Centricity Business Infrastructure
Part 1: Overview
Derek Allen, GE Healthcare
CHUG/CTC 2014

Imagination at work.
Presenter

Derek Allen, Network Engineer

National Product Release Team (NPRT)
Clinical Business Solutions
GE Healthcare IT

derek.allen@ge.com
Agenda

Definitions/Terminology
Components & Traffic Flows
Server Installation Overview
Component Redundancy
Load Balancing
Encryption
Desktop & Server Virtualization
Questions
Definitions/Terminology
Definitions/Terminology

Centricity Business - Character Cell
• Original application for ASCII Terminals or terminal emulation software

Centricity Business - Advanced Web
• Web-based GUI application built upon Character Cell
Definitions/Terminology

Centricity Framework

• An application “framework” is designed to allow multiple applications to be integrated into the same environment, providing a consistent “look and feel” and sharing the same database of application users & application settings

Products that can use the Centricity Framework

• Centricity Business - Advanced Web
• Centricity Business - Enterprise Task Manager (ETM)
• Centricity Patient Online / Centricity Referring Practice Online (POL/RPO)
• Centricity Enterprise
• Centricity Imaging
• Allscripts™ TouchWorks™
Components & Traffic Flows
Character Cell
Components – Character Cell

Client Device (Windows PC)
• IDXterm (terminal emulation) used to access the application

Patient Database Server(s)
• Caché Database containing patient data
• OpenVMS, HP-UX, AIX, Microsoft Windows running Ensemble/Caché
Traffic Flows – Character Cell

1. TELNET (PC to Caché)
Components & Traffic Flows
Advanced Web
Components – Advanced Web

Client Device (Windows PC)
- Internet Explorer (web browser) used to access the application

Patient Database Server(s)
- Caché Database containing patient data
- OpenVMS, HP-UX, AIX, Microsoft Windows running Ensemble/Caché

Web Server(s)
- Presentation tier for client device, containing screen layouts, etc.
- Microsoft Windows running Internet Information Services (IIS)

Framework Database Server(s)
- SQL Database containing user information, configuration settings, etc.
- Microsoft Windows running SQL
Traffic Flows – Advanced Web

1. HTTP (PC to Web)
2. SQL (Web to CF DB)
3. CSVR (PC to Caché)
4. TELNET (PC to Caché)
5. CSP HTTP (PC to Web)
6. CSP (Web to Caché)
Traffic Flows – Advanced Web

1. Client Device connects to Web Server using IE
   • Web Server provides initial login screen
   • Web connection is maintained for loading controls, screen layout information, etc.

2. Web server connects to Framework Database Server
   • Framework Database Server verifies login information
   • User configuration information sent back through Web Server to Client Device

3 & 4. Client Device connects to Patient Database Server
   • Direct TELNET & CSVR connections for patient data

5. Client Device creates CSP connection to Web Server
   • Web Server is running Caché Server Pages (CSP) Gateway software

6. Web Server connects to Patient Database Server
   • Web Server forwards CSP queries to Patient Database Server which responds back through the Web Server to the Client Device
Server Installation Overview
Server Installation Overview

Framework Database Server(s)
• SQL Database containing user information, configuration settings, etc.
• Microsoft Windows running SQL 2012, 2008 R2, 2008, or 2005

Installation/Configuration
• Customer typically installs operating system (Microsoft Windows)
• Customer or GE Healthcare can install Microsoft SQL Server
• Can alternately use customer’s existing SQL environment/servers
• Install requires local SQL account with sysadmin (sa) rights
• After install, application requires local SQL account with sa or dbo rights
Server Installation Overview

Web Server(s)
- Presentation tier for client device, containing screen layouts, etc.
- Windows Server 2008 R2 (64-bit), 2008 (32-bit), or 2003
- Internet Information Services (IIS)

Installation/Configuration
- Customer typically installs operating system (Microsoft Windows)
- Customer or GE Healthcare can install IIS, .NET, Java RTE
- GE installation requires local admin rights on the server
- GE installs CSP Gateway software (configured to point at Caché Server)
- GE installs JDBC drivers (to connect to Framework Database Server)
- GE installs/tests Centricity Framework & Centricity Business software
- GE modifies IIS settings (eTags, Thread Pools)
- GE configures/tests idxwfping.asp (load balancer health monitor)
Server Installation Overview

Patient Database Server(s)
• Caché Database containing patient data
• OpenVMS, HP-UX, AIX, Microsoft Windows running Ensemble/Caché

Installation/Configuration
• Performed by Caché resources within GE Healthcare’s NPRT Team
Server Installation Overview

Client Device (Windows PC)
• Internet Explorer (IE) web browser used to access the application

Installation/Configuration
• IE objects & controls are installed via Desktop Component Kit (DCK)
  • Can automatically push DCK to client devices
  • Can manually install DCK on client devices
  • If DCK is not installed on a client device, objects & controls will automatically be downloaded the first time a Web Server is accessed, but the user needs admin rights on the client device
Component Redundancy
Aspects of Redundancy

High Availability
• Provides multiple components to eliminate single point of failure
• If a single component fails (hardware, software, etc) the system still works

Load Distribution
• Needed when a single component is unable to handle entire system load
• Distributes traffic & load across multiple components
Examples of Redundancy

Active-Passive Cluster

- Provides High Availability but not Load Distribution
- Two nodes are configured in a cluster, but only one node is active
- Active node must be able to handle entire load
- If active node fails, all traffic is redirected to the other node
Examples of Redundancy

Round Robin DNS
- Provides Load Distribution but not High Availability
- Single DNS hostname configured with multiple node IP addresses
- When accessing DNS hostname, traffic is distributed across all nodes
- If a node fails, traffic continues to be sent to it
Examples of Redundancy

Hardware Load Balancing (with n+1 nodes)

- Provides High Availability and Load Distribution
- Load Balancer configured to distribute traffic across all nodes
- Load Balancer monitors status of each node
- If a node fails, Load Balancer redirects traffic to the other nodes
Redundancy – Framework Database Server(s)

High Availability can be provided by MS SQL Clustering

Stand-alone MS SQL Server
• Single server
• Lower costs
• OK for test/training/demo environments

MS SQL Clustered System
• Two servers in Active-Passive configuration
• High Availability with failover
• Central storage
• Higher costs and more administration
• Recommended for live/production environment
• Load Distribution not needed for Centricity Business low application load
Redundancy – Framework Database Server(s)

High Availability can be provided by VMware

Stand-alone VMware virtual SQL Server
• VMware dynamically handles failures
• For most types of failures, failover is immediate (except for OS corruption)

Can also configure MS SQL Cluster on VMware
Redundancy – Web Server(s)

High Availability and Load Distribution can be provided by hardware load balancers

• Client device connects to a Virtual IP (VIP) on the load balancer
• Load balancer continuously monitors status of load balanced servers
• Load balancer distributes traffic from client devices across all servers
• Include an additional server (n+1) so remaining servers can handle load if one server fails

Supported load balancing platforms

• F5: BIG-IP Local Traffic Manager (LTM) Switch
• A10: AX Series Application Delivery Controller
• Cisco: 11500 Series Content Services Switch (CSS)
Redundancy – Patient Database Server(s)

Multiple options for High Availability and/or Load Distribution:

- VMS cluster load balancing
- AIX HACMP (Active/Passive - High Availability only)
- Hardware load balancing

Note: Centricity Business has specific load balancing requirements for the CSVR & TELNET connections to the Patient Database Server(s)
Load Balancing
Load Balancing

High Availability and Load Distribution can be provided by hardware load balancers

- Client device connects to a Virtual IP (VIP) on the load balancer
- Load balancer continuously monitors status of load balanced servers
- Load balancer distributes traffic from client devices across all servers
- Include an additional server (n+1) so remaining servers can handle load if one server fails

Supported load balancing platforms

- F5: BIG-IP Local Traffic Manager (LTM) Switch
- A10: AX Series Application Delivery Controller
- Cisco: 11500 Series Content Services Switch (CSS)
Traffic Flows – Advanced Web

1. HTTP (PC to Web)
2. SQL (Web to CF DB)
3. CSVR (PC to Caché)
4. TELNET (PC to Caché)
5. CSP HTTP (PC to Web)
6. CSP (Web to Caché)
Traffic Flows – Load Balanced

1a. HTTP (PC to LB)
1b. HTTP (LB to Web)
2. SQL (Web to CF DB)
3. CSVR (PC to Caché)
4. TELNET (PC to Caché)
5a. CSP HTTP (PC to LB)
5b. CSP HTTP (LB to Web)
6. CSP (Web to Caché)
Load Balancing – Health Monitors

Servers are monitored to determine if ready to accept traffic

Sample monitors/keepalives

1. Ping (ICMP) – check if server is up and on the network
Load Balancing – Health Monitors

Servers are monitored to determine if ready to accept traffic

Sample monitors/keepalives

2. Open a specific TCP port – check if server is listening on that port
Load Balancing – Health Monitors

Servers are monitored to determine if ready to accept traffic

Sample monitors/keepalives

3. Open port 80 and send HTTP GET – check if web server responding
Load Balancing – Health Monitors

Servers are monitored to determine if ready to accept traffic

Sample monitors/keepalives

4. HTTP GET /idxwfping.asp – check for specific response from application
Load Balancing – Persistence/Stickiness

Ensures traffic from each client device is sent to same server
• Effectively “locks in” a user’s traffic to a particular server
• Required if application user/session state is maintained on the server

Common Persistence methods:
• Client Device IP (aka Source Address)
• HTTP Cookie

Persistence can be configured across multiple connections
• Example: To ensure both CSVR & TELNET connections to same server

Not required for core Centricity Business application web traffic
Encryption
Encryption

Encryption of application data “in-transit” across the network
• Purpose is to secure data so if it is intercepted, it cannot be read
• Main concerns: Protected Health Information (PHI), usernames/passwords
• Required by HIPAA if PHI is traversing an “open” (unsecured) network, such as the Internet, or any network that may have unauthorized users
• May also be required by an organization’s internal policies

Note: Simply encrypting Web Server traffic via HTTPS won’t secure all PHI. Encryption solutions for PHI must also address CSVR & TELNET connections.
Encryption

Raw network data showing login - without encryption:
Encryption

Raw network data showing login - with encryption:

```
0000 00 17 a4 3a f4 50 00 01 d7 4a 97 43 08 00 45 00 ...:"F...J.C..E.
0010 01 12 c5 b7 40 00 ff 06 a2 ff 0a 02 78 0b 0a 02 ...6...27....
0020 7a 1f 01 eb 1b 0a 99 7e c4 7f ae 28 70 1c 6c 50 18 ...z.........t..P..P.
0030 32 da 99 73 00 00 17 03 00 01 e5 04 5a 16 ef 0d ...Z.....2V...
0040 03 16 9e 1b 01 81 9a ac a8 cc 52 45 ee 13 b0 73 ...e.......E......
0050 51 da 27 e4 28 a6 4a 02 fa 59 bd 13 9b dd d0 b4 q"dC...Y........
0060 7e c2 73 07 6e fb 51 02 cb 43 e2 45 98 fd ec a5 ~s.n.q..E....
0070 31 23 f8 4c 3a 7a 05 51 95 8a 0d ab 18 40 46 b6 1#.
0080 5d f1 89 1f f2 8d 32 cb 00 e6 81 a6 0d 9f f0 24 ......2.........$
0090 94 b3 c8 a7 84 6b b7 25 e1 f8 8f 8e 9b c2 44 40 ....k..k.....d@
00a0 13 06 6f 2c f4 39 bd 25 d6 d3 e3 eb 8d 96 30 de ...o.9.8.....]
00b0 89 5c 01 0d 7b 3d 32 32 84 93 15 2e 9a bd 3c 51 ...v>.v>2........q
00c0 b6 35 11 13 30 6e 92 6e 02 9f 29 3a a2 0a 60 6b ..j.p.f...k....
00d0 82 35 f8 52 9a 3c 3c 29 a7 3d 30 7e bd 3a 52 68 ...<.q<.><<..>
00e0 3e c7 13 3b 3d 9c 60 fc 18 f8 44 88 81 c2 11 .:.;:.;m....a@
00f0 5c 69 42 6c 05 97 3b e2 40 25 09 bf 5a 93 34 39 \B\...6%....4Y
0100 63 7b 27 6e 0d 8d f2 ce 4d 41 51 64 b4 72 a2 30 c{/./.6..M..d.r.6
0110 63 86 61 0c c7 5a 4b db 82 95 b9 42 75 76 b5 ...a. u. ....Bux.
0120 00 00 00 00
```

Frame 424: 292 bytes on wire (2336 bits), 292 bytes captured (2336 bits)
Ethernet II, Src: 00:17:a3:a3:00:02, Dst: 00:17:a3:3a:34:50
Internet Protocol, Src: 10.9.100.11, Dst: 10.9.222.31
Transmission Control Protocol, Src Port: 443, Dst Port: 4249
SSLv3 Record Layer: Application Data Protocol: http
Content Type: Application Data (23)
Version: SSL 3.0 (0x0300)
Length: 229
Encrypted Application Data: 045a56efed0518919b4818ac08cc62a5ee13b0f351da27...
Encryption – Advanced Web

Encryption can be enabled/disabled per Framework “System”

- Requires F5 BIG-IP or A10 AX Series
- Requires SSL Certificate from trusted Certificate Authority (CA)
- Name on SSL Certificate must match the name in the URL used to access the application (e.g. “cbweb.mydomain.com”)
Traffic Flows – Load Balanced

1a. HTTP (PC to LB)
1b. HTTP (LB to Web)
2. SQL (Web to CF DB)
3. CSVR (PC to Caché)
4. TELNET (PC to Caché)
5a. CSP HTTP (PC to LB)
5b. CSP HTTP (LB to Web)
6. CSP (Web to Caché)
Traffic Flows – Encrypted

1a. HTTPS (PC to F5/A10)
1b. HTTP (F5/A10 to Web)
2. SQL (Web to CF DB)
3a. Encrypted CSVR (PC to F5/A10)
3b. Unencrypted CSVR (F5/A10 to Caché)
4a. Encrypted TELNET (PC to F5/A10)
4b. Unencrypted TELNET (F5/A10 to Caché)
5a. CSP HTTPS (PC to F5/A10)
5b. CSP HTTP (F5/A10 to Web)
6. CSP (Web to Caché)
Traffic Flows – Encrypted

1a. Client Device connects to F5/A10 VIP via HTTPS using IE
   • Web Server provides initial login screen
   • Web connection is maintained for loading controls, screen layout information, etc.
   • Connection via HTTPS instead of HTTP
   • If desired, F5/A10 VIP can automatically redirect HTTP requests to HTTPS

1b. F5/A10 connects to Web Server via HTTP
   • Responses from Web Server are sent back through F5/A10 to Client Device

2. Web Server connects to Framework Database Server
   • Framework Database Server verifies login information
   • User configuration information sent back through Web Server via F5/A10 to Client Device
   • User configuration information sent to Client Device includes encryption settings
Traffic Flows – Encrypted

3a & 4a. Client Device connects to F5/A10 VIP
• Encrypted CSVR & TELNET connections to F5/A10

3b & 4b. F5/A10 connects to Patient Database Server
• Unencrypted TELNET & CSVR connections for patient data
• Responses from Patient Database Server are sent back through F5/A10 to Client Device

5a. Client Device sends CSP traffic via HTTPS to F5/A10 VIP

5b. F5/A10 sends CSP traffic via HTTP to Web Server
• Web Server is running Caché Server Pages (CSP) Gateway software
• Responses from Web Server are sent back through the F5/A10 to the Client Device

6. Web Server connects to Patient Database Server
• Web Server forwards CSP queries to Patient Database Server which responds back through the Web Server via the F5/A10 to the Client Device
Encryption – Character Cell

Current versions of IDXterm support encryption

SSH-based Encryption (Secure Shell)
- Requires SSH Server running on Patient Database Server
- Configure IDXterm to use SSH, connect to Patient Database Server

SSL-based Encryption (Secure Sockets Layer)
- Requires F5/A10 configured for Advanced Web encryption
- IDXterm can use existing F5/A10 TELNET VIP used by Advanced Web
- Configure IDXterm to use SSL, connect to F5/A10 TELNET VIP
- F5/A10 makes unencrypted connection to Patient Database Server
Traffic Flows – Character Cell

1. TELNET (PC to Caché)
Traffic Flows – Character Cell with SSH Encryption

1. Encrypted SSH (PC to Caché)
Traffic Flows – Character Cell with SSL Encryption

1a. Encrypted TELNET (PC to F5/A10)
1b. Unencrypted TELNET (F5/A10 to Caché)
Desktop & Server Virtualization
Desktop Virtualization

From Centricity Business System Environment Specifications (SES):

The use of Virtual Desktop technology replaces the traditional client desktop PC with a larger PC server, and multiple remote desktop display devices. The Centricity Business desktop client software is a standard Windows 32-bit .Net application.

While Centricity Business software may run under this environment, GEHC does not provide support for the environment itself. GEHC requires that the customer maintain at least one traditional desktop PC for each user interface to demonstrate any failures of the GEHC software.

It should be noted that the Web-based Centricity Business does, at times, make intense use of the desktop resources in the normal course of operation. This should be taken into account when determining Virtual Desktop sizing and load requirements.
Desktop Virtualization

From Centricity Business System Environment Specifications (SES):

Some examples of Virtual Desktop technologies that have been used with Centricity Business include:

- Terminal Server (Windows Server 2003 – 32-bit)
- Microsoft RDS (Windows Server 2008 R2)
- Citrix Presentation Server
- Leostream™ Connection Broker paired with VMware virtual machines
Server Virtualization

From Centricity Business System Environment Specifications (SES):

The use of VMware is supported for use with certain Centricity Business servers identified below. We have had success using the following versions:

- Virtual Infrastructure (version 3.0 and 3.5)
- vSphere (version 4.1, 5.0, and 5.1)

While Centricity Business software runs under this environment, GEHC does not provide support for the environment itself. The customer is expected to provide sufficient VMware expertise to properly configure, manage, and diagnose issues with VMware.

GEHC also requires that the customer maintain at least one physical server capable of temporarily replacing any virtual machine implemented in order to demonstrate a suspected Centricity Business issue if necessary.
Server Virtualization

From Centricity Business System Environment Specifications (SES):

Virtualization is supported with the following Centricity Servers. Please see the individual sections of this document for any restrictions:

• Centricity Business Web Servers
• Centricity Framework Servers
• APC/DRG Server
• Enterprise Index Server
• Healthcare Objects Server
• EDM Server
• TeleForm/WCO Server (with restrictions)
• Reporter Server
• Informatics Web Server (with restrictions)
• Credit Card Server (See important note in the Credit Card section of this document)
Questions
Portions of this presentation General Electric reserves the right to make changes in specifications and features, or discontinue the product or service described at any time, without notice or obligation. This does not constitute a representation or warranty or documentation regarding the product or service featured. Illustrations are provided for informational purposed, and your configuration may differ.

This information does not constitute legal, financial, coding, or regulatory advice in connection with the use of the product or service. Please consult your professional advisors for any such advice. Operation of GE Healthcare products should neither circumvent nor take precedence over required patient care, including human intervention of healthcare providers. GE Healthcare products and services do not code medical procedures. Accurate coding is the responsibility of the provider or billing professional.

GE, the GE Monogram, Centricity and Imagination at Work are trademarks of General Electric Company.

©2014 General Electric Company – All rights reserved.