

ITS Forefront Management Server Infrastructure Build

Table of Contents

Infrastructure Architecture	2
Pre-requisites Setup.....	2
Firewall Rules	5
Forefront Client Security Installation.....	6
Database Server Setup.....	6
Collection, Reporting and Management Server Setup	7
Forefront Client Security Policy Setup	8
Resources	10

Infrastructure Architecture

We will be integrating FCS into our current SCCM architecture and the resulting infrastructure will consist of:

1. ITS-Manage hosting the VMs ITS-FCS and ITS-FCSDB
2. ITS-FCS hosting the FCS Management, Collection and Reporting Server roles
3. ITS-FCSDB hosting the FCS Collection and Reporting databases (SQL 2005)
4. ITS-SCCM01 hosting the SCCM Site Server, all SCCM roles and WSUS 3.1
5. ITS-SCCM02 hosting the SCCM Distribution Point
6. WES-SCOMDB01 hosting the WSUS, SCCM and SCOM databases (SQL 2005)

We will be building the first 3 as the other 3 already exist in our current environment. It will be a variation on the FCS five-server topology on Windows Server 2008 as we will not be deploying the FCS Distribution component. <http://technet.microsoft.com/en-us/library/cc901476.aspx>

A new campus-only subnet has been created for this implementation:
IP assignments for Forefront Infrastructure:

DRAC on ITS-Manage = 172.16.157.226
ITS-Manage NIC #1 = 172.16.157.227
ITS-Manage NIC #2 = 172.16.157.228
ITS-FCS = 172.16.157.229
ITS-FCSDB = 172.16.157.230

SM: 255.255.255.224
GW: 172.16.157.225

Pre-requisites Setup

<http://technet.microsoft.com/en-us/library/bb404274.aspx>

1. ITS-Manage – Physical Server
 - a. OS W2K8 Ent x64 SP2 w/ Hyper-V – RAID 6 w/ 1 hot spare, 50 GB for OS
2. ITS-FCSDB - One Hyper-V VM hosted on ITS-Manage - Combined: Collection database and reporting database
 - a. VM = 140 GB, 40 GB for OS and 100 GB for databases
 - b. OS W2K8 Ent x86 SP2 and latest security patches, 4 GB of RAM
 - c. Install .NET Framework 3.0 – Open Server Manager->Add Features in Windows Server 2008 in order to install .NET Framework 3.0 Features
 - d. SQL 2005 Ent x86 w/ SP3 - Min 100 GB HD Space
 - a. Install the following components: Database Services, Integration Services, and Workstation components
 - On the “Components to Install” dialog, click the “Advanced” button. On the “Feature Selection” dialog, change the installation path to install on a volume (E:\MSSQL2005\) with at least 100 GB free space.
 - Use in Windows Authentication mode and an Austin service account (Austin\its-ts-forefront). It is recommended that you use a domain user

- or network service account for the SQL Server and SQL Server Agent service accounts.
 - Check the SQL Server Agent service to start automatically.
 - If SQL is installed on C:\ and there is not at least 100GB free, In SQL Server Management Studio->Server Properties-> Database Settings->Change the default database location to a volume with at least 100 GB free or the subsequent FCS install will fail.
 - b. You are Required to run SQL Management Console with “Run as Administrator” on 2008 or the UAC will not allow login with Windows Authentication
3. ITS-FCS - One Hyper-V VM hosted on ITS-Manage - Combined: Management, collection, and reporting server
- a. VM = 50 GB
 - b. OS W2K8 Std x86 SP2 and latest security patches, 4 GB RAM
 - c. Install the IIS Web Server Role – How to install and how to configure SQL Server 2005 Reporting Services on a computer that is running Windows Server 2008 - <http://support.microsoft.com/kb/938245/>
 - a. In the Add Roles Wizard, make sure you install the following role services:
 - Static Content
 - Default Document
 - HTTP Redirection
 - Directory Browsing
 - ASP.NET
 - ISAPI Extension
 - ISAPI Filters
 - Windows Authentication
 - IIS Metabase
 - IIS 6 WMI
 - d. Install the Application Server Role – To allow techs MOM Operator Console to connect to the server
 - a. In the Add Roles Wizard, make sure you install the following role services:
 - Web Server (IIS) Support
 - COM+ Network Access
 - e. Install .NET Framework 3.0 – Open Server Manager->Add Features in Windows Server 2008 in order to install .NET Framework 3.0 Features
 - f. Group Policy Management Console (GPMC) with SP1 - <http://www.vista123.net/content/installing-gpmc-windows-server-2008-and-windows-vista-service-pack-1>
 - g. Microsoft Management Console (MMC) 3.0 (should already be installed w/ W2K8)
 - h. SQL 2005 Ent x86 w/ SP3 - [Installing the software prerequisites on the reporting server](#)
When installing SQL Server 2005, make sure to do the following:
 - Install only the Workstation components, Integration and Reporting Services **without configuring it**
 - Configure the reporting server and create the remote database. Because Reporting Services and the reporting database are not on the same server, your installation of SQL Server on the reporting server requires additional configuration. As part of that configuration, you must create the reporting database on the remote server.

On the management, collections, and reporting server, click Start, point to All Programs, point to Microsoft SQL Server 2005, point to Configuration Tools, and click SQL Server Surface Area Configuration.

- 1) On the SQL Server 2005 Surface Area Configuration page, click Surface Area Configuration for Services and Connections.
- 2) In the Surface Area Configuration for Services and Connections dialog box, select Service under the Reporting Services component, and then verify that it is running. Click OK.
- 3) Click Surface Area Configuration for Features.
- 4) In the Surface Area Configuration for Features dialog box, select Scheduled Events and Report Delivery under the Reporting Services component, and then verify that it is enabled.
- 5) Select Web Service and HTTP Access under the Reporting Services component, and then verify that it is enabled.
 - a. ***NOTE:** Because you have not yet configured Reporting Services, you cannot verify that Windows Integrated Security is enabled.
- 6) Click OK, and then close the SQL Server 2005 Surface Area Configuration page.
- 7) Click Start, point to All Programs, point to Microsoft SQL Server 2005, point to Configuration Tools, and then click Reporting Services Configuration.
- 8) Select the current server in the Machine Name box, and then click Connect.
- 9) On the Report Services Configuration page, click Report Server Virtual Directory.
- 10) Next to the Name box, click New.
- 11) In the Create a New Virtual Directory, ensure that the Web site is Default Web Site, verify the default value ReportServer is entered, and then click OK.
- 12) Click Report Manager Virtual Directory.
- 13) Next to the Name box, click New.
- 14) In the Create a New Virtual Directory, make sure the Web site is Default Web Site, verify the default value Reports is entered, and then click OK.
- 15) Click Web Service Identity.
- 16) In the Report Server and the Report Manager boxes, select DefaultAppPool. Click Apply.
 - a. ***NOTE:** For W2K8 IIS 7, use Classic .NET AppPool
- 17) Click Database Setup.
- 18) In the Server Name box, enter the reporting database server, and then click Connect. You must have permission to create a database and configure roles on that server. The Reporting Services Configuration tool will use your credentials to create the database. For a default instance, specify the server by either (a) the server's machine name only (no \\ or \), or (b) the server machine's IP address only (again, no \\ or \).
 - a. Important: For this step to succeed, you may need to disable the firewall on the reporting database server.
- 19) In the SQL Server Connection dialog box, click OK. Do not change the Credentials Type.
- 20) Next to Database Name, click New.

- 21) In the SQL Server Connection dialog box, keep the default values. Click OK.
- 22) In the Credentials Type box, select Windows Credentials. This is required for this version of Client Security.
- 23) In the Account Name and Password boxes, enter the domain user account and password that you want to use as the service account.
- 24) Click Apply.
- 25) In the SQL Server Connection dialog box, click OK. Do not change the Credentials Type.
- 26) Configure other settings as needed, and then verify the installation. For more information, see “How to: Verify a Reporting Services Installation” (<http://go.microsoft.com/fwlink/?LinkId=85560>).
- 27) Add the reporting server site to the Local intranet zone in Internet Explorer. In Internet Explorer, on the Tools menu, click Internet Options. On the Security tab, add the reporting server site to the Local intranet zone.
- 28) Initialize the Report Server
- 29) Disable Anonymous and Enable Windows Authentication in IIS 7 - <http://www.iis.net/ConfigReference/system.webServer/security/authentication/anonymousAuthentication>
- 30) Verify the Reporting Services Installation - <http://msdn.microsoft.com/en-us/library/ms143773.aspx>
- 31) Configure a Report Server for Local Administration on Windows Vista and Windows Server 2008 - <http://msdn.microsoft.com/en-us/library/bb630430.aspx>
- 32) Add the database server (its-fcsdb) to the Local Intranet zone in IE - <http://technet.microsoft.com/en-us/library/bb418961.aspx>

Firewall Rules

1. ITS-FCS
 - a. Allow MOM client Agents to communicate with server on UDP and TCP port 1270
 - b. Allow techs MOM Console to communicate with server on TCP Dynamic RPC
 - c. Allow COM+ Network Access (DCOM-In) on TCP 135 (techs MOM Console)
 - d. Allow File and Printer Sharing (Echo Request – ICMPv4-In and ICMPv6-In)
 - e. Remote Desktop (TCP-In) enabled and scoped
 - f. Core Networking Group rules enabled by default installation
 - g. WWWS (HTTPS Traffic-In) and (HTTP Traffic-In) enabled by adding Web Server Role
 - h. Network Discovery Group rules enabled by default installation
2. ITS-FCSDB
 - a. Allow SQL connection from ITS-FCS only to server on TCP 1433 (FCS Dashboard)
 - b. Allow HTTP connection from ITS-FCS only to server on port 80 (FCS Dashboard)
 - c. Allow File and Printer Sharing (Echo Request – ICMPv4-In and ICMPv6-In)
 - d. Remote Desktop (TCP-In) enabled and scoped
 - e. Core Networking rules enabled by default installation
 - f. Network Discovery Group rules enabled by default installation

Forefront Client Security Installation

<http://technet.microsoft.com/en-us/library/bb404252.aspx>

Retrieve and run "SW_CD_NTRL_Forefront_Client_Security_English_1_X13-62435.exe" from site-licensed share as Administrator to extract files to \\its-manage\e\$\ Forefront Client Security.

***NOTE:** *Install all forefront components using the service account, not an individual's account!!! Log onto the server as the service account and run the installation.*

Database Server Setup

On FCSDDB, install the Collection Database, Reporting Server and Reporting Database components. Before installing Client Security on ITS-FCS, the databases need to be configured on ITS-FCSDDB:

1. Browse to \\its-manage\e\$\Forefront Client Security\Server\
2. Right click and run ServerSetup.exe as Administrator to start install
 - a) Enter Name = ITS, Organization = UT Austin
 - b) Accept Terms
3. Select the Collection Database, Reporting Server and Reporting Database components
4. Collection Server
 - a) Name = ITS-FCS
 - b) Management Group Name = ForefrontClientSecurity
 - c) DAS account = Austin\its-ts-forefront
5. Collection Database
 - a) Name = ITS-FCSDDB
 - b) Leave "Re-use the DAS account for the reporting account" checked
6. Reporting Database
 - a) Name = ITS-FCSDDB - (db size set to 50 GB)
 - b) Leave "Re-use the DTS account for the reporting account" checked
7. Reporting Server
 - a) Name = ITS-FCS
 - b) Accept default Report Server and Report Manager URLs
8. Action Account
 - a) Accept Default "Action Account" = DAS account
9. Install to e:\FCS (new folder) - ***NOTE:** *We had to temporarily disable the Firewall on ITS-FCS to allow the install on ITS-FCSDDB to contact ITS-FCS, we were unable to determine the proper exceptions to manually configure*
10. Click Next to Install (this will take a while) and when it's done, Close
11. Configure Database Server ITS-FCSDDB
 - a) Configure the number of days to retain data in the SystemCenterReporting table.
 - i) Modify stored procedure, run the following command
 - ii) `exec p_updategroomdays 'TableName', DaysToRetainData`
 - iii) <http://support.microsoft.com/kb/887016/> for more info and which tables to run on
12. Verify All Settings in the following document are correct: <http://technet.microsoft.com/en-us/library/bb404260.aspx>
13. Verify the installation: <http://technet.microsoft.com/en-us/library/bb404209.aspx>

Collection, Reporting and Management Server Setup

On the FCS Server, install all FCS Management Infrastructure components with the exception of the Distribution Server component:

1. Browse to \\its-manage\efs\Forefront Client Security\Server\
2. Right click and run ServerSetup.exe as Administrator to start install
3. Enter Name = ITS, Organization = UT Austin
4. Accept Terms
5. Select only Management Server and Collection Server. Click OK when you get a prompt that this is an unsupported configuration.
6. Collection Server
 - a. Name = ITS-FCS
 - b. Management Group Name = ForefrontClientSecurity
 - c. DAS account = Austin\its-ts-forefront
7. Collection Database
 - a. Name = ITS-FCSDB
 - b. Leave "Re-use the DAS account for the reporting account" checked
8. Reporting Database
 - a. Name = ITS-FCSDB
 - b. Leave "Re-use the DTS account for the reporting account" checked
9. Reporting Server
 - a. Name = ITS-FCS
 - b. Accept default Report Server and Report Manager URLs
10. Action Account
 - a. Accept Default "Action Account" = DAS account
11. Install Location
 - a. Leave default location
12. Click Next to Install (this will take a while) and when it's done, Close (if you get an error on the MOM section, install .NET Framework 1.1 Redistributable, then retry)
13. Install SP-1 for Client Security
14. Open Microsoft Forefront Client Security (this is the client) pop-up in the system tray
15. After a few minutes the FCS client should get the latest definitions from WSUS or you can click the chevron next to the Help Question mark button and choose "Check for Updates"
16. Install update to ForeFront client (not through client UI, but through WindowsUpdate agent)
run wuauctl /detectnow
17. Click on the Home button and verify the definitions are up to date and Close
18. Open the Microsoft Forefront Client Security Console (Run as Administrator) to configure the FCS Server
19. Click Next
20. Enter the same information as when you ran the install above and complete the configuration wizard
21. The console will (Finally) Open
22. Go to Local Users and Groups and add the group with your server administrators in it to the following two groups: Distributed COM Users and MOM Administrators (this is for access to the MOM Administrator and Operator Consoles. <http://technet.microsoft.com/en-us/library/bb418908.aspx>)

Forefront Client Security Policy Setup

***NOTE:** Any FCS policy deployed through FCS Policy Management tab of the FCS Console **MUST** be higher (i.e. #1) in the GPO link order than the disable network scan policy or the settings in the disable network scan policy will be overwritten when the GPOs are applied.

1. Forefront Client Security Disable Network Scanning Policy: ITS - FCS - Disable Network Scan
 - Disable Network Scan. Enabled - <http://support.microsoft.com/kb/971026/>
2. Forefront Client Security Default Policy: ITS - FCS - Default Policy
 - Allow non-administrators access to console. Enabled
 - Apply settings for Forefront controlled by Group Policy. Enabled
 - Check for updates before scans. Enabled
 - Configure purge of quarantined files Enabled
 - Days to delay before deletion or 0 to not delete: 5
 - Configure quick scan multiple times a day. Enabled
 - Perform a quick scan every: Turn off multiple quick scans
 - Configure scheduled scans. Enabled
 - Scheduled scan day: Daily
 - Scheduled scan time: 12:00 AM
 - Scheduled scan type: Full scan
 - Forefront: Configure signature update interval. Enabled
 - Check for updates every: 6 hours
 - Check Microsoft Update for definitions if WSUS is not available. Enabled - <http://technet.microsoft.com/en-us/library/bb418851.aspx>
 - Configure SpyNet reporting Enabled
 - Select the level of SpyNet reporting: No SpyNet Reporting
 - Prevent User from adding exclusions. Enabled
 - Prompt user on unclassified software. Disabled
 - Turn off all real-time protection. Disabled
 - Turn off heuristics. Disabled
 - Turn off scanning of archive files. Disabled
 - Turn off spyware protection. Disabled
 - Turn off virus protection. Disabled
3. In the Default Policy, exclude recommended files, directories and extensions:

Files and Folders:

%PROGRAMFILES%\System Center Operations Manager 2007\Health Service State\Health Service Store
%ALLUSERSPROFILE%\Application Data\Microsoft\Microsoft Operations Manager\
%SystemDrive%\inetpub\temp\IIS Temporary Compressed Files
%SystemRoot%\iis temporary compressed files
%systemroot%\System32\DHCP
%systemroot%\system32\dns
%SystemRoot%\system32\inetpub
%SystemRoot%\System32\Inetsrv
%systemroot%\system32\wins
%systemroot%\sysvol
%systemroot%\sysvol\domain\DO_NOT_REMOVE_NtFrs_PreInstall_Directory

Forefront Management Server Infrastructure Build

%systemroot%\sysvol\staging
%systemroot%\sysvol\staging areas
%systemroot%\sysvol\sysvol
%windir%\ntds\Ntds.dit
%windir%\ntds\Ntds.pat
%windir%\ntfrs
%windir%\SoftwareDistribution\Datastore\Logs\Edbres00001.jrs
%windir%\SoftwareDistribution\Datastore\Logs\Edbres00002.jrs

Extensions:

.bak	.ldf	.pqf	.vfd
.cab	.log	.pqf0	.vhc
.chk	.mdb	.pqf1	.vhd
.edb	.mdf	.pst	.vsv
.iso	.ndf	.sdb	.vud
.ldb	.pol	.trn	.wkf

Resources

Microsoft Forefront Client Security - Verifying your system requirements

<http://technet.microsoft.com/en-us/library/bb404245.aspx>

Supported configurations for using WSUS to distribute Forefront Client Security Definition updates within SCCM 2007

<http://support.microsoft.com/default.aspx/kb/958491>

Deploying Microsoft Windows Server Update Services 3.0 SP1 - Appendix B: Configure Remote SQL

<http://www.microsoft.com/downloads/details.aspx?FamilyID=208e93d1-e1cd-4f38-ad1e-d993e05657c9&DisplayLang=en>

Deploying FCS definition updates with a shared System Center Configuration Manager WSUS infrastructure

<http://technet.microsoft.com/en-us/library/dd185652.aspx>

Deploying Forefront Client Security Using SCCM 2007 - Step-By-Step

<http://blogs.microsoft.co.il/blogs/yanivf/archive/2008/02/20/deploying-forefront-client-security-using-sccm-2007-step-by-step.aspx>

How to install Forefront client on a non-domain (Workgroup) computer

<http://social.technet.microsoft.com/Forums/en-US/Forefrontclientsetup/thread/b7bf4ebe-187c-482d-b513-7896c6aa841d>

Configuring fallback for updates

<http://technet.microsoft.com/en-us/library/bb418851.aspx>

WSUS settings to get Forefront Client Security to Rock!

<http://itbloggen.se/cs/blogs/blom/archive/2008/08/07/wsus-settings-to-get-forefront-client-security-to-rock.aspx>

Clinic 6079: Managing and Troubleshooting Operations in Microsoft® Forefront™ Client Security

<https://www.microsoftlearning.com/eLearning/courseDetail.aspx?courseId=76457>

Working with reports, alerts, and events

<http://technet.microsoft.com/en-us/library/bb418770.aspx>

Virus scanning recommendations for computers that are running Windows Server 2008 R2, Windows Server 2008, Windows Server 2003, Windows 2000, Windows XP, or Windows Vista

<http://support.microsoft.com/kb/822158>

Recommended Forefront Client Security file and folder exclusions for Microsoft products

<http://support.microsoft.com/kb/943556>

Antivirus Exclusions in MOM 2005 and OpsMgr 2007

<http://blogs.technet.com/kevinholman/archive/2007/12/12/antivirus-exclusions-for-mom-and-opsmgr.aspx>