

Software Procedure

SWP-0057 AFHCAN tConsult v4.4.1.0 Front End Server Build

Revision: 1

Effective Date: 7/14/2011

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
Material Requirements	2
Initialize Server	3
.Net Framework Installation	6
IIS Installation	7
Finalizing the OS Configurations	7
Installing Windows Applications	8
Configuring SNMP	8
Dell Management Software Installation	8
Security – Windows Update	9
Harden Server	9
Enabling MSDTC Services:	11

Purpose

The purpose of this document is to provide detailed steps for the building and configuration of a tConsult Telehealth server used as a front-end for the tConsult software which connects to a back-end SQL and IIS server.

Audience

This document is written for IT technicians and system administrators who are responsible for building, configuring or maintaining tConsult Servers. It is assumed readers are familiar with intermediate-level computer terms and concepts, as well as a basic working knowledge of the Windows 2003 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.

The boundaries of the tConsult software have expanded exponentially. SQL and IIS both compete with the tConsult Server service for resources. Splitting these services onto two separate host boxes should increase performance and reduce the amount of overhead.

This document provides detailed steps on building and configuration of an tConsult Front End Server with IIS 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. Documentation
 - Server configuration QA sheet
3. Miscellaneous – all may not be needed
 - LAN connection for server

WAN connectivity to core
CAT5 cables – regular, crossover
CAT5 female-female adapters

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.

For a five drive host server, create a single four-drive RAID5 container and establish the fifth drive as a hot spare. For a six drive host server, create a single five-drive RAID5 container and establish the sixth 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 2003 Server Initial Installation

Partition hard disks: Note: The sizes below reflect 146 Gb Hard Drives. Larger Hard Drives will allow for a 36 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

- Create C: partition – 36 Gbytes (36874)
- Create D: partition – 350 Gbytes (358537) 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 – 24 Gbytes (24576)
- Regional and Language Options – leave at default
- Name: “User”
- Organization: Use the organization name (e.g. “AFHCAN”)
- Product Key – enter key
- License - Per Server with (5) connections typically
- Computer Name: Enter appropriate name

Computer Name and Administrator Password:

- Name: Administrator / Password: “password”

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

Date & Time Settings

- 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.

Initial Logon

- Security Updates – Choose “Finish”

NOTE: These next steps will need to be completed for each administrator account as they log on for the first time

- “Manage your Server” window – check the “Don’t display this page at logon”
- Show My Computer on Desktop
- Adjust Tools / Folder Options / View in Explorer window

Recommendation: Uncheck “Hide protected operating system files”, click on “Apply” then “Apply to all folders”

Screen Resolution:

- Change screen resolution to 1024 X 768.
 - Set color depth as high as possible – preferably 32 bit.

Copy files to C:

- Copy “i386” folder files from W2K3 CD-ROM to C: drive
- Copy “ATS Downloads” folder from AFHCAN ATS Downloads CD-ROM

Log Files:

- Create “C:\Logs” folder

Device Manager:

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

Disk Management:

- Change DVD/CD-ROM drive assignment to R:
- Change the drive assignments so 2nd partition is D:
- Format D: drive – Format and change volume label to “Local Disk”
- Change the drive assignment so the 3rd partition is E:
- Format E: drive – Format and change volume label to “Local Disk”

Create/Modify Accounts:

- Change name of Administrator account. Use the OSBA#*** 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: P@ssw0rd

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
- Create AFHCANDirector1 account if server resides at AFHCAN
 - Password: password defined for this account
 - User **CANNOT** 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.

.Net Framework Installation

- Install .NET Framework 2 by double-clicking "C:\ATS Downloads\2.0 .Net Framework\dotnetfx2.exe"
- Install .NET Framework 3 by double-clicking "C:\ATS Downloads\3.0 .Net Framework\dotnetfx3.exe"

- 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

IIS Installation

- Browse to “C:\ATS Downloads\Registry and double-click on Setup.reg
- Browse to “C:\ATS Downloads\IIS Install and run the “installiis.bat” file
- Leave the default web site

Finalizing the OS Configurations

Install Optional Windows Components

- Uncheck “Accessories and Utilities”
- Leave Application Server checked
- Leave “Internet Explorer Enhanced Security Config...” checked
- “Management and Monitoring Tools” – click “Details”
 - Check “Simple Network Management Protocol”
- Check “Security Configuration Wizard”
- Uncheck “Update Root Certificates”
- Reboot server
- Within “System Properties”, enable “Remote Desktop”
- Apply Microsoft “WindowsServer2003-SP2”
- Reboot Server

Installing Windows Applications

Install Adobe Reader

Adobe Acrobat Reader - Run

“C:\ATSDownloads\Adobe\AdbeRdr1000_en_US.exe”. Accept all defaults

Delete any shortcut icons created on desktop

Configuring SNMP

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

Dell Management Software Installation

Install Dell OpenManage Server Administrator

Click on R:\SYSMGMT\srvadmin\windows\Setup.exe

Perform Custom install

Leave all selections at their default values and install

Restart the server

Note: tConsult Telehealth servers normally have IT Assistant installed. IT Assistant requires SQL and will install SQL Express as part of the installation process. It is a conscious decision to forego IT Assistant on a front-end tConsult Telehealth server.

Security – Windows Update

- Install Windows 2003 SP2
- Reboot Server
- Connect to Microsoft Windows Update site and download and install all security patches

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 Template and select Secure AFHCAN Server1.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 Analysis and select Open database
 - Name the database “Update”
 - Import Template – browse to and select C:\ATSDownloads\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

Review NIC settings for all NICs

On all NIC(s):

Ensure Firewall is turned on and the following exceptions are enabled:

- Port 80 TCP – http
- Port 443 TCP – https
- Remote Desktop - Port 3389 TCP

- Time Server - Port 123 UDP
- WCF - Port 6968 TCP
- MSDTC (Add Program: C:\Windows\System32\MSDTC.exe)

Security logging:

- Change log file location to C:\Logs\pfirewall.log

ICMP:

- Check "Allow incoming echo request"

General Tab:

- Ensure "Client for Microsoft Networks" is selected
- Ensure "File and Print Sharing for Microsoft Networks" Is selected
- Verify IP, SM, DG, DNS
- Disable any NICs that will not be connected to the network

System 32 Changes

- Run the "C:\ATS Downloads\Batch Files\ACLChange.Bat"

Change ACLs on partitions

C: Drive

Root (C:\)

- Remove Everyone, CREATOR OWNER, and Users groups

D: Drive

Root (D:\)

- Remove Everyone, CREATOR OWNER, and Users groups

E: Drive

Root (E:\)

- Remove Everyone, CREATOR OWNER, and Users groups

- Delete E:\Inetpub\AdminScripts folder

E:\Inetpub

- Add the IIS_WPG Group and give modify permissions
- Add the Web Applications Group and give modify permissions

E:\Inetpub\WWWRoot

- Remove the Internet Guest Account (IUSR)
- Remove the Users account
- Remove the Web Anonymous Users account

Indexing Service

- Turn off indexing service at the root of C:\

Right click on C: drive / Properties / General. Clear the checkmark for “Allow Indexing Service to index this disk”. When prompted – select option to apply changes to subfolders and files.

- Turn off indexing service at the root of D:\

When prompted – select option to apply changes to subfolders and files

- Turn off indexing service at the root of E:\

When prompted – select option to apply changes to subfolders and files.

Registry Changes:

- Run the C:\ATSDownloads\Registry\RegSecChanges.Reg

Enabling MSDTC Services:

Using Computer Management / Services, ensure the following five services are set to Automatic and Start each one:

- COM+ Event System
- COM+ System Application
- DCom Server Process Launcher
- Distributed Transaction Coordinator
- System Event Notification

User Accounts

- Delete the “Support...” account
- Disable the IUSR account
- Disable the IWAM account

Modify user’s Remote / Terminal Services settings

- Do the following for all users except AFHCANAdmin*** and OSBA

Remove ability to logon to Terminal Services

- Computer Management / User Properties / Terminal Services Profile.

Check the “Deny this use permission...” checkbox

- Under “Remote Control” tab, uncheck “Need User’s permission”
- Harden the AFHCANAdmin*** password
- Delete both Full Name and Description entries from all users

Group Accounts

- Within the IIS-WPG group, remove the IWAM user account

Disable Dump File Creation

- Disable System dump files

My Computer / Properties / Advanced / Startup and Recovery – Set “Write Debugging Information” at “(none)”

- Uncheck “Send an Administrative Alert”

Create/Set Pagefile Parameters

Go to System Properties / Advanced / Performance / Settings, then select Advanced tab / Virtual Memory

- On C: drive, create/set pagefile initial/max at 1024 MB
- On D: drive, create/set pagefile initial/max at 4096 MB

Do not restart your system at this time

Disable Application dump files

- Run drwtsn32.exe and uncheck everything but “Append to Existing Log File

Terminal Services

Administrative Tools / Terminal Services Configuration

RDP-TCP Properties

General Tab:

- Encryption Level: Client Compatible

Client Settings Tab:

- Uncheck “Use Connection Settings from User Settings”
- Uncheck “Connect Client Printers at Logon”
- Uncheck “Default to Main Client Printer”
- Under “Disable the Following”, check everything except “Drive

Mapping”

Sessions Tab:

- Check “Override User Settings”
- End a disconnected session in 30 minutes
- Limit active sessions length to 1 day
- Idle sessions Limit: 30 minutes

Network Adapter Tab

- Set maximum connections to 2

Server Settings

- Change Active Desktop to “Disable”

Configure MSDTC

Start / Programs / Administrative Tools / Component Services

Click the MSDTC tab of the My Computer Properties dialog and click the Security Configuration button.

Network DTC Access:

- Allow Remote Clients
- Allow Remote Administration

Transaction Manager Communication:

- Allow Inbound

- Allow Outbound
- No Authentication Required
- Enable Transaction Internet Protocol (TIP) Transactions

IIS

Web Sites – right-click and select Properties

Web Site Tab:

- Active log format – click Properties and change log file directory to

C:\Logs

- Advanced tab – check Cookie and Referer checkboxes

Directory Security Tab:

Authentication and access control – edit and Uncheck anonymous access – only Integrated Authentication allowed

Home Directory Tab:

Application Settings – click Configuration and remove all application extensions

Web Service Extensions

- Ensure ASP.NET v1.1.4322 is allowed
- Ensure ASP.NET v2.0.50727 is allowed
- Ensure ASP.NET v4.0.30319 is allowed
- Prohibit “Active Server pages”

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 the Desktop
 - Empty Recycle bin
 - Defrag the hard drives

End of procedure.