://vserver.sandbox.edcc.edu:8333/

Starting your virtual server

Once you have logged into the Vmware server, you should be able to see only your machine.



Click the "-" Status area to the middle right

Click on "Power on" in the Commands Area

Click on "**I copied it**" and "OK"

Using the keyboard key combination CTRL + ALT + Insert, your machine will open in another Window

At any time you may maximize your virtual server by clicking on the maximize button

To return to your host machine, use the keyboard key combination CTRL + ALT

Windows is now completing the installation of your virtual server

Patience! The server is thinking – This can take up to 45 minutes. (During this we will cover the remainder of the first class information.)

When language request comes up, verify

Country or Region: United States

Time and currency: English (United States)

Keyboard layout: US

Click next

Uncheck "Automatically activate Windows when I'm online"

Leave product key empty, Click next

Click on the checkbox to "I accept the license terms"

Click Next

Use your sandbox log in for your computer name, i.e. mine would be **mbaker**

Click Start

Patience! The server is thinking

To log in you use CTRL + ALT + Insert

Log in via Adminstrator

The password will need to be changed, click OK

use **Pa55word**. DO NOT CHANGE THIS ACCOUNT OR PASSWORD, AT THIS TIME.

Be careful that you click on the arrow and not the “Cancel” button.

Click OK, once you receive the screen that your password has been changed.

Patience! The server is thinking.

The computer is now setting up your desktop and will take a few moments.

Click on the Start

Click on Windows Update

Click on Check for Updates

Patience! The Windows update is thinking

Once the updates have been identified, click “Install updates”

Click “I accept the license terms”

Click Finish

Complete the Start Up Screen Capture Assignment.

Keep an eye on your virtual server, if required restart the machine.

If a restart is needed, log back into your virtual server

Click Start, Windows Updates. Click Install Updates

Check to see if there are any additional updates, click Check for Updates.

If Windows Update reports additional updates, click “Install updates”

To finish tonight:

Click on the start

Choose the lock and lock your virtual machine

You can now exit the virtual machine by select the X back

Lab 2

CIS 225 – Lab 2: Installing IIS

After this lab you should be able to:

Install IIS 7.0 along with Windows Server 2008.

By default, IIS 7.0 is not installed on Windows Server 2008. This is a change that took place in Windows Server 2003 from Windows NT. IIS should not be installed on a machine where other services do not require it.

Prep Step:

From your console

Start your server

Click on the console tab

Click within the console to open your server in a new window

Log into your virtual machine

Your machine should start in a new window.

If asked to activate Windows, select *Activate later*

Minimize the Initial Configuration Tasks window

Click on the summary tab

In the status area, click Install VMware tools

When the dialog box comes up, select *Install*

In the AutoPlay dialog box, now showing in your server, click Run setup.exe. The VMware Tools Wizard will start

On the Welcome screen, click *Next*

Select T*ypical*, and click *Next*

Click Install

Click *Finish*

When asked click *Yes* to restart your server

Step 1 – Assigning a static IP Address

Windows Server 2008 R2

Membership in Administrators, or equivalent, is the minimum required to perform these procedures.

Click *Start*, and then click *Control Panel*.

In Control Panel, if *Network and Internet* is showing, click *Network and Internet*. Network and Internet opens.

In Network and Internet, click *Network and Sharing Center*. Network and Sharing Center opens.

In Network and Sharing Center, click Manage Network Connections. Network Connections opens.

In Network Connections, right-click the Local Area Connection, and then click Properties.

In Local Area Connection Properties, in "This connection uses the following items:"

Unclick the checkbox next to: Internet Protocol Version 6 (TCP/IPv6)

Select *Internet Protocol Version 4 (TCP/IPv4)*, and then click *Properties* button. The Internet Protocol Version 4 (TCP/IPv4) Properties dialog box opens.

In Internet Protocol Version 4 (TCP/IPv4) Properties, on the General tab, click Use the following IP address radio button. In IP address, type the IP address that you want to use. We will be using 10.1.13.1XX, where XX is the number of the monitor that you are sitting. If your monitor does not have a number, please ask the instructor.

The Static IP Address of your machine: _____
Your machine name: _____

Press *tab* to place the cursor in Subnet mask. A default value for subnet mask is entered automatically. We will be using *255.255.252.0*

In Default gateway, type the IP address of your default gateway. The default gateway is *10.1.12.1*

In Preferred DNS server, type the IP address of your DNS server. We will be using *10.1.12.72*

In Alternate DNS Server, type the IP address of your alternate DNS server, if any. We will be using *10.1.12.80*

Click OK

You will receive a warning "The computer you are using… " click *Yes.*

Click *Close*.

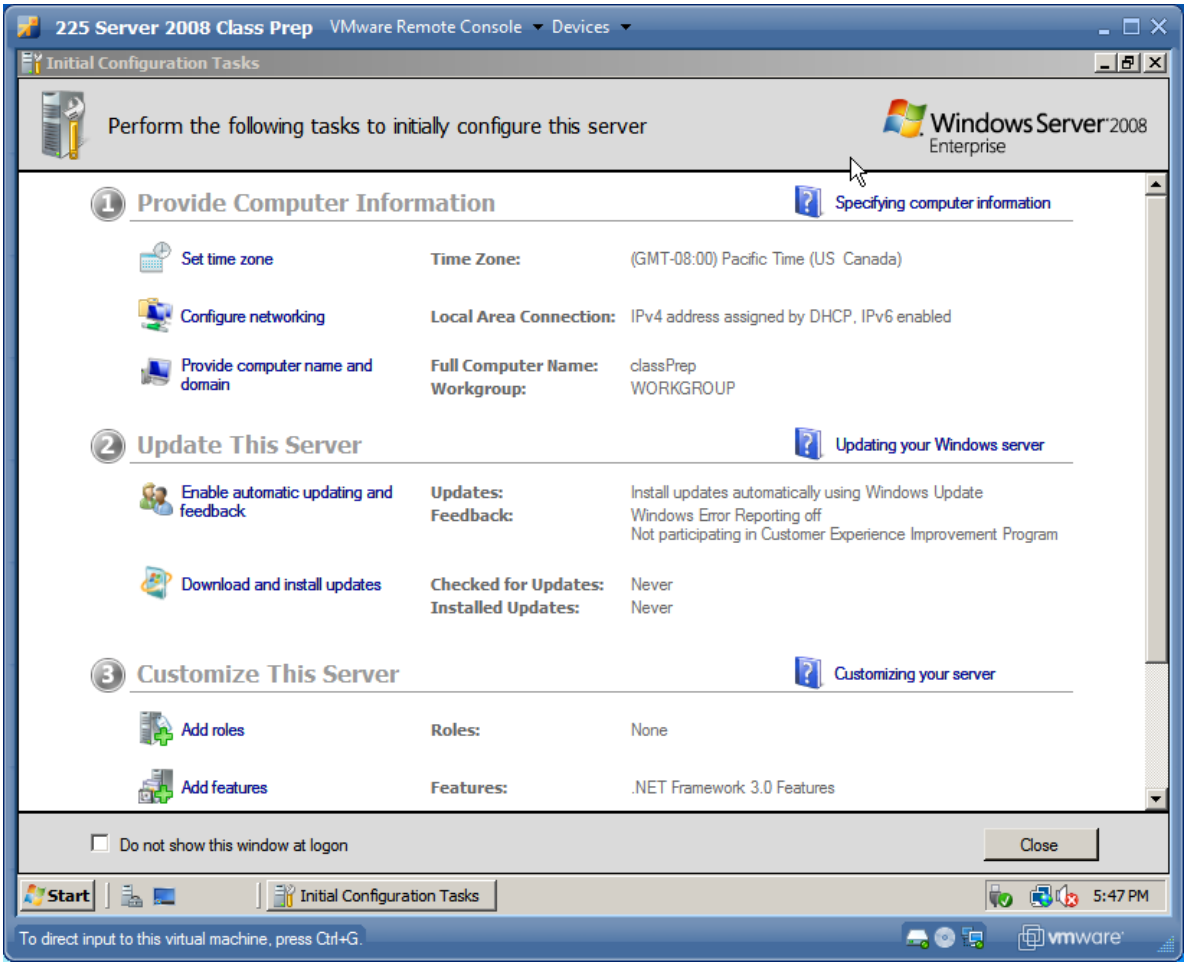
Write down the IP address and machine name for your computer.

Close the Network Connections window.

Close the Network and Sharing Center window.

Step 2

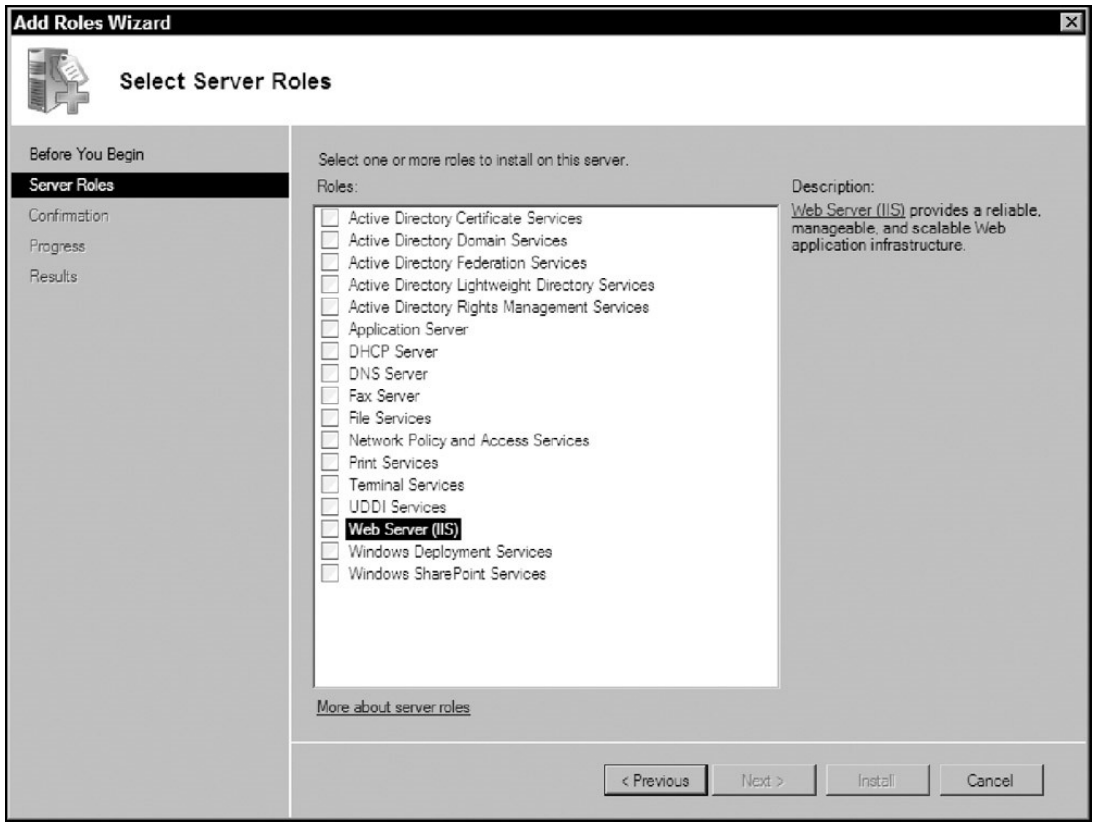
Once you have logged should see the following screen:



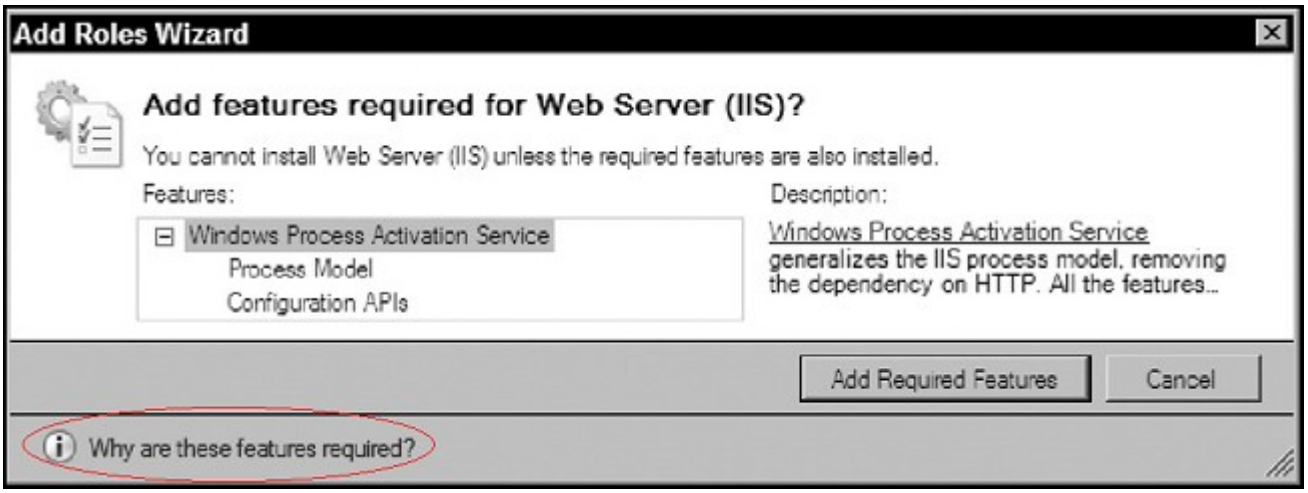
Select *Add rolls* under the Customize This Server

On the **Before You Begin** screen, select *Next*

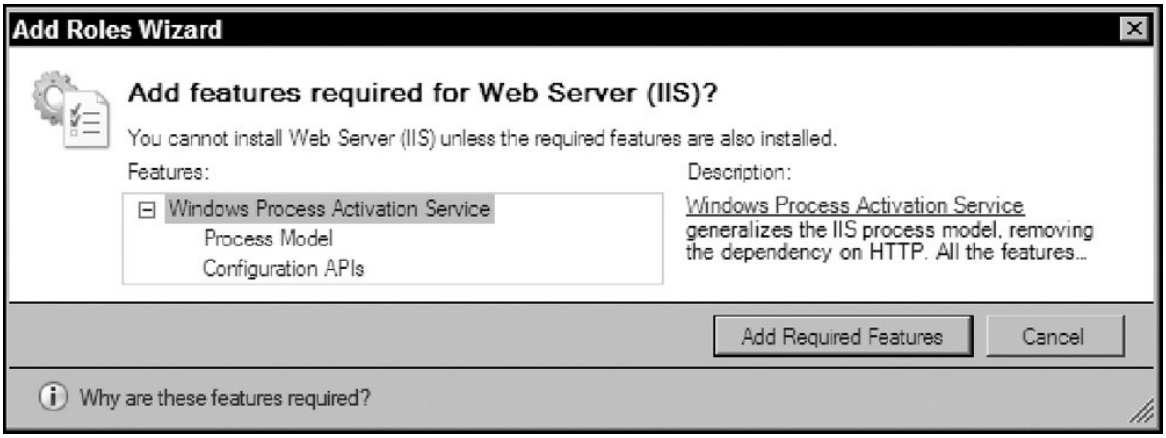
On the Select Server Roles screen, locate Web Server (IIS) in the list. Click the checkbox next to Web Server (IIS)



At the Add Roles Wizard, click *Why are these features required? b*efore continuing or clicking on *Add Required Features.*


Add Roles Wizard
Add features required for Web Server (IIS)?
You cannot install Web Server (IIS) unless the required features are also installed.
Features:
Windows Process Activation Service
Process Model
Configuration APIs
Description:
Windows Process Activation Service generalizes the IIS process model, removing the dependency on HTTP. All the features...
Add Required Features
Cancel
Why are these features required?

After reading Why are these features required? click Add Required Features, click Next.



If you would like to read the Introduction to IIS on the next screen, click Overview of Web Server (IIS), you may do so later by clicking Help from the start menu.

Click *Next*.

The next screen will allow you to choose the services that you want to install on your Server.

Select the following Services:

Under Common HTTP Features (select all)

Static Content

Default Document

Directory Browsing (for now)

HTTP Errors

HTTP Redirection

Under Application Development (Select all)

ASP.NET

When this option is clicked you will be asked to Add Required Features, click the "*Add Required Role Services"* button.

.NET Extensibility

ASP

CGI

ISAPI Extensions

ISAPI Filters

Server Side Includes

Health and Diagnositcs

HTTP Logging

Request Monitor

Security

Request Filtering

Performance (select all)

Static Content Compression

Dynamic Content Compression

Management Tools

IIS Management Console

IIS Script and Tools

FTP Publishing Services

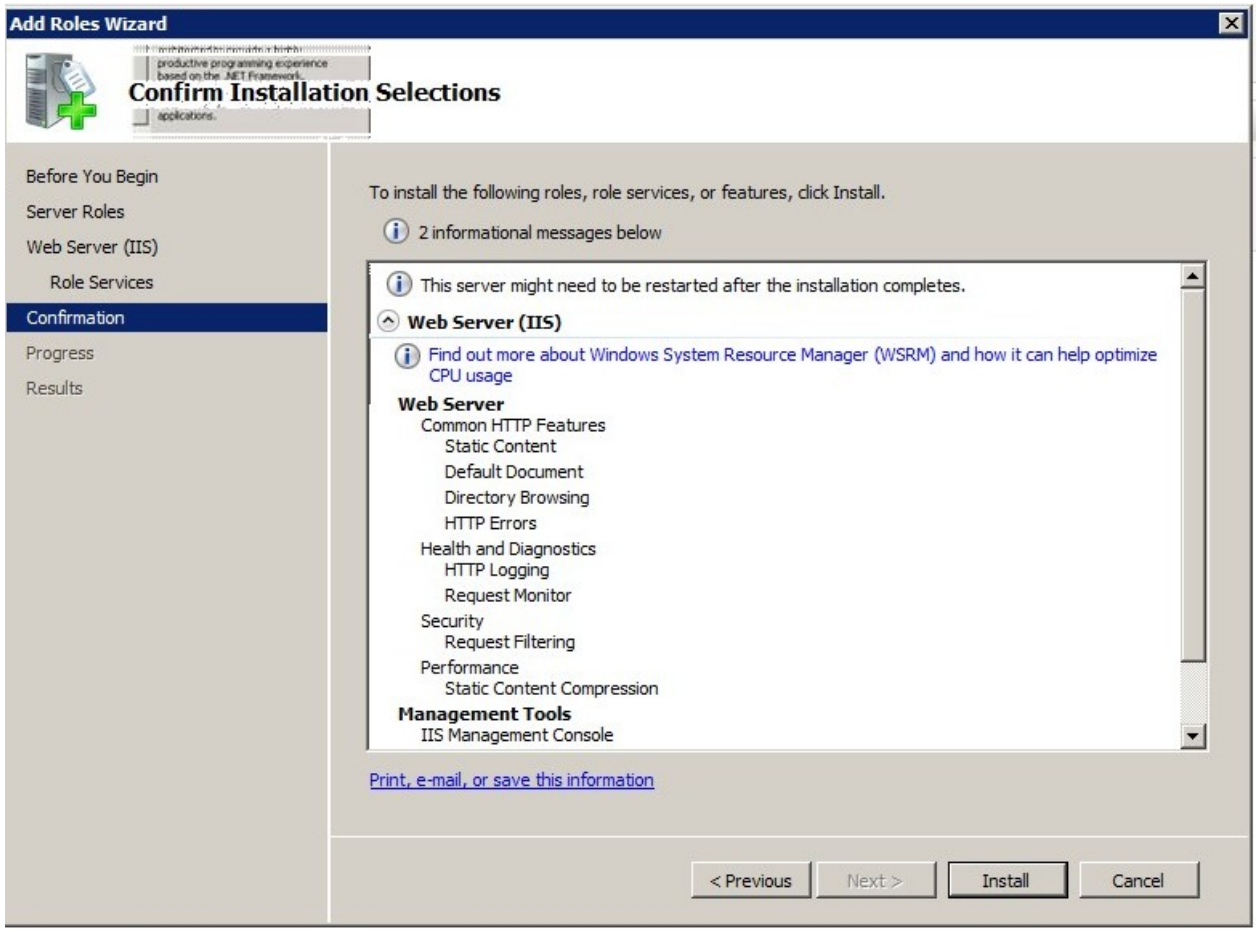
FTP Services

When this option is clicked you will be asked to Add Required Features, click the "*Add Required Role Services"* button.

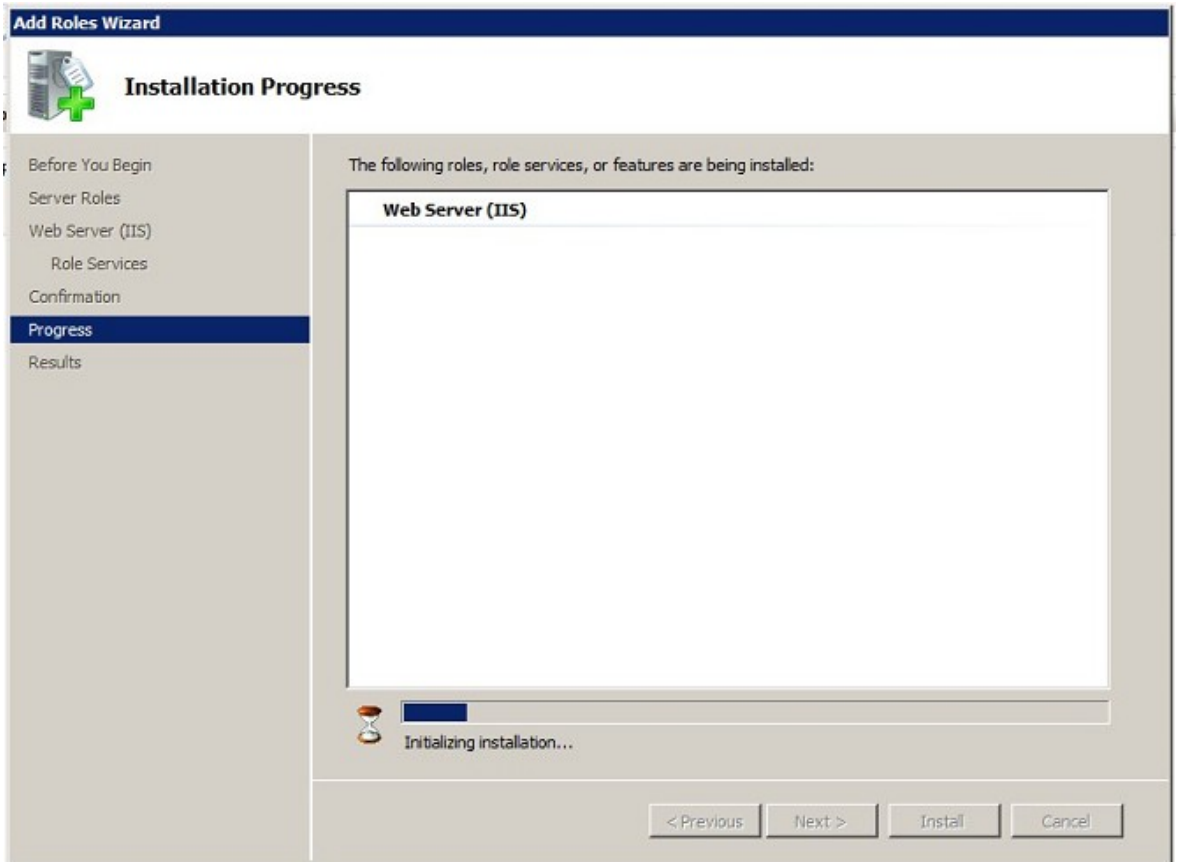
FTP Extensibility

Click *Next.*

Before installation, the Wizard will ask you to confirm your choices. Verify that choices above are selected


Add Roles Wizard
Confirm Installation Selections
Before You Begin
Server Roles
Web Server (IIS)
Role Services
Confirmation
Progress
Results
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
Print, e-mail, or save this information
< Previous
Next >
Install
Cancel

Click Install, and watch the installation.



What to turn in:

This document with your IP address and your server name.

This document signed with your name. back

Lab 3

[1]Student Name _____

_____

1

Lab 3 Working with Administration Tools

In this lab you will be setting up some of the basic requirements of IIS 7.5 and becoming familiar with the web administration tools included in IIS 7.5.

Directions:

Complete the required administration steps below.

Virtual Server Access:

The following instructions are written for Internet Explorer, please use IE for tonight.

Connect to https://vserver.sandbox.edcc.edu:8333/

Login to your server using your sandbox (Snohomish Hall 124) user and password

At any time if you should get a warning box "This website wants to run the following add-on: 'VMware Remote Console Plug-in…', click and choose "Run Add-on".

Choose "Continue to this website (not recommended)."

Go to Tools --> Internet Options --> Security (tab) --> Click on Trusted Sites, click on "Sites" button, click "add" button to add the https://vserver.sandbox.edcc.edu:8333/ to the trusted web sites

Go through "Close,Ok" to close all the dialog boxes.

Close your browser and reopen it

https://vserver.sandbox.edcc.edu:8333/

Choose "Continue to this website (not recommended)."

Click "Yes" on the dialog box "The current webpage is trying to open a site in your trusted..."

Click on "Certificate Error" in the URL field.

Click on "View certificates"

Click on "Install Certificate"

Click Next

Choose "Place certificate…"

Click Browse

Choose “Trusted Root Certificate Authorities”

Click “OK”

Click Next, finish

Click “YES”

Click through “OK, OK”

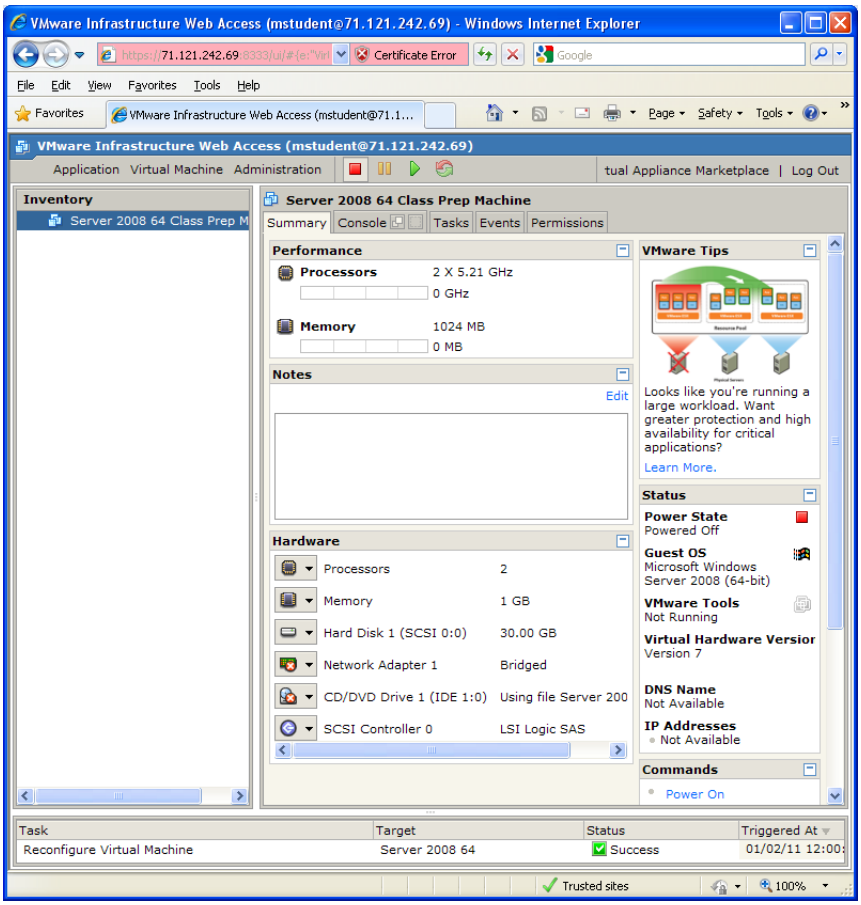
Close your browser and reopen it

https://vserver.sandbox.edcc.edu:8333/

Starting your virtual server

If your server needs to be restarted for updates, please restart your server.

Once you have logged into the VMware server, you should be able to see only your machine.



Click on the Console tab of the web interface.

Log in via Administrator

The password will need to be changed, click OK

Use **Pa55word**. DO NOT CHANGE THIS ACCOUNT OR PASSWORD, AT THIS TIME.

Be careful that you click on the arrow and not the “Cancel” button.

Click OK, once you receive the screen that your password has been changed.

Patience! The server is thinking.

It is possible that your server will ask for the reason it was shut down. If it does, please select Server Failure as the reason.

Because we are recovering from the failure of the original server – you will need to redo lab 3 at this point.

Once you have completed lab 3 you can move ahead to page 3 of this lab.

Creating a Web Site Using IIS Manager

IIS Manager presents the administrator with a GUI interface that allows the creation of a web site by following these steps:

Start IIS Manager by clicking Start ⇛ Run, entering **inetmgr**, and then pressing Enter.

Select the server to administer (your machine name). Expand the server by clicking on the +. Click the Sites icon, and then select Add Web Site from the Actions pane or by right-clicking the Sites icon. This will present the Add Web Site dialog, as shown in Figure 6-2.

Figure 6-2

Enter a web-site name; use your full name, without any prefix or any spaces. This name should include **NO SPACES**! Use camel case to help with readability: ie: martiBaker.

Select the application pool for your site, DefaultAppPool.

Click the start button, select computer, navigate to c:\inetpub\wwwroot. Create a folder in this location. Name this folder "yourName", where yourName is your full name with no spaces.

Set the path to the web-site files. Browse to the folder that you just created in c:\inetpub\wwwroot\yourName. Click OK.

Click "Test Settings". You will see a warning on "Authorization", there is no need to change this setting at this time. Click Close.

Enter binding details. Set this to HTTP.

Next, select the IP address to bind the site to; use the IP address of your machine.

Verify the port setting is 80.

Enter the Host name: www.yourpame.com.

Note: A host header entry is required if you are going to host multiple web-site domains on the same IP address. When first creating the site, enter your domain to get started, and you can later add additional

domains as required. There are some requirements when using host headers that are inherent to the HTTP v1.1 specification (which defined host headers). These requirements are discussed below in this lab.

Click OK.

Click on your newly made site and click Start.

You can now browse to your site by its domain name, provided the DNS is correctly configured. Figure 6-3 shows WebSite1 in the Sites menu.

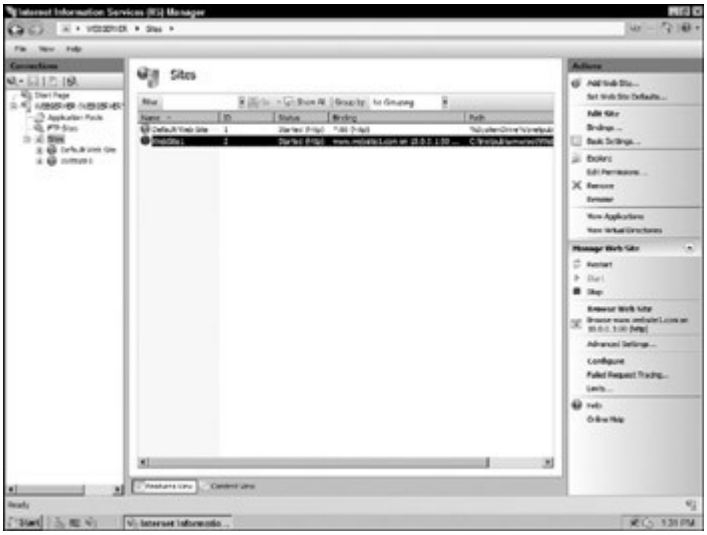


Figure 6-3

To start modifying the site configuration, simply click the site's name under the Sites list and you will be presented with the Features view, which gives you access to alter the configuration. The Content view shows the web-site files that are in the root directory of the site.

Creating a New Application Pool for Your Site

It is a good practice to create a new application pool for each site, especially when you are hosting more than one web site on the same server. This will ensure that each web application runs inside its own process such that if an application causes a failure, it does not affect any other sites. Further information on application pools is available in Chapter 8, “Web Application Pool Administration.” The Add Web Site tool in IIS Manager will automatically create a new application pool and map the site to it. If you chose not to create a new application pool when you created the site, or if you imported the site through a different method, you may need to manually create an application pool.

To create the new application pool, follow these steps:

Open IIS Manager, if it is not already open. (Start ⇛ Run, enter **inetmgr**, and press Enter.)

Select Application Pools under the server name from the Connections pane, and then select Add Application Pool from the Actions pane or right-click the Application Pools icon. This will present the Add Application Pools dialog. Figure 6-4 shows the Add Application Pool tool.

Figure 6-4

Set the name to something that is relevant — in this case, yourNameAppPool. (It might seem redundant to add AppPool to the end of the name; however, it does help for easing confusion with novice or other administrators.)

Select the .NET Framework version for the application pool to default to.

Select the Managed Pipeline Mode. For this site, we are going to use Integrated, which is the default setting. By default, the application pool will be created to run with the NetworkService identity.

Verify that the Start application pool immediately is checked, and click OK.

Now you can assign the new application pool to your site. To do this, select your web site under the server pane, then right-click or select View Applications from the Actions pane.

The View Applications, Select Application Defaults in the Actions area.

Click the Select button. In the drop down list select the yourNameAppPool. Click OK

Click OK again.

As soon as you click OK, the application is moved to the new application pool, which is then recycled. Be wary of this in production environment, lest you receive any unexpected results.

Enabling Logging

Before you can enable logging, you need to verify that Http Logging module has been installed in the server roles.

To install the Http Logging module, follow these steps:

Open Server Manager, if it is not already open. (Start ⇛ Run, enter **CompMgmtLauncher.exe**, and press Enter.)

Expand Roles, and look at the Web Server Role Services. Check to see if HTTP Logging is installed. If it is not, click Add Role Services.

Check the HTTP Logging box, click Next, then click Install.

Click Close to finish the dialog, and then close the Server Manager.

Once HTTP Logging is enabled, <log> tags are automatically created for the central binary log file and the central W3C log file in the applicationHost.config file.

Failed Request Tracing Logs

Failed request tracing logs are used as a logging tool and a diagnostic utility. In this lab, you will learn how to enable the trace logs and change the directory to which they are written. Chapter 20, "Diagnostics and Troubleshooting," will go into greater detail about the use of the trace logs.

W3C Logging

World Wide Web Consortium (W3C) logging writes log entries using a text-based, customizable ASCII format and is the default log format configured under IIS.

W3C logging is enabled initially on a per-site basis with a default location of %systemdrive%\inetpub\ logs\logfiles\W3SVC1. The number after W3SVC designates the site ID of the web site.

Logging can be set to log one file per site or one file for the entire server. This lab keeps the log file set to log at the site level. However, in the real world you would want to put your log files in a different location.

Open IIS Manager and navigate to the server, site, or application you want to configure logging for. Use your server, your site, your application. Under the Features view (found at the bottom of the middle pane), the Logging feature will be available if the module has been installed on the site/server/application.

Double-click Logging or select Logging and click Open Feature under the Actions pane, opening the Logging pane. This allows the administrator to enable the logging features.

As with previous versions of IIS, you have the option to select the format of your logging or define your own custom log handler. This is only available when configured for logging on a per-site basis, and you have the choice of

IIS — This is a fixed ASCII text-based format, and thus is not customizable on what can be logged.

W3C — The World Wide Web Consortium log format is discussed in more detail below in this chapter. This is the most widely utilized log format on web servers today.

NCSA — NCSA (National Center for SuperComputing Applications) generally is the default log format for Apache and other web servers. This is similar to the IIS format as it is fixed ASCII text that is noncustomizable.

Verify that the W3C format is selected.

Select the fields for IIS to record. This lab will use the default fields selected. Figure 6-6 shows the W3C Logging Fields dialog box.

Figure 6-6

Verify that the options above are selected. Click OK

The default location specified for logging is %systemdrive%\inetpub\logs\LogFiles\w3svc<siteID>, with the siteID value updating to the site ID for each site. Keep the default location for the logs.

Encoding can be set to either UTF-8 or ANSI. Use UTF-8.

The log file rollover can be set to create a new log file on a scheduled basis, when the file reaches a set size, or to not create a new log file at all. If the scheduled basis is selected, the time periods are hourly, daily, weekly, or monthly. Select weekly.

Click "Use local time for file naming and rollover"

Click Apply in the Actions pane.

You can enable the HTTP Logging module at the web server, site, or application level. This allows maxi-mum granularity in logging control.

Closing Your Server

Check for updates on your server

Lock your by clicking on the Start button and selecting lock

Leave your server running for the weekend.

What to turn in:

This lab with your name on it. back

Lab 4

Student Name: _____

Installing a Working Application

In this lab you will be placing a dynamic web site on your virtual server, configuring the site, and finally checking the site for functionality.

Often when working as a web administrator or developer, you are presented with a completed site that needs to be added to the server. Today you will be adding a site built by CIS 243 in 2010 as a working site on your virtual server.

If you are not currently logged into your virtual server, do so now.

Open up the Blackboard classroom and navigate to Labs → Lab 4, and download the file "ApplicationInstallation.zip" to your virtual server. Save this file in a location that you can easily navigate too.

Extract these files to c:\inetpub\wwwroot\cacApp. Note that "cacApp" is a new folder within wwwroot.

Move all files from within the ApplicationInstallation folder to cacApp.

Once the files have been moved, delete the folder ApplicationInstallation.

Using your previous knowledge (or Lab 3), create a new web site for this application. Call this web site "www.edccCAC.com"

Using your previous knowledge (or Lab 3), create a new application pool for this web site. Call this application pool "cacAppPool"

Assign cacAppPool to www.edccCAC.com

Open Internet Explorer and enter the following URL: http://localhost/cacApp/database/create_team_3.php

You should receive the response page saying: "database created"

Verify that the application is now working by typing in the URL: http://localhost/cacApp/

User name "*admin";* email address *admin@bojd.com*

If you have correctly completed lab 13 and the steps above you should see:

Configure site level ACL

In this step you will be configuring the ACL list in order to prevent unauthorized insertion into the newly created site and application.

From the site level, double-click the Authentication icon.

Click Anonymous Authentication, and then click Edit from the Actions pane.

From the Edit Anonymous Authentication Credentials dialog box, select “Application pool identity” (see Figure 8-28).

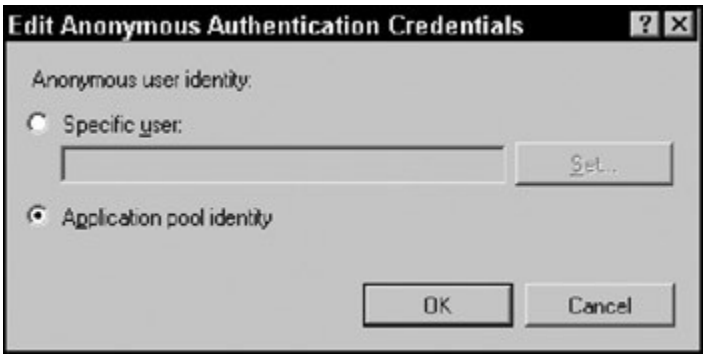


Figure 8-28

Click OK to save your selection. back

Lab 5

Student Name: _____

In this lab you will work with both remote administration of IIS and access control lists to web sites.

What you will be learning:

How to install or verify that remote administration is installed on your web server.

Create an access control list

Determine who should have access to the web server as a server administrator and be able to control the services of the web server

Determine who should have access to a web site as a site administrator and be able to control the a web site.

Practice using the tools of remote administration as both a server administrator and a site administrator

Verify installation of Management Service

Click Start, type **Server Manager** in the Search box, and then press Enter.

Expand Roles in the tree in the left-hand pane.

Right-click Web Server (IIS), right click and select Add Roll Service.

Verify that Management Service in the Management Tools section under Role Services (see Figure 9-1).

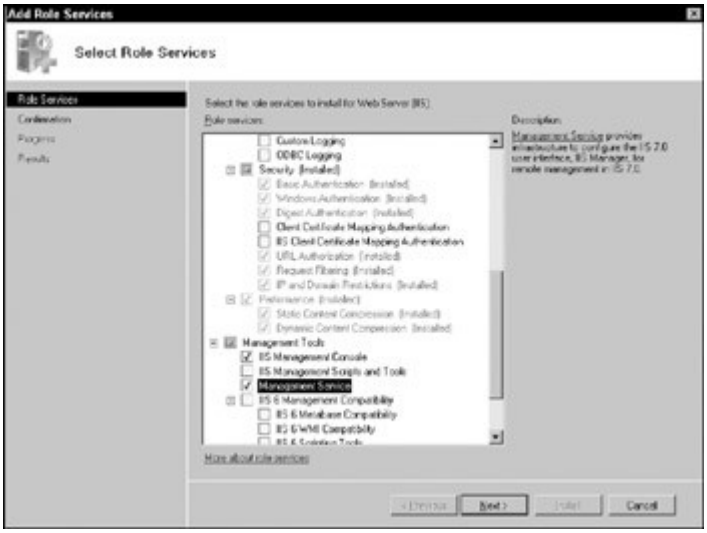


Figure 9-1

If it is installed:

Click **Cancel**

Click **Yes** to confirm cancelling the wizard

If it is not installed:

Click on the check box for **Management Service**

Click **Next**

Click **Install**

Enable Remote Administration

By default, no remote administration is allowed to IIS 7.X. When enabling remote administration you should establish procedures for authorization of those individuals that can remotely administer your server or a web site. When giving access to a web site to an individual, you should make them aware that they should guard their login and password, and not share it with additional individuals. Do make the option open for them to have additional logins to administer the site. This will help to protect you and them from harmful or an error in administering their web site.

Click **Start** type in **inetmgr** in the search box

Click on the server name

In the Management area of the of the features view (center pane), double click Management Services.

Click on the check box to **Enable remote connections**

Select the option **Windows credentials or IIS Manager credentials**

In the drop down list, select your IP address

In the Actions Panel (right panel), click **Apply**

Close inetmgr

Note: Changes to Remote Administration cannot be changed unless the service is first stopped. Make any changes that you need quickly so that you do not interrupt individuals working on their sites.

Creating a Windows user for authentication

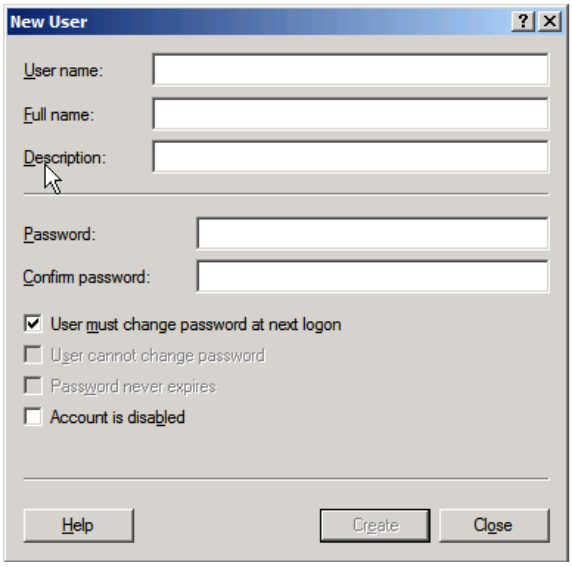
To demonstrate the possible different authentication types of IIS 7.X, you will create four users and give these three different types of access to your server and web sites.

Click **Start**

Type **compmgmt.msc** in the search box. Note: You are looking for Computer Management in your list and it may populate before completing the full program name in the search box.

Expand the **Local Users and Groups** by clicking on the **+**

Right click on **Users**, select **New User**, the new user dialog box will open



Create yourself as a new user on the server. Your user name should be the **same as the login you use for the sandbox**. Ie: mine would be mbaker

Type your full name in the Full name text box.

Type Server Administrator in the description text box.

Give your account the password of Pa55word

Uncheck the "User must change password at next login"

Check the "Password never expires" checkbox.

Click Create

Create a second user. User name **mbaker**

Full name: Marti Baker

Description: Server Administrator

Password "**Pa55word**"

Uncheck **User must change password at next login**

Check **Password never expires**

Click **Create**

Create a third user. User name **bojdDev**

Full Name: **John Smith**

Description: **BOJD Site Developer**

Repeat the password, uncheck, check from above, and create from above

Create your last user. User name defaultAdmin

Full Name: **James Jones**

Description: **Default Site Administrator**

Repeat the password, uncheck, check from above, and create from above

Click **Close**

Disable other built in accounts.

Right click on the guest account and select **Properties**

Verify that the guest account is disabled

Create Groups for site and server administration

As an administrator of a server you can create individual users and assign each user to permissions. It is better if you assign the user to a group, and assign the group the permissions to administer either a site or server.

If the Computer Management window is closed, re-open it by typing **compmgmt.msc** in the search box

If needed, expand **Local Users and Groups** by clicking the **+**

Right Click on Groups and select New group

Create a new group with the following information:

Group name: **BOJD Administrators**

Description: **www.bojd.com**

Click **Add**

In the object text box, type **bojdDev**, click **Check Names**. The server should automatically fill in the complete machine user name if the entry is correct.

Click **OK**

Click **Create**

Create a second group with the following information

Group Name: **Default site administrators**

Description: **Default web site**

Add members: **James Jones** (You will need to look above to determine their user name)

Click **OK**

Click **Create**

Click **Close**

Add your user name to the web server administrators; by doing this step you are giving yourself server administration rights.

Right click on the existing Administrators group

Select Add To Group

Click **Add**

Type in your user name. ie: mine would be mbaker

Click **Apply**

Repeat the steps above for user mbaker that you created in the users

Click **OK**

Log off of your server and **login** using your user name and password.

Return to Computer Management, disable the administrator's account that you have been using previously. This account will no longer be able to be used.

Expand the **Local Users and Groups** by clicking on the **+**

Click on **Users**

Locate **Administrator**

Right click on Administrator

Select **Properties**

Click on "**Account is disabled**"

Click on **Apply**

Click on **OK**

Close the Computer Management window.

Site and Application Level Authorization

Open IIS Manager

Navigate to the www.CAC.com site

In the Features view (center panel) locate and double click IIS Management Permissions

In the Actions pane (right panel), click Allow User

Verify that Windows is the type of user checked

Click **Select**

Click on **Object Types**

Type "**BOJD Administrators"** in the text box

Click **Check Names**; the server should automatically complete the full server name for the group

Click **OK**

Click **OK**

Repeat the steps in 5 above for your default web site using the **Default site administrators** group.

Delegating Premissions

Now we need to tell IIS what each user can do with their site or server.

If IIS Manager has been closed, re-open IIS Manger

Click on your server name and locate double click on Feature Delegation in the Management area of the Features Pane.

Click on Custom Site Delegation

In the drop down list in the Features Pane, Select cacApp

Note in the Actions pane (right panel) there are two options available

Reset all Delegation

Custom Site Delegation

Locate and click on Logging

Change the value to Read Only back

Lab 5-supplement

Student Name: _____

Now for some fun! Go to your Windows 7 Host Machine.

Installing IIS Manager for Remote Administration

Open IE and go to http://www.iis.net/download/IISManager

Click **Install Using Microsoft* Web Platform Installer**

If prompted, click **Allow** Web Platform Installer

If prompted, click **Allow** for "A website wants to open web content…"

Walk through the wizard when finished, click finish.

Switch desks with another student!

From the host Windows 7 machine, type in **inetmgr** in the search box of start.

Under the Connections (left panel) click the **globe** icon, select **Create New Connection**

For server name, type your IP address of your web server: 10.1.13.1XX (this is your web server IP not the desk you are sitting at).

Click **Next**

Type in your new administrator user name and password

Click **Next**

Type in a **description** (I used my machine name), click **Finish**

You can now administer your site from a different machine! back

Lab 6

Student Name: _____

In this lab you will be setting up FTP (File Transfer Protocol) services to your server.

FTP is the most common way that your web developers will place their web site documents on your server.

FTP is not encrypted. It is often recommended that you set up a separate user account and group for users for use with FTP. Give your user a password for FTP, and do not allow them to change it. This password should not be any password that you use for administration of your server. Sometimes these are simply created from a log file of passwords.

With Windows 2008, we can isolate our users to specific folders that they have access too. Because our machines have not been set up to use Active Directory Services, we will be using the Insolate user without Active Directory.

If needed, start IIS Manager

If needed expand your server by clicking on the **+**

Click on **FTP**

FTP is managed through the IIS 6.0 interface.

In the Features pane (center panel), click "**Click here to launch**", IIS 6.0 interface will open

Expand your server name by clicking on the **+**

Right click on **FTP**, select **New FTP site**

The FTP Site Creation Wizard will start

Click **Next**

Type in a description: **cacFTP**

Select your **IP address** from the drop down list.

Leave the default port to 21

Click **Next**

Select **Isolate Users** radio button, select **Next**

Click Browse, and navigate to the folder you created for the cacApp; **c:\inetpub\wwwroot\cacApp**

Click **OK**

Click **Next**

Select permissions **Read and Write**

Click **Next**

If you get a warning that the service did not start in a timely manner, click OK.

Click **Finish**

Right click on your newly created FTP site and select Permissions

Select **Edit**

Select **Add**

Type in **BOJD Administrators**

Click **Check Names**, the server should automatically complete the group name.

Click **OK**

Give BOJD Administrators the following permissions

Modify

Read & Execute

List Folder Contents

Read

Write

Click **OK**

Click **OK**

Right click on your newly created FTP site, and select Start back

Lab 7

Student Name _____

Web sites often need to respond to input from a user with an email. This can be done for recovering passwords, verifying that the user has provided a true email address, welcoming a user to a site, or perhaps confirming an ecommerce order.

While there are many third party software pieces that can be added to IIS to do add this functionality to a web site (most of them have a price attached to them), IIS provides SMTP (Simple Mail Transfer Protocol) as a part of its services.

Tonight, you will configure SMTP on your server.

Verify Installation of SMTP

The SMTP server is not installed by default.

1. Open Server Manager by right-clicking on **My Computer**, and selecting **Manage**. (Alternately, open **Control Panel**, click on **Programs and Features**, and then select **Turn Windows features on or off**.)

2. Under **Features**, select **Add Features**.

3. Scroll down and verify that SMTP Server is installed. If not, select the SMTP Server check box. If SMTP Server is installed, you can skip to Configure SMTP E-Mail for a Web Application

4. Click **Add Required Role Services**. If there are any missing roles required for the SMTP installation, Windows Server® 2008 R2 or Windows Server® 2008 installs them. Click **Next**.

5. You need to step through the entire wizard again, even though IIS is already installed (IIS 6 Management Compatibility and the IIS 6 Management Console must be installed for SMTP to work).

a. On the Introduction to Web Server (IIS), click **Next**

b. On the Select Role Services, click **Next**

c. On the Confirm Selections , click **Install**

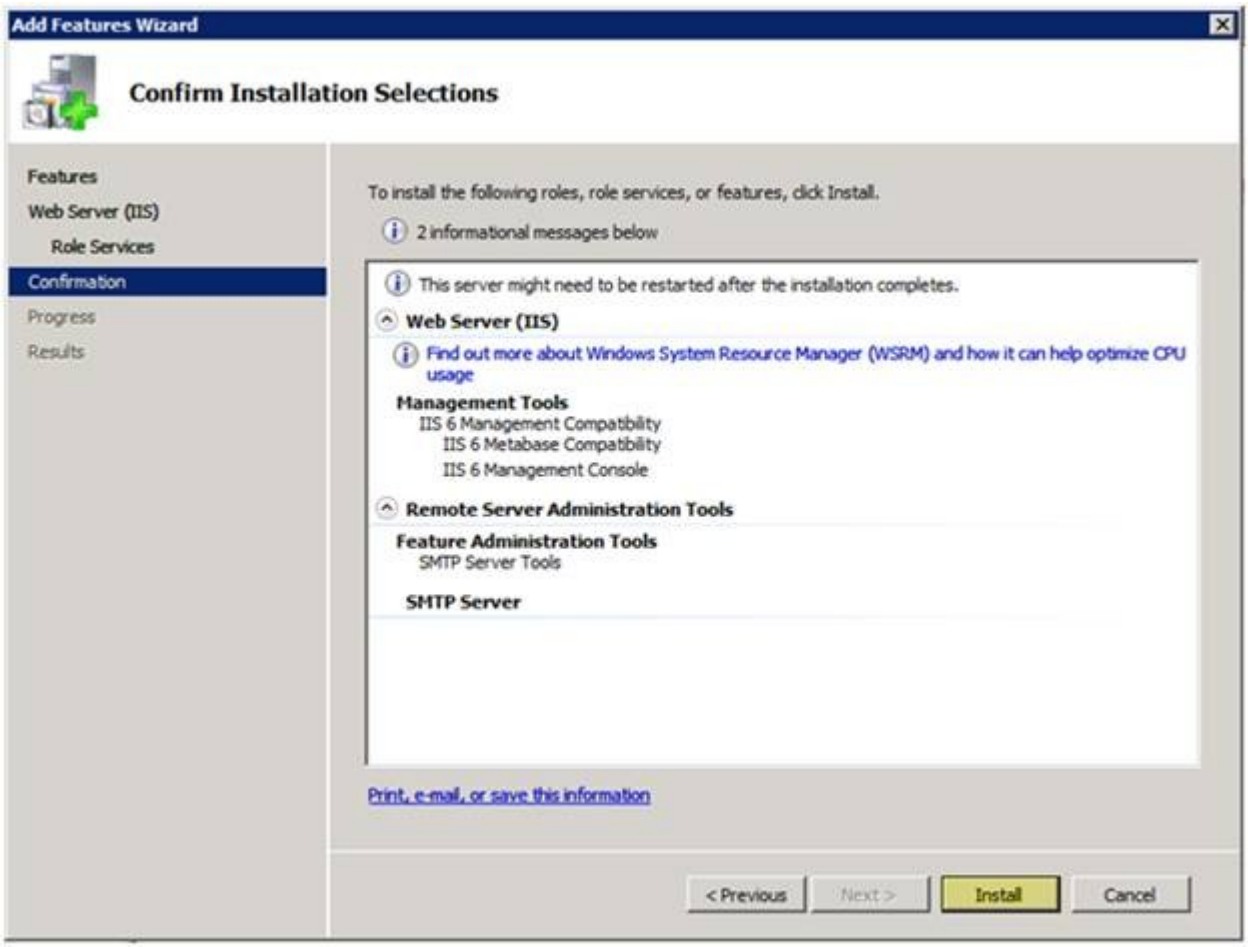


Figure 1: Confirm Installation Selections

6. Press **Close** when installation is complete.

Configure SMTP E-Mail for a Web Application

Once you have added SMTP, you can configure it for your PHP applications. You will be configuring your server with default information for cacApp. This can be done by using the user interface (UI), by running Appcmd.exe commands from a command prompt, by editing configuration files directly, or by writing Windows® Management Instrumentation (WMI) scripts. Note that you must have IIS 7 installed before enabling SMTP.

Open **Internet Information Services (IIS) Manager**, (inetmgr), and then navigate to the level you want to manage. (Note: You can manage SMTP at server level or site level.)

Expand your server by clicking on the +

Expand sites by clicking on the +

Click on cacApp

In **Features View**, double-click **SMTP E-mail**.

On the **SMTP E-mail** page, type the email address of the sender in the **E-mail address** text box. Use **questions@bojd.com**

On the SMTP E-mail page, select the following delivery methods:

Deliver email to SMTP server: to deliver email messages immediately. This requires an operational SMTP server for which the user has credentials.

Instead of supplying a SMTP server, type in your IP address 10.1.13.1XX.

Verify that port **25** is the selected port.

Port 25 is the SMTP standard TCP port and is the default setting. More than one virtual server can use the same TCP port if all servers are configured by using different IP addresses.

Under **Authentication Settings**, specify **Not Required**.

If Windows Authentication is selected, the application must provide Windows login credentials.

If Specify Credentials is selected, you can set up a specific Windows user that must be provided by the application.

Do **not** select **Store email in pickup directory**. While SMTP is a good tool for email being created from a web application, it is not a "full" email server; and it is not recommended to be used for an email server.

Click **Apply** in the **Actions** pane.

Close Internet Information Services (IIS) Manager

Use the Command Line

Deliver email messages immediately

To configure SMTP email to deliver email messages immediately, use the following syntax:

Click **Start**

Right click on Command Prompt and select **Run as administrator**

At the c prompt type:

C:\windows\system32\inetsrv\appcmd set config /commit:WEBROOT /section:smtp /from:*questions@bojd.com* /deliveryMethod:Network /network.port:*25*

Please note: the spaces , variables, Case Sensitive arguments, and slash direction are important here.

The variable **from** *string* is the email address of the sender. The variable **/deliveryMethod:network** configures IIS to deliver email messages immediately. The variable **/network.port** *int* sets the TCP port that is used by IIS to deliver email messages. The variable **/network.host** *string* specifies the host used for SMTP transactions. The variable **network.defaultCredentials:True**|**False** enables or disables authentication using the default network credentials. If **defaultCredentials** is set to **True**, Kerberos or NTLM are used if the server supports these protocols. The variables **network.userName:***string* and **network. password:***string* set a basic authentication user name and password.

If you have been successful at updating your configuration file you will see:

Applied configuration changes to section "system.net/mailSettings/smtp" for "MACHINE/WEBROOT/APPHOST" at configuration commit path "MACHINE/WEBROOT"

Close the command prompt window by typing “Exit” and hitting enter

Note: that when you use Appcmd.exe to configure the **<mailSettings>** element at the global level in IIS 7, you must specify **/commit:WEBROOT** in the command so that configuration changes are made to the root Web.config file instead of the ApplicationHost.config file.

Setting up PHP to use SMTP - Edit the Configuration Files

Preparation for configuring PHP

Right click on the **Start** button

Select Explore

Click on tools area, click **Organize** and select **Folder and Search Options**

Select the **View** tab

Under the Advanced Settings Pane, locate and uncheck **Hide extensions of Known Files**

Click **Apply**

Click **Apply to Folders**

Click **OK**

Configuring PHP to run with SMTP

Click Start

Type in **Notepad** in search

Browse to c:\php and locate php.ini

Right click on php.ini and select **copy**

Right click in an open area of your right pane and select paste

Rename this file phpBackup.ini

Each time you make a change on php.ini, I suggest that you make a copy of the file before changing it.

Using Notepad, open the original php.ini file

Click Edit → Find and search for: **[mail function]**

Scroll down and locate: ;For Win32only

Verify that the entries in php.ini are: (You may need to remove a semicolon from in front some lines)

; For Win32 only

; http://php.net/smtp

SMTP = 10.1.13.1XX

; http://php.net/smtp-port

smtp_port = 25

; For Win32 only

; http://php.net/sendmail-from

sendmail_from = question@bojd.com

Save and close the Php.ini file.

You may need to save this file to your desktop and then cut and paste it into c:/php/

If asked to you should provide administrator credentials while copying this file

Enable Relay for your IP Address

Open the Internet Information Services (IIS) 6.0 Manager by going to **Start → Administrative Tools →Internet Information Services (IIS) 6.0**

Expand your server by clicking **+**

Right-click on [**SMTP Virtual Server #1]**, select **Properties**

On the **General** tab:

Ip Address: From the drop down box, select your IP Address.

Click the **Advanced button**

Click **Add**

In the Identification dialog box, select the drop down menu and click on **(All Unassigned)**

Add TCP port **25**

Click **OK**

Click **OK**

On the **Access** tab, and then click on **Connection** button. You may see a list of the current IP addresses allowed to connect to the server.

Click the radio button for **Only the list below**

In the IP Address list, if the IP address **127.0.0.1** is not listed, click the **Add** button.

In the Single Computer IP Address, type **127.0.0.1**

The IP Address should now show in the list with “Granted” in front of it

Click **OK**

Repeat steps 3b through 3e for IP address **10.1.13.1XX** (your IP address)

Repeat steps 3b through 3e for domain: **localhost**

You will receive a warning box stating that the **Restricting access by domain name…**

Click **OK**

Click **OK**

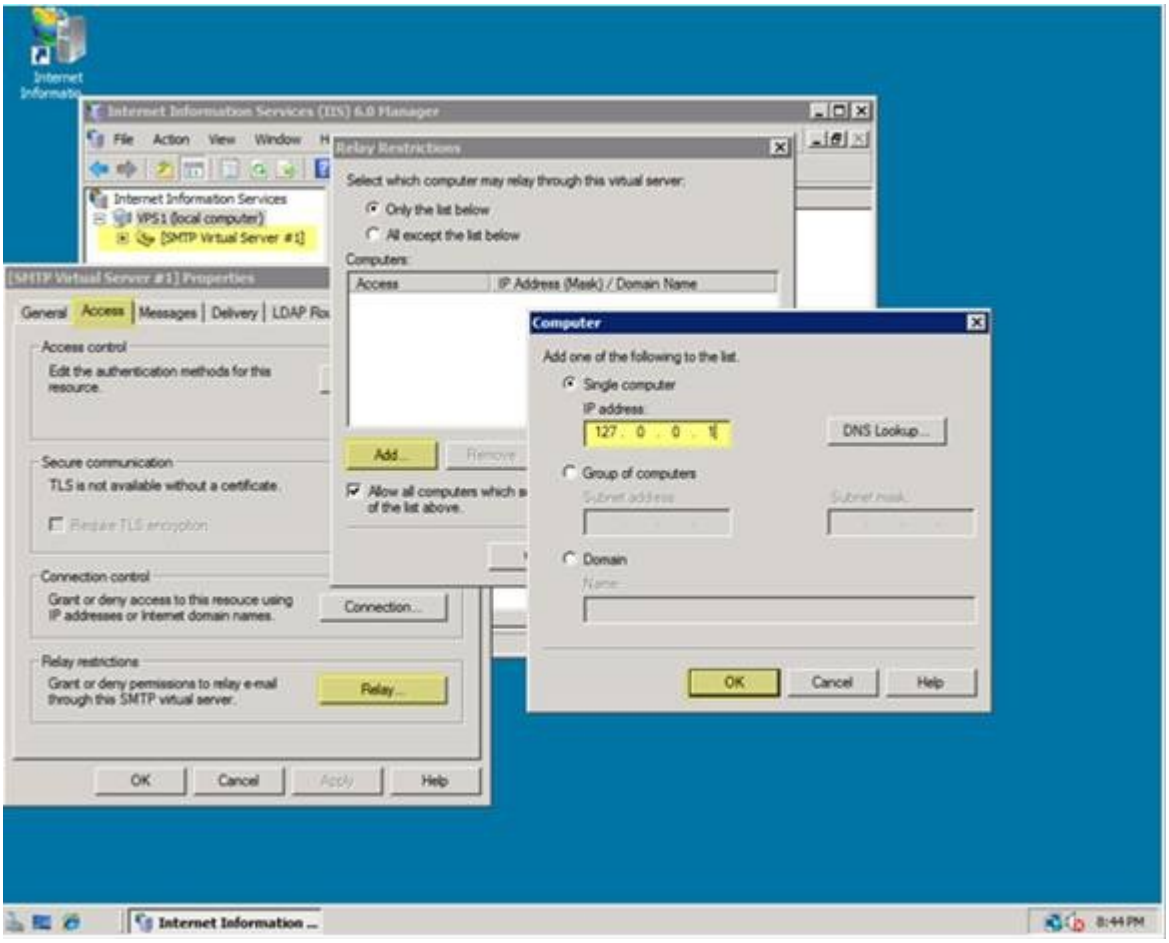


Figure 2: Enable Relay for localhost

While still in the Access tab, Click the Relay button, and set up the relay options for the server. Ensure the IP address 127.0.0.1 is granted permission to relay mail.

Click the radio button for **Only the list below**

In the IP Address list, if the IP address **127.0.0.1** is not listed, click the **Add** button.

In the Single Computer IP Address, type 127.0.0.1

The IP Address should now show in the list with “Granted” in front of it

Click OK.

Repeat steps 4b through 4e for IP address: **10.1.13.1XX** (your IP address)

Repeat steps 4b through 4e for domain: **localhost**

Click **OK**

C You will receive a warning box stating that the **Restricting access by domain name…**

Click **OK**

Click **OK**

Click Apply and OK

Close Inenter Information Services (IIS) 6.0 Manager

Return to IIS Manager (inetmgr)

Click on your server

Click **Stop**

Click **Start** IIS.

Checking the functionality of SMTP

After completing the steps above, you need to verify that SMTP is working. In order to get credit for completing this lab, you must successfully send me an email by running a small PHP script from your web server.

Open Notepad with a right click and select **Run as administrator**

Type the following PHP script

```
<?php

if (mail('mbaker@email.edcc.edu’, 'Test-Email', 'Email is working your name')){

        echo('Email is working');

}
```

```
else {
        echo('Email is not working');
}
?>
```

Save this file in **c:\inetpub\wwwroot** as emailTest.php

Open up **Internet Explorer**

In the URL type in "http://10.1.13.1xx/emailTest.php

If you have been successful, you will see "Email is working" back

Lab 7-supplement

Student Name _____

Adding a printer to your virtual server

On your virtual server

Start → Control Panel

verify you are in Classic View

Right click on Add Printer → Run as Administrator

Select **Add a network, wireless or Bluetooth printer**

When it starts searching for a printer, click **Stop**

Click on **The printer that I want isn't listed**

Select **Add a printer using TCP/IP address or host name**

In hostname or IP address type **10.1.12.245**

Click **Next**

When it finds the printer leave Set as default printer checked, click **Next**

Select Do Not share this printer, click **Next**

DO NOT PRINT A TEST PAGE, click **Finish** **back**

Lab 8

Student Name _____

Baseline Security

One of the best ways to manage the security risk of a Windows server is to check some of the basics

Are all updates applied to your server?

Have you disabled unnecessary accounts?

Have you assigned NTFS permissions (lab 9) to folders and files?

Have you used tool available to see how secure your server is? (This lab)

During this lab you will be working with Microsoft's Baseline Security Manager for Windows Server 2008. This lab is a bit different from other labs that you have worked with in that it asks you to install the baseline analyzer, a leaves it up to you to research security issues and make adjustments to your server.

Go to **Microsoft Baseline Security Analyzer 2.2** at **http://technet.microsoft.com/en-us/security/cc184923**

On the right side of the screen, click the link on the right, under Download Now "Microsoft Baseline Security Analyzer (available in English, French, German, and Japanese)"

Select **MBSASetup-x64-EN.msi**

Microsoft's blurb about this tool

Overview

To easily assess the security state of Windows machines, Microsoft offers the free Microsoft Baseline Security Analyzer (MBSA) scan tool. MBSA includes a graphical and command line interface that can perform local or remote scans of Microsoft Windows systems.

MBSA 2.2 builds on the previous MBSA 2.1.1 version that supports Windows 7 and Windows Server 2008 R2 and corrects minor issues reported by customers. As with the previous MBSA versions, MBSA 2.2 includes 64-

bit installation, security update and vulnerability assessment (VA) checks and support for the latest Windows Update Agent (WUA) and Microsoft Update technologies. More information on the capabilities of MBSA is available on the MBSA Web site.

MBSA 2.2 runs on Windows Server 2008 R2, Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003, Windows XP and Windows 2000 systems and will scan for missing security updates, rollups and service packs using Microsoft Update technologies. MBSA will also scan for common security misconfigurations (also called Vulnerability Assessment checks) using a known list of less secure settings and configurations for all versions of Windows, Internet Information Server (IIS) 5.0, 6.0 and 6.1, SQL Server 2000 and 2005, Internet Explorer (IE) 5.01 and later, and Office 2000, 2002 and 2003 only.

To assess missing security updates, MBSA will only scan for missing security updates, update rollups and service packs available from Microsoft Update. MBSA will not scan or report missing non-security updates, tools or drivers.

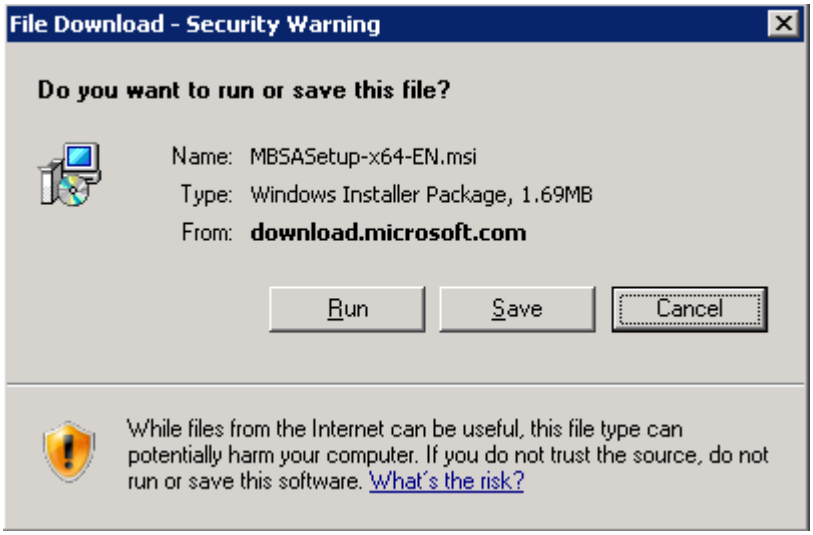
Choose the appropriate download below for English (EN), German (DE), French (FR) and Japanese (JA) for x86 (32-bit) or x64 (64-bit) platforms.

Instructions

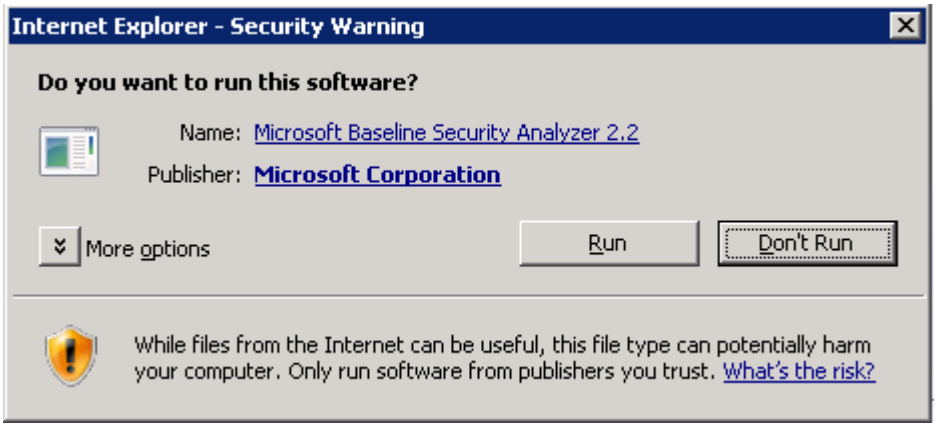
Note: Please view the readme.html file before running MBSA the first time. The readme.html file contains important information on system requirements, scan options, and tool support options.

Click the **Download** button on this page to start the download.

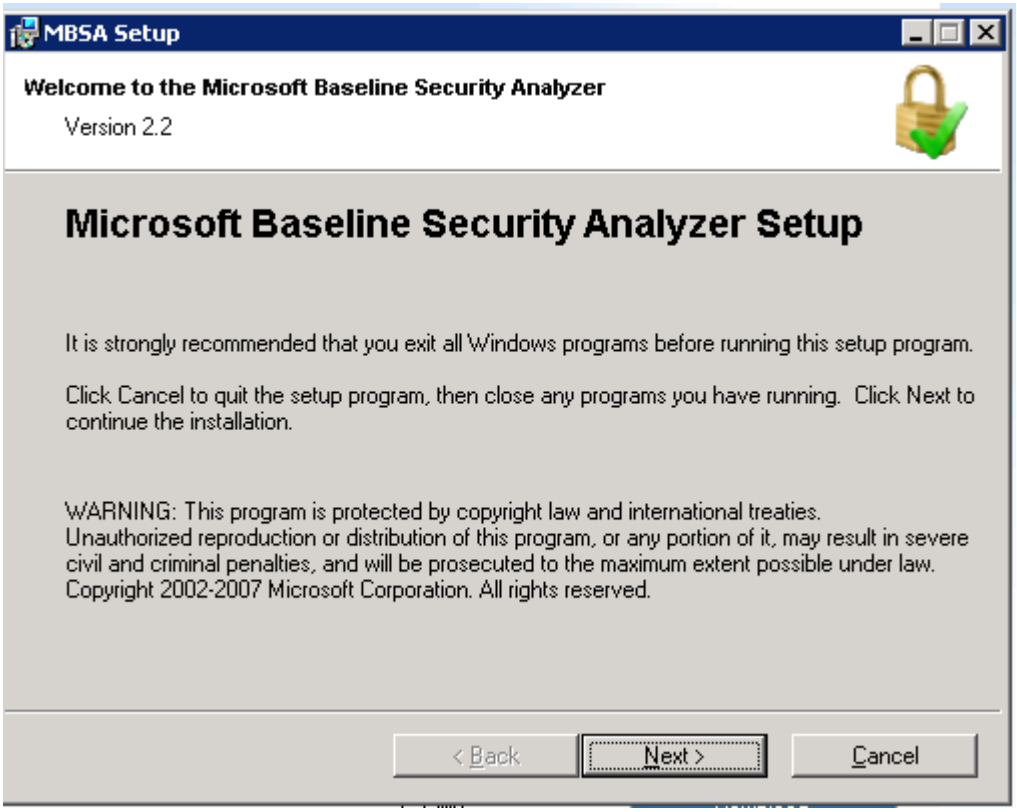
Start the installation immediately. When asked "Do you want to run or save this file?", select **Run**



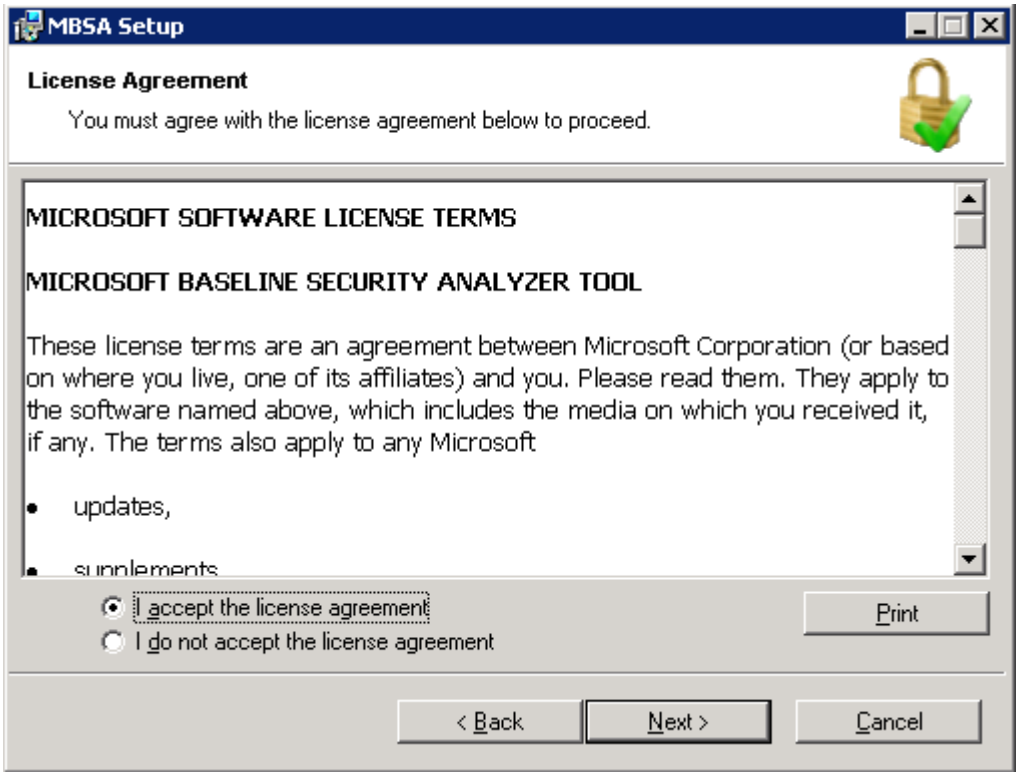
When asked "Do you want run this software?", select **Run**



On the Welcome to the Microsoft Baseline Security Analyzer, Click **Next**



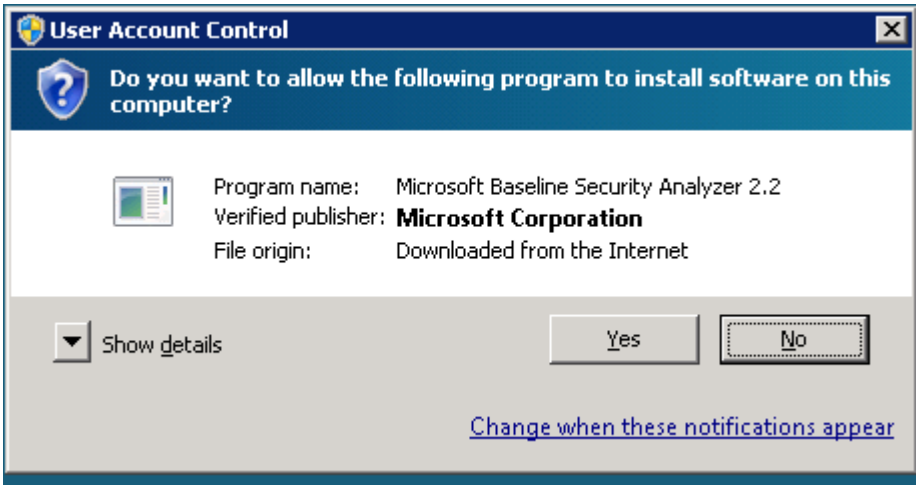
Accept the license agreement and click **Next**



Accept the default installation location, and click Next

Click Install

If you are asked if you want to run this program from the Internet, Select **Yes**



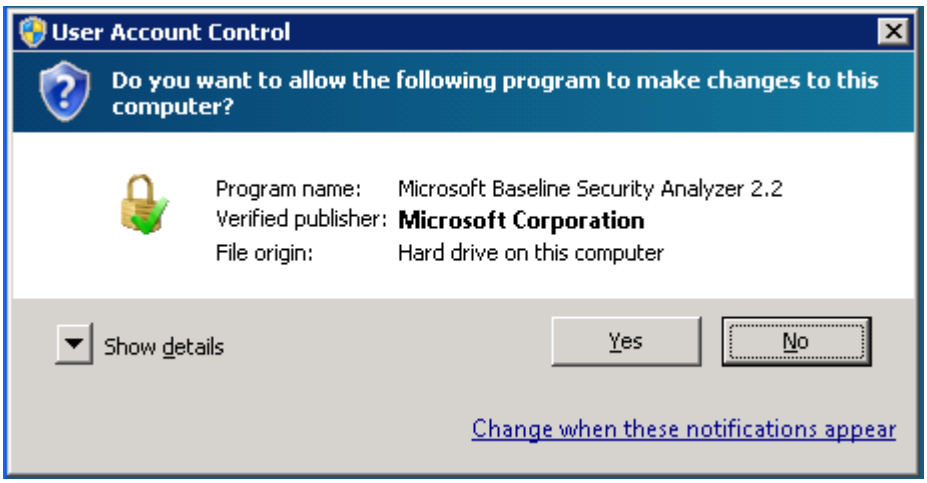
After the installation is complete, click **OK**

Immediately after the installation of MSBA 2.X.X.X – you should run a security analysis of your server.

Click Start

Click on Microsoft Baseline Security Analyzer 2.2

When asked Do you want to allow the following program to make changes to your computer, select **Yes**



Select "Scan a Computer"

Select the following options for your security scan:

Select this computer

Security Report name: leave the options that are currently in place

Options:

Leave the standard selected options

Click **Start Scan**

Your scan can take time depending on how many services, files, users, groups, programs there are installed on your server.

Print your security report

Read through your security issues report.

You should be concerned first with any score highlighted with the  symbol.

Read through the “Result Details”

Read through the “How to correct this”

You must make an intelligent decision about whether you will keep the vulnerability or correct the issue.

If you decide to do nothing about the vulnerability – Make note of this, it should be included in your documentation.

After making changes to your security setup:

Run another Scan of your computer

Compare the previous results with your new results.

If you are satisfied with your server’s baseline print the report

What to turn in:

This lab with a minimum of two security reports stapled to it. back

Lab 9

Student Name _____

Lab 9 NTFS and URL Authentication

In this lab you will be creating a new web site, determining Authentication and Authorization through NTFS and URL permissions of IIS 7.X.

This is portion of IIS security is a major step in locking down your server. By learning how to correctly configure permissions on resources to allow permitted users to access resources, while denying unauthorized users, you are creating the best line of defense for your web server.

Create a new web site

In order to work with these permissions, you will be creating yet another web site on you web server. (You may need to look at Lab 3 to remember how to create a site.)

From Blackboard

Using your previous working knowledge, and create a new web site.

Site and folder name: myGrill.com

Start by using the default application Pool

Create a new application pool for myGrill.com

Name the new application pool myGrillAppPool

Enable logging for the new site

Use W3C format

Verify that the following fields are being recorded for the log

Download MyGrill.zip available on Blackboard under Lab 9 Authentication

Unzip the files into the folder you have created for myGrill.com.

Be sure that the files index.asp resides directly under your myGrill.com folder. If you are unsure how to do this or if you are doing it correctly, please ask for help.

Creating ODBC Connections

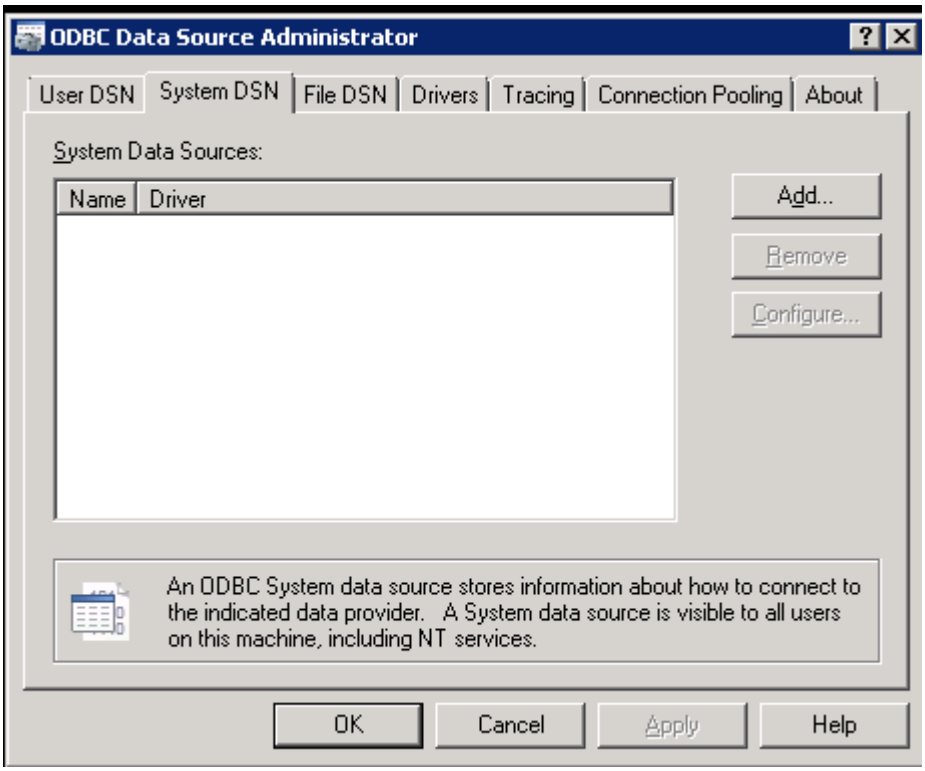
ODBC (Open database Connectivity) is a technology used by many Web applications. You will be creating an ODBC connection for myGrill.com. ODBC allows the web developer to establish a simple connection to a database and reuse that connection by referencing the name given to the connection.

Click on Start

In the Start Search box type **c:\windows\sysWOW64\odbcad32.exe, click** on odbcad32.exe when available from the list.

When the User Account Control dialog box appears, click Continue

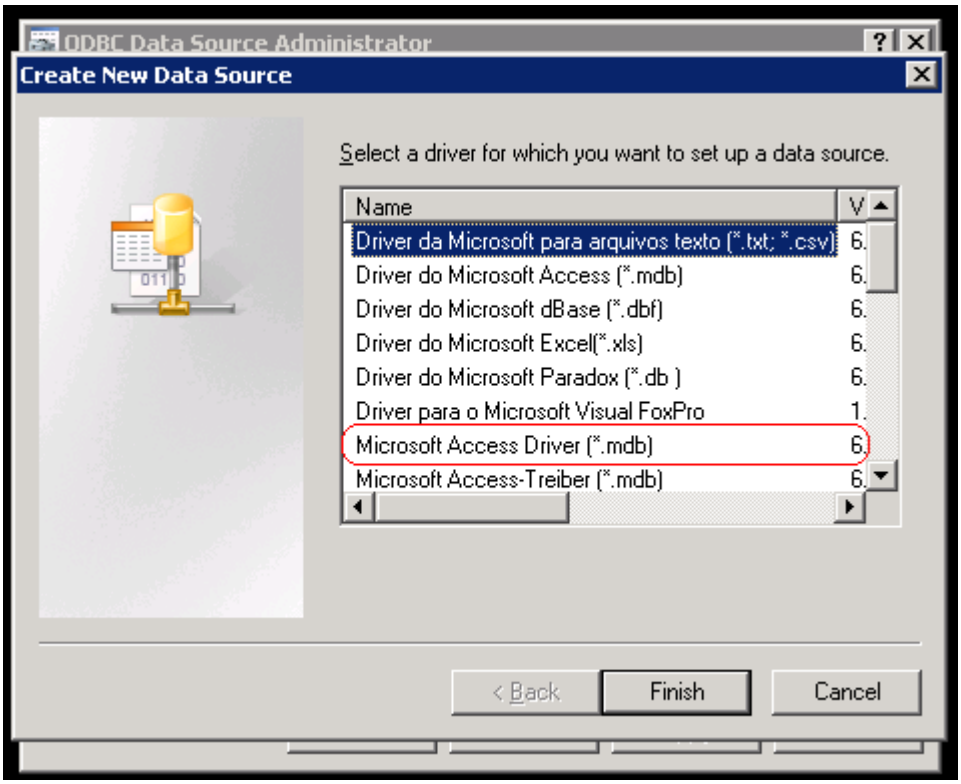
The ODBC Data Source Administrator dialog box will open



Select the **System DSN tab**

Click **Add**

Select **Microsoft Access Driver (.mdb)**



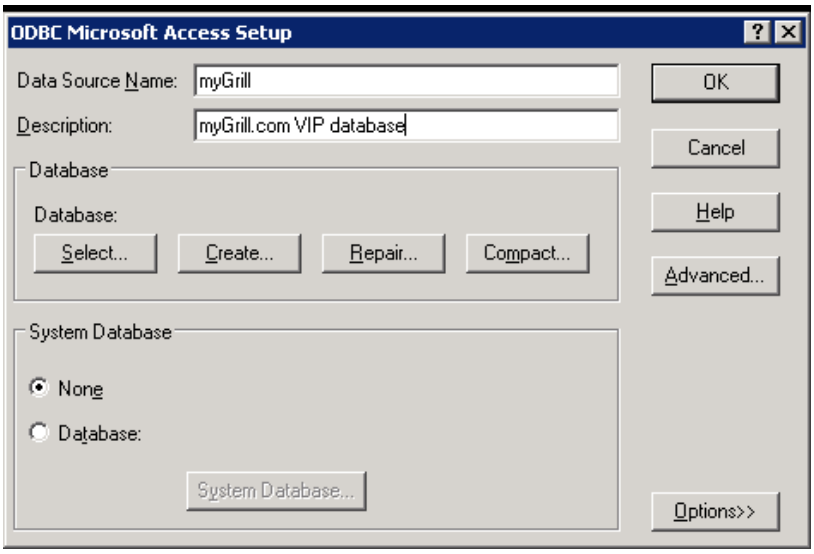
Click **Finish**

The ODBC Microsoft Access Setup dialog box will open

Complete the following information:

Data Source Name: myGrill

Description: myGrill.com VIP database



Click **Select**

Navigate to and select: **c:\inetpub\wwwroot\myGrill.com\database\grill.mdb**

Click **OK**

Click **OK**

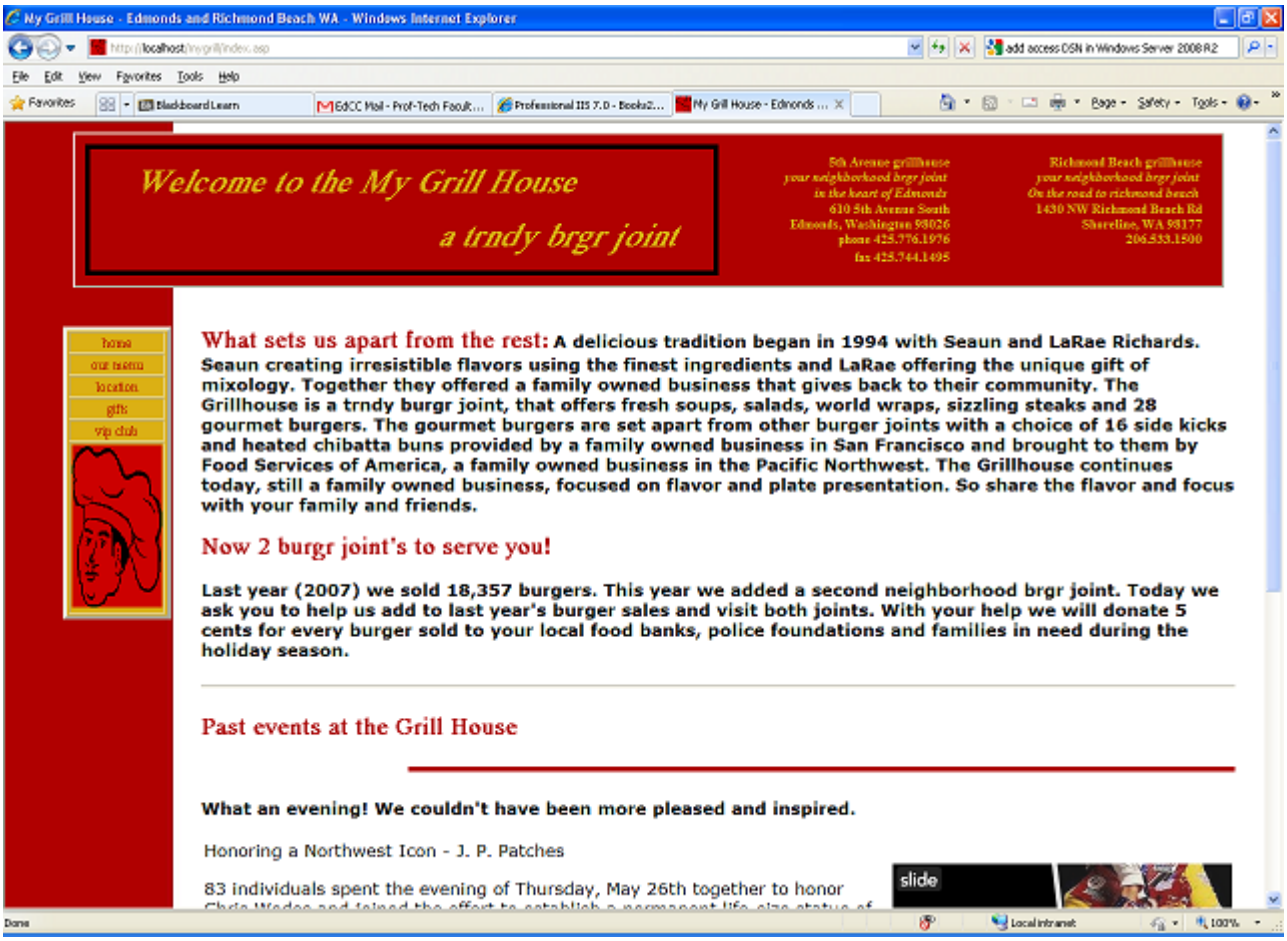
Click **OK**

Verify that myGrill.com is working

Open Internet Explorer

Type the URL: http://localhost/mygrill.com/index.asp

You should see the following screen if myGrill.com is working correctly:



Configuring Authentication

myGrill.com has three main purposes to being on the Web.

Attract new customers looking for a place to eat

Acquire new and existing customers' information by asking them to join the VIP club.

Allow the owners of myGrill.com to send emails to customers about specials and events happening at one or both of their restaurant locations.

Business rules about myGrill.com

The front end of myGrill.com should allow anonymous browsing by anyone on the World Wide Web.

The back end (located under the admin folder of the site) should only be accessed by the owners of the site).

To configure Anonymous authentication:

Open IIS Manager (Start Run, enter intemgr in the dialog box, and then press [Enter]).

You may want to consider pinning inetmgr to your task bar for easy access.

Locate myGrill.com root folder, you wish to configure Anonymous authentication for. Select the Authentication Feature option.

Select the Anonymous Authentication option, verify that Anonymous authentication is enabled.

If not: Click Enable in the Actions pane to enable Anonymous authentication.

Figure 14-1

Click Edit in the Actions pane to edit Anonymous authentication options, as shown in Figure 14-2. By default, the IUSR account is used for anonymously authenticated access for static files and Classic ASP files (ASP.NET file access occurs under the Web Application Pool's identity).

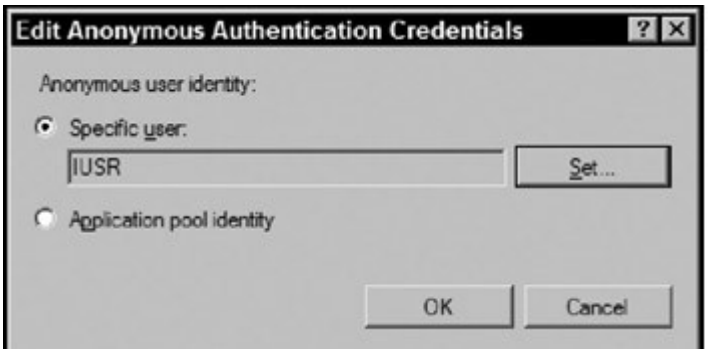


Figure 14-2

Click OK to confirm your changes.

Verify that anonymous browsing is still enabled, by refreshing Internet Explorer displaying MyGrill.com

Forms-Based Authentication

By default, Forms Based Authentication applies only to requests for files managed by .NET (e.g. ASPX pages), and not to other types of files (e.g. static files). To alter this configuration, so that Forms Based Authentication is used for all file types:

Open IIS Manager (Start ê Run, enter intemgr in the dialog, and then press [Enter]).

Locate the server node, and open the Modules feature.

Double click the FormsAuthentication module (Patience!)

Uncheck the “Invoke only for requests to ASP.NET applications or managed handlers” option.

Click OK commit your changes, and exit the dialogue boxes

Create a new application pool for the myGrill.com Admin folder.

Name the new application pool myGrillAdminAppPool

Apply this new application pool to c:\inetpub\wwwroot\mygrill.com\admin

Locate myGrill.com’s Application folder admin by expanding myGrill.com and expand the Admin folder in the navigation pane. Click on the folder.

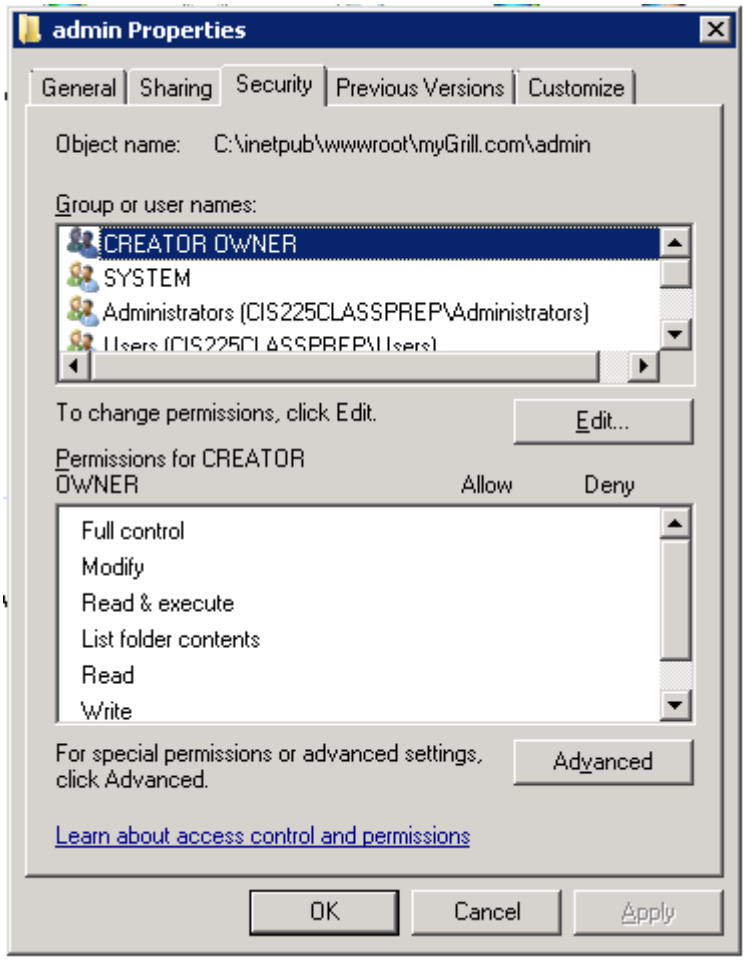
Double click on Authentication in the features pane

Click on Forms-Based Authentication option

Click the Edit Permissions link to edit configuration information for FBA.

The Properties Dialog box will open

Select the Security tab



Click on the advanced button

Click the Edit button

Uncheck the Include Inheritable permissions from this object's parent.

In the Windows Security dialog box, select Copy

Click Apply

Click OK

Click OK

Click OK

Double click Authentication again

Click Edit

Login URL — This is the page to which users will be redirected to enter their credentials. Enter: index.asp

Cookie Time-out — After the set period of inactivity (no requests from the browser), the user will need to reauthenticate. Leave the default 30 minutes.

Cookie Mode — Allows the Administrator to choose whether to use cookies, store authentication information in the URL, allow .NET to detect whether the device supports cookies via Javascript, or assume cookie support based on the browser's user agent string (this is the default setting).

Cookie Name. Enter: myGrillAdmin

Uncheck Require SSL for requests.

Whether to use a sliding cookie renewal or not. When using sliding renewal, each request resets the cookie time-out setting. If sliding renewal is disabled, the user will have to reauthenticate regardless of whether they are active or inactive when the cookie times out.

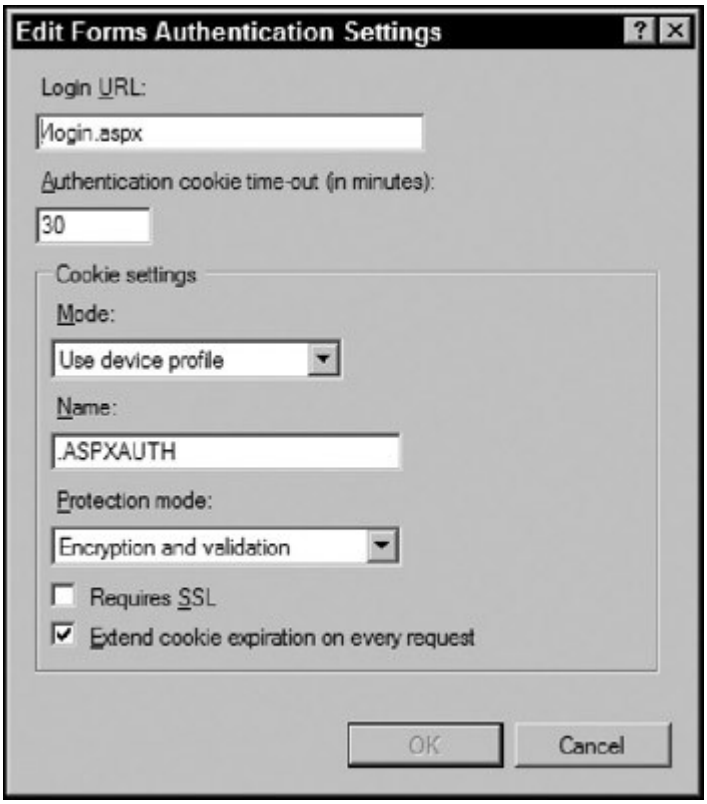


Figure 14-13

Click OK to commit changes and exit the dialog.

Note FBA settings are stored in the ASP.NET configuration section. This can either be the machine-wide root web.config file or in the <system.web> section of a web site's or web application's web.config file. FBA settings are not stored in IIS configuration files or sections.

Correcting buggy code (Developers never write buggy code!)

Replace the file located in c:\inetpub\wwwroot\mygrillhouse.com\admin\

Database.asp:

```
<%

' Database Connection

Dim ojbConn

Set objConn = Server.CreateObject ("ADODB.Connection")

objConn.Open "DSN=myGrill"

%>
```

Set up 32-bit acceptance of IIS 7.0

Open a command prompt as an administrator

Type the following command: (spaces are important). After typing the full command, press enter on your keyboard

```
C:\Windows\system32>c:\windows\system32\inetsrv\appcmd set config -section:applicationPools
-applicationPoolDefaults.enable32BitAppOnWin64:true
```

If successful, you should see

Applied configuration changes to section "system.applicationHost/applicationPools" for "MACHINE/WEBROOT/APPHOST" at configuration commit path "MACHINE/WEBROOT/APPHOST"

Exit the command window

Verify Form Authentication

In Internet Explorer type in the URL: http://localhost/mygrill.com/admin/index.asp

Type in user name: Seaun

Type password: Richards back

Lab 10

Student Name _____

TSL and its successor SSL are means of encrypting traffic (packets filled with information) across the WWW. Pages that request personal information should be accessed through encrypted pages. These include, but not restricted to:

Any personal information

User IDs

Passwords

Credit card numbers

Bank accounts

If you are at a site, and are asked for this type of information and are not on a page URI beginning with https:// you should verify that the form is sending the information encrypted before hitting submit.

FYI: you do not need to do this but you should be aware of how to do this as a savvy web user.

To verify that your information is being encrypted:

When asked for personal information

Look to see that the URL address includes: https:// at the beginning

If not, right click on the page and select View Source or View Page Source

Click on edit and search for the value of "**<form**"

Verify that the action attribute of the form element includes the value https://

Certificate Authorities

As you surf the web, you will run into certificates of authority and will at times accept these certificates. CA or Certificate Authorities are stored in your computer. These certificates often tell your browser to trust or un-trust a web site.

Viewing current CA's on your Web Server

To view a list of installed trusted CAs:

Click Start → Run, enter mmc.exe, and then press [Enter].

Choose File → Add/Remove Snapin.

Scroll through the list of Snapins and Select Certificates and click Add.

A prompt will appear offering a selection of the current user's account, a nominated service account, or the machine's account. Select Computer Account, click Next

Select Local Machine. Click Finish

Click OK to exit the Add/Remove Snapin dialog.

Expand the Trusted Root Certification Authorities node, and click on Certificates to view a list of installed trusted root CAs, as shown in Figure 15-1.

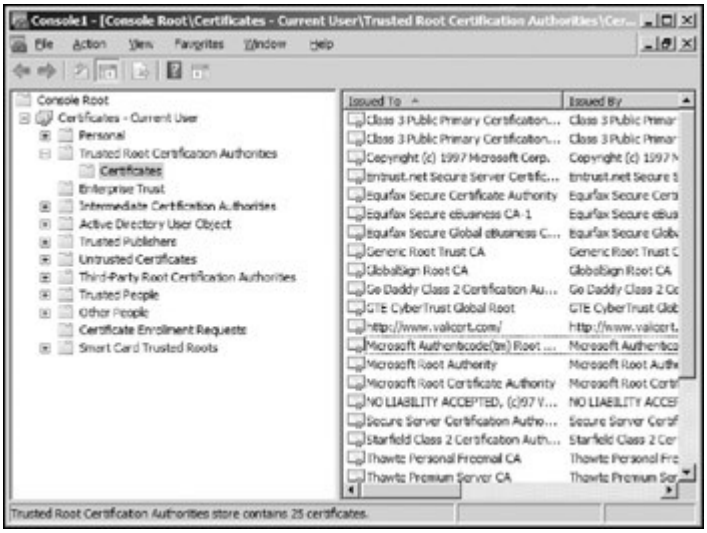


Figure 15-1

Close MMC

About Certificate Authorities

When establishing pages that should be viewed through encryption, you need to install a certificate on your Web server. This is a process that happens often in Web administration. Most ISP offer the services of getting

a certificate for you site from a respected certificate authority. The two most trusted certificate authorities (IMHO) are:

VeriSign

GoDaddy.com

Prices vary greatly depending on the type of certificate that you purchase.

In this lab, we are going to create a self-signing certificate authority. While this is good practice, if you are actually running a web site or server for live production of a web site where you are collecting information from your users, you should consider purchasing a Certificate from a respected CA.

Generate a self-signed Certificate

Creating a server level certificate

Open IIS Manager (inetmgr)

Click Continue if requested

Click on your machine name:

Double click Server Certificates

In the Actions Pane, click on “Create Self-Signed Certificate”

Create a friendly name for the certificate – this is a reference name and can be anything that will identify what the certificate is. I would use something like “Server self-signed certificate”

Click OK

The certificate is now listed in your list of server certificates

Applying a certificate for use.

Expand the sites node in IIS Manager

Expand the myGrill.com node

In the Actions pane, click on bindings

Click the Add button

In the Types drop down list, select https

In the IP Address list, select 10.1.13.1XX (Your IP address)

In the SSL Certificate drop down list, select the certificate you created in step 4a Creating a server level certificate.

Click the View button

On the general tab, verify that the certificate is:

Issued to: (your machine name)

Issued by: (your machine name)

Click OK

Click OK

Click Close

Expand the admin folder node (note: you must have downloaded and replaced adminheader.inc from Blackboard for this to work)

Click on the myGrillAdmin folder with the application pool icon

Under the IIS area of features, double click SSL Settings

Click the checkbox “Require SSL”

Click Apply

The result of this setting is that the files within the admin folder will no longer be accepted unless the user agent (browser) is using an https: connection

Restart your server

Click Start →the right arrow icon →Restart

It is possible that you may need to create the admin folder as a virtual application

Right click on the admin folder of mygrill.com

Select Convert to an Application

From the dropdown list select Application myGrillAdminPool

Click the Select button

For alias type “admin”

Browse for the physical path: c:\inetpub\wwwroot\mygrill.com\admin

Click OK

Creating a virtual directory for the admin folder in mygrill.com

Right click on the admin folder

Select Add virtual directory

Alias: admin

Browse for the physical path: c:\inetpub\wwwroot\mygrill.com\admin

Click OK

Test your new settings

From IIS Manager Open Internet Explorer

Type in the URL: http://10.1.13.1XX/mygrill.com (where 1XX represents your IP address)

This page should still display without a problem

Navigate to a couple of pages at this level (the public level set for anonymous browsing)

Type in the URL: http://10.1.13.1XX/admin

The page should no longer display for you under http:// protocol You should receive a 403.4 error

Type in the URL: https://10.1.13.1XX/admin

When asked if you want to continue over a secure connection click yes

The page should now display again back

Lab 10-supplement

Student Name _____

This quick lab will aid you throughout the execution of all labs involving browsing further labs.

Consider this lab when ever setting up a web site.

Ask your user what they will be using as a default document to be served.

In the case of mygrill.com, the default document for their web site is index.asp

Setting up a default document

Open IIS Manager (inetmgr)

Navigate to myGrill.com

Under IIS in the features pane, double click on Default Document

In the actions pane, click Add

In the dialog box, type in “index.asp”

Click OK

Verify that your default document is now working

Open up Internet Explorer

Type in the URL: http://localhost/mygrill.com

The opening page of myGrill.com should be served to you. back

Lab 11

Student Name _____

In lab 10, you installed a self-signing certificate on c:\inetpub\wwwroot\mygrill.com\admin. In this lab you will be creating another certificate request, but instead will be sending that request to a Certificate Authority and creating a new “virtual” path to a URL.

Start your Virtual Web Server

Using the knowledge you have acquired, start your web server and access it through Remote Desk Top (mstsc)

Generate a Certificate for Submission to a Certificate Authority

Creating a server level certificate

Open IIS Manager (**inetmgr**)

Click **Continue** if requested

Click on **your machine name**:

Under the IIS grouping in the Features view, double click **Server Certificates**

In the Actions Pane, click on "**Create Certificate Request…**"

In the "Distinguished Name Properties" dialog box, carefully complete the following information

Common Name: **[yourInitials]Admin.mygrill.com**

i.e.: mine is: **mjbAdmin.mygrill.com**

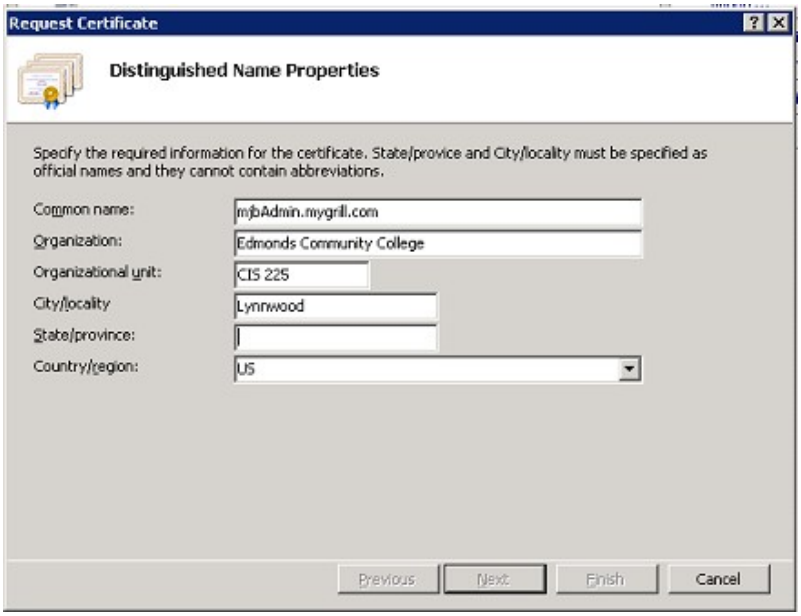
Organization: **Edmonds Community College**

Organization Unit: **CIS 225**

City: **Lynnwood**

State/province: **WA**

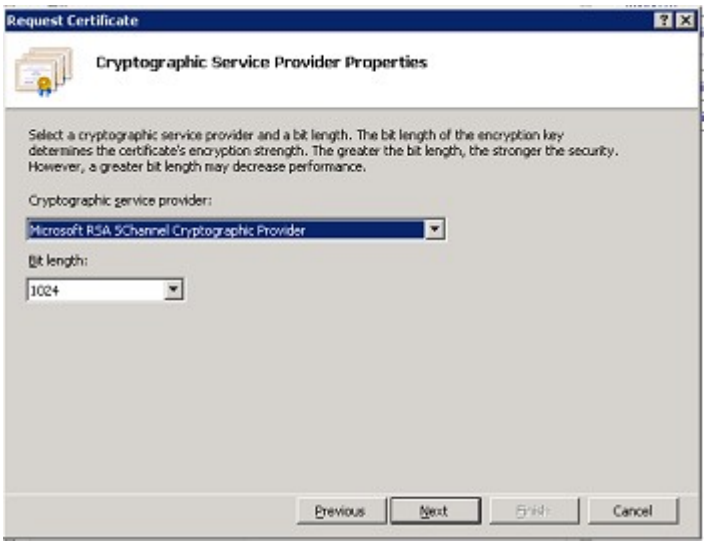
Country/region: **US**



Click **Next**

On the Cryptographic Service Provider Properties dialog box, accept the defaults

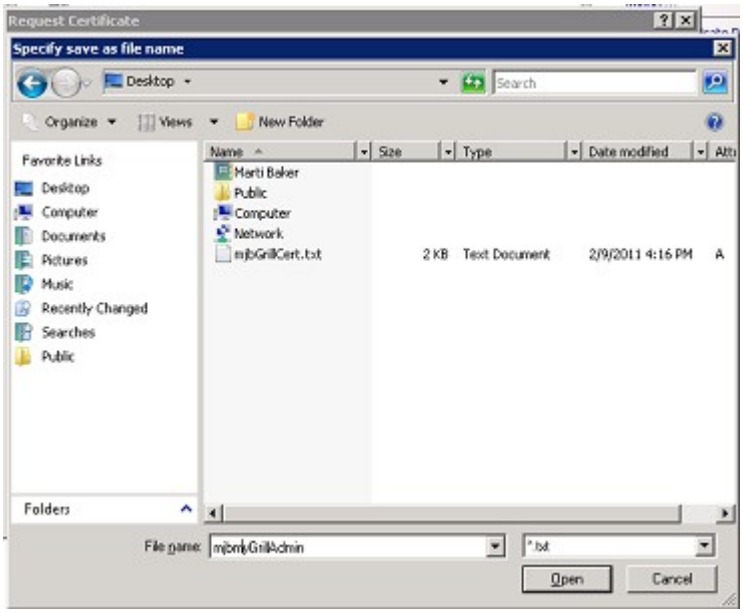
Click Next



In the text box located on the File Name dialog box

Browse to your desktop

In the file name, type: **[yourInitials]myGrillAdmin**



Click **Open**

Verify the file name to be: **C:\Users\mbaker\Desktop\[yourInitials]myGrillAdmin.txt**

Click **Finish**

A new file should be created on your desktop called [yourintials]myGrillAdmin.txt

This text file is what is sent to a Certificate Authority to create your TSL/SSL https connection

Note: At this point in the lab, you must either have an email address that you can access via a Web Browser, or a flash drive that you can bring to me at the instructor's station

Sending your Certificate Request

If you are sending this via email:

Open up Internet Explorer

Browse the web to your web-based email client

Create a new email to: mbaker@email.edcc.edu

Subject line: **Lab 11 Certificate Request**

Attach the file **[yourintials]myGrillAdmin.txt** to the email

Send the email, and let me know that you have sent the email.

If you are using a flash drive to send this:

Copy your file (**[yourintials]myGrillAdmin.txt**)to your flash drive

Bring the flash drive to the instructor's station

Note: Because the USB ports on the host machines have not been included in our configuration of our virtual servers, I must send myself an email from my host machine.

FYI: What I will be doing: (you do not need to do this, but I thought you might be interested in what the issuing Certificate Authority will be doing, this looks a lot like the a portion of lab 10).

From Microsoft Management Console

Certificate Authority Snap-In

Right Click Certificate Authority →All Tasks →Submit new Request

Select your request

Select Pending Requests

Select the certificate to issue

From the Action menu item

All Tasks

Select Issue

From Actions menu item

All Task

Export Binary Data

Select Binary Certificate

Save Binary to file → OK

Save file as [studentInitials] AdminMyGrill.tmp to my desktop

Either sending this file to you via email or to myself via so I can save it to a flash drive

Save this file to your desk top

Installing your Issued Certificate

Once you have received your issued certificate you can install the certificate

In Internet Services Manager, click on your server

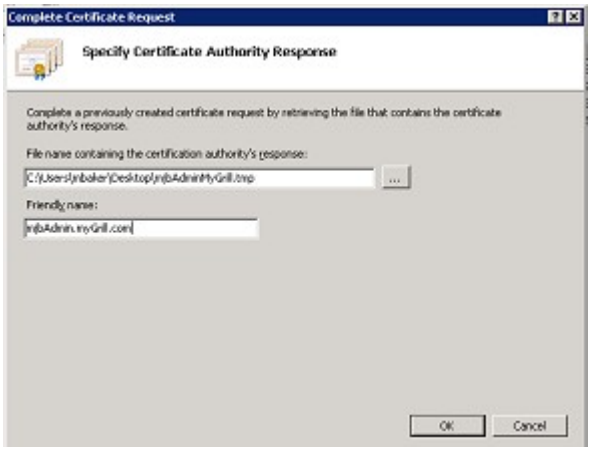
In the Features pane, under the IIS grouping, double click Server Certificates

In the Actions pane, select Complete Certificate Request

In the Specify Certificate Authority Response dialog box

Navigate to the location where you have saved file

For a friendly name: **[yourinititals]admin.mygrill.com**



Click OK

Creating [yourinititals]admin.mygrill.com

Start Internet Information Services Manager (inetmgr)

Click Continue

Expand your server by clicking +

Expand your sites by clicking +

Click on myGrill.com

In the Actions pane, click Bindings

Remove the https: binding from myGrill.com

Create a new website,

Right click on Sites, select **Add Web Site**

Enter the following information in the **Add Web Site dialog box**

Site Name: **[yourinititals]admin.mygrill.com**

Application Pool: **myGrillAdminAppPool**

Physical Path: **c:\inetpub\wwwroot\mygrill.com\admin**

Type: **https**

IP Address: **10.1.13.1XX** (where XX is your computer number)

Port: 443

SSL certificate: **[yourinititals]admin.mygrill.com**

Click **OK**

Right click on your new web site, select **Refresh**

Click on your new web site

In the Actions pane, under IIS, double click **Default Document**

Select **Add**

Add **index.asp**

Verifying your new installation

(Before completing these steps, you should complete the supplemental lab: Supplemental Lab: Updating your Hosts File)

Open Internet Explorer

Type in **http://[yourinititals]admin.mygrill.com** (note that the first request does not include the secure socket layer https)

You should receive either your IIS Start screen or an error message

Type in **https://[yourinititals]admin.mygrill.com**

You should receive the start page of the admin site of mygrillhouse.com

Remember to replace WINDOWS 7 HOSTS file! back

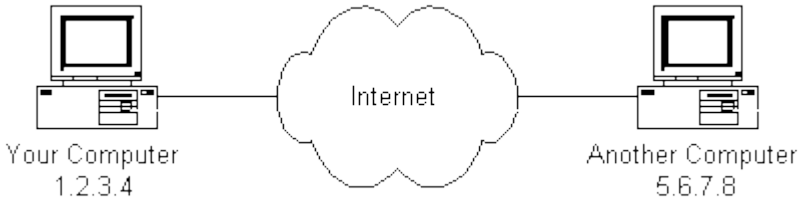
Lab 11-supplement

Student Name: _____

So how does the World Wide Web work? The normal user sees a simple process, but there is a lot going on behind the simple process. The web is configured to make browsing to web sites easy by creating domains that

we can easily remember. After all, which is simpler to remember, www.google.com or Google's IP address of 74.125.224.16? Of course, www.google.com is easier to remember. A domain name is simply and alias for an IP address.

When you type in a domain name into your browser's address bar, a domain name server (DNS) is contacted to translate the domain name to an IP address. The domain name server, simply put, looks down a list of domains finds the one that matches your request and the associated IP address. The page request is then sent to the IP address.



(Source: http://www.theshulers.com/whitepapers/internet_whitepaper/index.html)

However, there is an intermediate step not widely known. Before your computer sends the request out to a DNS, it checks a file "Hosts" to see if there is an IP listing for the domain you've asked for. If the domain is listed with an IP address, your computer will send out the request directly to the IP address and not to a DNS, bypassing the service. You can set any domain name to your own selected IP address by making changes to the Hosts file.

To read more about the Hosts file, read: http://en.wikipedia.org/wiki/Hosts_(file)

Setting up Pseudo IP Addressing

In this lab we will be making changes to the Hosts file.

On your web server, click **Start**

Right click on Notepad and select **Run as Administrator**

Click **Continue**

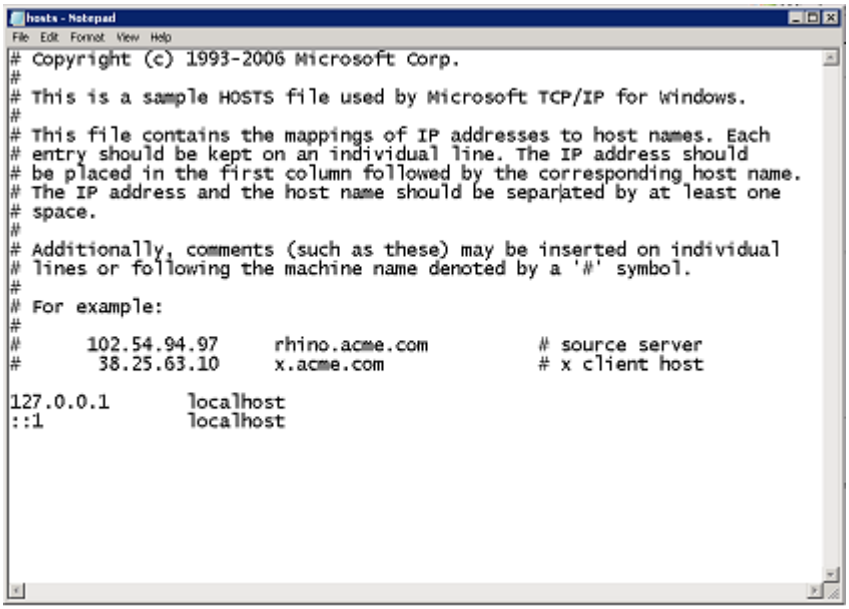
Select **File → Open**

Navigate to **c:\windows\system32\drivers\etc**

In the file type drop down box, select **All files (*.*)**

Click on **Hosts**, and select Open

Hosts file looks something like this in raw form:



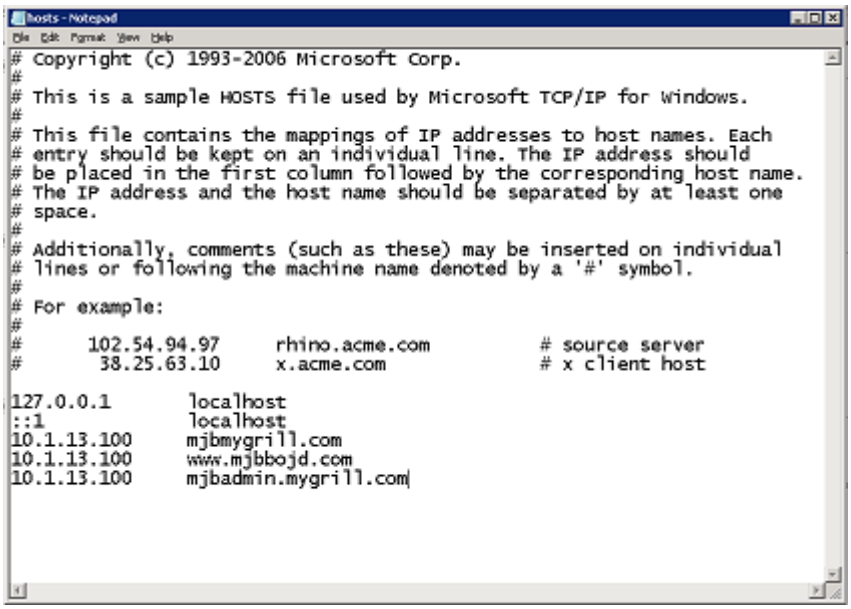
Add or verify that the following entries are in Hosts:

10.1.13.1XX [yourInitials]mygrill.com

10.1.13.1XX www. [yourInitials]bojd.com

10.1.13.1XX [yourInitials]admin.mygrill.com

(Where XX represents the IP address of your server)


hosts - Notepad
File Edit Format View Help
Copyright (c) 1993-2006 Microsoft Corp.
#
This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
This file contains the mappings of IP addresses to host names. Each
entry should be kept on an individual line. The IP address should
be placed in the first column followed by the corresponding host name.
The IP address and the host name should be separated by at least one
space.
#
Additionally, comments (such as these) may be inserted on individual
lines or following the machine name denoted by a '#' symbol.
#
For example:
#
102.54.94.97   rhino.acme.com   # source server
38.25.63.10   x.acme.com   # x client host
127.0.0.1   localhost
::1   localhost
10.1.13.100   mjbmygrill.com
10.1.13.100   www.mjbbojd.com
10.1.13.100   mjbadmin.mygrill.com

On your Windows 7 host, complete the following steps:

Click Start →All Programs → Accessories → Notepad

Navigate to **c:\windows\system32\drivers\etc**

In the file type drop down box, select **All files (*.*)**

Click on **Hosts**, and select **Open**

This step is important: IMMEDIALTEY save this file as **oldHost**

Click on File → Open →in the file type drop down box select **All Files (*.*)**

Click on **Hosts**, and select **Open**

Make the same entries into your Windows 7 Host file as you did in Step 8

At any time that you want to simulate a web connection you can do these steps

At the end of lab tonight, please replace the Hosts file that you created in Step 9, with information in **oldHost back**

Lab 11-supplement(2)

Student Name _____

Installing SQL Server Express

SQL Server 2008 R2 Express and MySQL reside very nicely together on the same computer.

Open Internet Explorer and navigate to SQL Server Express 2008 at
http://www.microsoft.com/express/Database/

Click the **64-bit** icon on the right side of the screen

Select English as your language from the drop down menu and click **Download Now**

At the top of the next Internet Explorer Window, there might be a warning box, click on the box and select "**Install this Add-on for All Users on this Computer**"

When you receive the User Access Control dialog box, select **Continue**

When you receive the Internet Explorer Add-On Installer – Security Warning, select **Install**

When you receive the Internet Explorer Security warning, select Allow

Save **SQLEXPRWT_x64_ENU.exe** to your desktop

After the download is complete, **Launch** the application installation

When the SQL Server Installation Center appears, click on **New Install or add features to an existing installation**

Accept the EULA by checking the "**I accept the license terms**" checkbox , click **Next**

Installation will start, be patient, this is an extensive installation and will take some time.

For Feature Selection, be sure that all features are selected; accept the default installation locations, click **Next**

Accept the default Installation Configuration (SQLExpress) by clicking **Next**

Accept the default Server Configuration by clicking Next

On the Database Engine Configuration window

Click the **Mixed Mode** radio button

Add the Server Administrator password of **Pa55word**, confirm the same password

Verify that your user name appears in the administration list

If not, click Add **Current User**

Click **Next**

Click **Next**

Patience!!!

Once your installation is complete, you can close the SQL Server 2008 R2 Setup.

Delete **SQLEXPRWT_x64_ENU.exe** from your desktop back

Lab 12

Student Name: _____

While your text book addresses the types of backup available to physical machines, there are other choices which are optimum for virtual servers, taking a snapshot or creating a copy.

Creating a VMWare Snapshot

Using remote desktop, login to your Windows 2008 R2 Server

Navigate to c:\inetpub\wwwroot\mygrill.com

To protect yourself during this lab we will be doing one more step

Right click on mygrill.com and select copy

Click on Documents

Right click in the right pane of Explorer and select paste; this process should take about 2 minutes

Log out of your Windows 2008 R2 Server

From your Windows 7 host machine

Double click your VMWare desktop icon

Click on your 225 Server 2008 R2 server

If needed start your server

In the Commands portion of the VMWare Web Access console

Click on “Take Snapshot”

If requested to replace an existing snapshot, click yes

The Snapshot process should take approximately 5 minutes

Making a drastic change to your server structure (ooops)

Using remote desktop, login to your Windows 2008 R2 virtual server

Right click on Start and select Explore

Navigate to c:\inetpub\wwwroot\mygrill.com

Right click on mygrill.com and select Delete

Click Yes

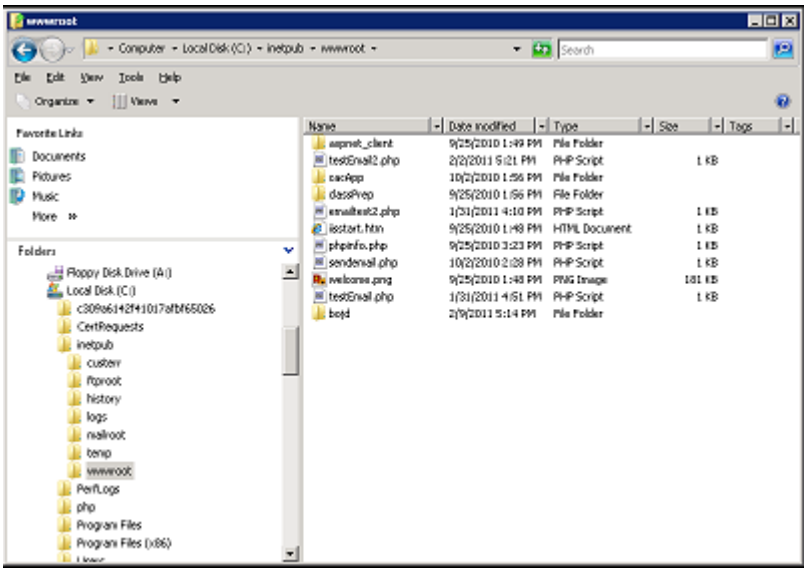
When asked to confirm this, select Continue

When asked to confirm this, select Continue

Ooops! – your really didn’t want to delete this web site!

To assure that you have completed this step, please paste a screen capture of your virtual server directory structure showing wwwroot and all sub folders here:

Example: (be sure to resize this in a manner that will allow the full screen to fit and be readable)



Log off of your Windows 2008 R2 virtual server

Restoring your Snapshot

Return to your Windows 7 host machine and the VMWare Web Access console

In the Commands area, click on Revert to Snapshot

When requested to confirm reverting to the Snapshot, Select Yes

This process should take less than one minute

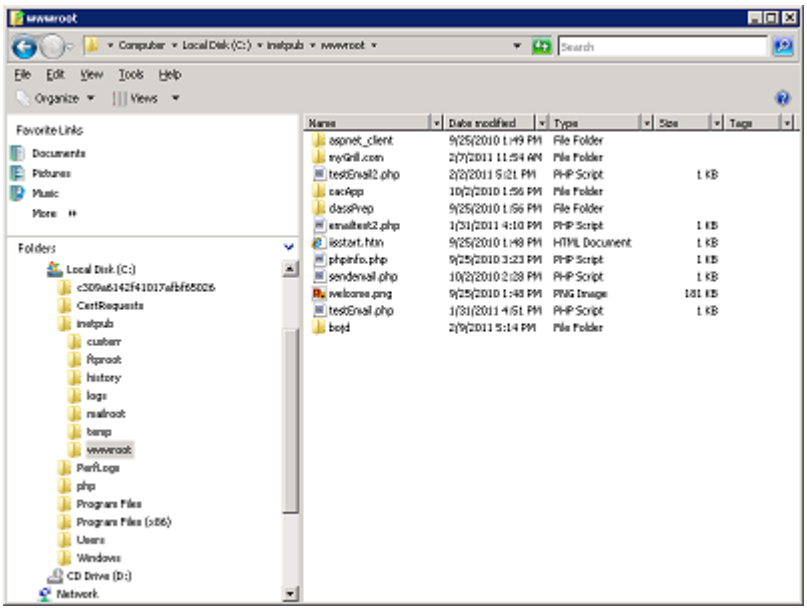
Verify the restoration of your file structure

Using remote desktop, login to your Windows 2008 R2 virtual server

Navigate to c:\inetpub\wwwroot and verify that mygrill.com has been returned to your directory structure.

Create a screen capture showing that myGrill.com has been returned to your file structure

Example: (be sure to resize this in a manner that will allow the full screen to fit and be readable)



Now that was painless!

Using Copy to Backup Your Virtual Server

While taking snapshots are a great interim backup method, there are hardware and software failures that could make snapshots unavailable for recovery. You should systematically create actual copies of your virtual servers on secondary storage devices.

In this lab, we are going to simulate creating a copy of your virtual server to a secondary storage device.

If needed, log off your Windows 2008 R2 virtual server

Return to your Windows 7 Host machine and the and the VMWare Web Access console

These steps are very important. PLEASE be careful as you do them.

In the Commands area of your VMWare Web Access console, click Configure VM

On the General tab: identify and write down the Working Directory name of your virtual server
Example: [standard] 225 Server 2008 R2
Your virtual server: _____

Click OK

Open Windows Explorer

Navigate to c:\Virtual Machines

Locate the folder named the same as the Working Directory specified above

Right click on the Working Directory and select Copy

Click on your Documents folder in Windows Explorer

Right click in the Document Library pane and select Paste

This process should take approximately one hour.

You have now created a backup "copy" of your virtual server.

At any time you could simply copy your virtual server back to its original location and be ready to fly!

back

Lab 12-supplement

Student name: _____

Installing Anti-Virus Software

Login to VMWare

Start your virtual server

Now that we've done so much work on our virtual server, we need to protect the work that we've completed to this point. VMWare allows us to create a "roll-back" point, called a "snapshot" (unfortunately, VMWare only allows you to take and keep one snapshot at a time. "Snapshots allow you to preserve the state of the virtual machine so you can return to the same state repeatedly. For example, you might use snapshots to test software. You can take a snapshot before installing different versions of an application to ensure that each test installation begins from the identical baseline." (VMWare Help)

On the summary tab, in the Commands area, click on "Take Snapshot"

Once the snapshot is complete, close VMWare, but do not "log off"

Login to your virtual server using a remote desk top connection

From your Windows 2007 host system

Click Start

In the search box type MSTSC

Enter your server IP address

Login into your virtual server

When prompted select “Activate Later”

Because we are in a lab situation, and are restricted by a cost, we will be working with freeware during this lab. If you were in a real business situation, you would want to research and choose the best commercial package that a budget can afford.

Open Internet Explorer and navigate to comodo.com (http://www.comodo.com/)

Click on the **Free Products** box about half way down the page on the left.

Scroll down the page and click on Comodo Anti-Virus (about ½ down the page)

Click on **Free Download**

In the drop down list, select Universal Windows Web Installer

Click **Download**

Click **Run** to execute the file cav_installer.exe

Click **Run** to execute COMODO Internet Security

Click **Run** to execute the installation

Click **Continue** to give permission

Select **English** as the language

Click **OK**

Accept the EULA by clicking **I accept**

Click **Next**

Uncheck the Install COMODO GeekBuddy option

Click **Next**

Accept the default Destination Folder location by clicking Next

Select the radio button “**I do not want to use COMODO SecureDNS server**”

Click **Next**

Click **Install –** installation should take about 3 minutes

Click **Finish**

Click **Finish** a second time

Click Yes to restart to complete the installation on your system

Give your system approximately 2 minutes to restart completely. Repeat **step 5** to log into your virtual server.

Like all software, updates to anti-virus software are important to maintain.

Double click the COMODO anti-virus software icon on your desktop

Select **Update Now**

This update should take approximately 2 minutes

Once the update of the virus database has completed, select **Do it now** to do an initial scan of your server.

While your scan is running, minimize the scan window.

This scan should take approximately 25 minutes

In the COMODO Antivirus main window, select **Defense**

Click Trusted Files (add MySQL to the list)

Click the **Add** button

Select **Browse Running Processes**

Scroll through the list of running processes and **click** on **mysqld.exe**

Click **Select**

Click **Close** **back**

Lab 13

Student name: _____

In this lab, you will be installing PHP (**PHP: Hypertext Preprocessor)** and **MySQL** on your server**.** These technologies are widely used to create web sites and web applications. Both are open-source technology and work very well on a Windows-based server.

PHP is a widely-used server-side scripting language. When IIS receives a request (request object) for a PHP scripted page, the server sends the file to a PHP processor which translates (interprets) the script into HTML. If

needed during the translation, PHP will connect to a database (in this case, we are going to use MySQL) pulls the records (a record set) needed to complete the request. Once the interpreter has completed the translation, the HTML is returned from the processor, and IIS returns (response object) the HTML to the browser.

This process must be completed before completing the Application Pool Lab.

Preperation:

Log into your virtual server.

Installing MySQL

It is recommended that you install MySQL on a dedicated server rather than installing MySQL on the same server that is running IIS 7. However, for our lab we will be The separation of database server and Web server makes overall installation more secure and manageable and avoids resource contentions between the database and Web server processes.

Open Internet Explorer on your virtual server.

Navigate to: http://dev.mysql.com/downloads/mysql

If needed, add the web sites to your list of trusted sites. Continue to add any needed web sites.

Download **MySQL Community Server**.

Downloading **Windows (x86, 64-bit), MSI Installer**. (Current version as 1/24/11 is 5.58 and the size is 122.7M)

This is the second item in the list of packages at: http://dev.mysql.com/downloads/mysql/

Select the correct 64-bit package

Click Download

Select the “No thanks, just take me to downloads link” to continue to the next page.

Select an appropriate HTTP location, select something close to you. (FTP locations do not seem to work.)

When requested to either Run or Save the file, Select Save.

Place this file in a location that you can access immediately after the save has been completed.

Once the download has completed either click “Run” or Navigate to the location where you saved the Windows Installer.

If Requested, because of an unknown publisher, click Run.

The **Windows Installer** will start, or extract all the files from the archive, and then start **Setup.exe**.

On the Welcome to MySQL 5.X screen, click **Next**

Accept the license agreement by clicking on the checkbox and select **Next**

Select a **Typical** setup by clicking on the button.

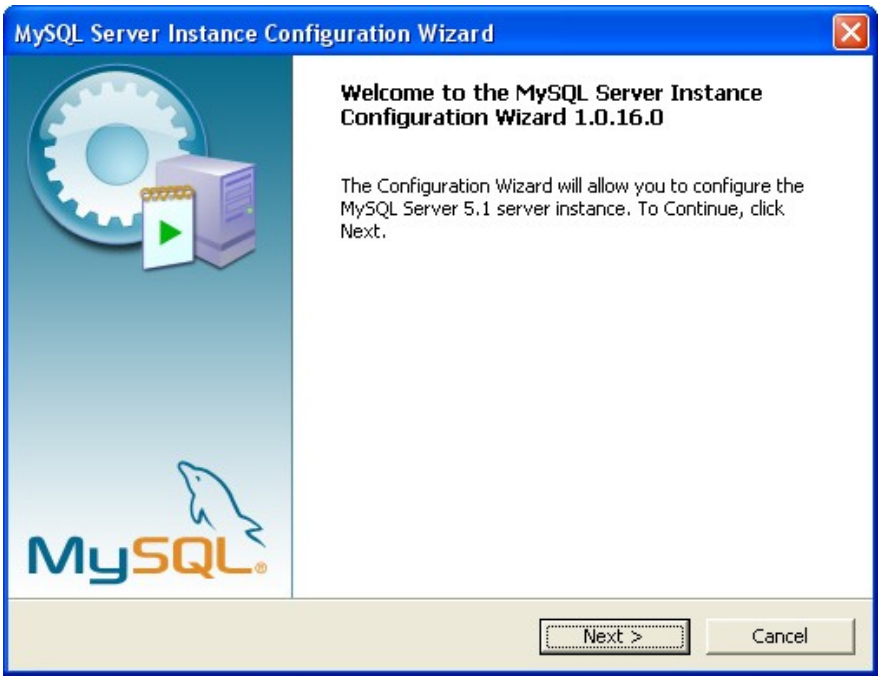
Click **Install**

If a popup window for MySQL comes up before seeing the last installation screen, you may need to click **Next** twice

leave the **Configure the MySQL Server now** check box selected and click **Finish**

Configure a MySQL Instance

If you left the checkbox selected, the **MySQL Server Instance Configuration Wizard** should start automatically after the installation wizard has completed. If not, go to Start → All Programs → MySQL → MySQL Server 5.X → **MySQL Server Configuration Wizard** (you version may be different then the version pictured).



On the Welcome to MySQL Server Instance Configuration Wizard will start, Click **Next**

Best practice recommendations are as follows:

Select **Detailed Configuration**, and then click **Next**.

Select **Developer Machine**, and click **Next**

Select a server **Multifunctional Database** as your server type, click **Next**

Accept the default installation path, and click **Next**

Select the Online Transaction Processing option, and click **Next**, you can accept 15 concurrent connections for now.

Accept the **Enable TCP/IP port of 3306**, BUT **uncheck** "Enable Strict Mode"

Accept the **Standard Character Set**, and click **Next**

Verify that **Install as a Windows Service** is selected, and **click** the **Include Bin Directory in Windows Path**, and click **Next**

PLEASE PAY CLOSE ATTENTION TO THESE NEXT STEPS!

In the security options, type in the password of "**root**", confirm the password "**root**"

You should not include the quotation marks in the password

Click **Next**

Select **Execute**

When installation is complete, click **Finish**

Get PHP

Open your web browser and go to **http://windows.php.net/download**, if needed accept all web sites

Follow the link to the VC9 x86 Thread Safe (2011-Jan-05 21:31:94) installer package

Select Save and place the msi file in a location that you can easily navigate to.

Once the download is complete, select **Run**

Once downloaded, extract all the zipped files to C:\PHP.

Installing PHP

At the Welcome to PHP 5.X.X Wizard window, select **Next**

Accept the License agreement, click on **Next**

Change the path of the installation to **c:\php**, select **Next**

Select **IIS FastCGI** as the type of server you want to set up, click Next

On the Items to install, you will be clicking through a series of drop down boxes and installing everything on the local hard drive.

Script Executables – local hard drive

Register *.php files – local hard drive

Extensions – accept the default installations

Extras

PHP Manual – local hard drive

Once the choices in step 5 above have been selected, click **Next**

Click Install

Click Finish

Test your PHP installation

Open up Notepad

Create a file called phpinfo.php in the root of your application with the following text

----------COPY EVERYTHING BELOW THIS LINE----------

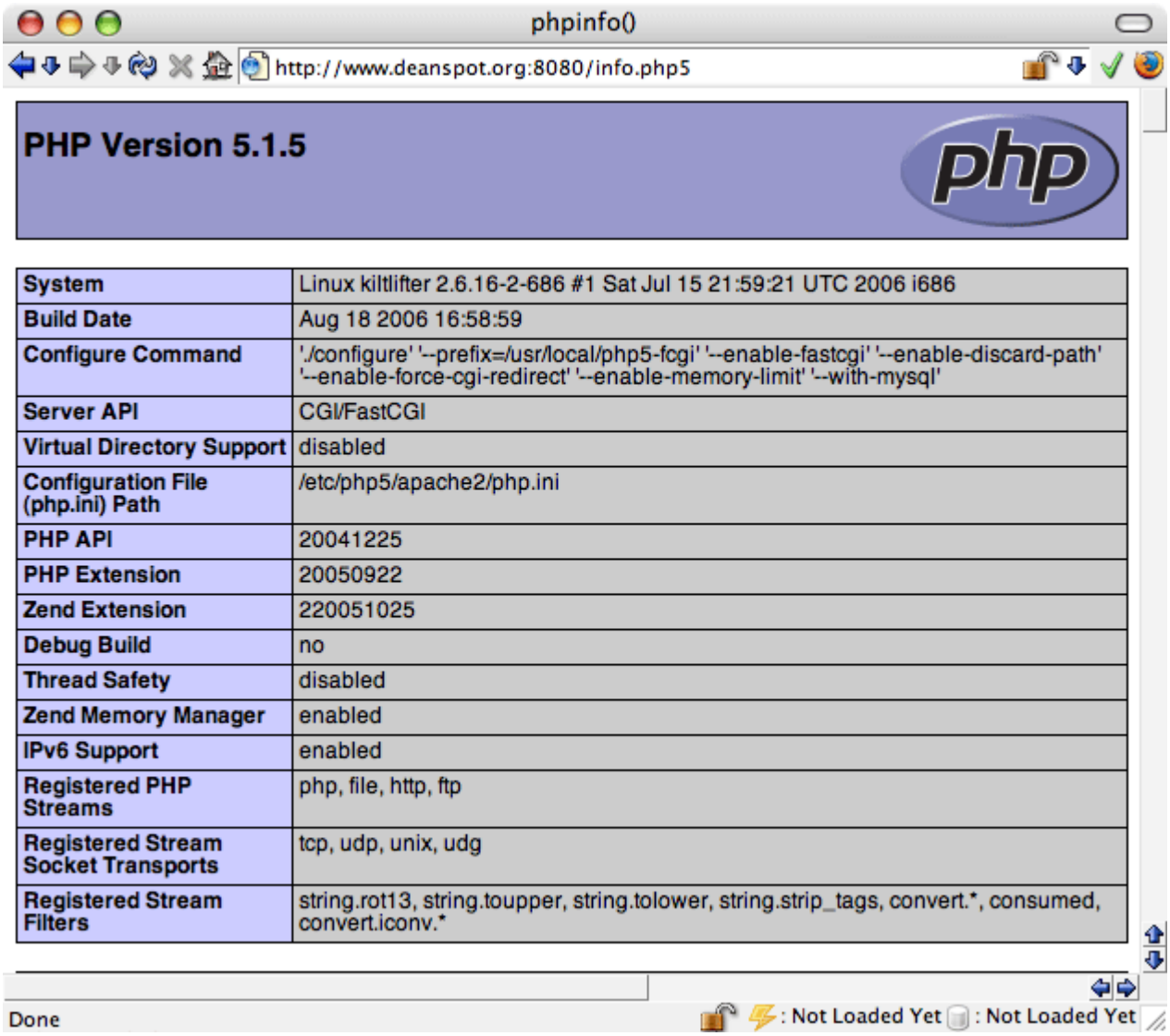
```
<?php
phpinfo();
?>
```

----------COPY EVERYTHING ABOVE THIS LINE----------

Save this file as phpinfo.php in c:\inetpub\wwwroot.

In internet Explorer go to the URL http://localhost/phpinfo.php

If everything turns out, you should get your standard phpinfo output.



System	Linux kiltlifter 2.6.16-2-686 #1 Sat Jul 15 21:59:21 UTC 2006 i686
Build Date	Aug 18 2006 16:58:59
Configure Command	'./configure' '--prefix=/usr/local/php5-fcgi' '--enable-fastcgi' '--enable-discard-path' '--enable-force-cgi-redirect' '--enable-memory-limit' '--with-mysql'
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2/php.ini
PHP API	20041225
PHP Extension	20050922
Zend Extension	220051025
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	php, file, http, ftp
Registered Stream Socket Transports	tcp, udp, unix, udg
Registered Stream Filters	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv.*

back

Lab 14

Student Name _____

In this lab you will be planning strategic processes for your web server. While this lab will not be turned in until your final project is due, it will give you some guidelines to help you create an essential portion of your final project.

To date, you have (or should have):

Installed IIS 7.0 on Windows 2008 R2

Installed Windows updates as needed (should be done weekly)

Created a default web site (empty)

Created a web site for bojd

Created a web site for myGrill.com

Created a secure web site for XXXadmin.myGrill.com

Created and applied application pools for each of these web sites

Created a FTP server

Installed and applied SMTP services

Verified baseline security using Microsoft's Baseline Security Analyzer

Created and worked with ODBC setup

Created different levels of site authentication and authorization

Created and installed certificates enabling TSL / SSL (https: / port 443)

Installed PHP capabilities on IIS

Created backups through both snapshots and copies

Your documentation should include processes to:

Add a new web site

Add a new application pool

Add an ODBC connection if needed

(Create and install) AND (request and install) TSL / SSL certificates

Maintaining records on existing web sites (a portion of this lab)

See attached example (you may want to include more)

Receive and implement change requests to an existing web site (a portion of this lab)

Client Assurance Agreement (a portion of this lab)

Back-up your virtual server (Lab 12)

Snapshot – include how often you will be creating snapshots

Copies – include how often you will be making copies

Maintaining Records of Existing Web Sites

Web site documentation has been completed for the BOJD site (see attached), which you can use as a portion of your web server documentation.

You need to complete the documentation for mygrill.com

Change Request Form

Using the example provided in chapter 18 of your text book, create a Request for Change form to be used to communicate changes that need to be made to a web site

Client Assurance Agreement

Do a web search for examples of web site client assurance agreements.

Read or scan a couple of these agreements. For the purpose of this class, you may copy one that you find on the Web. (Be sure to cite the location where you found the agreement you are using.

Back-up Plan

Create a back-up plan for your server back

Lab 14-supplement

Student Name _____

Multipurpose Internet Mail Extensions (MIME) types identify the types of content that can be served to a browser or a mail client from a Web server. When a browser requests content from a Web server, the browser also requests the MIME type of that content. IIS returns this MIME type as the **Content_Type** field in an HTTP header before returning the content, so that the browser knows how to process or display that content.

IIS uses a default list of global MIME types to determine which types of content to serve. If a client requests a MIME type that is not defined on the Web server, IIS returns a 404.3 error.

You should enable only those MIME types that are required for the types of content stored on your Web server. This best practice helps reduce the server's attack surface. A good list of MIME Types can be found at: WebMaster ToolKit :: Listing of MIME Types http://www.webmaster-toolkit.com/mime-types.shtml

FYI: MIME types can be configured at each of the following levels.

Web server

Site

Application

Physical and virtual directories

File (URL)

In this lab, a Web Developer has given you a set of additional MIME types that need to be enabled on their site.

Process to add a MIME type:

Open IIS Manager and navigate the myGrill.com public site.

In Features View, double-click MIME Types.

In the Actions pane, click Add.

In the Add MIME Type dialog box, type each of the file name extension in the File name extension text box. For example, type .xyz

Type a MIME type in the MIME type text box. For example, type application/octet-stream.

Click OK.

For each of the MIME types listed below, complete the Process to add a MIME type above. (These should be added to the myGrill.com public site)

File Name Extension	MIME Type	Short Description
.aif	audio/aiff	Audio Interchange File
.avi	video/avi	Audio Video Interleave File
.bmp	image/bmp	Windows OS/2 Bitmap Graphics
.gz	application/x-compressed	Compressed Archive
.mid	audio/midi	Musical Instrument Digital Interface
.mp3	video/mpeg	MPEG Audio Stream, Layer III

back

Lab 15

Student Name _____

One of the distinguishing differences between a good Web Server Administrator and an average Web Server Administrator is the monitoring and tuning capabilities and services that they provide to their developers. By

analyzing log files administrators can determine many problems on a web server. These include but are not restricted to:

Broken links

Visitation patterns

Attacks against servers and sites

Process failure rates

Application errors

In this lab we are going to simulate a number of requests and responses made by your server. You will then analyze the requests made and send recommendations to your developer.

Step 1. The first step in looking at log files is to download and work with a web request simulator. We will be using a 30 day trial version of TestMaster.

Login to your virtual web server using remote desktop (mstsc)

Open Internet Explorer and navigate to http://www.siteloadtesting.com/

Read through the information provided for you on the page

Scroll down the page and locate link Download the 30-day trial version, follow the link,

On the download page, click Download

When asked on the File Download – Security Warning dialog box, select Run

When asked on the Internet Explorer – Security Warning dialog box, select Run

When asked on the User Account Control, select Allow

From the TestMaster 1.7.X Setup

Welcome screen, select Next

On the EULA, click I Agree

Accept the default installation location by clicking Next

Accept the default Icon and QuickLaunch toolbar settings, click Install

Installation should take approximately 30 seconds

On the Completing TestMaster 1.7.X screen, verify that the Run TestMaster 1.7.X is checked

Click Finish

If referred to the Web page for TestMaster, click X to close Internet Explorer

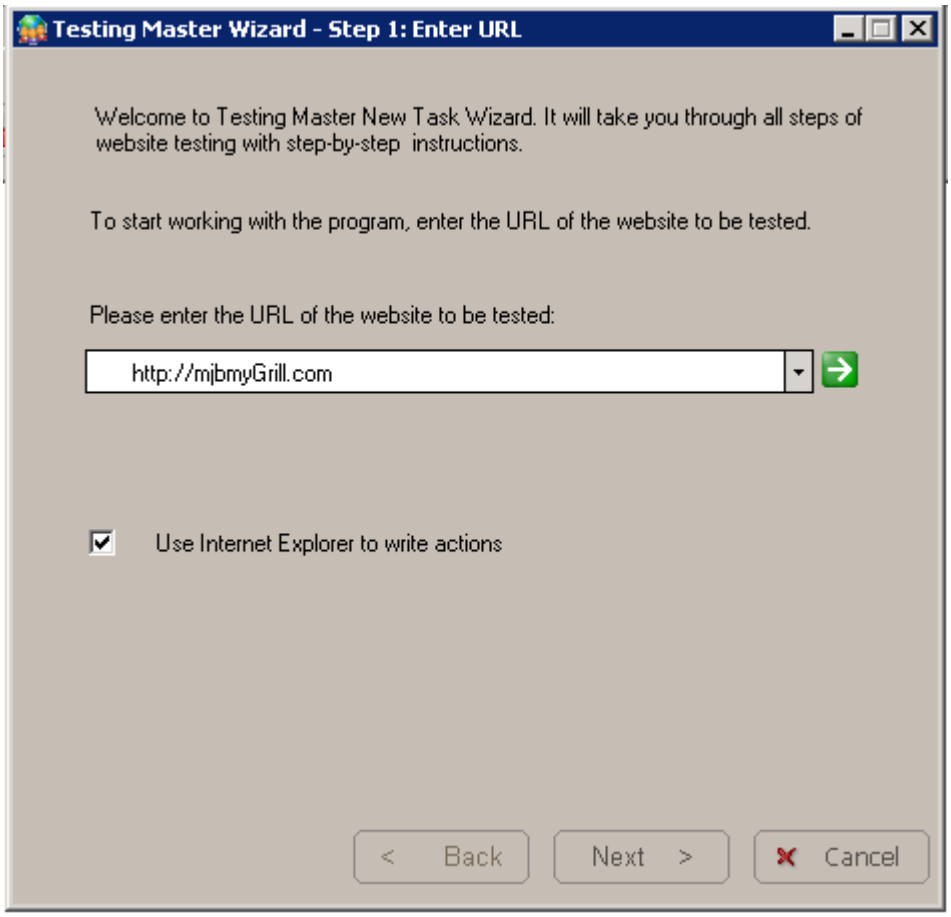
Click the TestMaster Icon on your taskbar

Click OK

If you receive a strange dialog box, with strange characters, click OK

If you receive a “More stable verison…” click Close

On the Testing Master Wizard, enter your URL http://XXXmygrill.com (Where XXX represents your initials),check the Internet Explorer check box, click Next



Internet Explorer should open to your web site

Click around the grill web site, visiting as many links (including menu links) on the grill web site.

Add your name to the VIP list

Return to TestMaster, click Next

Testing Paramters:

Number of visitors, scroll and select 5

Number of repetitions for each visitor, select 10

Click Next

On the Step 4 – Run test screen, click Start Test

TestMaster will now simulate 15 visitors to your site, using 10 different actions each.

This process should take approximately 5 minutes

Step 2. Downloading and installing a web log analyzer

Web log analyzers will give you information about the activity of your web server. Some of the statistics that you can analyze are:

General statistics

Activity statistics: daily, by hours of the day, by days of the week, by weeks and by months

Access statistics: statistics for pages, files, images, directories, queries, view time, entry pages, exit pages, bounces, paths through the site, file types and virtual domains

Information about visitors: hosts, top-level domains, countries, states, cities, organizations, authenticated users, screen resolutions and color depth

Referrers: referring sites, URLs, search engines (including information about search phrases and keywords)

Browsers, operating systems and spiders statistics

Information about errors: error types, detailed error information

Goals statistics

Tracked files statistics

Click overlay report

Support for custom reports

On your virtual web server, open Internet Explorer and navigate to Web Log Expert at http://www.weblogexpert.com/

Click on the Download link in the navigation menu

Select the link to download WebLog Expert Std/Pro/Ent 7.1

When you receive the File Download – Security Warning dialog box, click Run

This download should take approximately 4 minutes

When you receive the Internet Explorer – Security Warning dialog box, click Run

On the Welcome screen, click Next

Click on the I accept radio button on the EULA, and click Next

Accept the default installation location, click Next

Accept the default installation menu option, click Next

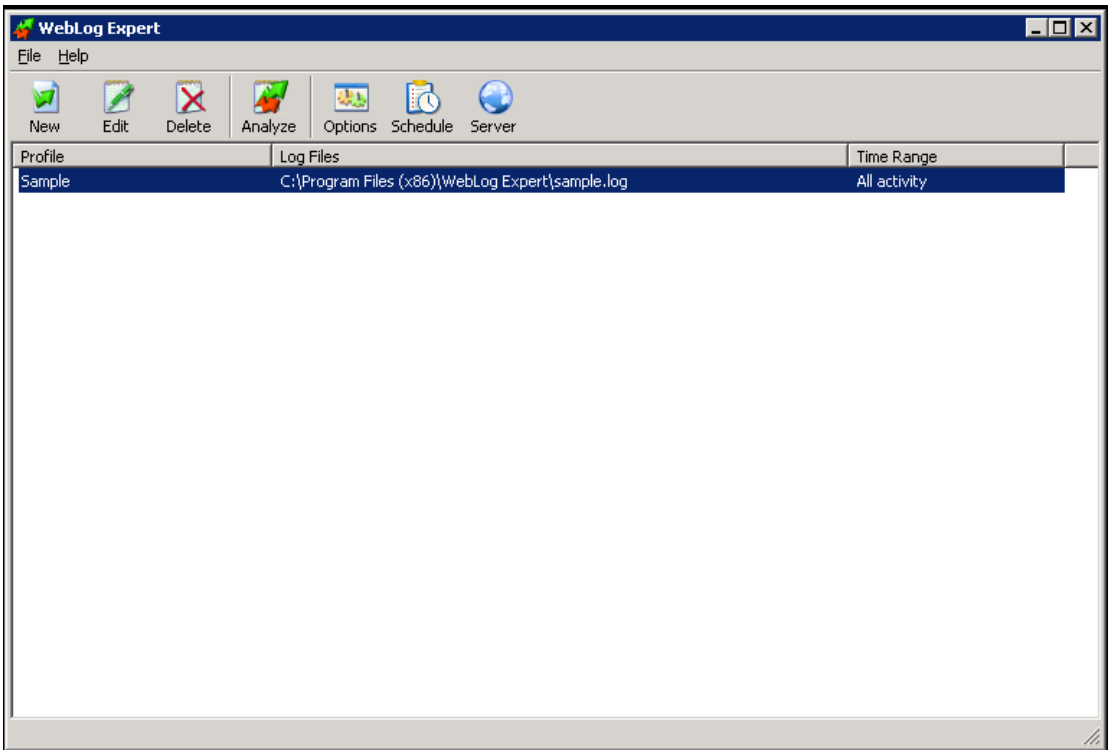
On the installation summary screen, click Install

Installation should take approximately 30 seconds

Leave the Launch WebLog Expert checkbox checked, click Finish

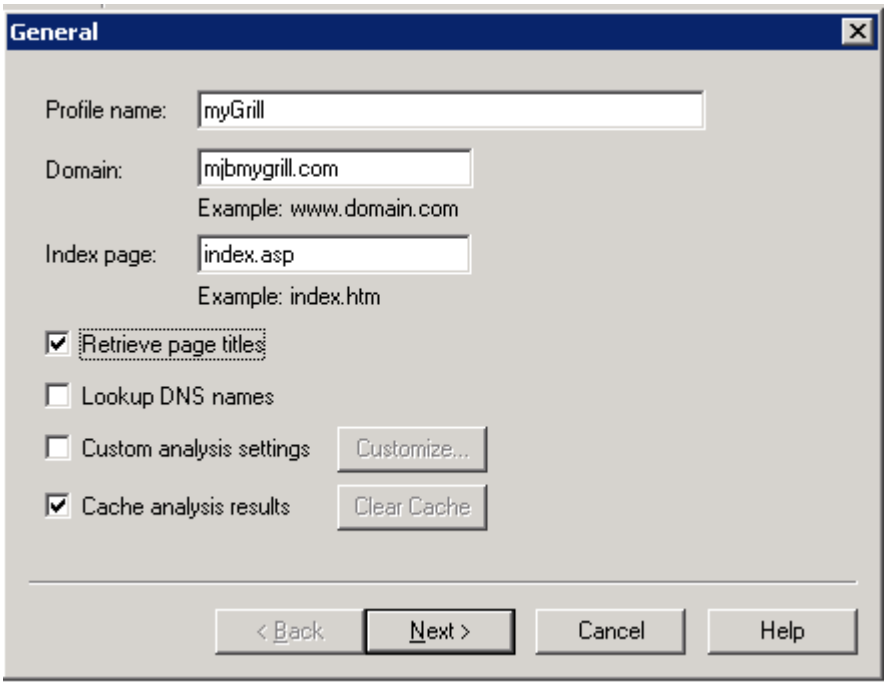
When WebLog Expert starts, select Enterprise and Click Run

WebLog Expert UI will open



Click New

In the General dialog box enter the following values:



Profile Name: myGrill

Domain: XXXmyGrill.com (where XXX represents your initials)

Index.asp

Verify check boxes:

Retrieve page titles is checked

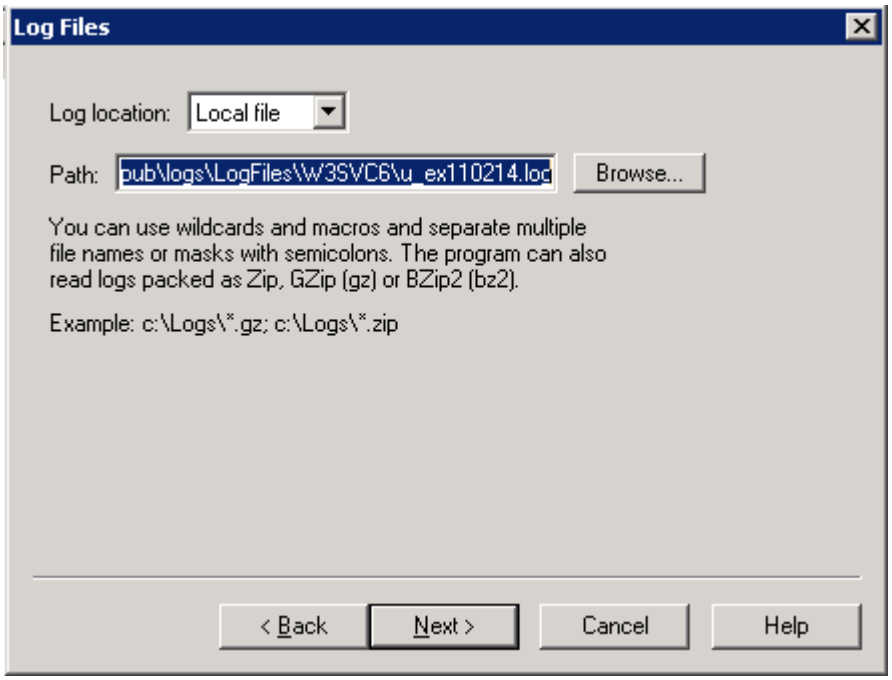
Lookup DNS names is unchecked

Custom analysis settings is unchecked

Cache analysis results is checked

Click Next

In the Log Files dialog box enter the following values:



Navigate to: C:\inetpub\logs\LogFiles\W3SVCX\x_xxxxxxxx.log

Where the X in W3SVCX is the largest number available

Where x in the .log file is the newest date and time available

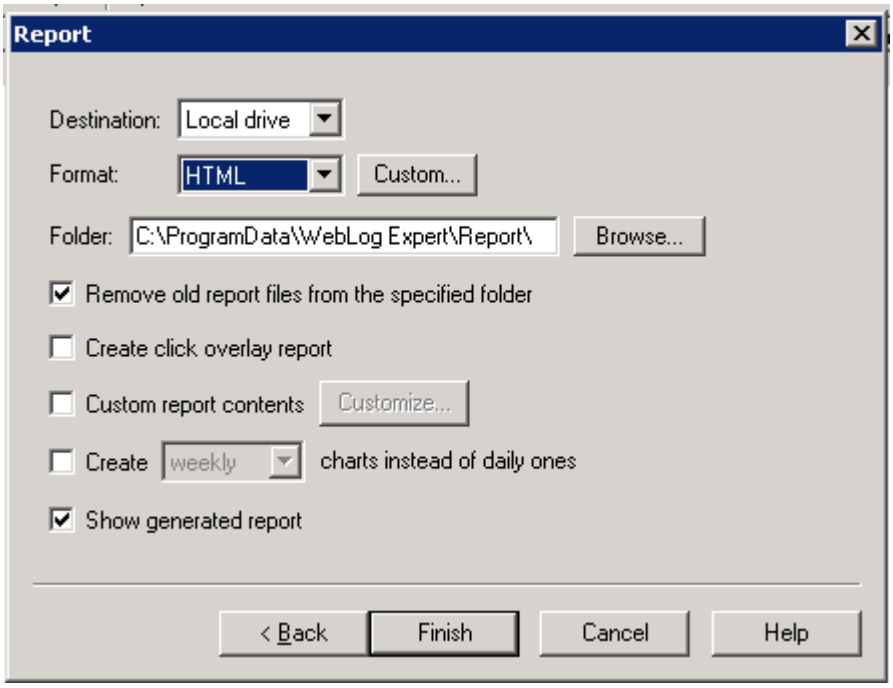
Click Next

In the Time Range dialog box, accept all the defaults, and click Next

In the Tracking dialog box, click Next

In the Filters dialog box, click Next

In the Format dialog box, verify the following values



:

Destination: Local drive

Format: HTML

Folder: C:ProgramData\WebLog Expert\Report\

Remove old report files from the specified folder is checked

Show generated report is checked

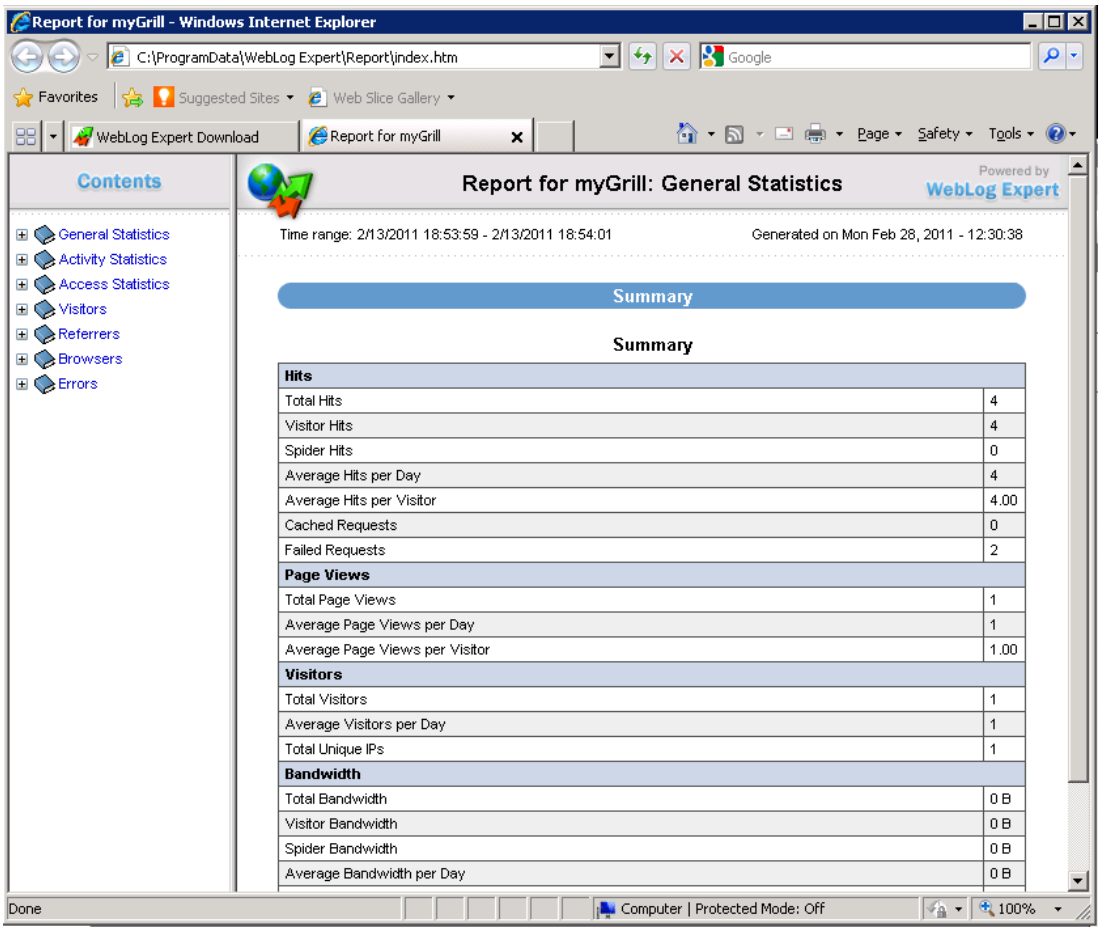
Click Finish

Your report is now available for running

Double click “myGrill” in the list

This report should take approximately 30 seconds to be displayed

If you receive a warning on Internet Explorer about blocked content, click “Allow blocked Content”



Look at the Errors area of your web site.

Note any errors that are listed

Repeat the creation of a new report for your XXXadmin.mygrill.com site (Steps 4 through 6 of this Lab) with the following exception:

Log files: Browse through the .log files that you find at c:\inetpub\logFiles and find the .log file that is the largest

you may need to go through a number of folders called W3SVCX (where X repents a number)

Note any errors that are listed for the site

Close Web Log Expert

back

Baseline Analyzer Report

back