Software Procedure

SWP-0056 AFHCAN tConsult Server 2008 Build and Configuration

Revision: 1

Effective Date: 6/7/2011

Alaska Native Tribal Health Consortium
Division of Health Information & Technology
4000 Ambassador Drive
Anchorage, AK 99508
Tel: (907) 729-2260
Fax: (907) 729-2269

Contents

Contents **1**
Purpose **2**
Audience **2**
Scope **2**
Additional Resources ..... Error! Bookmark not defined.
Acronyms and Abbreviations ..... Error! Bookmark not defined.
Material Requirements **3**
Initialize Server **3**
Initial Logon **4**
User Access Control **6**
IIS Installation **6**
Move IIS **6**
.Net Framework Installation **7**
Finalizing the OS Configurations **7**
Installing Windows Applications **7**
Configure SNMP **9**
Install Dell OpenManage Server Administrator **9**
Install Dell OpenManage IT Assistant **9**
Connect to Windows Update **10**
Harden Server **10**
Note: Appendix A contains a complete listing of the changes made here 12
Cleanup Server **15**
Review / Make Final Configuration Changes **16**
Appendix A **16**

Purpose

The purpose of this procedure is to provide detailed guidance for loading the Windows 2008 SP2 operating system, SQL 2005, IIS, and the subsequent security configuration for use as a tConsult healthcare server.

Audience

This document is written for IT technicians and system administrators who are responsible for building, configuring or maintaining a tConsult Server. It is assumed readers are familiar with intermediate-level computer terms and concepts, as well as a basic working knowledge of the Windows 2008 Server operating system.

Scope

AFHCAN developed a set standard for building a secure, robust Telehealth server that complies with the HIPAA Privacy Rule. A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. To achieve this goal AFHCAN has implemented the latest best practices in security into the server builds.

This document then, provides detailed steps on building and configuration of an AFHCAN tConsult Server used in a production environment.

Material Requirements

1. Server
    a. Server CPU w/NIC(s)
    b. Manufacturer CDROMS/DVDs – drivers disk
    c. Monitor
    d. Keyboard
    e. Mouse
2. Software
    a. Windows 2008 CD-ROM/DVD w/license key (plus CALs)
    b. SQL Server 2008 CD-ROM/DVD w/license key (plus CALs if not processor license)
    c. ATS Downloads DVD dated 6/30/2011 or later (can be obtained from AFHCAN)
    d. Perc Firmware Update (if applicable)
3. Documentation
    a. Server Configuration QA Sheets – Appendix A of this document
4. Miscellaneous – all may not be needed
    a. LAN Connection for Server
    b. WAN Connectivity to Core
    c. CAT5 cables – regular, cross-over

Initialize Server

It is assumed that the server is installed with a monitor, keyboard and mouse (or KVM equivalent).

IMPORTANT: DO NOT CONNECT THE LAN AT THIS POINT – the server is vulnerable to attacks until it is hardened.

1. BIOS Configuration – Boot Sequence:
    ☐ CD-ROM
    ☐ Hard Drive
    ☐ Floppy
2. RAID-5 configuration

Follow the manufacturer's documentation provided for the RAID software installation/hardware configuration. To access the Dell RAID BIOS select Ctl-M during the POST process.

☐ Create a single four-drive RAID5 container and establish the fifth drive as a hot spare.

1. Perc Firmware update – Depends on Dell PowerEdge Model which version to be updated.

   ☐ Insert bootable firmware update floppy

   ☐ Reboot system

   ☐ Follow instructions on screen to update

   ☐ Reboot system

2. Windows 2008 Server Initial Installation (x86 OR x64 versions)

   Partition hard disks: Note: The sizes below reflect 146 Gb Hard Drives. Larger Hard Drives will allow for a 40 Gb C partition and a 24 Gb E partition with the remaining disk space for the D partition.

IMPORTANT: Use NTFS file format for ALL partitions throughout this process

☐ Accept default, install now

☐ Select WS2008 Standard (x86 or x64 depending in hardware)

☐ Accept license

☐ Install clean copy

☐ Create C: partition – 40 Gbytes (40960) (minimum)

☐ Create D: partition – 75.5 Gbytes (77312) or the amount of the remaining space available after calculating the space necessary for the C and E partitions *Remember to leave 8 Mb free.

☐ Create E: Partition – 20 Gbytes (20480)

☐ Enter new password when prompted

NOTE: This will change later with stronger account names and passwords

Initial Logon

1. Initial Configuration Tasks

Set Time Zone

☐ Adjust as necessary. Use Alaska Time Zone with automatic adjustment for daylight savings unless Server is being deployed elsewhere – check deployment for Time Zone location.

Computer Name

☐ Enter appropriate name – do not join a domain at this time

☐ Change Workgroup to AFHCAN

☐ Reboot server

2. View Parameters, device manager, hard drive assignments

☐ Check "Do not show the Initial Configuration Tasks Window at logon"

☐ Server Manager window – check "Do not show me this console at logon"

☐ Place shortcut to Computer on desktop

☐ Adjust Tools / Folder Options/ View in Explorer window

Recommendation: Show hidden files and folders, Uncheck "Hide extensions for known file types", Uncheck "Hide protected operating system files", click on "Apply". Click OK, t hen Adjust Tools / Folder Options / View in Explorer window and "Apply to all folders"

☐ Create new folder "ATSDownloads" on the C:\ drive

☐ Copy x86 or x64 "ATS Downloads" folder from the appropriate AFHCAN ATS Downloads DVD to C:\ drive

☐ Check Device manager and update/install drivers as necessary – update existing Perc controller

☐ Change DVD/CDROM drive assignment to R:

☐ Change drive assignments if necessary so 2nd partition is D: and 3rd partition is E:

☐ Format D: drive – Format and change volume label to "Local Disk"

☐ Format E: drive – Format and change volume label to "Local Disk"

☐ Change screen resolution to 1024x768.

☐ Set color depth as high as possible – preferably 32 bit.

3. Create/Modify Accounts:

☐ Change name of Administrator account. Use the OSBA#*** name defined for this server.

☐ Password: Use complex password defined for this account

- ☐ User **CANNOT** change password, and password never expires.

- ☐ Create decoy Administrator account:
  - ☐ User name: "Administrator"
  - ☐ Password: "Password@2000"
  - ☐ User **CANNOT** change password, and password never expires
  - ☐ **NOT** a member of the administrator group

- ☐ Create AFHCANAdmin*** account
  - ☐ Use the name defined for this server
  - ☐ Password: password

    Do not use the complex password yet, due to the many reboots that will be coming up. This will be done at the end.
  - ☐ User **CAN** change password, and password never expires
  - ☐ Member of the administrators group

☐ Log out and log back in with the "AFHCANAdmin***" account. The "Administrator" account no longer has any privileges.

User Access Control

☐ Using Control Panel | User Accounts, Turn User Account control on or off, select Continue to turn off User Access Control

☐ Remove the checkmark from in front of Use User Account Control (UAC)…….

☐ Reboot Server

IIS Installation

☐ Administrative tools | Server Manager | Add Roles, Select Web Server (IIS)

☐ At prompt Add Required Features – Windows Process Activation Service

☐ Add Role Services – select ASP.NET, Add Required Role Services

☐ Add Role Services – select Windows Authentication under Security

Move IIS

☐ Open Command prompt and browse to C:\ATS Downloads\Move IIS

☐ Type "moveiis7root.bat e"

☐ Once verified that E:\Inetpub exists, delete C:\Inetpub

.Net Framework Installation

☐ Install .Net Framework 3.0 via Administrative Tools | Server Manager | Add Features, select .NET Framework 3.0 Features

☐ Install MSXML6, SP1 by double-clicking "C:\ATS Downloads\MSXML6.0\msxml6_x86.msi"

☐ Reboot

☐ Install .NET Framework 3.5 SP1

☐ Upon completion reboot- This also updates .Net 2.0 and .Net 3.0 to SP2.

☐ Install .NET Framework 4.0

☐ Reboot

Finalizing the OS Configurations

Administrative Tools | Server Manager | Add Features

☐ Check "SNMP Services"

☐ Within "System Properties", enable "Remote Desktop" by checking "Allow connections from computers running any version……."

☐ Create "C:\Logs" folder

☐ Reboot Server

Installing Windows Applications

1. Install Adobe Reader

   ☐ Adobe Acrobat Reader - Run "C:\ATSDownloads\Adobe\AdbeRdr1000_en_US.exe". Accept all defaults

   ☐ Delete any shortcut icons created on desktop

2. Install SQL Server 2008 Standard

   ☐ Insert CD/DVD – if it doesn't autostart, click on Setup.exe

   ☐ Allow SQL Server 2008 Setup to update the Windows Installer and Microsoft .Net Framework

☐ Reboot Server

☐ Once logged back in, SQL Server 2008 may need to be accessed via the Setup.exe command. Select Installation at the SQL Server Installation Center, and click on "New SQL Server stand-alone installation……."

☐ Click OK at the Setup Support Rules

☐ Enter Product Key

☐ Accept License Terms

☐ Click on Install for Setup Support Files

☐ Click Next at the second Setup Support Rules

☐ Feature Selection:

- ☐ Select Database Engine Services with Full-Text Search
- ☐ Select Client Tools Backwards Compatibility
- ☐ Select Client Tools Connectivity, Management Tools – Basic and Complete

☐ Accept default Instance configuration

☐ Accept Disk Space Requirements

☐ Server Configuration

- ☐ Use Network Service for SQL Server Agent and SQL Server Database Engine
- ☐ SQL Server Agent and SQL Server Database Engine set to Automatic
- ☐ SQL Full-Text Filter Daemon Launcher set to Manual
- ☐ SQL Browser set to Disabled

☐ Database Engine Configuration

- ☐ Select Windows authentication mode (Unless installing for a Back-End SQL Server)
- ☐ Add Current User as SQL Server Administrator
- ☐ Select D:\ as Data root directory
- ☐ Accept the default entries for the remainder (D:\MSSQL10.MSSQLServer\MSSQL\.....)

☐ Do not report Errors

☐ Click Next at Installation Rules

☐ At the Ready to Install screen, click Install

☐ Close all Installation dialogs when complete

3. MSSQL Server Configuration Manager

☐ SQL Server Network Configuration | Protocols for MSSQLSERVER | Enable Named Pipes

☐ SQL Server Network Configuration | Protocols for MSSQLSERVER | Disable TCP/IP

Configure SNMP

(Note – configure this only if being hosted locally by AFHCAN)

Open "SNMP Service Properties" in services

"Traps" Tab

☐ Set Community name – site unique

☐ Set trap destination – use IP address of server

"Security" Tab

☐ Uncheck "Send Authentication Trap" checkbox

☐ Set the community to be "Read Only"

☐ "Accept SNMP packets from these hosts" – add the server's IP address

Install Dell OpenManage Server Administrator

☐ Run "C:\ATSDownloads\OpenManage\srvadmin\windows\setup.exe"

☐ Perform a "Custom" install

☐ Leave all selections at their default and install

☐ Restart the server

Install Dell OpenManage IT Assistant

☐ Run "C:\ATSDownloads\ITAssistant\setup.exe"

☐ Install prerequisite for Microsoft Visual Studio

☐ Accept all default settings and install

☐ Restart the server

☐ Install the Java runtime component accepting defaults by connecting to www.java.com

☐ Using Control Panel, click on the Java icon

☐ Advanced tab: Remove the checkmark from Java Plug-in

☐ Java tab: In Runtime Parameters add:
-Djava.net.preferIPv6Addresses=true

☐ Java tab: Add –Xmx256M

☐ Ensure that DSM IT Assistant Connection Service is set to Automatic and Started

☐ Open It Assistant

☐ Add to trusted site

Connect to Windows Update

☐ Connect to Microsoft Windows Update site to obtain and apply the latest patches/hotfixes/service packs.

☐ Reboot server when complete

(May have to repeat this step a couple of times)

Harden Server

Operating System Services and Security policies

☐ Within "Administrative Tools" select and run the Security Configuration Wizard. When

prompted, select "Apply an existing security policy"

☐ Browse to "C:\ATSDownloads\Security Templates" and select "tConsultServer2008.xml"

☐ Accept all defaults and apply the template

☐ Select "Start/Run…" and enter "MMC"

☐ Add the "Security Configuration and Analysis" MMC snap-in to the MMC

☐ Right-click "Security Configuration and Analysis" and select "Open database'

☐ Name the database "Update"

☐ "Import Template" – browse to and select "C:\Downloads\Security Template,

select "Secure AFHCAN Server2", and click "Open"

☐ Again right-click "Security Configuration and Analysis" and select

"Configure computer now…" and apply the template

☐ Close the MMC and DO NOT save when prompted.

Note: Appendix A contains a complete listing of the changes made here

Administrative Tools | Services:

☐ Stop and Disable the DHCP client service

Windows Firewall: (Use Administrative Tools | Windows Firewall with Advanced Security)

With Windows Firewall with Advanced Security on Local Computer highlighted, Ensure Firewall is turned on, and the following Inbound Rules exist:

☐ Port 80 TCP

☐ Port 443 TCP

☐ Remote Desktop (TCP Port 3389)

☐ Time Server (UDP Port 123)

☐ ICMPv4 allows echo request

☐ On the **Program** page, click **All programs**, and then click **Next**.

☐ On the **Protocol and Ports** page, select **ICMPv4** or **ICMPv6** from the **Protocol type** list. If you use both IPv4 and IPv6 on your network, you must create a separate ICMP rule for each. Click **Customize**.

☐ In the **Customize ICMP Settings** dialog box, click **Specific ICMP types**, and then select Echo Request. Click **OK**.

☐ Allow all IP addresses on the Scope page.

☐ Select Allow the connection

☐ Leave the default on the Profile page

☐ On the Name page, enter ICMP and click Finish

Security logging: Returning to Windows Firewall with Advanced Security on Local Computer highlighted, Under Public Profile, select Windows Firewall Properties

☐ Change log file location to C:\Logs\firewall.log

Review NIC settings for all NICs

On all NIC(s):

☐ Deselect “Client for Microsoft Networks”

☐ Deselect “File and Print Sharing for Microsoft Networks”

☐ Verify IP, SM, DG, DNS

Select radio button in TCP/IP Properties / Advanced / WINS

☐ “Disable NetBIOS over TCP/IP”

☐ Uncheck “Enable LMHOSTS lookup”

☐ DISABLE any NICs that will not be connected to network

System32 Changes

Note: Appendix A contains a complete listing of the changes made here

☐ Run the “C:\ATSDownloads\Batch Files\Server2008ACLChange.Bat”

Change ACLs on partitions

C: Drive

Root (C:\)

☐ Remove Everyone, CREATOR OWNER, and Users groups

C:\Program files\Microsoft SQL Server

☐ Remove everyone EXCEPT Administrator & System

D: Drive

Root (D:\)

☐ Remove Everyone, CREATOR OWNER, and Users groups

E: Drive

Root (E:\)

☐ Remove Everyone, CREATOR OWNER, and Users groups

E:\Inetpub\WWWRoot

☐ Remove the Users account

☐ Remove the Creator Owner account

☐ Add the IIS_IUSRS Group and give modify permissions

Indexing Service

☐ Turn off indexing service at root of C:\

Right click on C: drive / Properties / General. Remove the check for "Allow

Indexing Service to index this disk …". When prompted – select option to

apply changes to subfolders and files.

☐ Turn off indexing at root of D:\ When prompted – select option to

apply changes to subfolders and files.

☐ Turn off indexing at root of E:\ When prompted – select option to

apply changes to subfolders and files.

Registry Changes

☐ Run the C:\Downloads\Registry\RegSecChanges.Reg.

Note: Appendix A contains a complete listing of the changes made here

Harden User Accounts Password and Information

☐ Harden the AFHCANAdmin*** password

☐ Delete both Full Name and Description entries from all users

DISABLE Netbios over TCP/IP

☐ Do this for all network cards at once by using Computer Management / System Tools /

Device Manager / View / Show Hidden Devices & Devices by Connection.

☐ Double click on "NETBT". On Driver tab, change startup to "Disabled". Do NOT restart your system at this time.

Disable Dump File Creation

☐ Disable System dump files

My Computer / Properties / Advanced System Settings / Advanced / Startup and Recovery – Set

"Write Debugging Information" at "(none)"

Create/Set Pagefile Parameters

Go to System Properties/Advanced System Settings / Advanced / Performance Settings / Advanced / Virtual Memory

☐ On C: drive, create/set pagefile initial/max at 1024 MB

☐ On D: drive, create/set pagefile initial/max at 4095 MB

Do NOT restart your system at this time.

Terminal Services

Administrative Tools / Terminal Services Configuration

RDP-TCP Properties

General Tab

☐ Encryption Level: Client Compatible

Client Settings Tab

☐ Under Redirection, disable everything except Drive and Clipboard

Sessions Tab

☐ Check "Override user settings" and End a disconnected session after "30 Minutes"

☐ Limit active sessions length to 1 day

☐ Idle sessions Limit; 30 minutes

☐ Check "Override User Settings"

☐ End session

Network Adapter Tab

☐ Set maximum connections to 2

IIS

Clicking on Server Name | Select Logging under IIS

☐ Active log format – click Browse under Directory and change log file directory to

c:\logs

☐ Click Select Fields under Format – check Cookie and Referrer checkboxes

Select Authentication under IIS

☐ Disable Anonymous Authentication

☐ Enable Windows Authentication

ISAPI and CGI Restrictions

☐ Ensure ASP.NET v2.0.50727 is allowed

☐ Ensure ASP.NET v4.0.30319 is allowed

☐ Reboot Server

Cleanup Server

☐ Check for FTP service and uninstall if present

☐ Clear the log files using Event Viewer

☐ Delete Security Configuration Wizard shortcut from desktop

☐ Empty Recycle bin

☐ Defrag

Review / Make Final Configuration Changes

☐ Review NIC settings for all NICs

BIOS Configuration

Set BIOS password (if server is not being shipped to customer)

Set AC Power Recovery to ON

Set Boot sequence

Hard Drive

CDROM

Floppy

End of procedure.

Appendix A

Service Name="AeLookupSvc" StartupMode="Disabled"
Service Name="ALG" StartupMode="Disabled"
Service Name="AppMgmt" StartupMode="Disabled"
Service Name="AudioEndpointBuilder" StartupMode="Disabled"
Service Name="Audiosrv" StartupMode="Disabled"
Service Name="BITS" StartupMode="Disabled"
Service Name="Browser" StartupMode="Disabled"
Service Name="CertPropSvc" StartupMode="Disabled"
Service Name="clr_optimization_v2.0.50727_32" StartupMode="Disabled"
Service Name="clr_optimization_v2.0.50727_64" StartupMode="Disabled"
Service Name="clr_optimization_v2.0.50727_I64" StartupMode="Disabled"
Service Name="ClusSvc" StartupMode="Disabled"
Service Name="COMSysApp" StartupMode="Disabled"
Service Name="CscService" StartupMode="Disabled"
Service Name="DHCPServer" StartupMode="Disabled"
Service Name="DNS" StartupMode="Disabled"
Service Name="Dnscache" StartupMode="Disabled"
Service Name="dot3svc" StartupMode="Disabled"
Service Name="DPS" StartupMode="Disabled"
Service Name="EapHost" StartupMode="Disabled"
Service Name="FCRegSvc" StartupMode="Automatic"
Service Name="fdPHost" StartupMode="Disabled"
Service Name="FDResPub" StartupMode="Disabled"
Service Name="hkmsvc" StartupMode="Disabled"
Service Name="IPBusEnum" StartupMode="Disabled"
Service Name="KeyIso" StartupMode="Manual"
Service Name="KtmRm" StartupMode="Disabled"

Service Name="LanmanServer" StartupMode="Disabled"
Service Name="LanmanWorkstation" StartupMode="Disabled"
Service Name="lltdsvc" StartupMode="Disabled"
Service Name="lmhosts" StartupMode="Disabled"
Service Name="LPDSVC" StartupMode="Disabled"
Service Name="MSDTC" StartupMode="Disabled"
Service Name="MSiSCSI" StartupMode="Disabled"
Service Name="msiserver" StartupMode="Manual"
Service Name="napagent" StartupMode="Disabled"
Service Name="Netlogon" StartupMode="Disabled"
Service Name="pla" StartupMode="Disabled"
Service Name="PolicyAgent" StartupMode="Disabled"
Service Name="RasAuto" StartupMode="Disabled"
Service Name="RasMan" StartupMode="Disabled"
Service Name="RemoteAccess" StartupMode="Disabled
"Service Name="RemoteRegistry" StartupMode="Automatic"
Service Name="RpcLocator" StartupMode="Disabled"
Service Name="RSoPProv" StartupMode="Disabled"
Service Name="sacsvr" StartupMode="Disabled"
Service Name="SCardSvr" StartupMode="Disabled"
Service Name="SCPolicySvc" StartupMode="Disabled"
Service Name="seclogon" StartupMode="Disabled"
Service Name="SENS" StartupMode="Disabled"
Service Name="SessionEnv" StartupMode="Disabled"
Service Name="SharedAccess" StartupMode="Disabled"
Service Name="SNMPTRAP" StartupMode="Disabled"
Service Name="Spooler" StartupMode="Disabled"
Service Name="SrmSvc" StartupMode="Disabled"
Service Name="SrmReports" StartupMode="Disabled"
Service Name="SSDPSRV" StartupMode="Disabled"
Service Name="swprv" StartupMode="Disabled"
Service Name="TapiSrv" StartupMode="Disabled"
Service Name="TBS" StartupMode="Disabled"
Service Name="TermService" StartupMode="Disabled"
Service Name="TrkWks" StartupMode="Disabled"
Service Name="upnphost" StartupMode="Disabled"
Service Name="UI0Detect" StartupMode="Disabled"
Service Name="UmRdpService" StartupMode="Disabled"
Service Name="VSS" StartupMode="Disabled"
Service Name="W32Time" StartupMode="Automatic"
Service Name="WcsPlugInService" StartupMode="Disabled"
Service Name="WdiServiceHost" StartupMode="Disabled"
Service Name="WdiSystemHost" StartupMode="Disabled"
Service Name="Wecsvc" StartupMode="Disabled"
Service Name="wercplsupport" StartupMode="Disabled"
Service Name="WerSvc" StartupMode="Disabled"
Service Name="WinHttpAutoProxySvc" StartupMode="Disabled"
Service Name="WinRM" StartupMode="Disabled"

Service Name="wmiApSrv" StartupMode="Disabled"
Service Name="WPDBusEnum" StartupMode="Disabled"
Service Name="wuauserv" StartupMode="Disabled"
Service Name="wudfsvc" StartupMode="Disabled"
Service Name="AdRmsLoggingService" StartupMode="Disabled"
Service Name="AppHostSvc" StartupMode="Automatic"
Service Name="aspnet_state" StartupMode="Automatic"
Service Name="CertSvc" StartupMode="Disabled"
Service Name="CISVC" StartupMode="Disabled"
Service Name="DFS" StartupMode="Disabled"
Service Name="DFSR" StartupMode="Disabled"
Service Name="Fax" StartupMode="Disabled"
Service Name="FontCache3.0.0.0" StartupMode="Manual"
Service Name="IAS" StartupMode="Disabled"
Service Name="IASJet" StartupMode="Disabled"
Service Name="idsvc" StartupMode="Manual"
Service Name="IISADMIN" StartupMode="Disabled"
Service Name="ifssvc" StartupMode="Disabled"
Service Name="IsmServ" StartupMode="Disabled"
Service Name="kdc" StartupMode="Disabled"
Service Name="MSFTPSVC" StartupMode="Disabled"
Service Name="MSiSNS" StartupMode="Disabled"
Service Name="MSMQ" StartupMode="Disabled"
Service Name="MSMQTriggers" StartupMode="Disabled"
Service Name="MQDS" StartupMode="Disabled"
Service Name="MSSQL$MICROSOFT##SSEE" StartupMode="Disabled"
Service Name="NetMsmqActivator" StartupMode="Disabled"
Service Name="NetPipeActivator" StartupMode="Automatic"
Service Name="NetTcpActivator" StartupMode="Automatic"
Service Name="NetTcpPortSharing" StartupMode="Automatic"
Service Name="NisSvc" StartupMode="Disabled"
Service Name="nfssvc" StartupMode="Disabled"
Service Name="nfsclnt" StartupMode="Disabled"
Service Name="NTDS" StartupMode="Disabled
"Service Name="NtFrs" StartupMode="Disabled"
Service Name="NtmsSvc" StartupMode="Disabled"
Service Name="OCSPSvc" StartupMode="Disabled"
Service Name="p2pimsvc" StartupMode="Disabled"
Service Name="PNRPAutoReg" StartupMode="Disabled
"Service Name="PNRPsvc" StartupMode="Disabled"
Service Name="QWAVE" StartupMode="Disabled"
Service Name="rqs" StartupMode="Disabled"
Service Name="SimpTcp" StartupMode="Disabled"
Service Name="SMTPSVC" StartupMode="Disabled"
Service Name="SPAdmin" StartupMode="Disabled"
Service Name="SPTimerV3" StartupMode="Disabled"
Service Name="SPSearch" StartupMode="Disabled"
Service Name="SPTrace" StartupMode="Disabled"

Service Name="SPWriter" StartupMode="Disabled"
Service Name="SQLWriter" StartupMode="Disabled"
Service Name="SNMP" StartupMode="Automatic"
Service Name="SstpSvc" StartupMode="Disabled"
Service Name="TlntSvr" StartupMode="Disabled"
Service Name="TermServLicensing" StartupMode="Disabled"
Service Name="TSGateway" StartupMode="Disabled"
Service Name="Tssdis" StartupMode="Disabled"
Service Name="WAS" StartupMode="Automatic"
Service Name="wbengine" StartupMode="Disabled"
Service Name="WDSServer" StartupMode="Disabled"
Service Name="WebClient" StartupMode="Disabled"
Service Name="WINS" StartupMode="Disabled"
Service Name="W3SVC" StartupMode="Automatic"
Service Name="WMSvc" StartupMode="Disabled"
Service Name="WSearch" StartupMode="Disabled"
Service Name="wsrm" StartupMode="Disabled"
Service Name="Appinfo" StartupMode="Manual"
Service Name="DcomLaunch" StartupMode="Automatic"
Service Name="Dhcp" StartupMode="Automatic"
Service Name="Eventlog" StartupMode="Automatic"
Service Name="EventSystem" StartupMode="Automatic"
Service Name="IKEEXT" StartupMode="Automatic"
Service Name="PlugPlay" StartupMode="Automatic"
Service Name="RpcSs" StartupMode="Automatic"
Service Name="SamSs" StartupMode="Automatic"
Service Name="Schedule" StartupMode="Automatic"
Service Name="ShellHWDetection" StartupMode="Automatic"
Service Name="slsvc" StartupMode="Automatic"
Service Name="SLUINotify" StartupMode="Manual"
Service Name="THREADORDER" StartupMode="Disabled"
Service Name="TrustedInstaller" StartupMode="Manual"
Service Name="UxSms" StartupMode="Automatic"
Service Name="vds" StartupMode="Manual"
Service Name="Winmgmt" StartupMode="Automatic"
Service Name="CryptSvc" StartupMode="Automatic"
Service Name="ProtectedStorage" StartupMode="Manual"
Service Name="gpsvc" StartupMode="Automatic"
Service Name="iphlpsvc" StartupMode="Automatic"
Service Name="MMCSS" StartupMode="Disabled"
Service Name="MpsSvc" StartupMode="Automatic"
Service Name="ProfSvc" StartupMode="Automatic"
Service Name="nsi" StartupMode="Automatic"
Service Name="Netman" StartupMode="Manual"
Service Name="BFE" StartupMode="Automatic"
Service Name="NlaSvc" StartupMode="Automatic"
Service Name="netprofm" StartupMode="Automatic"
Service Name="hidserv" StartupMode="Disabled"

Service Name="Themes" StartupMode="Disabled"
Service Name="SysMain" StartupMode="Disabled"
Service Name="clr_optimization_v4.0.30319_32" StartupMode="Automatic"
Service Name="dcconnsvc" StartupMode="Automatic"
Service Name="dcevt32" StartupMode="Automatic"
Service Name="dcnetmon" StartupMode="Automatic"
Service Name="dcstor32" StartupMode="Automatic"
Service Name="mr2kserv" StartupMode="Automatic"
Service Name="MSSQLFDLauncher" StartupMode="Manual"
Service Name="MSSQLSERVER" StartupMode="Automatic"
Service Name="MSSQLServerADHelper100" StartupMode="Disabled"
Service Name="omsad" StartupMode="Automatic"
Service Name="Server Administrator" StartupMode="Automatic"
Service Name="SQLBrowser" StartupMode="Disabled"
Service Name="SQLSERVERAGENT" StartupMode="Automatic"
Service Name="WPFFontCache_v0400" StartupMode="Manual"
Firewall Mode="On"
FirewallRules
FirewallRule Id="2e7435c1-4737-4194-a114-3cd8a82c3fa7" Name="Allow inbound connections for service: MSSQLSERVER for protocol: TCP" Description="This rule was generated by SCW as an intelligent guess based on the current connection activity of the service." Profile="All" ProtocolKeyword="TCP" Direction="Inbound" Program="%PROGRAMFILES%\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn\sqlservr.exe" Service="MSSQLSERVER" Enabled="True" Action="AllowConnections"
FirewallRule Id="38ea6962-7492-4023-97fb-7d3a249f63a2" Name="Allow inbound connections for service: Server Administrator for protocol: TCP" Description="This rule was generated by SCW as an intelligent guess based on the current connection activity of the service." Profile="All" ProtocolKeyword="TCP" Direction="Inbound" Program="%PROGRAMFILES%\Dell\SysMgt\iws\bin\win32\dsm_om_connsvc32.exe" Enabled="True" Action="AllowConnections"
FirewallRule Id="aed4e7a1-6dba-4a75-ad19-71f84b720985" Name="Allow inbound connections for service: MSSQLSERVER for protocol: TCP" Description="This rule was generated by SCW as an intelligent guess based on the current connection activity of the service." Profile="All" ProtocolKeyword="TCP" Direction="Inbound" Program="%PROGRAMFILES%\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn\sqlservr.exe" Service="MSSQLSERVER" Enabled="True" Action="AllowConnections"
FirewallRule Id="cc7837f1-d1ed-4126-b9bb-bcab0917fdaf" Name="Allow inbound connections for service: dcconnsvc for protocol: TCP" Description="This rule was generated by SCW as an intelligent guess based on the current connection activity of the service." Profile="All" ProtocolKeyword="TCP" Direction="Inbound" Program="%PROGRAMFILES%\Dell\SysMgt\ITAssistant\iws\bin\win32\dsm_om_connsvc32.exe" Enabled="True" Action="AllowConnections"
FirewallRule Id="corenet-dhcp-in" Name="@firewallapi.dll,-25301" Description="@firewallapi.dll,-25303" Profile="All" Group="@firewallapi.dll,-25000" ProtocolKeyword="UDP" Direction="Inbound" Program="%systemroot%\system32\svchost.exe" Service="dhcp" Enabled="False" Action="AllowConnections"
LocalPorts Port Value="68”
RemotePorts Port Value="67"
FirewallRule Id="corenet-dhcp-out" Name="@firewallapi.dll,-25302" Description="@firewallapi.dll,-25303" Profile="All" Group="@firewallapi.dll,-25000" ProtocolKeyword="UDP" Direction="Outbound" Program="%systemroot%\system32\svchost.exe" Service="dhcp" Enabled="False" Action="AllowConnections"
LocalPorts Port Value="68”
RemotePorts Port Value="67"

FirewallRule Id="corenet-icmp4-dufrag-in" Name="@firewallapi.dll,-25251" Description="@firewallapi.dll,-25257" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V4" Direction="Inbound" Program="system" Enabled="True"
Action="AllowConnections"
ICMP Type="3" Code="4"
FirewallRule Id="corenet-icmp6-du-in" Name="@firewallapi.dll,-25110" Description="@firewallapi.dll,-25112" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Inbound" Program="system" Enabled="True"
Action="AllowConnections
ICMP Type="1" Code="*"
FirewallRule Id="corenet-icmp6-ld-in" Name="@firewallapi.dll,-25082" Description="@firewallapi.dll,-25088" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Inbound" Program="system" Enabled="True"
Action="AllowConnections
RemoteAddresses DefaultGateway="False" WINSServers="False" DHCPServers="False" DNSServers="False" LocalSubnet="True"
ICMP Type="132" Code="*"
FirewallRule Id="corenet-icmp6-ld-out" Name="@firewallapi.dll,-25083" Description="@firewallapi.dll,-25088" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Outbound" Program="system" Enabled="True"
Action="AllowConnections"
RemoteAddresses DefaultGateway="False" WINSServers="False" DHCPServers="False" DNSServers="False" LocalSubnet="True"
ICMP Type="132" Code="*"
FirewallRule Id="corenet-icmp6-lq-in" Name="@firewallapi.dll,-25061" Description="@firewallapi.dll,-25067" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Inbound" Program="system" Enabled="True"
Action="AllowConnections"
RemoteAddresses DefaultGateway="False" WINSServers="False" DHCPServers="False" DNSServers="False" LocalSubnet="True"
ICMP Type="130" Code="*"
FirewallRule Id="corenet-icmp6-lq-out" Name="@firewallapi.dll,-25062" Description="@firewallapi.dll,-25067" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Outbound" Program="system" Enabled="True"
Action="AllowConnections"
RemoteAddresses DefaultGateway="False" WINSServers="False" DHCPServers="False" DNSServers="False" LocalSubnet="True"
ICMP Type="130" Code="*"
FirewallRule Id="corenet-icmp6-lr-in" Name="@firewallapi.dll,-25068" Description="@firewallapi.dll,-25074" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Inbound" Program="system" Enabled="True"
Action="AllowConnections"><RemoteAddresses DefaultGateway="False" WINSServers="False" DHCPServers="False"
DNSServers="False" LocalSubnet="True"
ICMP Type="131" Code="*"
FirewallRule Id="corenet-icmp6-lr-out" Name="@firewallapi.dll,-25069" Description="@firewallapi.dll,-25074" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Outbound" Program="system" Enabled="True"
Action="AllowConnections"
RemoteAddresses DefaultGateway="False" WINSServers="False" DHCPServers="False" DNSServers="False" LocalSubnet="True"
ICMP Type="131" Code="*"
FirewallRule Id="corenet-icmp6-lr2-in" Name="@firewallapi.dll,-25075" Description="@firewallapi.dll,-25081" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Inbound" Program="system" Enabled="True"
Action="AllowConnections"
RemoteAddresses DefaultGateway="False" WINSServers="False" DHCPServers="False" DNSServers="False" LocalSubnet="True"
ICMP Type="143" Code="*"
FirewallRule Id="corenet-icmp6-lr2-out" Name="@firewallapi.dll,-25076" Description="@firewallapi.dll,-25081" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Outbound" Program="system" Enabled="True"
Action="AllowConnections"
RemoteAddresses DefaultGateway="False" WINSServers="False" DHCPServers="False" DNSServers="False" LocalSubnet="True"
ICMP Type="143" Code="*"

FirewallRule Id="corenet-icmp6-nda-in" Name="@firewallapi.dll,-25026" Description="@firewallapi.dll,-25032" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Inbound" Program="system" Enabled="True"
Action="AllowConnections"
RemoteAddresses DefaultGateway="False" WINSServers="False" DHCPServers="False" DNSServers="False" LocalSubnet="True"
ICMP Type="136" Code="*"
FirewallRule Id="corenet-icmp6-nda-out" Name="@firewallapi.dll,-25027" Description="@firewallapi.dll,-25032" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Outbound" Program="system" Enabled="True"
Action="AllowConnections"
RemoteAddresses DefaultGateway="False" WINSServers="False" DHCPServers="False" DNSServers="False" LocalSubnet="True"
ICMP Type="136" Code="*"
FirewallRule Id="corenet-icmp6-nds-in" Name="@firewallapi.dll,-25019" Description="@firewallapi.dll,-25025" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Inbound" Program="system" Enabled="True"
Action="AllowConnections"
RemoteAddresses DefaultGateway="False" WINSServers="False" DHCPServers="False" DNSServers="False" LocalSubnet="True"
ICMP Type="135" Code="*"
FirewallRule Id="corenet-icmp6-nds-out" Name="@firewallapi.dll,-25020" Description="@firewallapi.dll,-25025" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Outbound" Program="system" Enabled="True"
Action="AllowConnections"
RemoteAddresses DefaultGateway="False" WINSServers="False" DHCPServers="False" DNSServers="False" LocalSubnet="True"
ICMP Type="135" Code="*"
FirewallRule Id="corenet-icmp6-pp-in" Name="@firewallapi.dll,-25116" Description="@firewallapi.dll,-25118" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Inbound" Program="system" Enabled="True"
Action="AllowConnections"
ICMP Type="4" Code="*"
FirewallRule Id="corenet-icmp6-pp-out" Name="@firewallapi.dll,-25117" Description="@firewallapi.dll,-25118" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Outbound" Program="system" Enabled="True"
Action="AllowConnections"
ICMP Type="4" Code="*"
FirewallRule Id="corenet-icmp6-ptb-in" Name="@firewallapi.dll,-25001" Description="@firewallapi.dll,-25007" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Inbound" Program="system" Enabled="True"
Action="AllowConnections"
ICMP Type="2" Code="*"
FirewallRule Id="corenet-icmp6-ptb-out" Name="@firewallapi.dll,-25002" Description="@firewallapi.dll,-25007" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Outbound" Program="system" Enabled="True"
Action="AllowConnections"
ICMP Type="2" Code="*"
FirewallRule Id="corenet-icmp6-ra-in" Name="@firewallapi.dll,-25012" Description="@firewallapi.dll,-25018" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Inbound" Program="system" Enabled="True"
Action="AllowConnections"
RemoteAddresses DefaultGateway="False" WINSServers="False" DHCPServers="False" DNSServers="False" LocalSubnet="True”
ICMP Type="134" Code="*"
FirewallRule Id="corenet-icmp6-ra-out" Name="@firewallapi.dll,-25013" Description="@firewallapi.dll,-25018" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Outbound" Program="system" Enabled="True"
Action="AllowConnections"
RemoteAddresses DefaultGateway="False" WINSServers="False" DHCPServers="False" DNSServers="False" LocalSubnet="True"
ICMP Type="134" Code="*"

FirewallRule Id="corenet-icmp6-rs-out" Name="@firewallapi.dll,-25008" Description="@firewallapi.dll,-25011" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Outbound" Program="system" Enabled="True"
Action="AllowConnections"
RemoteAddresses DefaultGateway="False" WINSServers="False" DHCPServers="False" DNSServers="False" LocalSubnet="True"
ICMP Type="133" Code="*"
FirewallRule Id="corenet-icmp6-te-in" Name="@firewallapi.dll,-25113" Description="@firewallapi.dll,-25115" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Inbound" Program="system" Enabled="True"
Action="AllowConnections"
ICMP Type="3" Code="*"
FirewallRule Id="corenet-icmp6-te-out" Name="@firewallapi.dll,-25114" Description="@firewallapi.dll,-25115" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="ICMP_V6" Direction="Outbound" Program="system" Enabled="True"
Action="AllowConnections"
ICMP Type="3" Code="*"
FirewallRule Id="corenet-igmp-in" Name="@firewallapi.dll,-25376" Description="@firewallapi.dll,-25382" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="IGMP" Direction="Inbound" Program="system" Enabled="True"
Action="AllowConnections”
FirewallRule Id="corenet-igmp-out" Name="@firewallapi.dll,-25377" Description="@firewallapi.dll,-25382" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="IGMP" Direction="Outbound" Program="system" Enabled="True"
Action="AllowConnections"
FirewallRule Id="corenet-ipv6-in" Name="@firewallapi.dll,-25351" Description="@firewallapi.dll,-25357" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="IPV6" Direction="Inbound" Program="system" Enabled="True"
Action="AllowConnections"
FirewallRule Id="corenet-ipv6-out" Name="@firewallapi.dll,-25352" Description="@firewallapi.dll,-25358" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="IPV6" Direction="Outbound" Program="system" Enabled="True"
Action="AllowConnections"
FirewallRule Id="corenet-teredo-in" Name="@firewallapi.dll,-25326" Description="@firewallapi.dll,-25332" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="UDP" Direction="Inbound" Program="%systemroot%\system32\svchost.exe"
Service="iphlpsvc" Enabled="True" Action="AllowConnections"
Port Value="0"
FirewallRule Id="corenet-teredo-out" Name="@firewallapi.dll,-25327" Description="@firewallapi.dll,-25333" Profile="All"
Group="@firewallapi.dll,-25000" ProtocolKeyword="UDP" Direction="Outbound" Program="%systemroot%\system32\svchost.exe"
Service="iphlpsvc" Enabled="True" Action="AllowConnections"
FirewallRule Id="e54f9c71-db3d-49e7-bc4d-babb289b0ee3" Name="Allow inbound connections for service: Server Administrator
for protocol: TCP" Description="This rule was generated by SCW as an intelligent guess based on the current connection activity of
the service." Profile="All" ProtocolKeyword="TCP" Direction="Inbound"
Program="%PROGRAMFILES%\Dell\SysMgt\iws\bin\win32\dsm_om_connsvc32.exe" Enabled="True"
Action="AllowConnections"
FirewallRule Id="fa2ad23b-f164-415d-9239-b52b6bdccc50" Name="Allow inbound connections for service: dcnetmon for protocol:
TCP" Description="This rule was generated by SCW as an intelligent guess based on the current connection activity of the service."
Profile="All" ProtocolKeyword="TCP" Direction="Inbound"
Program="%PROGRAMFILES%\Dell\SysMgt\ITAssistant\bin\DSM_ITA_Netmon32.exe" Enabled="True"
Action="AllowConnections"
FirewallRule Id="iis-webserverrole-http-in-tcp" Name="@%windir%\system32\inetsrv\iisres.dll,-30500"
Description="@%windir%\system32\inetsrv\iisres.dll,-30510" Profile="All" Group="@%windir%\system32\inetsrv\iisres.dll,-30501"
ProtocolKeyword="TCP" Direction="Inbound" Program="system" Enabled="True" Action="AllowConnections"
Port Value="80"

FirewallRule Id="iis-webserverrole-https-in-tcp" Name="@%windir%\system32\inetsrv\iisres.dll,-30502"
Description="@%windir%\system32\inetsrv\iisres.dll,-30512" Profile="All" Group="@%windir%\system32\inetsrv\iisres.dll,-30503"
ProtocolKeyword="TCP" Direction="Inbound" Program="system" Enabled="True" Action="AllowConnections"
Port Value="443"
FirewallRule Id="SCW-Remote-Operations-For-Scshost-RPC" Name="@scwcmd.exe,-8001" Description="@scwcmd.exe,-8002"
Profile="All" Group="@scwcmd.exe,-8000" ProtocolKeyword="TCP" Direction="Inbound"
Program="%systemroot%\system32\scshost.exe" Enabled="True" Action="AllowConnections"
LocalPorts SpecialPorts="DynamicRPC"
FirewallRule Id="SCW-Remote-Operations-For-Scshost-RPC-EndPointMapper" Name="@scwcmd.exe,-8003"
Description="@scwcmd.exe,-8004" Profile="All" Group="@scwcmd.exe,-8000" ProtocolKeyword="TCP" Direction="Inbound"
Program="%systemroot%\system32\scshost.exe" Enabled="True" Action="AllowConnections"><LocalPorts
SpecialPorts="RPCEndPointMapper"
FirewallRule Id="SCW-Remote-Operations-For-Svchost-TCP" Name="@scwcmd.exe,-8005" Description="@scwcmd.exe,-8006"
Profile="All" Group="@scwcmd.exe,-8000" ProtocolKeyword="TCP" Direction="Inbound"
Program="%systemroot%\system32\svchost.exe" Enabled="True" Action="AllowConnections"
Port Value="135"
FirewallRule Id="SCW-Remote-Operations-For-System-TCP" Name="@scwcmd.exe,-8007" Description="@scwcmd.exe,-8008"
Profile="All" Group="@scwcmd.exe,-8000" ProtocolKeyword="TCP" Direction="Inbound" Program="system" Enabled="True"
Action="AllowConnections"
Port Value="139"Port Value="445"
FirewallRule Id="SCW-Remote-Operations-For-System-UDP" Name="@scwcmd.exe,-8009" Description="@scwcmd.exe,-8010"
Profile="All" Group="@scwcmd.exe,-8000" ProtocolKeyword="UDP" Direction="Inbound" Program="system" Enabled="True"
Action="AllowConnections"
Port Value="137"
FirewallRule Id="snmp-in-udp" Name="@snmp.exe,-8" Description="@snmp.exe,-10" Profile="All" Group="@snmp.exe,-3"
ProtocolKeyword="UDP" Direction="Inbound" Program="%systemroot%\system32\snmp.exe" Service="snmp" Enabled="True"
Action="AllowConnections"
Port Value="161"
FirewallRule Id="snmp-in-udp-noscope" Name="@snmp.exe,-8" Description="@snmp.exe,-10" Profile="Domain"
Group="@snmp.exe,-3" ProtocolKeyword="UDP" Direction="Inbound" Program="%systemroot%\system32\snmp.exe"
Service="snmp" Enabled="True" Action="AllowConnections"
Port Value="161"
FirewallRule Id="wcf-nettcpactivator-in-tcp-32bit" Name="@%systemroot%\microsoft.net\framework\v3.0\windows communication
foundation\servicemodelevents.dll,-2000" Description="@%systemroot%\microsoft.net\framework\v3.0\windows communication
foundation\servicemodelevents.dll,-2001" Profile="All" Group="@%systemroot%\microsoft.net\framework\v3.0\windows
communication foundation\servicemodelevents.dll,-2002" ProtocolKeyword="TCP" Direction="Inbound"
Program="%systemroot%\microsoft.net\framework\v3.0\windows communication foundation\smsvchost.exe"
Service="nettcpactivator" Enabled="True" Action="AllowConnections"
Port Value="808"
FirewallRule Id="wcf-nettcpactivator-in-tcp-64bit" Name="@%systemroot%\microsoft.net\framework64\v3.0\windows
communication foundation\servicemodelevents.dll,-2000" Description="@%systemroot%\microsoft.net\framework64\v3.0\windows
communication foundation\servicemodelevents.dll,-2001" Profile="All"
Group="@%systemroot%\microsoft.net\framework64\v3.0\windows communication foundation\servicemodelevents.dll,-2002"
ProtocolKeyword="TCP" Direction="Inbound" Program="%systemroot%\microsoft.net\framework64\v3.0\windows communication
foundation\smsvchost.exe" Service="nettcpactivator" Enabled="True" Action="AllowConnections"
Port Value="808”

"Microsoft.OS.Registry.Values" Order="1"
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters]
Requiresecuritysignature=REG_DWORD=0
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
Lmcompatibilitylevel=REG_DWORD==2
PolicyAuthoringData Extension ID="{53F6F305-1C1A-4768-A255-81F6145BE09F}" Name="SCW"
PrototypeMachineName="SERVER2008" AppServerFoundation
ASPNetState
NPActivation
RemoteSCWEngine
SNMP
TcpActivation
WAS
Web
TimeSync
.NETv3.0
Install
MSFCPRS
clr_optimization_v4.0.30319_32
dcconnsvc
dcevt32
dcnetmon
dcstor32
mr2kserv
MSSQLFDLauncher
MSSQLSERVER
Omsad
ServerAdministrator
SQLSERVERAGENT
WPFFontCache_v0400
UnspecifiedService CheckBox="False"UnselectionFirewallRules
FirewallRule Id="microsoft-windows-certificateservices-certsvc-dcom-in" Scope="KB"Source Role="CertServer"
FirewallRule Id="microsoft-windows-certificateservices-certsvc-rpc-epmap-in" Scope="KB"Source Role="CertServer"
FirewallRule Id="microsoft-windows-certificateservices-certsvc-rpc-np-in" Scope="KB"Source Role="CertServer"
FirewallRule Id="microsoft-windows-certificateservices-certsvc-rpc-tcp-in" Scope="KB"Source Role="CertServer"
FirewallRule Id="microsoft-windows-certificateservices-certsvc-tcp-out" Scope="KB"Source Role="CertServer"
FirewallRule Id="dfsr-dfsrsvc-in-tcp" Scope="KB" Source Role="DFSR"
FirewallRule Id="dfsr-dfsrsvc-rpcss-in-tcp" Scope="KB"Source Role="DFSR"
FirewallRule Id="microsoft-windows-dhcp-clientsvc-dhcpv4-in" Scope="KB"Source Role="DHCPServer"
FirewallRule Id="microsoft-windows-dhcp-clientsvc-dhcpv6-in" Scope="KB"Source Role="DHCPServer"
FirewallRule Id="dnssrv-dns-tcp-in" Scope="KB"Source Role="DNSServer"
FirewallRule Id="dnssrv-dns-udp-in" Scope="KB"Source Role="DNSServer"
FirewallRule Id="dnssrv-tcp-out" Scope="KB"Source Role="DNSServer"
FirewallRule Id="dnssrv-udp-out" Scope="KB"Source Role="DNSServer"
FirewallRule Id="adds-icmp4-in" Scope="KB"Source Role="DomainController"
FirewallRule Id="adds-icmp4-out" Scope="KB"Source Role="DomainController"
FirewallRule Id="adds-icmp6-in" Scope="KB"Source Role="DomainController"
FirewallRule Id="adds-icmp6-out" Scope="KB”Source Role="DomainController"

FirewallRule Id="adds-kerberos-password-tcp-in" Scope="KB"Source Role="DomainController"
FirewallRule Id="adds-kerberos-password-udp-in" Scope="KB"Source Role="DomainController"
FirewallRule Id="adds-kerberos-tcp-in" Scope="KB"Source Role="DomainController"
FirewallRule Id="adds-kerberos-udp-in" Scope="KB"Source Role="DomainController"
FirewallRule Id="adds-ldap-tcp-in" Scope="KB"Source Role="DomainController"
FirewallRule Id="adds-ldap-udp-in" Scope="KB"Source Role="DomainController"
FirewallRule Id="adds-ldapgc-tcp-in" Scope="KB"Source Role="DomainController"
FirewallRule Id="adds-ldapgcsec-tcp-in" Scope="KB"Source Role="DomainController"
FirewallRule Id="adds-ldapsec-tcp-in" Scope="KB"Source Role="DomainController"
FirewallRule Id="adds-nb-datagram-udp-in" Scope="KB"Source Role="DomainController"
FirewallRule Id="adds-np-tcp-in" Scope="KB"Source Role="DomainController"
FirewallRule Id="adds-np-udp-in" Scope="KB"Source Role="DomainController"
FirewallRule Id="adds-rpc-tcp-in" Scope="KB"Source Role="DomainController"
FirewallRule Id="adds-rpcepmap-tcp-in" Scope="KB"Source Role="DomainController"
FirewallRule Id="adds-tcp-out" Scope="KB"Source Role="DomainController"
FirewallRule Id="adds-udp-out" Scope="KB"Source Role="DomainController"
FirewallRule Id="corenet-dns-out-udp" Scope="KB"Source Role="DomainController"Source Role="DNSClient"
FirewallRule Id="corenet-gp-lsass-out-tcp" Scope="KB"Source Role="DomainController"Source Role="DomainMember"
FirewallRule Id="corenet-gp-np-out-tcp" Scope="KB"Source Role="DomainController"Source Role="DomainMember"
FirewallRule Id="corenet-gp-out-tcp" Scope="KB"Source Role="DomainController"Source Role="DomainMember"
FirewallRule Id="fps-icmp4-erq-out" Scope="KB"Source Role="DomainController"Source Role="MSClient"
FirewallRule Id="fps-icmp6-erq-out" Scope="KB"Source Role="DomainController"Source Role="MSClient"
FirewallRule Id="fps-nb_datagram-out-udp-noscope" Scope="KB"Source Role="DomainController"Source Role="MSClient"Source Role="BrowserServer"
FirewallRule Id="fps-nb_name-out-udp-noscope" Scope="KB"Source Role="DomainController"Source Role="MSClient"Source Role="BrowserServer"
FirewallRule Id="fps-nb_session-out-tcp-noscope" Scope="KB"Source Role="DomainController"Source Role="MSClient"
FirewallRule Id="fps-smb-out-tcp-noscope" Scope="KB"Source Role="DomainController"Source Role="MSClient"
FirewallRule Id="netlogon-namedpipe-in" Scope="KB"Source Role="DomainController"Source Role="DomainMember"
FirewallRule Id="w32time-ntp-udp-in" Scope="KB"Source Role="DomainController"
FirewallRule Id="failovercluster-cprepsrv-tcp-in" Scope="KB"Source Role="FailoverCluster"
FirewallRule Id="failovercluster-dcom-tcp-in" Scope="KB"Source Role="FailoverCluster"
FirewallRule Id="failovercluster-eventlog-tcp-in" Scope="KB"Source Role="FailoverCluster"
FirewallRule Id="failovercluster-services-tcp-in" Scope="KB"Source Role="FailoverCluster"
FirewallRule Id="failovercluster-smb-tcp-in" Scope="KB"Source Role="FailoverCluster"
FirewallRule Id="failovercluster-winmgmt-tcp-in" Scope="KB"Source Role="FailoverCluster"
FirewallRule Id="failoverclustering-clussvc-tcp-in" Scope="KB"Source Role="FailoverCluster"
FirewallRule Id="failoverclustering-clussvc-tcp-out" Scope="KB"Source Role="FailoverCluster"
FirewallRule Id="failoverclustering-clussvcrpc-tcp-in" Scope="KB"Source Role="FailoverCluster"
FirewallRule Id="failoverclustering-icmpv4-er-in" Scope="KB"Source Role="FailoverCluster"
FirewallRule Id="failoverclustering-icmpv4-er-out" Scope="KB"Source Role="FailoverCluster"
FirewallRule Id="failoverclustering-icmpv4-erq-in" Scope="KB"Source Role="FailoverCluster"
FirewallRule Id="failoverclustering-icmpv4-erq-out" Scope="KB"Source Role="FailoverCluster"
FirewallRule Id="failoverclustering-icmpv6-er-in" Scope="KB"Source Role="FailoverCluster"
FirewallRule Id="failoverclustering-icmpv6-er-out" Scope="KB"Source Role="FailoverCluster"
FirewallRule Id="failoverclustering-icmpv6-erq-in" Scope="KB"Source Role="FailoverCluster"
FirewallRule Id="failoverclustering-icmpv6-erq-out" Scope="KB"Source Role="FailoverCluster"
FirewallRule Id="failoverclustering-netft-udp-in" Scope="KB"Source Role="FailoverCluster"

FirewallRule Id="failoverclustering-netft-udp-out" Scope="KB"Source Role="FailoverCluster"
FirewallRule Id="iis-webserverrole-ftp-in-tcp" Scope="KB"Source Role="FTPServer"
FirewallRule Id="microsoft-windows-isns_service-tcp-in" Scope="KB"Source Role="iSNS"
FirewallRule Id="microsoft-windows-isns_service-tcp-out" Scope="KB"Source Role="iSNS"
FirewallRule Id="lpdprinterserver-tcp-in" Scope="KB"Source Role="LPD"
FirewallRule Id="fps-icmp4-erq-in" Scope="KB"Source Role="MSServer"
FirewallRule><FirewallRule Id="fps-icmp6-erq-in" Scope="KB"Source Role="MSServer"
FirewallRule Id="fps-nb_datagram-in-udp-noscope" Scope="KB"Source Role="MSServer"Source Role="BrowserServer"
FirewallRule Id="fps-nb_name-in-udp-noscope" Scope="KB"Source Role="MSServer"Source Role="BrowserServer"
FirewallRule Id="fps-nb_session-in-tcp-noscope" Scope="KB"Source Role="MSServer"
FirewallRule Id="fps-rpcss-in-tcp-noscope" Scope="KB"Source Role="MSServer"
FirewallRule Id="fps-smb-in-tcp-noscope" Scope="KB"Source Role="MSServer"
FirewallRule Id="msmq-in-tcp" Scope="KB"Source Role="MSMQ"
FirewallRule Id="msmq-in-udp" Scope="KB"Source Role="MSMQ"
FirewallRule Id="msmq-out-tcp" Scope="KB"Source Role="MSMQ"
FirewallRule Id="msmq-out-udp" Scope="KB"Source Role="MSMQ"
FirewallRule Id="microsoft-windows-nfs-clientcore-nfsclnt-tcp-in" Scope="KB"Source Role="NFS"
FirewallRule Id="microsoft-windows-nfs-clientcore-nfsclnt-tcp-out" Scope="KB"Source Role="NFS"
FirewallRule Id="microsoft-windows-nfs-clientcore-nfsclnt-udp-in" Scope="KB"Source Role="NFS"
FirewallRule Id="microsoft-windows-nfs-clientcore-nfsclnt-udp-out" Scope="KB"Source Role="NFS"
FirewallRule Id="microsoft-windows-nfs-openportmapper-portmap-tcp-in" Scope="KB"Source Role="NFS"
FirewallRule Id="microsoft-windows-nfs-openportmapper-portmap-tcp-out" Scope="KB"Source Role="NFS"
FirewallRule Id="microsoft-windows-nfs-openportmapper-portmap-udp-in" Scope="KB"Source Role="NFS"
FirewallRule Id="microsoft-windows-nfs-openportmapper-portmap-udp-out" Scope="KB"Source Role="NFS"
FirewallRule Id="microsoft-windows-nfs-servercore-nfssvc-mount-tcp-in" Scope="KB"Source Role="NFS"
FirewallRule Id="microsoft-windows-nfs-servercore-nfssvc-mount-udp-in" Scope="KB"Source Role="NFS"
FirewallRule Id="microsoft-windows-nfs-servercore-nfssvc-nfs-tcp-in" Scope="KB"Source Role="NFS"
FirewallRule Id="microsoft-windows-nfs-servercore-nfssvc-nfs-tcp-out" Scope="KB"Source Role="NFS"
FirewallRule Id="microsoft-windows-nfs-servercore-nfssvc-nfs-udp-in" Scope="KB"Source Role="NFS"
FirewallRule Id="microsoft-windows-nfs-servercore-nfssvc-nfs-udp-out" Scope="KB"Source Role="NFS"
FirewallRule Id="microsoft-windows-nfs-servercore-nfssvc-nlm-tcp-in" Scope="KB"Source Role="NFS"
FirewallRule Id="microsoft-windows-nfs-servercore-nfssvc-nlm-udp-in" Scope="KB"Source Role="NFS"
FirewallRule Id="microsoft-windows-nfs-servercore-nfssvc-nsm-tcp-in" Scope="KB"Source Role="NFS"
FirewallRule Id="microsoft-windows-nfs-servercore-nfssvc-nsm-udp-in" Scope="KB"Source Role="NFS"
FirewallRule Id="nps-npssvc-in-udp-1645" Scope="KB"Source Role="NPS"
FirewallRule Id="nps-npssvc-in-udp-1646" Scope="KB"Source Role="NPS"
FirewallRule Id="nps-npssvc-in-udp-1812" Scope="KB"Source Role="NPS"
FirewallRule Id="nps-npssvc-in-udp-1813" Scope="KB"Source Role="NPS"
FirewallRule Id="fps-spoolsvc-in-tcp-noscope" Scope="KB"Source Role="Print"
FirewallRule Id="psync-lsass-tcp-in" Scope="KB"Source Role="PSYNC"
FirewallRule Id="complusnetworkaccess-dcom-in" Scope="KB"Source Role="RemoteCOM+"
FirewallRule Id="msdtc-in-tcp" Scope="KB"Source Role="RemoteDTC"
FirewallRule Id="msdtc-out-tcp" Scope="KB"Source Role="RemoteDTC"
FirewallRule Id="msdtc-rpcss-in-tcp" Scope="KB"Source Role="RemoteDTC"
FirewallRule Id="SCW-Remote-Operations-For-Scshost-RPC" Scope="KB"Source Role="RemoteSCWEngine"
FirewallRule Id="SCW-Remote-Operations-For-Scshost-RPC-EndPointMapper" Scope="KB"Source Role="RemoteSCWEngine"
FirewallRule Id="SCW-Remote-Operations-For-Svchost-TCP" Scope="KB"Source Role="RemoteSCWEngine"
FirewallRule Id="SCW-Remote-Operations-For-System-TCP" Scope="KB"Source Role="RemoteSCWEngine"

FirewallRule Id="SCW-Remote-Operations-For-System-UDP" Scope="KB"Source Role="RemoteSCWEngine"
FirewallRule Id="rras-gre-in" Scope="KB”Source Role="RRASx32"Source Role="RRASx64"
FirewallRule Id="rras-gre-out" Scope="KB"Source Role="RRASx32"Source Role="RRASx64"
FirewallRule Id="rras-l2tp-in-udp" Scope="KB"Source Role="RRASx32"Source Role="RRASx64"
FirewallRule Id="rras-l2tp-out-udp" Scope="KB"Source Role="RRASx32"Source Role="RRASx64"
FirewallRule Id="rras-pptp-in-tcp" Scope="KB"Source Role="RRASx32"Source Role="RRASx64"
FirewallRule Id="rras-pptp-out-tcp" Scope="KB"Source Role="RRASx32"Source Role="RRASx64"
FirewallRule Id="sstp-in-tcp" Scope="KB"><Source Role="RRASx32"Source Role="RRASx64"
FirewallRule Id="rqs-in-tcp" Scope="KB"Source Role="RRASx64"
FirewallRule Id="smtpsvc-service-in-tcp" Scope="KB"Source Role="SMTP"Source Role="MailBasedRepl"
FirewallRule Id="nis-server-in-rpc-epmap" Scope="KB"Source Role="SNIS"
FirewallRule Id="nis-server-in-rpc-tcp" Scope="KB" Source Role="SNIS"
FirewallRule Id="nis-server-in-rpc-udp" Scope="KB" Source Role="SNIS"
FirewallRule Id="snmp-in-udp" Scope="KB" Source Role="SNMP"
FirewallRule Id="snmp-in-udp-noscope" Scope="KB" Source Role="SNMP"
FirewallRule Id="snmptrap-in-udp" Scope="KB" Source Role="SNMPTrap"
FirewallRule Id="snmptrap-in-udp-noscope" Scope="KB" Source Role="SNMPTrap"
FirewallRule Id="wcf-nettcpactivator-in-tcp-32bit" Scope="KB" Source Role="TcpActivation"
FirewallRule Id="wcf-nettcpactivator-in-tcp-64bit" Scope="KB" Source Role="TcpActivation"
FirewallRule Id="telnetserver-tlntsvr-tcp-in" Scope="KB" Source Role="TelnetServer"
FirewallRule Id="remotedesktop-in-tcp" Scope="KB" Source Role="TerminalServer"Source Role="RemoteDesktop"
FirewallRule Id="termservlicensing-in-tcp" Scope="KB" Source Role="TSLicense"
FirewallRule Id="termservlicensing-np-in-tcp" Scope="KB" Source Role="TSLicense"
FirewallRule Id="termservlicensing-rpcss-in-tcp" Scope="KB" Source Role="TSLicense"
FirewallRule Id="termservlicensing-wmi-dcom-in-tcp" Scope="KB" Source Role="TSLicense"
FirewallRule Id="termservlicensing-wmi-in-tcp" Scope="KB" Source Role="TSLicense"
FirewallRule Id="termservlicensing-wmi-out-tcp" Scope="KB" Source Role="TSLicense"
FirewallRule Id="sessiondirectoryservice-in-tcp" Scope="KB" Source Role="TSSession"
FirewallRule Id="sessiondirectoryservice-np-in-tcp" Scope="KB" Source Role="TSSession"
FirewallRule Id="sessiondirectoryservice-rpcss-in-tcp" Scope="KB" Source Role="TSSession"
FirewallRule Id="sessiondirectoryservice-wmi-dcom-in-tcp" Scope="KB" Source Role="TSSession"
FirewallRule Id="sessiondirectoryservice-wmi-in-tcp" Scope="KB" Source Role="TSSession"
FirewallRule Id="sessiondirectoryservice-wmi-out-tcp" Scope="KB" Source Role="TSSession"
FirewallRule Id="wds-np-in-tcp" Scope="KB" Source Role="WDS"
FirewallRule Id="wds-rpc-in-tcp" Scope="KB" Source Role="WDS"
FirewallRule Id="wds-rpcss-in-tcp" Scope="KB" Source Role="WDS"
FirewallRule Id="wds-wdsserver-in-udp" Scope="KB" Source Role="WDS"
FirewallRule Id="iis-webserverrole-http-in-tcp" Scope="KB" Source Role="Web"
FirewallRule Id="iis-webserverrole-https-in-tcp" Scope="KB" Source Role="Web"
FirewallRule Id="winrm-http-in-tcp" Scope="KB" Source Role="WinRM"
FirewallRule Id="wins-service-in-nb-name-udp" Scope="KB" Source Role="WINS"Source Role="WINSClient"
FirewallRule Id="wins-service-in-tcp" Scope="KB" Source Role="WINS"
FirewallRule Id="wins-service-in-udp" Scope="KB" Source Role="WINS"
FirewallRule Id="wins-service-out-tcp" Scope="KB" Source Role="WINS"
FirewallRule Id="wins-service-out-udp" Scope="KB" Source Role="WINS"
FirewallRule Id="netdis-llmnr-in-udp" Scope="KB" Source Role="LLMNR-DNS"Source Role="NetworkDiscovery"
FirewallRule Id="netdis-llmnr-out-udp" Scope="KB" Source Role="LLMNR-DNS"Source Role="NetworkDiscovery"
FirewallRule Id="netdis-fdphost-in-udp" Scope="KB" Source Role="NetworkDiscovery"

FirewallRule Id="netdis-fdphost-out-udp" Scope="KB" Source Role="NetworkDiscovery"
FirewallRule Id="netdis-fdrespub-wsd-in-udp" Scope="KB" Source Role="NetworkDiscovery"
FirewallRule Id="netdis-fdrespub-wsd-out-udp" Scope="KB" Source Role="NetworkDiscovery"
FirewallRule Id="netdis-nb_datagram-in-udp" Scope="KB" Source Role="NetworkDiscovery"
FirewallRule Id="netdis-nb_datagram-out-udp" Scope="KB" Source Role="NetworkDiscovery"
FirewallRule Id="netdis-nb_name-in-udp" Scope="KB" Source Role="NetworkDiscovery"
FirewallRule Id="netdis-nb_name-out-udp" Scope="KB" Source Role="NetworkDiscovery"
FirewallRule Id="netdis-ssdpsrv-in-udp" Scope="KB" Source Role="NetworkDiscovery"
FirewallRule Id="netdis-ssdpsrv-out-udp" Scope="KB" Source Role="NetworkDiscovery"
FirewallRule Id="netdis-upnp-out-tcp" Scope="KB" Source Role="NetworkDiscovery"
FirewallRule Id="netdis-upnphost-in-tcp" Scope="KB" Source Role="NetworkDiscovery"
FirewallRule Id="netdis-upnphost-out-tcp" Scope="KB" Source Role="NetworkDiscovery"
FirewallRule Id="netdis-wsdevnt-in-tcp" Scope="KB" Source Role="NetworkDiscovery"
FirewallRule Id="netdis-wsdevnt-out-tcp" Scope="KB" Source Role="NetworkDiscovery"
FirewallRule Id="netdis-wsdevnts-in-tcp" Scope="KB" Source Role="NetworkDiscovery"
FirewallRule Id="netdis-wsdevnts-out-tcp" Scope="KB" Source Role="NetworkDiscovery"
FirewallRule Id="corenet-dhcp-in" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-dhcp-out" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp4-dufrag-in" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-du-in" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-ld-in" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-ld-out" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-lq-in" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-lq-out" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-lr-in" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-lr-out" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-lr2-in" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-lr2-out" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-nda-in" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-nda-out" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-nds-in" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-nds-out" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-pp-in" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-pp-out" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-ptb-in" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-ptb-out" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-ra-in" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-ra-out" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-rs-out" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-te-in" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-icmp6-te-out" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-igmp-in" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-igmp-out" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-ipv6-in" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-ipv6-out" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-teredo-in" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="corenet-teredo-out" Scope="KB" Source Role="SecurityandNetwork"
FirewallRule Id="bitssvc-in-tcp" Scope="KB" Source Role="BITSPeerCaching"

FirewallRule Id="bitssvc-out-tcp" Scope="KB" Source Role="BITSPeerCaching"
FirewallRule Id="bitssvc-rpc-in-tcp" Scope="KB" Source Role="BITSPeerCaching"
FirewallRule Id="bitssvc-rpcss-in-tcp" Scope="KB" Source Role="BITSPeerCaching"
FirewallRule Id="bitssvc-wsd-in-udp" Scope="KB" Source Role="BITSPeerCaching"
FirewallRule Id="bitssvc-wsd-out-udp" Scope="KB" Source Role="BITSPeerCaching"
FirewallRule Id="ntfrs-ntfrssvc-in-tcp" Scope="KB" Source Role="FRS"
FirewallRule Id="ntfrs-ntfrssvc-rpcss-in-tcp" Scope="KB" Source Role="FRS"
FirewallRule Id="slsvc-in-tcp" Scope="KB" Source Role="KMS"
FirewallRule Id="msmqdssvc-in-tcp" Scope="KB" Source Role="MQDS"
FirewallRule Id="msmqdssvc-in-udp" Scope="KB" Source Role="MQDS"
FirewallRule Id="msmqdssvc-out-tcp" Scope="KB" Source Role="MQDS"
FirewallRule Id="msmqdssvc-out-udp" Scope="KB" Source Role="MQDS"
FirewallRule Id="msmq-pgm-in" Scope="KB" Source Role="MQMS"
FirewallRule Id="msmq-pgm-out" Scope="KB" Source Role="MQMS"
FirewallRule Id="microsoft-windows-peertopeerpnrp-pnrpsvc-udp-in" Scope="KB" Source Role="PNRP"
FirewallRule Id="remoteassistance-dcom-in-tcp-noscope" Scope="KB" Source Role="RemoteAssistance"
FirewallRule Id="remoteassistance-in-tcp-edgescope" Scope="KB" Source Role="RemoteAssistance"
FirewallRule Id="remoteassistance-out-tcp" Scope="KB" Source Role="RemoteAssistance"
FirewallRule Id="remoteassistance-raserver-in-tcp-noscope" Scope="KB" Source Role="RemoteAssistance"
FirewallRule Id="remoteassistance-raserver-out-tcp-noscope" Scope="KB" Source Role="RemoteAssistance"
FirewallRule Id="remoteassistance-ssdpsrv-in-udp" Scope="KB" Source Role="RemoteAssistance"
FirewallRule Id="remoteassistance-ssdpsrv-out-udp" Scope="KB" Source Role="RemoteAssistance"
FirewallRule Id="remoteassistance-upnp-out-tcp" Scope="KB" Source Role="RemoteAssistance"
FirewallRule Id="remoteassistance-upnphost-in-tcp" Scope="KB" Source Role="RemoteAssistance"
FirewallRule Id="remoteassistance-upnphost-out-tcp" Scope="KB" Source Role="RemoteAssistance"
FirewallRule Id="microsoft-windows-removablestoragemanagement-client-dcom-in" Scope="KB" Source Role="RSM"
FirewallRule Id="microsoft-windows-removablestoragemanagement-client-rpcss-tcp-in" Scope="KB" Source Role="RSM"
FirewallRule Id="microsoft-windows-removablestoragemanagement-server-dcom-in" Scope="KB" Source Role="RSM"
FirewallRule Id="microsoft-windows-removablestoragemanagement-server-rpcss-tcp-in" Scope="KB" Source Role="RSM"
FirewallRule Id="rvm-rpcss-in-tcp" Scope="KB" Source Role="SMfS-X32"Source Role="SMfS-X64"Source Role="RemoteAdminVDS"
FirewallRule Id="rvm-vds-in-tcp" Scope="KB" Source Role="SMfS-X32"Source Role="SMfS-X64"Source Role="RemoteAdminVDS"
FirewallRule Id="rvm-vdsldr-in-tcp" Scope="KB" Source Role="SMfS-X32"Source Role="SMfS-X64"Source Role="RemoteAdminVDS"
FirewallRule Id="microsoft-windows-certificateservices-ocspsvc-rpc-tcp-in" Scope="KB" Source Role="RemoteCertServerOCSPAdmin"
FirewallRule Id="microsoft-windows-onlinerevocationservices-ocspsvc-dcom-in" Scope="KB" Source Role="RemoteCertServerOCSPAdmin"
FirewallRule Id="microsoft-windows-onlinerevocationservices-ocspsvc-tcp-out" Scope="KB" Source Role="RemoteCertServerOCSPAdmin"
FirewallRule Id="remoteeventlogsvc-in-tcp" Scope="KB" Source Role="RemoteAdminEventLogSvc"
FirewallRule Id="remoteeventlogsvc-np-in-tcp" Scope="KB" Source Role="RemoteAdminEventLogSvc"
FirewallRule Id="remoteeventlogsvc-rpcss-in-tcp" Scope="KB" Source Role="RemoteAdminEventLogSvc"
FirewallRule Id="remotefwadmin-in-tcp" Scope="KB" Source Role="RemoteAdminFirewall"
FirewallRule Id="remotefwadmin-rpcss-in-tcp" Scope="KB" Source Role="RemoteAdminFirewall"
FirewallRule Id="nps-npssvc-in-dcom" Scope="KB" Source Role="RemoteNPSAdmin"
FirewallRule Id="nps-npssvc-in-rpc" Scope="KB" Source Role="RemoteNPSAdmin"

FirewallRule Id="remrras-in-dcom" Scope="KB" Source Role="RemoteAdminRRAS"
FirewallRule Id="remrras-in-rpc" Scope="KB" Source Role="RemoteAdminRRAS"
FirewallRule Id="remotetask-in-tcp" Scope="KB" Source Role="RemoteAdminSchedule"
FirewallRule Id="remotetask-rpcss-in-tcp" Scope="KB" Source Role="RemoteAdminSchedule"
FirewallRule Id="telnetserver-tlntadmn-dcom-in" Scope="KB" Source Role="RemoteAdminTelnet"
FirewallRule Id="telnetserver-tlntadmn-np-in" Scope="KB" Source Role="RemoteAdminTelnet"
FirewallRule Id="telnetserver-tlntadmn-rpc-in" Scope="KB" Source Role="RemoteAdminTelnet"
FirewallRule Id="telnetserver-tlntadmn-rpcss-epmap-in" Scope="KB" Source Role="RemoteAdminTelnet"
FirewallRule Id="iis-webserverrole-wmsvc-in-tcp" Scope="KB" Source Role="RemoteAdminWEB"
FirewallRule Id="wins-service-in-np" Scope="KB" Source Role="RemoteAdminWINS"
FirewallRule Id="wins-service-in-rpc" Scope="KB" Source Role="RemoteAdminWINS"
FirewallRule Id="wins-service-in-rpcss-epmap" Scope="KB" Source Role="RemoteAdminWINS"
FirewallRule Id="windowsserverbackup-wbengine-in-tcp-noscope" Scope="KB" Source Role="RemoteAdminWSBackup"
FirewallRule Id="windowsserverbackup-wbengine-rpcss-in-tcp-noscope" Scope="KB" Source Role="RemoteAdminWSBackup"
FirewallRule Id="dfsmgmt-dcom-in-tcp" Scope="KB" Source Role="RemoteDFSRAdmin"
FirewallRule Id="dfsmgmt-in-tcp" Scope="KB" Source Role="RemoteDFSRAdmin"
FirewallRule Id="dfsmgmt-smb-in-tcp" Scope="KB" Source Role="RemoteDFSRAdmin"
FirewallRule Id="dfsmgmt-wmi-in-tcp" Scope="KB" Source Role="RemoteDFSRAdmin"
FirewallRule Id="microsoft-windows-dhcp-clientsvc-rpc-tcp-in" Scope="KB" Source Role="RemoteDHCPAdmin"
FirewallRule Id="microsoft-windows-dhcp-clientsvc-rpcss-tcp-in" Scope="KB" Source Role="RemoteDHCPAdmin"
FirewallRule Id="dnssrv-rpc-tcp-in" Scope="KB" Source Role="RemoteDNSAdmin"
FirewallRule Id="dnssrv-rpcepmap-tcp-in" Scope="KB" Source Role="RemoteDNSAdmin"
FirewallRule Id="fsrm-remoteregistry-in (rpc)" Scope="KB" Source Role="FSRMRemoteAdmin"
FirewallRule Id="fsrm-rpcss-in (rpc-epmap)" Scope="KB" Source Role="FSRMRemoteAdmin"
FirewallRule Id="fsrm-srmreports-in (rpc)" Scope="KB" Source Role="FSRMRemoteAdmin"
FirewallRule Id="fsrm-srmsvc-in (rpc)" Scope="KB" Source Role="FSRMRemoteAdmin"
FirewallRule Id="fsrm-system-in (tcp-445)" Scope="KB" Source Role="FSRMRemoteAdmin"
FirewallRule Id="fsrm-task-scheduler-in (rpc)" Scope="KB" Source Role="FSRMRemoteAdmin"
FirewallRule Id="fsrm-wmi-async-in-tcp" Scope="KB" Source Role="FSRMRemoteAdmin"
FirewallRule Id="fsrm-wmi-winmgmt-in-tcp" Scope="KB" Source Role="FSRMRemoteAdmin"
FirewallRule Id="microsoft-windows-nfs-clientcore-remoteregistry-in" Scope="KB" Source Role="RemoteNFSAdmin"
FirewallRule Id="microsoft-windows-nfs-servercore-remoteregistry-in" Scope="KB" Source Role="RemoteNFSAdmin"
FirewallRule Id="networkloadbalancing-dcom-tcp-in" Scope="KB" Source Role="RemoteNLBAdmin"
FirewallRule Id="networkloadbalancing-icmpv4-du-in" Scope="KB" Source Role="RemoteNLBAdmin"
FirewallRule Id="networkloadbalancing-icmpv4-er-in" Scope="KB" Source Role="RemoteNLBAdmin"
FirewallRule Id="networkloadbalancing-icmpv4-er-out" Scope="KB" Source Role="RemoteNLBAdmin"
FirewallRule Id="networkloadbalancing-icmpv4-erq-in" Scope="KB" Source Role="RemoteNLBAdmin"
FirewallRule Id="networkloadbalancing-icmpv4-erq-out" Scope="KB" Source Role="RemoteNLBAdmin"
FirewallRule Id="networkloadbalancing-icmpv6-du-in" Scope="KB" Source Role="RemoteNLBAdmin"
FirewallRule Id="networkloadbalancing-icmpv6-er-in" Scope="KB" Source Role="RemoteNLBAdmin"
FirewallRule Id="networkloadbalancing-icmpv6-er-out" Scope="KB" Source Role="RemoteNLBAdmin"
FirewallRule Id="networkloadbalancing-icmpv6-erq-in" Scope="KB" Source Role="RemoteNLBAdmin"
FirewallRule Id="networkloadbalancing-icmpv6-erq-out" Scope="KB" Source Role="RemoteNLBAdmin"
FirewallRule Id="networkloadbalancing-rpcss-tcp-in" Scope="KB" Source Role="RemoteNLBAdmin"
FirewallRule Id="networkloadbalancing-winmgmt-tcp-in" Scope="KB" Source Role="RemoteNLBAdmin"
FirewallRule Id="remoteadmin-in-tcp" Scope="KB" Source Role="RemoteWindowsAdministration"
FirewallRule Id="remoteadmin-np-in-tcp" Scope="KB" Source Role="RemoteWindowsAdministration"
FirewallRule Id="remoteadmin-rpcss-in-tcp" Scope="KB" Source Role="RemoteWindowsAdministration"

FirewallRule Id="wmi-async-in-tcp" Scope="KB" Source Role="RemoteWMI"
FirewallRule Id="wmi-rpcss-in-tcp" Scope="KB" Source Role="RemoteWMI"
FirewallRule Id="wmi-winmgmt-in-tcp" Scope="KB" Source Role="RemoteWMI"
FirewallRule Id="wmi-winmgmt-out-tcp" Scope="KB" Source Role="RemoteWMI"
FirewallRule Id="termservice-in-tcp" Scope="KB" Source Role="TSRemoteAdmin"
FirewallRule Id="termservice-np-in-tcp" Scope="KB" Source Role="TSRemoteAdmin"
FirewallRule Id="termservice-rpcss-in-tcp" Scope="KB" Source Role="TSRemoteAdmin"
FirewallRule Id="termservice-wmi-dcom-in-tcp" Scope="KB" Source Role="TSRemoteAdmin"
FirewallRule Id="termservice-wmi-in-tcp" Scope="KB" Source Role="TSRemoteAdmin"
FirewallRule Id="termservice-wmi-out-tcp" Scope="KB" Source Role="TSRemoteAdmin"
FirewallRule Id="wsrmservice-dcom-in" Scope="KB" Source Role="WSRMRemote"
FirewallRule Id="wsrmservice-dcomclient-in" Scope="KB" Source Role="WSRMRemote"
FirewallRule Id="2e7435c1-4737-4194-a114-3cd8a82c3fa7" Scope="Auto" Source Service="MSSQLSERVER"
FirewallRule Id="38ea6962-7492-4023-97fb-7d3a249f63a2" Scope="Auto" Source Service="Server Administrator"
FirewallRule Id="cc7837f1-d1ed-4126-b9bb-bcab0917fdaf" Scope="Auto" Source Service="dcconnsvc"
FirewallRule Id="fa2ad23b-f164-415d-9239-b52b6bdccc50" Scope="Auto" Source Service="dcnetmon"
FirewallRule Id="aed4e7a1-6dba-4a75-ad19-71f84b720985" Scope="Auto" Source Service="MSSQLSERVER"
FirewallRule Id="e54f9c71-db3d-49e7-bc4d-babb289b0ee3" Scope="Auto" Source Service="Server Administrator"
RegistryPageCheckBox SMBPage CheckBox="1"LDAPage CheckBox="-1"OutboundPage CheckBox="3"OutboundDomainPage CheckBox="1"OutboundLocalPage CheckBox="1"InboundPage CheckBox="-1" DefaultAuditTemplate CheckBox="False"

Changes made by implementing the “Secure AFHCAN Server 2” template.

Local Security Policies:

Password Policy

Enforce password history	5 passwords remembered
Maximum password age	90 days
Minimum password age	0 days
Minimum password length	8 characters
Passwords must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled

Account Lockout Policy

Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

Audit Policy

Audit account logon events	Success, Failure

Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	No auditing
Audit system events	Success, Failure

Event Log Settings

Maximum application log size
2048 kilobytes

Maximum security log size
2048 kilobytes

Maximum system log size
2048 kilobytes

Restrict guest access to application log
Enabled

Restrict guest access to security log
Enabled

Restrict guest access to system log
Enabled

Retention method for application log
As Needed

Retention method for security log
As Needed

Retention method for system log
As Needed

Registry Changes made by running “RegSecChanges.Bat”

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application]

"File"=hex(2):43,00,3a,00,5c,00,6c,00,6f,00,67,00,73,00,5c,00,41,00,70,00,70,\

00,45,00,76,00,65,00,6e,00,74,00,2e,00,45,00,76,00,74,00,00,00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security]

"File"=hex(2):63,00,3a,00,5c,00,6c,00,6f,00,67,00,73,00,5c,00,53,00,65,00,63,\

00,45,00,76,00,65,00,6e,00,74,00,2e,00,45,00,76,00,74,00,00,00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\System]

"File"=hex(2):63,00,3a,00,5c,00,6c,00,6f,00,67,00,73,00,5c,00,53,00,79,00,73,\

00,45,00,76,00,65,00,6e,00,74,00,2e,00,45,00,76,00,74,00,00,00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems]

"Optional"=hex(7):00,00

"Posix"=-

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters]

“NoNameReleaseOnDemand”=dword:00000001

System32 modifications

Running the “C:\ATSDownloads\Batch Files\Server2008ACLChange.Bat” assigns Administrators to Take Ownership and Full Control of all files in the System32 folder structure.