

Configuration Manager 2012 Architecture

INFRONT CONSULTING GROUP | USA | Canada | Europe | Asia

**FOR HUMANA INC**

INFRONT CONSULTING GROUP

2013

© 2013 Infront Consulting Group. All rights reserved. INFRONT CONFIDENTIAL. The information contained in this document represents the current view of Infront Consulting Group on the issues discussed as of the date of publication and is subject to change at any time without notice to you. This document and its contents are provided AS IS without warranty of any kind, and should not be interpreted as an offer or commitment on the part of Infront, and Infront cannot guarantee the accuracy of any information presented. INFRONT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Infront Consulting Group.

Infront may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Infront, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies’ products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Infront. Infront cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

We will not knowingly provide advice that conflicts with local, regional, or international laws, however, it is your responsibility to confirm your implementation of our advice is in accordance with all applicable laws.

Change History and Reviewer Signoff

**Change History**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Changes |
| Feb 20, 2013 | James Mymryk | 1.0 | Initial Document Created |
| Feb 24, 2013 | James Mymryk | 1.1 | Updated Information additional Appendix |
| Feb 25, 2013 | James Mymryk | 1.2 | Work Estimates and minor corrections |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Reviewers**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version Approved | Reviewer | Position |
| Feb 25, 2012 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[Glossary of Key Terms 1](#_Toc349578011)

[Overview 3](#_Toc349578012)

[Humana Requirements 4](#_Toc349578013)

[Availability 4](#_Toc349578014)

[Features 4](#_Toc349578015)

[Migration 4](#_Toc349578016)

[Work from Home 5](#_Toc349578017)

[Security 5](#_Toc349578018)

[Growth 5](#_Toc349578019)

[Cross Domain Access 5](#_Toc349578020)

[Network Bandwidth and Server Infrastructure Efficiencies 6](#_Toc349578021)

[Size 6](#_Toc349578022)

[Integration with HP Server Deployment Solutions 6](#_Toc349578023)

[Architecture 7](#_Toc349578024)

[Proposed Architecture 1: Single Primary Site 7](#_Toc349578025)

[Recommended Architecture 2: CAS with 2 Primary Sites 7](#_Toc349578026)

[System Sizing 9](#_Toc349578027)

[SQL 9](#_Toc349578028)

[CAS SQL Instance 9](#_Toc349578029)

[Primary SQL Instances 9](#_Toc349578030)

[Site Servers 10](#_Toc349578031)

[CAS Site Server 10](#_Toc349578032)

[Primary Site Servers 10](#_Toc349578033)

[Role Servers 10](#_Toc349578034)

[NAS 10](#_Toc349578035)

[Backup 11](#_Toc349578036)

[Estimates for Planning and Deployment 12](#_Toc349578037)

[Test Environment - 15 days 12](#_Toc349578038)

[Deployment Plan, plus Build and test - 15 days 12](#_Toc349578039)

[Deploy and Migrate - 20 Days 12](#_Toc349578040)

[Scripting and Automation – 5 Days 12](#_Toc349578041)

[Appendix A: Survey Information 13](#_Toc349578042)

[Appendix B: AD Sites 17](#_Toc349578043)

[Appendix C: Workstation Population by AD site 18](#_Toc349578044)

[Appendix D: Full Glossary of Terms 20](#_Toc349578045)

Glossary of Key Terms

| **Item** | **Extended Version** | **Details** |
| --- | --- | --- |
| Site code CAS | Central Administration Site | CAS is the 3 letter site code being used to designate the Central Administration site the 2 Primary Sites Louisville and Simpsonville report into. |
| Site code  LDC | Louisville Data Center | LDC is the 3 letter site code being used to designate the Primary site in Louisville |
| Site code  SDC | Simpsonville Data Center | SDC is the 3 letter site code being used to designate the Primary site in Simpsonville |
|  |  |  |
| AD | Active Directory | Directory service managing and containing Users, computers, groups and organizational units |
| AI | Asset Intelligence Synchronization Point | A site system role that connects to Microsoft to download Asset Intelligence catalog information and upload uncategorized titles so that they can be considered for future inclusion in the catalog |
| App Catalog | Application Catalog | Combination of the Configuration Manager roles: Application Catalog web service point and Application Catalog website point |
| CAS | Central Administration Site | Central Configuration Manager site used to manage environments requiring multiple primaries. The CAS does not contain any clients |
| DP | Distribution Point | A system client systems connect to for installation of software |
| Enrollment point | Enrollment point | A site system role that uses PKI certificates for Configuration Manager to enroll mobile devices and Mac computers, and to provision Intel AMT-based computers |
| Enrollment proxy point | Enrollment proxy point | A site system role that manages Configuration Manager enrollment requests from mobile devices and Mac computers |
| FSP | Fallback Status Point | A site system role that helps you monitor client installation and identify the clients that are unmanaged because they cannot communicate with their management point. |
| MDT | Microsoft Deployment Toolkit | Extends the abilities of OSD to enable complex deployment tasks |
| MP | Management Point | Website where SCCM Clients retrieve policies from and submit data to |
| OSD | Operating System Deployment |  |
| PS | Primary Site | Configuration Manager site which contains and manages configuration manager clients |
| RSP | Reporting Services Point | A site system role that integrates with SQL Server Reporting Services to create and manage reports for Configuration Manager |
| SCCM | System Center Configuration Manager | Microsoft’s system configuration management solution |
| SMP | State Migration Point | Used in Operating System Deployment (OSD) for the migration of user data between systems |
| SS | Secondary Site | Configuration Manager site which supports the activities of a primary site, does not have clients of its own |
| SUP | Software Update Point | A WSUS server that is controlled by SCCM to manage updates on SCCM client systems |
| WSUS | Windows Software Update Service | A windows server component which is used to patch windows systems |

Overview

Humana Inc has engaged Infront Consulting group to lead a System Center 2012 Configuration Manager Architecture and Design Workshop to deliver:

1. SCCM Server Sizing and role replacement recommendations
2. Visio diagram of the SCCM solution architecture
3. Next phase estimates for planning and deployment.

The process used to achieve the above items was to engage the various teams from Humana through conference calls to determine requirements, discuss features, and transfer knowledge about the product and the environment it is to be used within. Significant knowledge transfer was provided from both sides to understand the various needs and challenges of the environment as well as the product.

The result of the workshop for the design is to recommend Humana Implement a Configuration Manager 2012 SP1 environment consisting of three sites, a CAS, Central Administration Site; a Primary site for Louisville; and a Primary site in Simpsonville. The workstations and servers will all be managed through the Central administration site leveraging the new role based security model in Configuration Manager 2012 which provides very granular security to ensure appropriate separation of administration. The CAS based hierarchy was primarily selected to ensure the availability of an environment to provision and manage server and workstation systems in the event of the loss of a primary datacenter. The design allows for other environments to be provisioned / recovered in parallel with the recovery of the lost portions of the SCCM environment. It will not delay recovery of other environments by having to wait for the SCCM environment to be brought online before being able to begin recovery processes.

Humana Requirements

Through the discussions generated in the workshop and from the information provided through the survey completed by the different Information Technology groups within Humana a number of items were identified as being requirements. The discussion of the various requirements was used to develop an architecture which could support the requirements. Requirements from the discussion and survey were as follows:

# Availability

* Environment needs to have a high level of availability to deploy operating systems, patches and software to both workstations and servers.
* With this to become a Server OS deployment solution it would be considered a Tier 1 DR plan, up within 24 hours. Due to the fact that other DR environments would also be relying on this the solution requires a higher level of availability.

# Features

Humana is interested in the following features:

* Hardware and Software Inventory
* Software Distribution – New Package Model of great interest
* Patch Management
* OS Deployment (Image and scripted) – Identified a minor challenge with SP1 since it uses PE 4 which is windows 8 based, systems which have processors without the NX (No-eXecute) feature may have issues deploying, but to mitigate this, queries are being run on the existing systems and they are likely to be scheduled to be replaced due to age.
* Compliance Settings (Previously Desired Configuration Management)
* AppV Integration
* Maintenance Windows – For servers and workstations.
* Integration with System Center Suite – able to leverage other portions of the suite with Configuration manager like Orchestrator for complex patch management and Service Manager for Inventory management and software procurement workflow.

# Migration

* Existing SCCM 2007 environment for the workstation environment
* Looking to move to new Application Model for software packages
  + Ability to check if application already installed at runtime before the application runs
  + Ability to check for requirements on the target system at runtime
* Migration of existing work with collections and software distribution to be retained with client install status by leveraging the migration tools included in Configuration Manager 2012

# Work from Home

* Humana has a growing work from home / remote worker environment of over 6,000 users
* Desire to alleviate traffic on corporate VPN by leveraging clients to connect to Microsoft updates to pull down the actual patches while Humana’s systems provide the authorization and reporting
* Enable remote workers to receive software without requiring manual VPN initiation. This is possible through Internet based client management with SCCM or through Microsoft Direct Access VPN solution with the newer windows clients and appropriate supporting server infrastructure.

# Security

* Ability to separate various roles e.g., Workstation Administrators from Server Administrators, Application Deployment Admins, Package Quality Assurance.
* The new Role Based security model introduced in Configuration Manager 2012 allows for granular role delegation, access to systems, and access to the hierarchy.
* The granularity allows for Server Administrators to never see Workstation related items (computers, software) and vice versa with Workstation Administrators. The only group that would be able to see both sides of the fence are the SCCM Full administrator accounts. It is recommended to keep these accounts separate and not used for day to day administration of workstations or servers to further reduce the possibility of unintended interruptions.

# Growth

* Humana grows regularly and quickly, the design needs to be able to handle rapid growth especially through acquisitions.
* The recommended Architecture provides for future growth.

# Cross Domain Access

* Ability of client systems in different domains than the site servers to communicate
* Achieved through setting MSI properties on client installs to specify an initial Management Point and / or domain suffix and specify the site the system is to join
* Publishing systems to DNS, still requires MSI properties being set
* Acquisitions and DMZ systems will be able to install and access the environment provided the correct switches and settings are included on the installation command line.
* Client Installation Properties
  + <http://technet.microsoft.com/en-ca/library/gg699356.aspx>
* How to Provision Client Installation Properties (Group Policy and Software Update-Based Client Installation)
  + <http://technet.microsoft.com/en-us/library/gg712298.aspx#BKMK_Provision>

# Network Bandwidth and Server Infrastructure Efficiencies

* Interested in keeping architecture as lean as possible outside of the core datacenters
* Humana already has an investment in using 1e Nomad product and will continue to do so onto the new version in the new environment. The product allows PXE everywhere for OS deployments and removes the need for servers to provide software distribution points in the client locations.
* Humana leverages virtualization where possible and the existing Configuration Manager 2007 environment has been successfully running in a virtualized environment. There is hope this will continue with the 2012 version.

# Size

* Humana has approximately 48,000 workstation systems and 8,000 servers so the solution must be able to support over 65,000 systems
* Existing Package and OS sizes for workstations
  + >1 TB Packages
  + 37 GB OSD
* Existing Package and OS sizes for Servers
  + 73 GB Packages
  + 3.5 GB OS Configuration
  + 19 GB HP Hardware Packages

# Integration with HP Server Deployment Solutions

HP provides integration with the Microsoft System Center suite of products through Insight Control for Microsoft system Center <http://h18013.www1.hp.com/products/servers/management/integration-msc.html> Listed as features are:

* The HP ProLiant Server Operating System Deployment (OSD) feature provides quick and reliable Windows deployment to bare metal HP servers, including pre-deployment hardware and BIOS configuration, and post-OS HP driver and agent installation.
* The HP ProLiant Updates Catalog ensures consistency and maximizes uptime with simplified Windows driver and firmware updates using the HP Service Pack for ProLiant.
* The HP ProLiant Hardware Inventory Tool provides detailed component level inventory of every managed HP Windows server.
* Supports SCCM 2007 and SCCM 2012 (including SP1).

Architecture

Discussion of the requirements then lead to the discussion of the various configurations available in the deployment of Configuration Manager and the discussion of which configuration would be most suitable for Humana. In addition it is recommended to have a test / development environment to test upgrades to the environment and do initial package creation on while allowing QA in production environment. Unlike with previous versions of Configuration Manager servers and workstation systems are able to co-exist in the same site and still have their own specific client and security settings providing for separation of the environments through role based security.

# Proposed Architecture 1: Single Primary Site

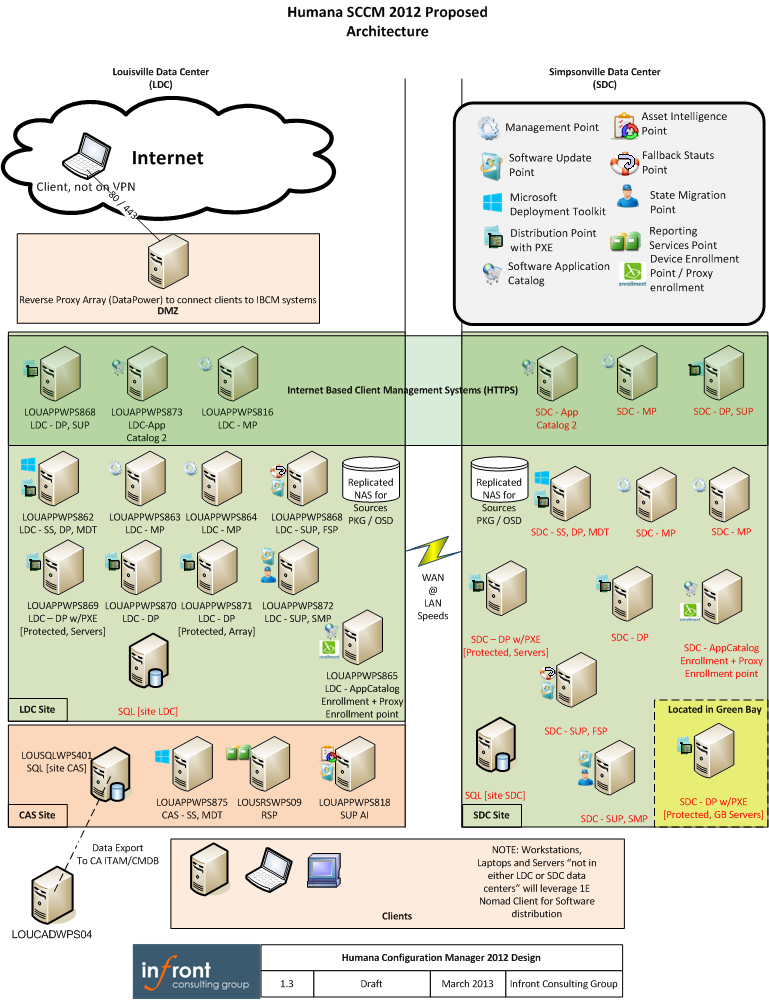
Humana’s size (number of client systems) and the fact technologies like 1e Nomad are being leveraged would allow Humana to have a single primary site install of configuration manager. The challenge for this architecture would be the availability of the environment in the situation of a Disaster recovery scenario. With Server OS deployments and workstation deployments happening during DR the recovery time of the site could significantly impact the timelines to recover other systems within the DR time-lines.

# Recommended Architecture 2: CAS with 2 Primary Sites

Evaluation of Humana’s requirements leads to the recommendation of a design leveraging a CAS (Central Administration Site) with two Primary sites. The design will meet all the requirements and fulfil the Disaster Recovery requirements. Designing the environment with the two Primary sites ensures OSD / Software Deployment to the server environment will still be available if one of the primary datacenters is lost. These services are required for Humana to achieve return to service targets for all environments following the loss of a Primary datacenter. Workstations and Servers will be a member of one of the two Primary Sites either LDC or SDC.

Key Points:

* Assuming 1e Nomad product will be used for all Client workstations plus servers outside of LDC and SDC. Recommend input from 1e on the design to ensure supportability.
* Workstation DP will be a Nomad enabled DP, Server DP’s in the datacenters will not and will be there to service server clients
* Assuming PKI infrastructure meets SCCM’s requirements as per: <http://technet.microsoft.com/en-ca/library/gg699362.aspx> and Certificate revocation lists are published and accessible to clients internally and externally
* Internet Based Client Management Systems on a segregated network but part of the same domain as rest of Configuration Manager systems



System Sizing

Installation of Configuration Manager components onto systems requires some planning and system configuration to ensure Configuration manager does not install in unintended locations.

Ensure NO\_SMS\_ON\_DRIVE.SMS exists on all drives on SCCM servers and SQL Servers where you do NOT want SCCM files to install to. There are some required application files for SCCM to install onto the SQL Server and by default, for all situations, it will choose the largest free space drive on the system.

With Humana already having an existing Configuration Manager 2007 environment it is possible to leverage the existing sizing information from the environment and provide good requirements numbers based on existing usage. Sizing using these existing numbers are more accurate than Sizing spreadsheets which are only estimates of what will happen in an environment

# SQL

Humana will leverage a Metro Cluster for Configuration Manager to provide as high availability as possible. The cluster will have three Instances with two active at one of the datacenters and the third instance active at the alternate datacenter.

It is expected there will be a minimum of 8 cores running the instances.

## CAS SQL Instance

The CAS SQL Instance will be leveraged for reporting and administration of the environment. In addition it is the synchronization point for Software updates and Asset intelligence information. No client processing happens at the CAS the client data is processed at the primaries and then replicated to the CAS. If there is to be an increase in the number of software metering rules and an increase in duration on the retention of metering information the growth of the database will need to be monitored and if required expanded.

| **Item** |  |  |
| --- | --- | --- |
| Memory | 24 GB RAM |  |
| Disk Sizing | 175 GB DB | 50 GB LOG |

## Primary SQL Instances

Each of the Primary site servers require their own instance to ensure there are no issues with maintenance backup / recovery / single user mode or other related databases which may have the same names such as a Software Update Point database. In the Humana environment there will be two primary SQL Instances each configured as:

| **Item** |  |  |
| --- | --- | --- |
| Memory | 24 GB RAM |  |
| Disk Sizing | 175 GB DB | 50 GB LOG |

# Site Servers

The site servers are the hubs of the Configuration Manager environment, they process the client information, updating the database, transfer content to the appropriate role servers or clients. Humana has already proven the capabilities of virtualization in their environment and intend to continue to leverage it for the site servers.

## CAS Site Server

The CAS will be the administration point for the entire hierarchy

| **Item** |  |  |
| --- | --- | --- |
| vCPU | 4 |  |
| Memory | 8 GB RAM |  |
| Disk Sizing | 100 GB Application |  |

## Primary Site Servers

The two Primary Site servers should have the following configuration

| **Item** |  |  |
| --- | --- | --- |
| vCPU | 4 |  |
| Memory | 8 GB RAM |  |
| Disk Sizing | 500 GB Application / Distribution Point |  |

# Role Servers

The role Servers are used for items like Software Update Points, Management Points, Asset Intelligence synchronization points, etc. The configuration of theses is standard for memory CPU, and diskspace except for Distribution points (larger Hard drive configuration), and Reporting Points (increased Memory and CPU)

| **Item** |  |  |
| --- | --- | --- |
| vCPU | 2 | Reporting Services Point Server 4 vCPU |
| Memory | 4 GB RAM | Reporting Services Point Server 8 GB RAM |
| Disk Sizing | 50 GB Application | Distribution Point: 500 GB |

# NAS

Sufficient Drive space for source files of Packages and OSD. The NAS should be replicated between both sites for availability and be backed up on a regular basis.

Currently there is over 2TB required

# Backup

Configuration Manager is only supported to be recovered using its own backup. The backup is a point in time backup of SQL and the site server configuration. The backup can be directed to a network location where both the Site server and the SQL Server computer accounts require full control to complete their backup tasks. The size required will depend on the size of the databases being backed up plus and additional amount of space for files from the site server.

Estimates for Planning and Deployment

The following are the rough estimates of work involved in documenting, building and testing the architecture, please note this excludes any work required for Nomad Installation and Configuration. The amount of time required here can change depending on the number of resources applied either by Humana or outside resources. The estimate of the total amount of work for this is 55 days.

# Test Environment - 15 days

* Develop Detailed Test Plan, determine items to be validated (e.g. Migration, Client Deployment, Client Settings)
* Build Test Environment
* Validate required functionality in Test

# Deployment Plan, plus Build and test - 15 days

* Develop Deployment plan for production based on results of Test environment
* Choose items to be migrated
* Build Production
* QA Production (Validate functionality of features in production environment before bringing on real clients)

# Deploy and Migrate - 20 Days

* Migrate from previous systems
* Migrate and Deploy clients
* Migration Cleanup (removal of 2007 environment, validating 2007 information removed from AD, DNS, WINS

# Scripting and Automation – 5 Days

* Scripts and automations to support the environment

Appendix A: Survey Information

| **Topic** | **Inquiry result** |
| --- | --- |
| What are the goals that management expects to fulfill with this deployment of Configuration Manager? | Asset Management, Software Delivery, patching, reporting, compliance, system builds. For server deployment solution we need to deploy various operating systems (Windows Server 2003, 2008, 2008 R2, 2012; Redhat Linux versions) from either scripted or image base deployments. This will need to be available as a pxe network request to choose bare metal hardware, VMware server, and Hyper-V.  Long term, we want to consolidate to using Microsoft SCCM to replace ConfigureSoft VCM for software patching and compliance for servers, as well as replace Altiris RDP which is currently used for server builds and software delivery for servers |
| Is there an existing SMS solution | SCCM 2007 for workstations only. For server deployment solution we currently use HP RDP (Altiris) v7.x. |
| What is the structure of your organization? Are there parent companies or umbrella organizations? Are there child subsidiaries? If there are multiple relationships how is Information Technology managed within the organization? | Humana is the parent company (Humad.com), with acquisitions in various stages of connectivity/integration, as well as our Humana Government group which has a virtual separation due to auditing requirements. |
| Are there any changes to the company expected in the next 6-12 months? Does the company grow regularly through Mergers or acquisitions? | Grows very regular -> fast. Acquisitions are normal and can happen at any time. |
| What is the availability or SLA required from Configuration Manager? Is it a critical path for Disaster recovery / business continuance plans e.g. to be used as the OS deployment and configuration to bring environment back on-line? | Due to the plans for OSD for servers, this will be considered a Tier I DR plan, up within 24 hours. Humana will be looking for SLAs of four nines or better. |
| What features of Configuration Manager is your organization interested in? |  Hardware/Software Inventory   Software Distribution   Patch Management   OS Deployment (Both image and scripted deploy’s.)   Desired Configuration Management   AppV integration   Device Management   Maintenance Windows   Added benefits of tying in with MS VMM and SCOM or other MS System Center 2012 sp1 products. |
| Environment Information – Active Directory | Humana has an empty forest root – ADEA.HUM. Humana has a parent (accounts domain) - Humad.com and six child domains PNA, LOUDCU, TS, RSC, HMHSCHAMP and WAP. HUMAD has a one trust relationship with several other domains and this is in place so that support staff can manage the other domains. HUMAD accounts can also be given access to resources in those trusted domains. There are 11 such trust relationships.  Forest(s), Domain(s), trusts – ADEA.HUM – empty forest root  HUMAD.COM, RSC.HUMAD.COM, PNA.HUMAD.COM, TS.HUMAD.COM, LOUDCU.HUMAD.COM, HMHSCHAMP.HUMAD.COM, WAP.HUMAD.COM  DMZAD.HUM – Domain in the DMZ  CRMAD.HUM – Domain for Exposing applications to the internal humad.com (workstations) rsc.humad.com (servers) ts.humad.com (Citrix environment) hmhschamp.humad.com (Humana Government)  Management –  Q: Organization of users, groups, resource accounts are they separated out mixed together etc…  A: Separated in AD  Q: Are obsolete computers / accounts regularly removed?  A: Yes  Q: Is the AD Schema already extended for Configuration Manager?  A: Yes, from SCCM 2007 |
| Environment Information – Network Infrastructure | LAN speeds and design (VLANS)  Humana has an extended number of vlans with layer 2 reachability between dual data centers. We use VLANs, VDC, VrF and other Cisco solutions. The speeds range from 100 Meg, 1Gig, and 10 Gig server/LAN connections.  Server – Servers are ESX, and some stand alone. Virtual is the continued direction.  WAN topology is : Hub, Spoke, Hub Spoke; Single hub and Spoke; Mesh  Humana uses Hub and Spoke for most connections back to a dual data center. We do have a Mesh at some of our larger sites that connection back to dual data centers. MPLS is the primary WAN connection.  Connection speeds: T1, T3, OC3, OC12, MetroE, 10meg, 50 meg, 100 meg  (attach diagram if possible) Humana is willing have a conference call or sit down and talk about our infrastructure, but we generally do not hand out network diagrams.  Q: Utilization on WAN links or are there connections that are known to already have bandwidth contention?  A: Humana utilized the bandwidth at each site. We have T1’s at sites < 50 associations, T3 at sites >100 and OC3 at sites larger than 1000. These are primarily MPLS connections back to our two data centers.  Q: Off Hours timeframe? (Considered for pushing of software to distribution points, patching of systems)  A: Humana is a 7x24 business. Our remote sites can by open until 1am EST. Software pushes and patching can occur after hours depending on the site. This is coordinated through DSI at each site. Usually from 1am until 5am the site has little or no activity.  Q: DMZ information / VPN configuration  A: Humana as a DMZ with a front side and back side firewall. We NAT addresses from the public side to the private side. Humana has separate firewalls that control VPN configuration. This is also managed by our Security Department. All access is located down to specific ports and IP addresses.  Q: QoS implementation, is there one?  A: Yes, Humana does implement QoS, but primarily for voice and other important traffic. The default Best Effort queue is used for all other traffic.  Q: Any plans to change the network in the near future (6-18mo)?  A: The basic principle will stay the same, but we plan in upgrade the core infrastructure with new hardware |
| Environment Information – Client Information | Q: How many users?  A: 40,000  Q: How many users in each site / across each WAN link?  A: varies widely, thousands to just ten  Q: How many workstations?  A: 48,000  Q: How many servers?  A: 8058  Q: OS and service pack levels of Servers and workstations?  A: Workstations:  Windows XP SP3  Windows 7 SP1  A: Servers:  2003 x64 Enterprise v9.10  2003 x86 Enterprise v9.10  2008 x64 Enterp/Stand v2012.06.0  2008 x86 Enterp/Stand v2012.06.0  2008 R2 x64 Enterp/Stand v2012.06.0  2008 R2 SP1 x64 Enterp/Stand v2012.06.0  MS 2012 DataCenter Core  MS 2012 DataCenter  MS 2012 Standard  MS Hyper-V 2012  Q: Are there workgroup or DMZ domain systems to be managed?  A: Yes  Q: How do remote users connect?  A: Array, Citrix, and My PC  Q: VPN, single access to desktop, move to citrix for richer experience (printing, dual monitors etc)  A: Both |
| Environment Information – Patch Management process | Q: What is your current patch management product?  A: WSUS, ConfigureSoft VCM (a.k.a. ECM) for servers  Q: What is your current patch management process? If so what about it is working for you what is not working for you?  A: CVE’s are determined by TVM who in turn passes that on to Client Innovations for the determination of what patches need to be pushed. Client Management then packages, certifies and deploys the patches.  Q: What is the structure for approving, testing, and deploying Patches, Software, Operating systems? Ie. Is this all done by the same team, separate teams?  A: Patches are determined by Client Innovations. O/S is handled by LOS and regular software is packaged by ATS. Client Management handles the certification of the changes and deploys those changes once approved.  Q: How much isolation of roles is required for the environment? Ie, do the staff who create the packages also deploy them and also administer the system?  A: Client Management does approve and deploy software.  Q: Are your systems located within the same time zone? During patching is Local time used or is it all based on a specific time zone?  A: Systems are located in multiple different time zones and Local time is used for deployments. |
| Remote clients (outside firewalls) | Yes, at several acquisitions and clients when not connected to VPN (dedicated work-at-home machines) |
| Virtualization Technology | VMWare, testing with Hyper-V |
| Hardware/Server availability for new site (On hand or ?) | The majority of servers have been provisioned. VM is always available. Physical hardware would have to be procured. |

Appendix B: AD Sites



Appendix C: Workstation Population by AD site

| **ADSite** | **Total** |
| --- | --- |
| ATLANTA | 71 |
| AUSTIN | 45 |
| CHICAGO | 229 |
| CINCINNAT1 | 1108 |
| CINCINNATI2 | 1441 |
| CORPUSCHRISTI | 29 |
| DALLAS | 27 |
| DAYTONA | 6 |
| Default-First-Site-Name | 10 |
| ElPaso | 1 |
| GLENDALE | 922 |
| GREENBAY | 3758 |
| HOUSTON | 10 |
| JACKSONVILLE | 110 |
| KANSAS | 120 |
| Knoxville | 210 |
| LANCASTER | 128 |
| LASCOLINAS | 521 |
| LOUISVILLE | 25594 |
| MADISON | 353 |
| Maine | 1 |
| MIAMI | 2086 |
| MIAMI2 | 35 |
| MILWAUKEE | 221 |
| NEWORLEANS | 212 |
| Oakland | 8 |
| Orlando | 51 |
| PEORIA | 54 |
| PHOENIX | 156 |
| PHOENIX2 | 719 |
| PHOENIX3 | 405 |
| PHOENIX4 | 127 |
| PUERTORICO | 846 |
| ROSWELL | 165 |
| SANANTONIO | 449 |
| ServiceCenter | 106 |
| Syracuse | 1 |
| TAMPA | 1585 |
| TAMPA3 | 289 |
| TAMPA4 | 255 |
| US-SC-Lancaster | 46 |

Appendix D: Full Glossary of Terms

| **Term** | **Definition** |
| --- | --- |
|  |  |
| Active Directory Delta Discovery | A discovery option that allows Configuration Manager to discover only new or changed resources in Active Directory independently of a full discovery cycle. |
| Active Directory Forest Discovery method | A Configuration Manager discovery method that searches for Active Directory sites and subnets in Active Directory forests. |
| Active Directory Group Discovery method | A Configuration Manager discovery method that searches for the group memberships of computers and users by polling Active Directory Domain Services. |
| Active Directory System Discovery method | A Configuration Manager discovery method that searches for system resources by polling Active Directory Domain Services. |
| Active Directory User Discovery method | A Configuration Manager discovery method that searches for computer user resources by polling Active Directory Domain Services. |
| Active Management Technology (AMT) | See Other Term: Intel Active Management Technology |
| Active software update point | The software update point for a site that interacts with Windows Server Update Services (WSUS) to configure software updates settings and manage software updates synchronization. The active software update point can accept connections from the intranet and the Internet. |
| Application Administrator | A security role that grants permissions to administrative users so that they can perform both the Application Deployment Manager role and the Application Author role. |
| Application Author | A security role that grants permissions to administrative users so that they can create, modify, and retire applications. |
| Application Catalog web service point | A site system role that provides software information to the Application Catalog website from the Software Library. |
| Application Catalog website point | A site system role that provides users with a list of available software from the Application Catalog. |
| Application Deployment Manager | A security role that grants permissions to administrative users so that they can deploy and monitor applications. |
| Asset Intelligence | A Configuration Manager feature that allows administrators to inventory and manage software license usage throughout their enterprise. |
| Asset Intelligence catalog | A Configuration Manager catalog that contains categorization and identification information for software titles and versions, which is used to classify inventoried software. |
| Asset Intelligence synchronization point | A site system role that connects to System Center Online to download Asset Intelligence catalog information and upload uncategorized titles so that they can be considered for future inclusion in the catalog. |
| Asset Manager | A security role that grants permissions to administrative users so that they can manage the Asset Intelligence synchronization point, Asset Intelligence reporting classes, software inventory, hardware inventory, and metering rules. |
| Assigned management point | A management point in a primary site that is assigned to the Configuration Manager client. |
| Assigned site | A site to which a Configuration Manager client is currently assigned. |
| Binary delta replication | A Configuration Manager process that copies only the changed portions of a package or content  file rather than the entire file when an update has been made. |
| Boundary | An IP subnet, IP address range, IPv6 prefix, or Active Directory site that identifies the network location of clients in the Configuration Manager hierarchy. |
| Central administration site | The central administration site coordinates intersite data replication across the hierarchy by using Configuration Manager database replication. It also enables the administration of hierarchy-wide configurations for client agents, discovery, and other operations. |
| Collection | A set of resources in the Configuration Manager hierarchy. |
| Compliance Settings Manager | A security role that grants permissions to administrative users so that they can define and monitor Compliance Settings. |
| Component server | A server that runs Configuration Manager services. When you install all the site system roles except for the distribution point role, Configuration Manager automatically installs the component server. |
| Configuration Manager Application Catalog | The web-based view of the applications that are available for a user to search, browse, request, and install. |
| Configuration Manager Software Center | The end-user program that allows the user to set preferences for how their software is installed. End users can also use Configuration Manager Software Center to request, install, remove, and monitor the software that is deployed by using System Center 2012 Configuration Manager. |
| Configuration Manager software inventory | A Configuration Manager feature that automatically gathers information about software on client computers. |
| Configuration Manager software metering | The Configuration Manager feature that monitors software usage on client computers. |
| Data discovery Record (DDR) | The file format (.ddr) and the actual file that is used by Configuration Manager to report discovery data to a Configuration Manager site database. |
| Database replication | A type of data replication in System Center 2012 Configuration Manager that uses SQL Server replication. |
| Delta inventory file | A file generated after Configuration Manager performs a complete inventory, containing only hardware or software properties that were added, removed, or changed since the previous inventory cycle. |
| Delta replication | The copying of only the changed files in a Configuration Manager package when an update has been made to the package. |
| Deployment purpose | An application state that is associated with the deployment of software, such as Available or Required. |
| Deployment type | A technology that is used to deploy an application to devices. A deployment type is contained within an application; for example, Windows Installer could be a deployment type for the “Visio 2007” application. |
| Discovery data | A set of properties collected by a discovery method that reflects the attributes of a Configuration Manager resource. |
| Discovery data record (DDR) | The file format (.ddr) and the actual file that is used by Configuration Manager to report discovery data to a Configuration Manager site database. |
| Distribution point | A site system role that contains source files for clients to download, such as application content, software packages, software updates, operating system images, and boot images. |
| Distribution point group | A set of distribution points that you can manage as a single entity. |
| Endpoint Protection Manager | A security role that grants permissions to administrative users so that they can define and monitor security policies. |
| Endpoint Protection point | A site system role that Configuration Manager uses to accept the Endpoint Protection license terms and to configure the default membership for Microsoft Active Protection Service. |
| Enrolment point | A site system role that uses PKI certificates to complete mobile device enrolment and to provision Intel AMT-based computers. |
| Enrolment proxy point | A site system role that manages enrolment requests from mobile devices so that they can be managed by Configuration Manager. |
| Exchange Server connector | A Configuration Manager technology that connects to Exchange Server to discover and manage mobile devices. |
| Fallback site | The site in the hierarchy that clients are assigned to when they are installed by using automatic site assignment and they are not in a boundary group that has an assigned site. |
| Fallback status point | A site system role that helps you monitor client installation and identify the clients that are unmanaged because they cannot communicate with their management point. |
| Full Administrator | A security role that grants all permissions in Configuration Manager to an administrative user. |
| Global conditions | A setting or an expression that is used to define rules that specify how an application is deployed on client devices.  See Also: requirement rules |
| Global data | A set of administrator-created objects that are replicated to all sites throughout the hierarchy. Secondary sites receive a subset of this data.  See Also: local data |
| Heartbeat Discovery method | A Configuration Manager discovery method that is used to update data discovery records (DDRs) for each Configuration Manager client on a set schedule to ensure that they remain current in the site database. |
| IDMIF file | A type of Management Information Format (MIF) file that can be used to add new architectures or updates to existing architectures in the Configuration Manager site database to accommodate custom hardware inventory properties. |
| Incremental collection evaluation | A feature that enables you to evaluate new or changed members of a collection. |
| Incremental collection member evaluation | A process that periodically scans for new or changed resources from the previous collection evaluation and then updates the collection membership with only these resources. |
| Infrastructure Administrator | A security role that grants permissions to administrative users so that they can perform migration tasks and create, delete, and modify the Configuration Manager server infrastructure. |
| Intel Active Management Technology (AMT) | An Intel networking management technology that is supported by Configuration Manager out of band management, which enables a Configuration Manager administrator to manage desktop computers independently from the Configuration Manager client or the computer operating system. |
| Internet-based client management | A feature in Configuration Manager that allows you to manage computers that have the Configuration Manager client agent but do not connect into the network through a VPN or dial-up connection. |
| Internet-based site system | A site system role that allows connections from clients when they are managed over the Internet. |
| Internet-based software update point | The software update point for a site that accepts communication from only client computers on the Internet. There can be only one active Internet-based software update point. |
| local data | A set of objects that are automatically created by Configuration Manager. This data is not replicated to other sites.  See Also: global data |
| Maintenance window | A period of time, defined by administrators, when changes can be made on the computers that are members of a Configuration Manager collection. |
| Managed Object Format (MOF) | The file type, based on the Interface Definition Language (IDL), that describes management information. The MOF syntax is a way to describe object definitions in textual form. |
| Management controller | The hardware and firmware component on computer motherboards that supports out of band management. |
| Management Information Format (MIF) file | The file type (.mif) that can be used to modify the Configuration Manager database by creating architectures, object classes, and attributes. |
| Management point | A site system role that provides policy and service location information to clients and receives configuration data from clients. |
| Membership rule | The criteria by which Configuration Manager evaluates whether a resource belongs to a particular collection. |
| Network Discovery method | The Configuration Manager discovery method that enables the Configuration Manager administrator to discover any network resources that are IP addressable. |
| NOIDMIF file | A custom Management Information Format (MIF) file that Configuration Manager administrators can use to modify or append object classes and properties to existing client inventory data. |
| Non-peak power plan | A Configuration Manager power plan that you can configure with power settings that are applied outside peak hours or business hours. |
| Operating system deployment | A Configuration Manager feature that allows you to create operating system images and deploy those images to target computers |
| Operating System Deployment Manager | A security role that grants permissions to administrative users so that they can create, deploy, and manage operating system images. |
| Operations Administrator | A security role that grants permissions to administrative users so that they can perform all actions in Configuration Manager except for those that are required to manage security. |
| Out of band management | A feature in Configuration Manager that allows computers to be managed outside standard management channels by connecting to a supported management controller. This management channel is independent from the Configuration Manager client and the operating system. |
| Out of band service point | A site system role that provisions and configures Intel AMT-based computers for out of band management. |
| Package | A Configuration Manager object that contains the content files and instructions for distributing programs, software updates, boot images, operating system images, and drivers to Configuration Manager clients. |
| Package definition file | An ASCII text file that contains predefined software distribution objects, such as programs and packages that are used for software deployment. |
| Package share | A network share that includes the software installation files for a package. |
| Package source directory | A directory that contains Configuration Manager package source files that are used for package distribution. |
| Package update | A Configuration Manager operation that increments the package version and updates all distribution points with only the files that have changed in the package. |
| Peak power plan | A Configuration Manager power plan that you can configure with power settings that are applied during the peak hours or business hours that you specify. |
| Power plan | A group of Windows-based power settings that you can apply to computers by using Configuration Manager power management. |
| Preferred distribution point | A distribution point with an associated boundary group that includes the client’s current location on the network. |
| Prestart command | A script or an executable file that supports operating system deployment and that can interact with the user in Windows PE before a task sequence runs. |
| Primary device | A software deployment condition that defines one or more devices that a specific user uses. A primary device is typically determined either by frequency of use or by business requirements. |
| Primary site | A Configuration Manager site that has clients assigned to it and that processes client-generated data. |
| Primary user | The main user of a device. (A device can have more than one primary user.) |
| Read-only Analyst | A security role that grants permissions to administrative users so that they can view all objects in Configuration Manager. |
| Reinstate | To bring an application out of retirement and back into service. |
| Remediation server | A server that is used to update the computer state by providing software updates, new antivirus signatures, additional intrusion detection signatures, and so on. |
| Remote Tools Operator | A security role that grants permissions to administrative users so that they can run and audit remote administration tools. |
| Replication Link Analyzer | A Configuration Manager tool that detects, analyzes, and remediates database replication issues in a hierarchy. |
| Reporting services point | A site system role that integrates with SQL Server Reporting Services to create and manage reports for Configuration Manager. |
| Resource Explorer | A Configuration Manager console feature that displays the hardware and software inventory that has been collected from clients. |
| Retire | To remove an application from service. |
| Role-based administration | The method in which System Center 2012 Configuration Manager secures objects. |
| Secondary site | A child of a primary Configuration Manager site. |
| Security Administrator | A security role that grants permissions to administrative users so that they can add, remove, and modify administrative users and their administrative assignments. |
| Security role | A set of permissions that defines what an administrative user can do and see in the Configuration Manager console. |
| Security scope | A method that, when used in conjunction with security roles, limits which objects an administrative user can use and see. |
| Sender | A Configuration Manager communication mechanism that lets you create and send package information to another Configuration Manager site by using standard network channels. |
| Shared distribution point | A distribution point in a Configuration Manager 2007 hierarchy that clients can use to download the content and packages that have been migrated to System Center 2012 Configuration Manager. |
| Site assignment | The process of including selected resources in a Configuration Manager site. |
| Site code | A three-character code that Configuration Manager uses to uniquely identify a Configuration Manager site. |
| Site control file | An ASCII text file that contains the settings of a Configuration Manager site. |
| Site data | The operational information that is created by a Configuration Manager site and that is replicated to the central administration site. Site data includes hardware inventory data, status messages, alerts, and the results of query-based collection rules. |
| Site database server | A server that hosts the SQL Server database, which stores information about Configuration Manager assets and site data. |
| Site server | A computer on which you run the Configuration Manager setup program and which provides the core functionality for the site. |
| Site system | A server that provides Configuration Manager functionality to a Configuration Manager site. |
| SMS Executive | The primary Configuration Manager service that accesses and updates the database and manages many different process threads. |
| SMS Provider | A WMI provider that allows both read and write access to the Configuration Manager site database. |
| Software update point | A site system role that integrates with Windows Server Update Services (WSUS) to provide software updates to Configuration Manager clients. |
| Stand-alone site | A Configuration Manager primary site with no parent sites and no child sites. |
| State message | A message type that is used to identify at what stage a Configuration Manager client process has succeeded, failed, or stopped. |
| State migration point | A site system role that stores user state data when a computer is migrated to a new operating system. |
| Status filter rule | A filtering rule that controls how status messages are reported and viewed. |
| Status message | A message generated by a Configuration Manager component and viewed in the Status Message Viewer. |
| Status message threshold | The limit that defines when the summary status for a component or site system should indicate OK, Warning, or Critical status. |
| Status Message Viewer | A tool in the Configuration Manager console that is used to browse the status messages in the Configuration Manager site database. |
| Status summarizer | A component that consolidates the data generated by Configuration Manager status messages into a succinct view of the status of a component, a server, a package, or an advertisement. |
| Supersedence | A deployment behavior that specifies how new software replaces existing software. |
| System Health Validator point | A site system role that validates Configuration Manager Network Access Protection (NAP) policies. It must be installed on a NAP health policy server. |
| Task sequence | The mechanism in Configuration Manager for performing multiple steps or tasks on a client computer at the command-line level without requiring user intervention. |
| Tiered secondary | In Configuration Manager, a secondary site that receives deployment content from another secondary site. |
| Trusted root key | An encryption key used in Configuration Manager to help clients identify valid management points. |
| Uninterpreted configuration item | An imported configuration item that cannot be interpreted by the Configuration Manager console and whose properties cannot be viewed or edited in the console. |
| Unmanaged client | A client that is not communicating with its assigned site in the Configuration Manager hierarchy and therefore cannot receive policy or upload inventory data. |
| User device affinity | The mapping of a user to a device, which enables deployment conditions and simplifies the complexity of the deployment. |
| Wake-up packet | A packet that is sent by a Configuration Manager primary site server to bring computers out of a sleep state so that they can perform a management function, such as installing a mandatory software update. |
| Wipe | To remove all data from a mobile device that has been lost, stolen, or compromised. |