Technical Guide



Core Infrastructure

Prepared for

[Type Customer Name Here]

9/22/2017

Version 1 Draft

Prepared by

**[Type Author Here]**

[Type Author Position Here]

[Type Author Email Here]

Contributors

**[Type Contributors Here]**

Revision and Signoff Sheet

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
|  |  | 1 | Initial draft for review/discussion |
|  |  |  |  |
|  |  |  |  |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Version Approved | Position | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Overview 7](#_Toc474760235)

[2 Technical Design 8](#_Toc474760236)

[2.1 Core Infrastructure Dependencies 11](#_Toc474760237)

[2.2 Azure IaaS Prerequisites 15](#_Toc474760238)

[2.3 Environment Prerequisites 15](#_Toc474760239)

[2.4 Configuration 19](#_Toc474760240)

[2.5 Environment 23](#_Toc474760241)

[2.6 Platform 26](#_Toc474760242)

[3 Technical Implementation 33](#_Toc474760243)

[3.1 Power BI Dashboard 34](#_Toc474760244)

[3.2 Implementation Activities and Tasks 35](#_Toc474760245)

[3.3 Active Directory 37](#_Toc474760246)

[3.4 Database 39](#_Toc474760247)

[3.5 Hierarchy 40](#_Toc474760248)

[3.6 Platform Configuration 42](#_Toc474760249)

[3.7 Client Agent 44](#_Toc474760250)

[3.8 Capabilities 46](#_Toc474760251)

[3.9 Content 49](#_Toc474760252)

[3.10 Software Inventory 50](#_Toc474760253)

[3.11 Software Metering 51](#_Toc474760254)

[3.12 Asset Intelligence 52](#_Toc474760255)

[3.13 Hardware Inventory 53](#_Toc474760256)

[3.14 Power BI Dashboard 55](#_Toc474760257)

[3.15 Remote Administration 56](#_Toc474760258)

[4 Test Plan 57](#_Toc474760259)

[4.1 Infrastructure Validation 58](#_Toc474760260)

[4.2 Site Communication 60](#_Toc474760261)

[4.3 Policy Configuration 62](#_Toc474760262)

[4.4 Reporting 64](#_Toc474760263)

[4.5 Access Control 65](#_Toc474760264)

[4.6 Hardware Inventory 65](#_Toc474760265)

[4.7 Software Inventory 66](#_Toc474760266)

[4.8 Remote Administration 67](#_Toc474760267)

[5 Component Operation 68](#_Toc474760268)

We are very interested in your input!  If you have comments or would like to request an update to this document, please provide your feedback to the [SDM Suggestions alias](mailto:msdmods@microsoft.com).   Attach the document and clearly describe the changes you would like and explain why the changes are needed.

**Spell/grammar check is turned ON within all SDM Word templates -** Remember to turn off spell/grammar check before sending out the document if you want to avoid showing spelling and grammar red mark-ups. To turn this feature off, do the following:

1. Click on File
2. Click on the Options on the left
3. Click on Proofing
4. Scroll to bottom and check the two boxes shown below:



**To remove all the Visible Guidance (Hot Pink text with Grey Background) all at once:**

1. Click Ctrl H to open the Find and Replace box
2. Make sure your cursor is in the ‘Find what’ box.
3. Click on the More button at the bottom left
4. Click on the Format Button at the bottom left and select Style
5. Scroll down, locate select the “Visible Guidance”
6. Make sure the ‘Replace with’ box is empty:
7. Click ‘Replace All”
8. If not empty - click on the format button in the lower left hand corner. Scroll down and chose ‘(no style)’then replace all.

**IMPORTANT – Finalize This Document**

**REMOVE** all pink text, guidance, comments, changes, and hidden text in this document before submitting it to the customer. You can do this in two ways:

* **Save as PDF** and send the PDF version to the customer.   
  ~ OR ~
* **Inspect document and remove comments, revisions, any document properties you do not want included, personal information, and hidden text.** For guidance on how to do this, see [Remove hidden data and personal information from Office documents](http://office.microsoft.com/client/helppreview.aspx?AssetID=HA100375931033&QueryID=ALdFua2no0&respos=6&rt=2&ns=WINWORD&lcid=1033&pid=CH100487501033#3).

1. Overview

The purpose of this document is to detail all aspects of the Core Infrastructure design and implementation as it relates to the <CUSTOMERNAME> - <PROJECTNAME> project. This document is for use by the <PROJECTNAME> project manager, <DELIVERYORG> technical specialists and <CUSTOMERNAME> IS and IT teams.

This document includes the design of features to support the Core Infrastructure design including:

* Configuration of core infrastructure elements
* Accommodation of environment requirements and constraints into the design
* Platform design to support the pilot implementation and <CUSTOMERNAME> production environment

1. Technical Design

This section outlines the design options, customer decisions and configuration for the capability.

The design will identify the appropriate hardware, software, configurations, customers, and external services that are required to successfully implement and operate the capability.

The design comprises of three key areas:

* Core infrastructure dependencies – all dependent services required for capability to operate.
* External prerequisites – all external prerequisites for System Center Configuration Manager.
* Design – details each of the features of the capability, including decisions and configuration parameters as discussed and captured through the design workshop for this capability.

The table below identifies key decisions that impact the overall implementation and ownership of the capability:

|  |  |  |
| --- | --- | --- |
| Decision | Justification | Impact |
| A Standalone Primary site will be configured as the top-level site in the hierarchy | The size and configuration of the customer environment do not require the use of a CAS in the environment, and this configuration will support up to 175,000 client and devices, in line with current and future capacity requirements | Minimal – should the environment require a Central Administration Site in the future, it can be added to expand the hierarchy. |
| The design will support the following capabilities:   * Device Management * Application Management * Platform Delivery * Servicing | The selected features have been identified as requirements as part of the assessment phase of the System Center Configuration Manager project. | Each capability has specific infrastructure requirement that may impact budget to provide the capability at scale in the production environment. Refer to the Technical Planning Spreadsheet for further information. |
| The design will install the Site Server roles to support the required capabilities:   * Reporting Point * Application Catalog Web Service Point * Application Catalog Website Point * Software Update Point * Endpoint Protection Point * Service Connection Point | The selected features have been identified as requirements as part of the assessment phase of the System Center Configuration Manager project. | The Application Catalog Web Service Point, Application Catalog Website Point, and Software Update Point all require additional infrastructure to provide services to client devices in the estate |
| The following roles will be designed for resilience:   * Management Point * Software Update Point * Distribution Point | If the features described were to go offline for a period it would impact the ability of the company to respond to a sudden change in configuration or the ability to address security threats quickly, as such these roles must be made resilient. | Additional infrastructure is required for distribution point and management point roles to support resiliency. The software update role will be co-located with existing infrastructure in the production environment that has extra capacity to support client requests |
| The database will be located on the Primary Site Server | The number of supported devices in the estate is within supported limits to locate the database on the site server, to reduce infrastructure requirements and ensure there is no latency between the site server and the database. | The Database management team will need to be involved with the setup and configuration of the database to ensure it can be supported per production environment requirements. |
| Software Inventory will / won’t be supported in the environment. | A core feature of System Center Configuration Manager is to provide several asset management features such as software inventory. | Software inventory feature will provide information about the software that exists on company computers and retrieve data about its usage and licensing. |
| Software Metering will / won’t be supported in the environment. | A core feature of System Center Configuration Manager is to provide several asset management features such as software metering. | Software metering feature will provide information about the usage of software on company computers. |
| Asset Intelligence will / won’t be supported in the environment. | A core feature of System Center Configuration Manager is to provides intelligence into asset management. | Asset intelligence feature will provide information about the licensing of software that exists on company computers. |
| Hardware Inventory feature will / won’t be supported in the environment. | A core feature of System Center Configuration Manager is to collect information about the hardware configuration of client devices in organization. | Hardware inventory feature will provide information about the hardware of client computers and mobile devices that are enrolled by Configuration Manager. |
| The Remote Administration feature will / won’t be supported in the environment. | A core feature of System Center Configuration Manager is to remotely administer, aid, or view any client computer in the hierarchy. | Remote Administration feature will provide help desk support when access to the user’s computer is required using remote control, remote assistance or remote desktop from Configuration Manager console. |

Table 1: Core Infrastructure Design Decisions

When considering the core architecture design, the process is separated into several key areas:

Delete any features from the list below if Core Architecture <FEATURE> is not being implemented in the customer environment.

* **Configuration**
* Resource Discovery
* Collection Structure
* Content Management - Distribution Point Placement, Configuration, Content Replication
* Client Installation
* Client Policy Configuration - Target Devices, Client Policy, Computer Agent, Restart
* Software Asset Management – Software Inventory, Software Metering, Asset Intelligence
* Hardware Inventory – Client computers, mobile devices
* Remote Administration – Remote Control, Remote Assistance, Remote Desktop
* Core Configuration – Management Point
* Role Based Access Control
* **Environment**
* Environment Size, Locations
* Supported Users, Devices, Operating Systems
* Capacity Planning
* Design Constraints
* Diagnostics & Usage Data
* Naming Convention
* Standards & Compliance
* Active Directory
* **Platform**
* Hierarchy - Central Administration Site, Central Administration Site Capabilities
* Hierarchy – Primary Site, Primary Site Capabilities
* Hierarchy - Secondary Site, Secondary Site Capabilities
* Hierarchy - Resilience
* Communication
* Site Server - Operating System
* Database
* Boundaries
* Language
* Administrative Access
  1. Core Infrastructure Dependencies

This section identifies services required for the capability to operate. This includes the following mandatory services:

|  |  |
| --- | --- |
| Component | Description |
| Environment | The refers to the computing environment in which the devices will be managed. This environment consists of the infrastructure, software, tools, applications, and source files that will be used to successfully manage in-scope devices |
| Networking | DNS, DHCP are required for communication with managed devices |
| Operating System | A supported Operating System is required to install System Center Configuration Manager. It is recommended that Windows Server 2012 R2 Standard is used to support site system roles. |
| Active Directory Domain Services | Active Directory Domain Services is required for authentication and authorization of the device to connect to the core infrastructure. |
| Reporting services point | To be able to use the reports in Configuration Manager for asset management & support, you must first install and configure a reporting services point. |

Table 2: Infrastructure Dependencies

The following diagram shows the design of the core infrastructure in the production environment:

**Design Diagram – Pilot Implementation**

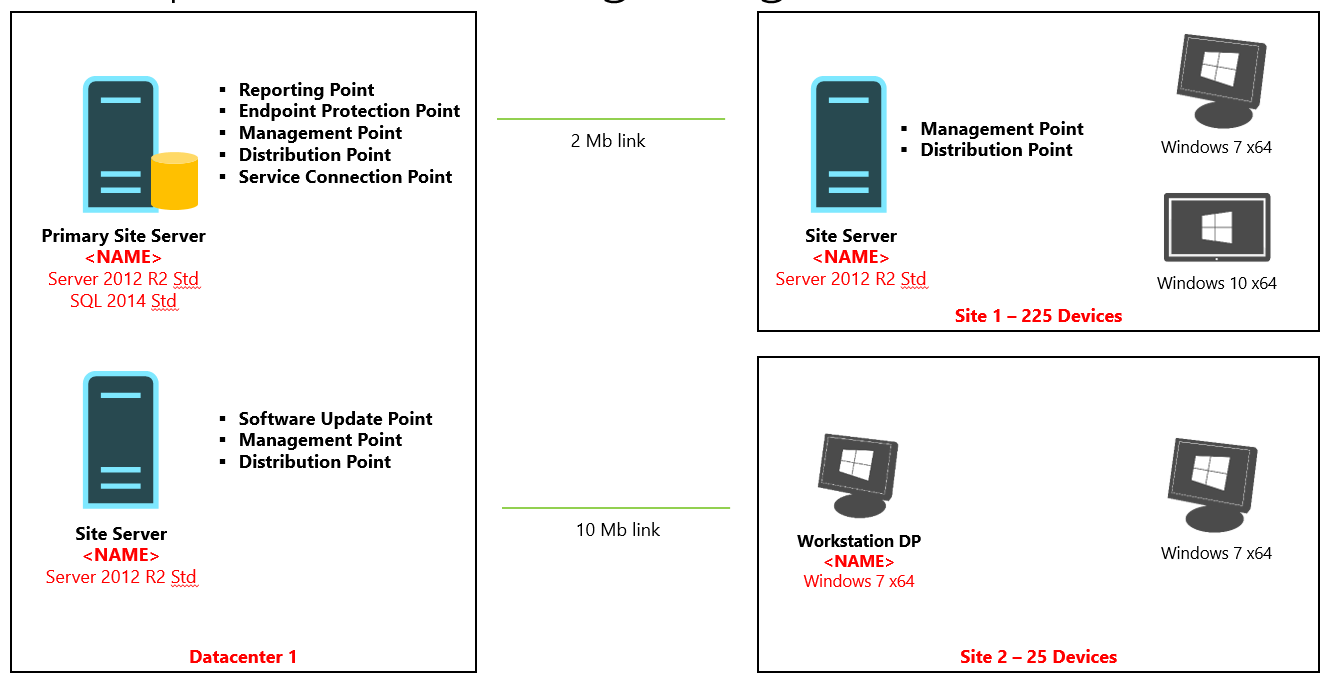


Figure 1: Pilot implementation for Core Infrastructure.

**Design Diagram for <CUSTOMERNAME> Complete Production Implementation**

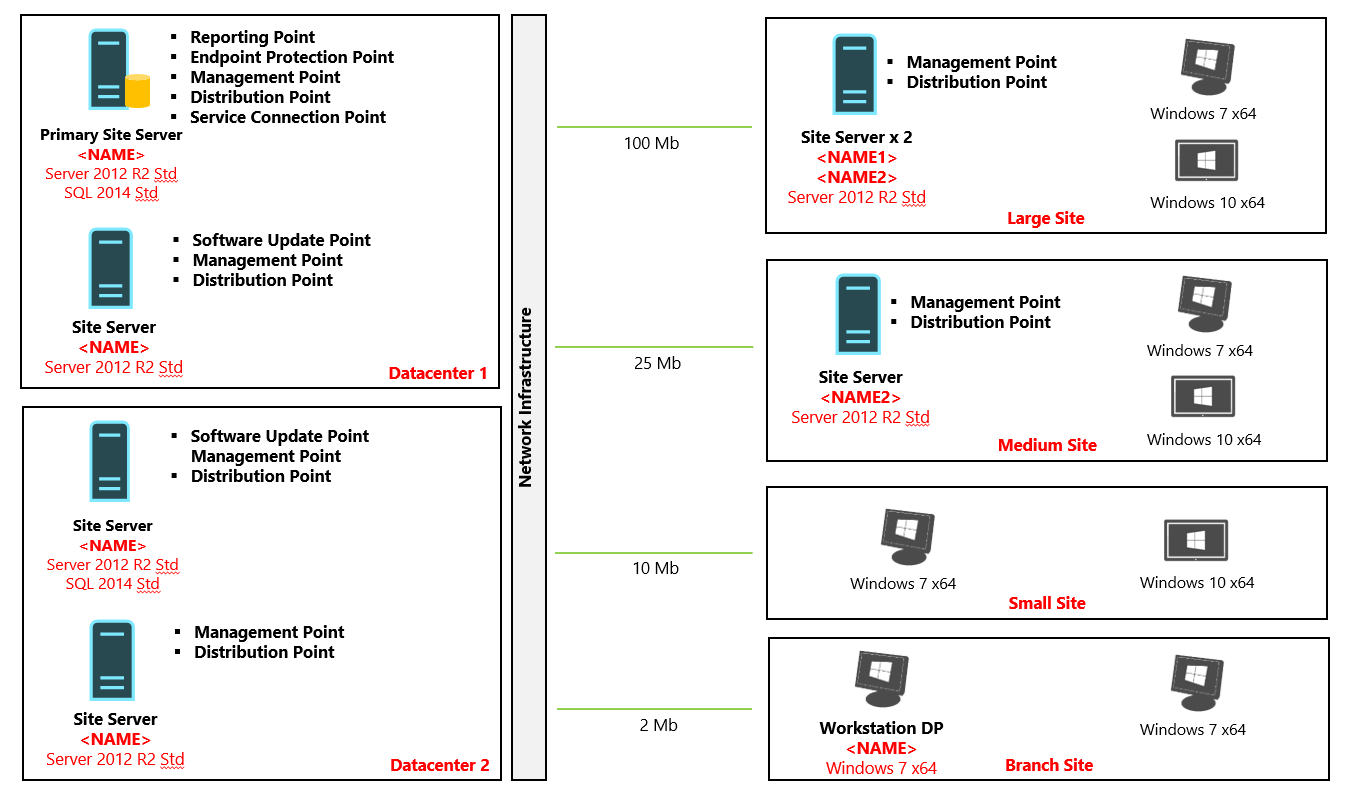


Figure 2: Pilot implementation for Core Infrastructure.

* 1. Azure IaaS Prerequisites

This section details Azure IaaS prerequisites for the core infrastructure and provides context for the design decisions documented in subsequent sections. If you choose to use Azure, you will use these in addition to the Environmental Prerequisites below.

|  |  |
| --- | --- |
| Item | Description |
| [Networking](https://docs.microsoft.com/en-us/sccm/core/understand/configuration-manager-on-azure#networking) | Networking speeds and latency can affect functionality between the site server and remote site systems and any client communication to the site system. Our recommendation is to use ExpressRoute. But there is no Configuration Manager limitation to stop you from using Azure VPN Gateway |
| [Availability](https://docs.microsoft.com/en-us/sccm/core/understand/configuration-manager-on-azure#availability) | Azure VM Availability sets can be used for redundant site system roles like distribution points and management point.  Central administration sites and primary sites can all be in the same availability set which can help you ensure that they are not rebooted at the same time. |
| [Performance](https://docs.microsoft.com/en-us/sccm/core/understand/configuration-manager-on-azure#performance) | Azure VM size and type, Azure VM disks (premium storage is recommended, especially for SQL server), networking latency, and speed are the most important areas  In general, your computer power (CPU and memory) need to meet the recommended hardware for System Center Configuration Manager. |
|  |  |

* 1. Environment Prerequisites

This section details prerequisites for the core infrastructure and provides context for the design decisions documented in subsequent sections.

|  |  |
| --- | --- |
| Item | Description |
| System Center Configuration Manager Active Directory Schema | The schema must be updated to support the integration of System Center Configuration Manager into the Active Directory environment. The customer performs this engagement pre-requisite. |
| Internet Connectivity | Internet connectivity is required to support chosen site system roles e.g. software update management |
| Site Server Infrastructure | The site server infrastructure must be made available to support the design decisions that will be implemented in the pilot deployment. |
| Configuration Manager on Azure | Azure infrastructure considerations must be validated before implementing Configuration Manager on Azure For information on when to use and how to configure Configuration Manager on Azure, see [Configuration Manager on Azure](https://docs.microsoft.com/en-us/sccm/core/understand/configuration-manager-on-azure). |
| Use cloud services with System Center Configuration Manager | For information, see [How to use cloud services with System Center Configuration Manager](https://docs.microsoft.com/en-us/sccm/core/understand/use-cloud-services). |
| Site Server Configuration | The site servers must be configured to support the roles and features that will be installed as part of the design. Review the Technical Planning Spreadsheet (CORE-OS) to review the Operating System configuration required to support the chosen site system roles. |
| Software inventory must be enabled for clients to collect inventory | For information about how to enable and configure software inventory, see [Software Inventory in Configuration Manager](https://technet.microsoft.com/en-us/library/mt488795.aspx). |
| Reporting services point (Software Inventory, Software Metering) | The reporting services point site system role must be installed before you can run reports for software inventory. For more information, see [Reporting in Configuration Manager](https://technet.microsoft.com/en-us/library/mt634338.aspx). |
| Client settings for software metering | To use software metering, the client setting **Enable software metering on clients** must be enabled and deployed to computers. You can deploy software metering settings to all computers in the hierarchy, or you can deploy custom settings to groups of computers. For more information, see [Monitor app usage with software metering in System Center Configuration Manager](https://technet.microsoft.com/en-us/library/mt627957.aspx). |
| Auditing of Success Logon Events Prerequisites (Asset Intelligence) | For Asset Intelligence reports display information gathered from the Windows Security event logs on client computers. If the Security event log settings are not configured to log all Success logon events, these reports contain no data even if the appropriate hardware inventory reporting class is enabled.  The following Asset Intelligence reports depend on collected Windows Security event log information:   * Hardware 03A - Primary Computer Users * Hardware 03B - Computers for a Specific Primary Console User * Hardware 04A - Shared (Multi-user) Computers * Hardware 05A - Console Users on a Specific Computer   To enable the Hardware Inventory Client Agent to inventory the information required to support these reports, you must first modify the Windows Security event log settings on clients to log all Success logon events, and enable the SMS\_SystemConsoleUser hardware inventory reporting class. For more information about modifying Security event log settings to log all Success logon events, see [Enable Auditing of Success Logon Events](https://technet.microsoft.com/en-us/library/gg712322.aspx#BKMK_EnableSuccessLogonEvents). |
| Client Agent Prerequisites (Asset Intelligence) | The Asset Intelligence reports depend on client information that is obtained through client hardware and software inventory reports. To obtain the information necessary for all Asset Intelligence reports, the following client agents must be enabled:   * Hardware Inventory Client Agent   Software Metering Client Agent |
| Hardware Inventory Client Agent Dependencies (Asset Intelligence) | To collect inventory data required for some Asset Intelligence reports, the Hardware Inventory Client Agent must be enabled. In addition, some hardware inventory reporting classes that Asset Intelligence reports depend on must be enabled on primary site server computers.  For information about enabling the Hardware Inventory Client Agent, see [Configuring Hardware Inventory in Configuration Manager](https://technet.microsoft.com/en-us/library/mt488789.aspx). |
| Software Metering Client Agent Dependencies (Asset Intelligence) | Several Asset Intelligence software reports depend on the Software Metering Client Agent for data. For information about enabling the Software Metering Client Agent, see [Monitor app usage with software metering in System Center Configuration Manager](https://technet.microsoft.com/en-us/library/mt627957.aspx) .The following Asset Intelligence reports depend on the Software Metering Client Agent to provide data:   * Software 07A - Recently Used Executables by Number of Computers * Software 07B - Computers that Recently Used a Specified Executable * Software 07C - Recently Used Executables on a Specific Computer * Software 08A - Recently Used Executables by Number of Users * Software 08B - Users that Recently Used a Specified Executable * Software 08C - Recently Used Executables by a Specified User |
| Reporting services point | The reporting services point site system role must be installed before inventory reports can be displayed. For more information about creating a reporting services point, see [Reporting in Configuration Manager](https://technet.microsoft.com/en-us/library/mt634338.aspx). |
| Firewall Configuration (Remote Administration) | If traffic passes through a firewall, TCP port 2701 is required to allow remote control packets to pass between the device that is remote controlled and the device where an administration console is installed. For remote administration, TCP port 3389 is required to support this functionality. |

Table 3: Environment Prerequisites of Core Infrastructure.

This section should be changed and/or completed to detail the Core Infrastructure prerequisites design decisions specified by the customer. Update this section as required

The following table describes how the infrastructure considerations and prerequisites are addressed:

|  |  |  |
| --- | --- | --- |
| Component | Prerequisite Met | Description of service required |
| System Center Configuration Manager Schema | <YES/NO> | The update of the production environment Active Directory schema to support System Center Configuration Manager. |
| Internet Connectivity | <YES/NO> | To enable the download of content to support platform capabilities and features. |
| Site Server Infrastructure | <YES/NO> | Installation of the hardware, networking, storage, operating system, tools, and applications that create the supported environment to install the System Center Configuration Manager platform. |
| Site Server Configuration | <YES/NO> | Configuration of the host operating system as defined in the Technical Planning Spreadsheet (CORE-OS) to support Site Server roles. |
| Software Inventory Enabled | <YES/NO> | Configuration Manager client settings configured to enable Software Inventory on target devices. |
| Reporting Services Point Installed | <YES/NO> | Reporting Services Point site system role installed on a system in the Configuration Manager hierarchy. |
| Software Metering Enabled | <YES/NO> | Configuration Manager client settings configured to enable Software Metering on target devices. |
| Success Logon Attempts Logged | <YES/NO> | Windows Security log configured to log all successful logon attempts on target devices. |
| Firewall Configuration (Remote Administration) | <YES/NO> | Firewall configured to allow Remote administration traffic on the network. |

Table 4: Core Infrastructure Considerations and Prerequisites

* 1. Configuration

This section details decisions related to the configuration of the platform, before devices are managed in the production environment. The scope of the project provides for the design of resource discovery, collection structure, configuration of the client agents, implementation of a default role based access control model and the enabling of capabilities (defined as part of the assessment phase of the project) to provide additional features and functionality to managed devices. Detailed configuration settings are provided in the Technical Planning Spreadsheet, and should be reviewed alongside this document to ensure the configuration of the environment is understood. The table below provides a list of all design decisions related to the implementation in the customer production environment.

|  |  |  |  |
| --- | --- | --- | --- |
| Design Decision | Design Options | Decision | Justification |
| Resource Discovery | * Active Directory Forest Discovery **(Default)** * Active Directory System Discovery **(Default)** * Active Directory Group Discovery **(Default)** * Active Directory User Discovery **(Default)** * Heartbeat Discovery **(Default)** * Delta Discovery **(Default)** * Network Discovery | * **Active Directory Forest Discovery** * **Active Directory System Discovery** * **Active Directory Group Discovery** * **Active Directory User Discovery** * **Heartbeat Discovery** * **Delta Discovery** | This approach ensures all required resources are discovered in the production environment and are updated whilst minimizing impact on domain controllers |
| Content Management – Distribution Point Placement | * Deploy to large sites **(Default)** * Deploy to medium sites **(Default)** * Deploy to small sites * Deploy to cloud * Custom placement | * **Deploy to large sites** * **Deploy to medium sites** | Small sites have sufficient network connections to accommodate content delivery from distribution points in larger sites |
| Content Management – Distribution Point Configuration | * Allow distribution points to respond to incoming PXE requests **(Default)** * Enable distribution points for pre-staged content * Enable unknown computer PXE support | **Allow distribution points to respond to incoming PXE requests** | All distribution points must support a platform delivery capability using PXE |
| Content Management – Content Replication | * Configure Distribution Point Groups **(Default)** * Enable distribution points to pull content from other distribution points * (Design only) Plan to use BranchCache to support content replication * (Design only) Plan to use Alternate Content Providers to support content replication * Not Configured | **Distribution Point Groups** | Distribution points will be grouped to provide resilience for client devices to obtain content |
| Client Installation | * Client Push **(Default)** * Platform Delivery **(Default)** * Automatic Upgrade * Software Update Point * Group Policy * Login Script * Manual * Pre-staged in WIM image | **Client Push**  **Platform Delivery** | The client push method combined with the ability to deploy the latest version of the Configuration Manager client agent satisfy all required client agent deployment scenarios for the production environment |
| Client Policy Configuration – Target Devices | * Client Devices **(Default)** * Server Devices | **Client Devices** | Only client devices will be supported for the implementation of the platform in the production environment |
| Client Policy Configuration – Client Policy | * 60 Minutes **(Default)** * Custom | **60 minutes** | A polling interval of 60 minutes is satisfactory for all devices in the production environment |
| Client Policy Configuration – Computer Agent | * Use default deployment deadlines (every 48 hours, then every 4 hours < 24 hours before deadline, then every 15 mins < 1 hour before deadline) **(Default)** * Custom deployment deadlines | **Default deployment deadlines** | Default deployment deadlines are satisfactory for all devices in the production environment |
| Client Policy Configuration – Client Restart | * Default restart notifications (90 minutes warning, 15 minutes’ countdown box) **(Default)** * Custom restart notifications | **Default restart notifications** | Default restart notifications are satisfactory for all devices in the production environment |
| Client Policy Configuration – Client Cache Settings | * Default Configure client cache size **(Default)** | **Default client size** | Default client cache size are satisfactory for all devices in the production environment |
| Core Configuration – Management Point | * No additional configuration **(Default)** * Use Management Point Affinity | **No additional configuration** | The default configuration of a management point is sufficient support clients in the environment |
| Role Based Access Control | * Use Default Groups **(Default)** * Not Configured * Custom (Out of Scope) | **Use Default Groups** | The customer will refine the role based administration model as the deployment of the platform extends throughout the production environment |
| Enable Software Inventory | * Client devices **(Default)** * Server devices * Not configured | **Client Devices** | Software inventory is required to provide information about the software that exists on client devices |
| Enable Software Metering | * Not configured **(Default)** * Yes | **Not configured** | Software metering is not required to provide information about the software used in the environment |
| Enable Asset Intelligence | * Not configured **(Default)** | **Not configured** | Asset Intelligence functionality is not required in the environment |
| Enable Hardware Inventory | * Client devices **(Default)** * Server devices * Not configured | **Client Devices** | Hardware inventory is required to provide information about the software that exists on client devices |
| Configure Custom Hardware Inventory | * Not configured **(Default)** * Configured | **Not configured** | Custom hardware inventory functionality is not required in the environment |
| Hardware Inventory Data Retention | * 90 Days **(Default)** * Custom | **90 Days** | This is the default setting and no justification exists to change it |
| Enable Remote Control | * No **(Default)** * Yes | **No** | Remote Control is not required to support users in the environment |
| Enable Prompt users for permission to transfer content from shared clipboard | * No (**Default)** * Yes | **No** | Prompt for permission to transfer content from shared clipboard is not required to support users in the environment |
| Enable Remote Assistance | * No **(Default)** * Yes | **No** | Remote Assistance is not required to support users in the environment |
| Enable Power BI Dash | * Not configured **(Default)** * Configured | **Not configured** | Power BI Dashboard is not required in the environment |

Table 5: Design decisions for Configuration

* 1. Environment

This section details decisions related to the environment where the platform will be implemented, and covers the key inputs that are required to ensure the platform meets all environment requirements. The scope of the project provides for the design of the platform to accommodate in-scope users and devices, standards and compliance requirements, capacity requirements, environment constraints and environment naming conventions. The table below provides a list of all design decisions related to the implementation in the customer production environment.

|  |  |  |  |
| --- | --- | --- | --- |
| Design Decision | Design Options | Decision | Justification |
| Environment Size | * Small (Up to 50k) **(Default)** * Medium (50k-175K) * Large (Over 175k) | **Small (Up to 50k)** | The environment is considered small in System Center Configuration Manager terms; this design will ensure only required infrastructure is utilized to support the design |
| Environment Locations | * Design to support all locations **(Default)** * Design to support selected locations | **Design to support all locations** | All locations in the environment will be managed by the platform |
| Supported users | * All users * Selected users (by location) * Selected users (by business unit) | **All users** | All users in the environment will be managed by the platform |
| Supported device Operating Systems for pilot implementation | * Windows 7 **(Default)** * Windows 10 * Windows Server 2012 R2 | **Windows 7** | The customer currently has Windows 7 deployed in the estate and the platform is configured to support client devices only; as such this will be the supported OS for pilot implementation. Note – this does no limit the supported operating systems of the platform for future use |
| Capacity Planning | * Plan for capacity increase as part of design **(Default)** * Do not plan for additional capacity | **Plan for capacity increase as part of design** | It is expected that the environment will see an increase in the number of devices over the next 5 years. Refer to the Technical Planning Spreadsheet (CORE-ENV) for further information |
| Design Constraints | * No design constraints **(Default)** * Infrastructure constraints * Legal constraints * Administrative constraints * Return to Operation constraint * Recovery Point Objective constraint | **No design constraints** | There are no additional environment constraints that should be considered as part of the design |
| Diagnostics & Usage Data | * Enhanced **(Default)** * Basic * Full | **Enhanced** | This level provides Microsoft with the minimum data required to make useful improvements in future versions of products and services |
| Naming Convention | * Use new naming convention **(Default)** * Use existing naming convention | **Use new naming convention** | An existing naming convention has not been identified. Refer to the Technical Planning Spreadsheet (CORE-ENV) for further information. |
| Standards & Compliance | * No standards and compliance requirement **(Default)** * ITIL * MSF * Sarbanes Oxley * Custom | **No standards and compliance requirement** | No existing standards and compliance requirements exist in the production environment. |
| Active Directory | * Single Forest/Single Domain **(Default)** * Multiple Forest/Single Domain * Multiple Forests * Non-Domain Joined | **Single Forest/Single Domain** | N/A |

Table 6: Design decisions for Environment

* 1. Platform

This section details decisions related to the platform that will be used to provide infrastructure management capabilities in the production environment. The scope of the project provides for the design of all required platform features and infrastructure, and the implementation of the design to support up to 250 devices across two customer locations.

The scope of this project does not cover either the design or implementation of features of functionality that extend security of the platform, including but not limited those services which rely on a certificate infrastructure. The table below provides a list of all design decisions related to the implementation in the customer production environment. Detailed configuration settings that expand on this design feature can be found in the Technical Planning Spreadsheet.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Design Decision | Design Options | Decision | | Justification |
| (OPTIONAL) Hierarchy – Central Administration Site | * Not included in hierarchy **(Default)** * Included in hierarchy | **Not included in hierarchy** | The size and configuration of the customer environment do not require the use of a CAS in the environment | | |
| (OPTIONAL) Hierarchy – Central Administration Site Capabilities | * Endpoint Protection Point **(Default)** * Reporting Services Point **(Default)** * Service Connection Point **(Default)** * Software Update Point * Asset Intelligence Synchronization Point | * **Endpoint Protection Point** * **Software Update Point** * **Reporting Services Point** * **Service Connection Point** | All site system roles are required to be installed at the top level or to support platform capabilities requested. | | |
| Hierarchy – Primary Site | * Primary – Standalone **(Default)** * Primary - Hierarchy) | **Primary -Standalone** | * Supported number of devices is within Primary site limits * No requirement for CAS infrastructure | | |
| Hierarchy – Primary Site Capabilities | * Reporting Point **(Default)** * Endpoint Protection Point (Standalone Only) **(Default)** * Application Catalog Web Service Point **(Default)** * Application Catalog Website Point **(Default)** * Software Update Point **(Default)** * Service Connection Point **(Default)** * Asset Intelligence Synchronization Point (Standalone Only) * (Design Only) State Migration Point | * **Reporting Point** * **Application Catalog Web Service Point** * **Application Catalog Website Point** * **Software Update Point** * **Endpoint Protection Point** * **Service Connection Point** | The selected features have been identified as requirements as part of the assessment phase of the System Center Configuration Manager project. Refer to the Technical Planning Spreadsheet (CORE-HIERARCHY, CORE-CAPABILITY) for further information. | | |
| Hierarchy – Azure or On-Premises infrastructure | * Physical Hardware * On-Premises Virtualization **(Default)** * Azure Hosted * Hybrid Azure | * **On Premises Virtualization** | The System Center Configuration Manager hierarchy will be installed on-premises | | |
| (OPTIONAL) Hierarchy – Secondary Site | * Not included in hierarchy **(Default)** * Included in hierarchy | **Not included in hierarchy** | Distribution points will be used to support content replication to remote sites  Network links in the environment support communication from remote sites to the centralized management point infrastructure | | |
| (OPTIONAL) Hierarchy – Secondary Site Capabilities | * Distribution Point * Software Update Point * State Migration Point * No additional capabilities | **No additional capabilities** | * The selected features have been identified as requirements as part of the assessment phase of the System Center Configuration Manager project. * These capabilities will be managed across multiple servers in the production environment | | |
| Hardware | * Virtual Instances **(Default)** * Physical Hardware * Azure Hosted | **Virtual Instances** | The production environment supports the use of virtual machine instances that can support the System Center Configuration Manager solution, and provides scalability and resilience benefits over physical hardware | | |
| Hierarchy – Resilience | * Management point * Distribution point * State migration point * Application Catalog web service point * Application Catalog website point * Software update point * Database Cluster | **Management Point**  **Software Update Point**  **Distribution Point** | * A dedicated database team will separately manage resiliency of the database. * X number of distribution points will be installed per location to support resiliency for content delivery * X number of management points will be installed per location to support resiliency for management features * X number of software update points will be installed per location to support resiliency for update management | | |
| Communication | * HTTP **(Default)** * HTTPS (Out of scope) | **HTTP** | There are no requirements to support secure communications on the production network, which has adequate controls to ensure security within the network boundaries. | | |
| Site Server - Operating System | * Windows Server 2012 R2 (CAS, Primary, Secondary) **(Default)** * Windows Server 2012 (CAS, Primary, Secondary) * Windows Server 2008 R2 (CAS, Primary, Secondary) | **Windows Server 2012 R2 Standard Edition** | Windows Server 2012 R2 Standard provides the longest supportability of the Microsoft Server operating system family and provides for the ability to perform servicing to Windows 10 if used as a Software Update Point when WSUS is installed. | | |
| Database | * Locate on site server (CAS) * Locate on site server (Primary) **(Default)** * Locate on standalone server (CAS) * Locate on standalone server (Primary) * Locate on shared server (CAS/Primary) – Note: implementation may impact other services * Use SQL Always on Availability Groups (Design Option) * Use Database Replicas for Management Points | **Locate on the site server (Primary)** | The number of supported devices in the estate is within supported limits to locate the database on the site server, to reduce infrastructure requirements and ensure there is no latency between the site server and the database. | | |
| Boundaries | * Manually define boundaries **(Default)** * Align boundaries with AD subnets | **Manually define boundaries** | Boundaries will be manually defined to ensure no overlap with existing infrastructure management tools. Refer to the Technical Planning Spreadsheet (CORE-CONFIG) for further information | | |
| Boundary Group | * Configure Relationship tab for fallback of content **(Default)** * Not configured | **Configure Relationship tab for fallback of content** | Boundary Groups will be configured for fallback of content using the Relationship tab between the current boundary group and neighbor boundary groups | | |
| Client Language | * English * <LANGUAGE> | **English** | Client devices are configured in the English language | | |
| Administrative Access | * Connect via Site server (Default) * Use remote console connection | **Connect via Site Server** | The number of administrators in the environment do not warrant the installation of additional consoles to manage the environment. | | |

Table 7: Design decisions for Platform

1. Technical Implementation

This section details the implementation of the core infrastructure developed for the production environment and the steps to install, configure, and operate the platform. The following high-level activities are needed:

|  |  |
| --- | --- |
| Section | Activity |
| 3.3 | Active Directory |
| 3.4 | Database |
| 3.5 | Hierarchy |
| 3.6 | Platform Configuration |
| 3.7 | Client Agent |
| 3.8 | Capabilities |
| 3.9 | Content |
| 3.10 | Software Inventory |
| 3.11 | Software Metering |
| 3.12 | Asset Intelligence |
| 3.13 | Hardware Inventory |
| 3.14 | * 1. Power BI Dashboard   The installation of the Power BI Dashboard is required in the environment, which can be performed using the steps below.   |  |  |  | | --- | --- | --- | | Task | Rationale | Implementation Guidance | | Configure Power BI Dashboard | The Power BI template allows you to do things like:   * Compare key System Center Configuration Manager metrics to personalize targets and see how they trend over time * Identify trouble spots and get the information you need to understand what needs to be done | Refer to the GitHub article for configuration instructions:   * https://github.com/Microsoft/Business-platform-solution-templates/tree/master/Template/Microsoft-SCCMTemplate |   Remote Administration |

Table 8: List of tasks to prepare for Core Infrastructure

* 1. Implementation Activities and Tasks

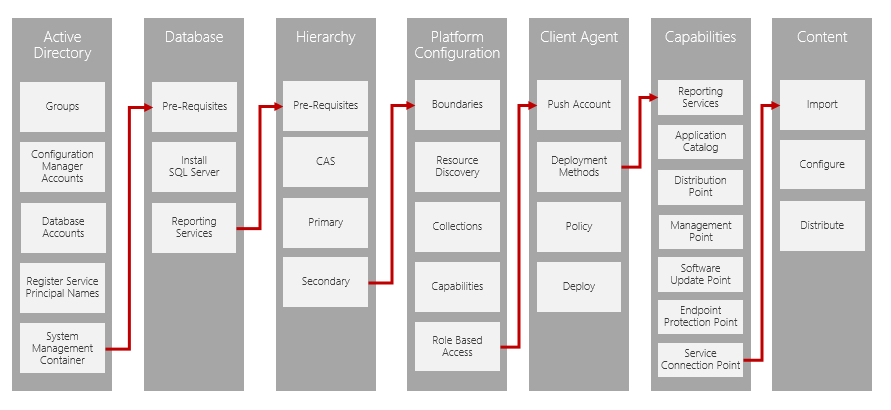


Figure 3: Core Infrastructure Implementation Steps 3.1 to 3.7

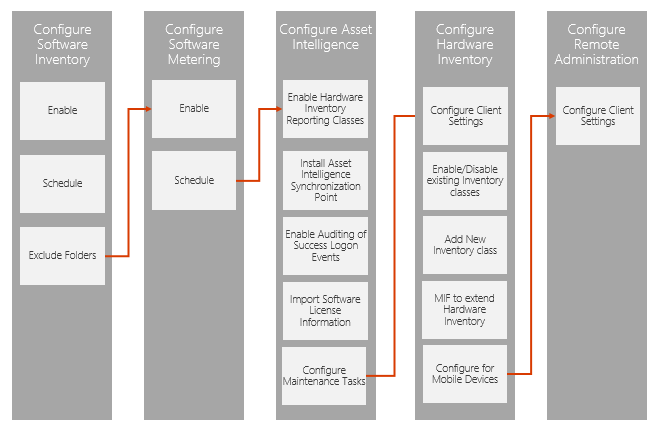


Figure 4: Core Infrastructure Implementation Steps 3.8 to 3.12

* 1. Active Directory

Active Directory must be configured to support the implementation of the platform in the production environment. All the environment pre-requisites outlined in Section 2.2 must be met ahead of performing the steps below.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Create Active Directory Groups | These groups will be used to configure console role based access | * Refer to the Technical Planning Spreadsheet (CORE-AD) for the Active Directory Accounts required for System Center Configuration Manager * Refer to <https://technet.microsoft.com/en-us/library/cc783256(v=ws.10).aspx> to create active directory groups |
| Create Active Directory Accounts | These accounts will be service accounts used to allow for example the System Center Configuration Manager client to be installed. | * Refer to the Technical Planning Spreadsheet (CORE-AD) for the Active Directory Accounts required for System Center Configuration Manager * Refer to <https://technet.microsoft.com/en-us/library/mt627794.aspx> for account requirements. * Refer to <https://technet.microsoft.com/en-us/library/cc784390(v=ws.10).aspx> to create active directory user accounts: |
| Create the SQL Server Service Account | This account will be used to run the SQL Server services | * Refer to the Technical Planning Spreadsheet (CORE-AD) for the Active Directory Accounts required for System Center Configuration Manager * Refer to https://technet.microsoft.com/en-us/library/mt627794.aspx for account requirements. * Refer to <https://technet.microsoft.com/en-us/library/cc784390(v=ws.10).aspx> to create active directory user accounts: |
| Register Service Principal Name | A service principal name (SPN) is the name by which a client uniquely identifies an instance of a service. If you install multiple instances of a service on computers throughout a forest, each instance must have its own SPN. | * Refer to the Technical Planning Spreadsheet (CORE-AD) for the Active Directory Accounts required for System Center Configuration Manager * Execute the following commands: * setspn –A MSSQLSvc/<SQL Server computer name>:1433 <Domain\Account> * setspn -A MSSQLSvc/<SQL Server FQDN>:1433 <Domain\Account> |
| Create System Management Container | System Center 2012 R2 Configuration Manager uses the system management container to publish data and ease administration of the platform. | Refer to the following article to set System Management Container Permissions: <https://technet.microsoft.com/en-us/library/mt345589.aspx> |
| Set System Management Container Permissions | The site server computer account requires access to the system management container so it can publish required data. | Refer to the following article to set System Management Container Permissions: <https://technet.microsoft.com/en-us/library/mt345589.aspx> |

Table 9: Active Directory Configuration Implementation Steps

* 1. Database

A supported version of SQL server is required to support the System Center Configuration Manager implementation. This can be performed using the steps below.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Check Pre-Requisites | Ensure all pre-requisites are available and configured before starting the implementation of the database. | Refer to Technical Planning Spreadsheet (CORE-AD, CORE-HIERARCHY, CORE-DB) to confirm the pre-requisites are available in the environment |
| Install SQL Server | A supported version of SQL server is required to support the System Center Configuration Manager implementation | * Refer to Technical Planning Spreadsheet (CORE-DBCONFIG) for the version and configuration of SQL to be used * Refer to <http://social.technet.microsoft.com/wiki/contents/articles/23878.installing-sql-server-2014-step-by-step-tutorial.aspx> to install SQL Server in the environment |
| Install SQL Server Reporting Services | SQL Server Reporting Services is required to support Reporting functionality in the System Center Configuration Manager environment | * Refer to Technical Planning Spreadsheet (CORE-DBCONFIG) for the version and configuration of SQL Reporting Services to be used * Refer to <http://social.technet.microsoft.com/wiki/contents/articles/23878.installing-sql-server-2014-step-by-step-tutorial.aspx> to install SQL Reporting Services in the environment |
| Configure SQL Server AlwaysOn Availability Groups | Whilst out of scope of this engagement, the steps to migrate a database to SQL AOAG are provided for reference for a move to a highly available site database | * Refer to <https://technet.microsoft.com/en-us/library/mt651651.aspx> for more information |

Table 10: Database Implementation Steps

* 1. Hierarchy

When all pre-requisites are validated, the hierarchy can be implemented in the production environment This can be performed using the steps below.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Check Pre-Requisites | Ensure all pre-requisites are available and configured before starting the implementation of the database. | Refer to Technical Planning Spreadsheet (CORE-AD, CORE-HIERARCHY, CORE-DB) confirm the pre-requisites are available in the environment |
| Run Setup Downloader | Configuration Manager Setup Downloader is a stand-alone application that verifies and downloads required prerequisite redistributable files, language packs, and the latest product updates for Setup. | * Refer to (CORE-HIERARCHY) to determine where to save setup downloader output * Refer to <https://technet.microsoft.com/en-US/library/mt590197.aspx> to start setup downloader |
| Install Central Administration Site (CAS) | Use a central administration site to configure hierarchy-wide settings and to monitor all sites and objects in the hierarchy. A CAS is required when more than one primary site is required in the hierarchy. | * Refer to (CORE-HIERARCHY) to determine where the required site servers will be installed * Refer to <https://technet.microsoft.com/en-US/library/mt590197.aspx> for steps to install a Central Administration Site |
| Install Primary Site | A minimum of one primary site is required in all System Center Configuration Manager implementations | * Refer to (CORE-HIERARCHY) to determine where the required site servers will be installed * Refer to <https://technet.microsoft.com/en-US/library/mt590197.aspx> for steps to install a Primary Site |
| Install Secondary Site | Optional site role that provides management and content to a subset of devices | * Refer to (CORE-HIERARCHY) to determine where the required site servers will be installed * Refer to <https://technet.microsoft.com/en-US/library/mt590197.aspx> for steps to install a Secondary Site |
| Publish Site Data to Active Directory | Each site publishes its own site-specific information to the System Management container within its domain partition in the Active Directory schema | Refer to <https://technet.microsoft.com/en-us/library/mt345589.aspx> to publish site data to Active Directory |
| Install Administrative Console | The installation of administration consoles allows administrative tasks to be performed without the need to connect to a site server | * Refer to (CORE-HIERARCHY) to determine where the required administrative consoles will be installed * Refer to <https://technet.microsoft.com/en-US/library/mt590197.aspx> for steps to install an Administrative Console |

Table 11: Hierarchy Implementation Steps

* 1. Platform Configuration

Boundaries are required to enable client devices to receive content from selected distribution points, and configuration from the appropriate site server in the platform hierarchy. Boundary configuration is performed using the steps below.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Configure Diagnostics & Usage Data | The service connection point provides diagnostic and usage data to Microsoft to improve the installation experience, quality, and security of future releases | * Refer to Section 2.4 – Environment to confirm the chosen diagnostic & usage data setting. Note – the Technical Planning Spreadsheet (CORE-ENV) also contains the chosen setting * To change the setting, launch the System Center Configuration Manager Console and click the blue tab at the top left corner of the console. Select ‘Usage Data’ and select the desired option |
| Configure Boundaries | Boundaries are required to enable client devices to receive content from selected distribution points, and configuration from the appropriate site server in the platform hierarchy | * Refer to the Technical Planning Spreadsheet (CORE-CONFIG) to determine which boundaries to configure * Refer to <https://docs.microsoft.com/en-us/sccm/core/servers/deploy/configure/define-site-boundaries-and-boundary-groups> in order to configure boundaries |
| Configure Boundary Groups | You create boundary groups to logically group related network locations (boundaries) to make it easier to manage your infrastructure. You must assign boundaries to boundary groups before you can use the boundary group. Clients use the boundary group configuration for:   * Automatic site assignment * Content location * Preferred management points | * Refer to the Technical Planning Spreadsheet (CORE-CONFIG) to determine which boundary groups to configure * Refer to <https://docs.microsoft.com/en-us/sccm/core/servers/deploy/configure/define-site-boundaries-and-boundary-groups> in order to configure boundary groups. |
| Configure Resource Discovery | Resource discovery ensures that devices in the environment can be located by the platform and managed per the configuration defined by the environment | * Refer to the Technical Planning Spreadsheet (CORE-CONFIG) to determine which discovery methods to activate * Refer to <https://technet.microsoft.com/en-us/library/mt621991.aspx> to configure discovery |
| Configure Collections | A collection structure can be defined as part of the initial platform implementation, to establish a model to support simplified administration of devices in the environment. | * Refer to the Technical Planning Spreadsheet (CORE-CONFIG) to determine which user and device collections to implement * Refer to <https://technet.microsoft.com/en-us/library/mt629371.aspx> to add and configure user and device collections |
| Configure Distribution Point Groups | Distribution point groups provide a logical grouping of distribution points and collections for content distribution | * Refer to the Technical Planning Spreadsheet (CORE-CONFIG) to determine which distribution point groups to activate * Refer to <https://technet.microsoft.com/en-us/library/mt607024.aspx> for steps to create and configure distribution point groups and distribution point group membership |
| Configure Role Based Access | Role based access for administration of the platform is recommended as part of the implementation process. | * Refer to the Technical Planning Spreadsheet (CORE-AD) to configure the default Role Based Administration settings for the environment * For a custom RBAC implementation, refer to <https://technet.microsoft.com/en-us/library/mt592975.aspx> for more information |

Table 12: Platform Configuration Implementation Steps

* 1. Client Agent

When a client is installed on a device, it communicates with the platform to determine what configuration should be applied to the device, based on collection membership. The installation and configuration of the client agent can be performed using the steps below.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Configure Client Push Account | A client push account should be configured to ensure this deployment method can be used to install and upgrade configuration manager agents in the environment. | * Refer to the Technical Planning Spreadsheet (CORE-AD) for the Client Push Account service account details * Refer to <https://technet.microsoft.com/en-US/library/mt627902.aspx> for account requirements. * Add the Client Push Account using the Accounts tab in the Client Push Installation Method via the System Center Configuration Manager Console. |
| Select Client Deployment Methods | Deployment methods determine how the Configuration Manager client will be installed onto applicable devices. | * Refer to the Technical Planning Spreadsheet (CORE-CONFIG) for configuring client policy * Refer to <https://technet.microsoft.com/en-US/library/mt627814.aspx> to implement client deployment methods |
| Configure Client Settings | Client settings must be configured to ensure managed devices are managed per business and technical requirements in the organization | * Refer to the Technical Planning Spreadsheet (CORE-CONFIG) for configuring client policy * Refer to <https://technet.microsoft.com/en-us/library/mt627896.aspx> and <https://technet.microsoft.com/en-US/library/mt629384.aspx> to configure default and custom client settings |
| Deploy Clients | For workgroup and domain joined Windows devices to be managed, a Configuration Manager client must be installed on the device | * Refer to the Technical Planning Spreadsheet (CORE-CONFIG) for collections to deploy clients to * Refer to <https://technet.microsoft.com/en-us/library/mt627886.aspx> for more information |

Table 13: Client Agent Implementation Steps

* 1. Capabilities

Platform capabilities required by devices in the production environment can be configured using the steps below.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Add a Reporting Services Point | A Reporting Services Point is an optional site system role that provides comprehensive reporting functionality for the System Center Configuration Manager infrastructure. | * Refer to the Technical Planning Spreadsheet (CORE-HIERARCHY, CORE-CAPBILITY) to determine where the site server role will be installed and how it will be configured * Refer to <https://technet.microsoft.com/en-us/library/mt488903.aspx> to confirm site role pre-requisites * Refer to <https://technet.microsoft.com/en-us/library/mt488921.aspx> to install a Reporting Services Point |
| Add an Application Catalog Website Point | The Application Catalog website point is an optional site system role that provides users with a list of available software. | * Refer to the Technical Planning Spreadsheet (CORE-HIERARCHY, CORE-CAPBILITY) to determine where the site server role will be installed and how it will be configured * Refer to <https://technet.microsoft.com/en-us/library/mt621989.aspx#BKMK_Options_SiteSystemRoles> for steps to install the site server role on an existing or new site system server |
| Add an Application Catalog Web Service Point | The Application Catalog web service point is an optional site system role that provides information about available software from the Software Library to the Application Catalog website. | * Refer to the Technical Planning Spreadsheet (CORE-HIERARCHY, CORE-CAPBILITY) to determine where the site server role will be installed and how it will be configured * Refer to <https://technet.microsoft.com/en-us/library/mt621989.aspx#BKMK_Options_SiteSystemRoles> for steps to install the site server role on an existing or new site system server |
| Add a Distribution Point | Site system role that provides content delivery to managed devices. | * Refer to the Technical Planning Spreadsheet (CORE-HIERARCHY, CORE-CAPBILITY) to determine where the site server role will be installed and how it will be configured * Refer to <https://technet.microsoft.com/en-us/library/mt621989.aspx#BKMK_Options_SiteSystemRoles> for steps to install the site server role on an existing or new site system server |
| Add a Cloud Distribution Point | Provides the capabilities of a distribution point for use in Microsoft Azure | * Refer to the Technical Planning Spreadsheet (CORE-HIERARCHY, CORE-CAPBILITY) to determine where the site server role will be installed and how it will be configured * Refer to <https://technet.microsoft.com/en-us/library/mt621989.aspx#BKMK_Options_SiteSystemRoles> for steps to install the Cloud Distribution Point |
| Add a Fallback Status Point | Optional site system role that provides the ability to monitor client deployment for Windows computers and identify the clients on these computers that are unmanaged because they cannot communicate with a management point | * Refer to the Technical Planning Spreadsheet (CORE-HIERARCHY, CORE-CAPBILITY) to determine where the site server role will be installed and how it will be configured * Refer to <https://technet.microsoft.com/en-us/library/mt621989.aspx#BKMK_Options_SiteSystemRoles> for steps to install the site server role on an existing or new site system server |
| Add a Management Point | Site system role that provides configuration and policy to managed devices | * Refer to the Technical Planning Spreadsheet (CORE-HIERARCHY, CORE-CAPBILITY) to determine where the site server role will be installed and how it will be configured * Refer to <https://technet.microsoft.com/en-us/library/mt608546.aspx> to create database replicas for management point use |
| Add a Software Update Point | Optional site system role that provides software update management functionality to supported devices | * Confirm the Software Update Point pre-requisites are in place * Refer to the Technical Planning Spreadsheet (CORE-HIERARCHY, CORE-CAPBILITY) to determine where the site server role will be installed and how it will be configured * Refer to <https://technet.microsoft.com/en-us/library/mt612804.aspx> to install a Software Update Point |
| Add an Endpoint Protection Point | Optional site system role that provides anti-virus and anti-malware functionality to supported devices | * Refer to the Technical Planning Spreadsheet (CORE-HIERARCHY, CORE-CAPBILITY) to determine where the site server role will be installed and how it will be configured * Refer to <https://technet.microsoft.com/en-us/library/mt613207.aspx> to install the Endpoint Protection Point |
| Add an Asset Intelligence Synchronization Point | Optional site system role used to connect to System Center Online (by using TCP port 443) to manage dynamic Asset Intelligence catalog information updates. | * Refer to the Technical Planning Spreadsheet (CORE-HIERARCHY, CORE-CAPBILITY) to determine where the site server role will be installed and how it will be configured * Refer to <https://technet.microsoft.com/en-us/library/mt488912.aspx> for steps to install the site server role on an existing or new site system server |
| Add a Service Connection Point | Site system role that provides:   * Connectivity to a Microsoft Intune tenant that enables Mobile Device Management through the System Center Configuration Manager console * An in-console update capability to the System Center Configuration Manager Platform * In-console servicing data to be populated for the Windows 10 servicing capability | * Refer to the Technical Planning Spreadsheet (CORE-HIERARCHY, CORE-CAPBILITY) to determine where the site server role will be installed and how it will be configured * Refer to <https://technet.microsoft.com/en-us/library/mt627781.aspx> to install the Service Connection Point |

Table 14: Capability Implementation Steps

* 1. Content

The import and configuration of content into the platform is required to support platform features and functionality. This can be performed using the steps below.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Import Content | For content to be distributed to managed devices, it must be imported into the System Center Configuration Manager environment | * Refer to the Technical Planning Spreadsheet (CORE-CONTENT) to determine where content resides in the production environment * Applications - Refer to the Application Management Technical Guide for information on how to import Applications * Software Updates –Refer to the Application Management Technical Guide for information on how to import Applications |
| Configure Content | Content may be required to be configured to support business and technical requirements ahead of delivery | * Refer to <https://technet.microsoft.com/en-us/library/mt607024.aspx> for information<https://technet.microsoft.com/en-us/library/gg682115.aspx> on how to configure content |
| Distribute Content | Content delivery is a key feature of System Center Configuration Manager | * Refer to <https://technet.microsoft.com/en-us/library/mt607024.aspx> for information on how to distribute content. |

Table 15: Content Implementation Steps

* 1. Software Inventory

The environment must be prepared to support Software Inventory in the production environment, which can be performed using the steps below.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Enable software inventory on clients | Must be set to true to take advantage of this feature | Refer to the Technical Planning Spreadsheet (CORE-SWINV) to determine where content resides in the production environment |
| Schedule software inventory and file collection schedule | Configures interval at which clients collect software inventory and files | Refer to the Technical Planning Spreadsheet (CORE-SWINV) to determine how Software Inventory should be configured in the production environment |
| Exclude folders | Use to exclude specific folders from Software Inventory | Refer to TechNet article for further guidance: <https://technet.microsoft.com/en-us/library/mt488908.aspx> |

Table 16: Software Inventory Implementation Steps

* 1. Software Metering

The environment must be prepared to support Software Metering in the production environment, which can be performed using the steps below.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Enable software metering | Must be set to true to take advantage of this feature | * Refer to the Technical Planning Spreadsheet (CORE-SWMETERING) to determine how Software Metering should be configured in the production environment * For more information, refer to the following article: <https://technet.microsoft.com/en-us/library/mt627957.aspx> |
| Schedule data collection | Configure how often software metering data is collected from client computers | * Refer to the Technical Planning Spreadsheet (CORE-SWMETERING) to determine how Software Metering should be configured in the production environment * For more information, refer to the following article: <https://technet.microsoft.com/en-us/library/mt627957.aspx> |

Table 17: Software Metering Implementation Steps

* 1. Asset Intelligence

The environment must be prepared to support Asset Intelligence in the production environment, which can be performed using the steps below.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Enable asset intelligence hardware inventory reporting classes | Must be enabled to take advantage of this feature | * Refer to the Technical Planning Spreadsheet (CORE-ASSETINTEL) to determine how Asset Intelligence should be configured in the production environment * For more information, refer to the following article: <https://technet.microsoft.com/en-us/library/mt488912.aspx> |
| Install an Asset Intelligence Synchronization Point | The Asset Intelligence synchronization point site system role is used to connect Configuration Manager sites to System Center Online to synchronize Asset Intelligence catalog information. | * Refer to the Technical Planning Spreadsheet (CORE-ASSETINTEL) to determine how Asset Intelligence should be configured in the production environment * For more information, refer to the following article: <https://technet.microsoft.com/en-us/library/mt488912.aspx> |
| Enable Auditing of Success Logon Events | Four Asset Intelligence reports display information gathered from the Windows Security event logs on client computers. If the Security event log settings are not configured to log all Success logon events, these reports contain no data even if the appropriate hardware inventory reporting class is enabled. | * Refer to the Technical Planning Spreadsheet (CORE-ASSETINTEL) to determine how Asset Intelligence should be configured in the production environment * For more information, refer to the following article: <https://technet.microsoft.com/en-us/library/mt488912.aspx> |
| Import Software License Information | The Import Software License Wizard is used to import Microsoft Volume Licensing (MVLS) information and general license statements into the Asset Intelligence catalog. | * Refer to the Technical Planning Spreadsheet (CORE-ASSETINTEL) to determine how Asset Intelligence should be configured in the production environment * For more information, refer to the following article: <https://technet.microsoft.com/en-us/library/mt488912.aspx> |

Table 18: Asset Intelligence Implementation Steps

* 1. Hardware Inventory

The environment must be prepared to support Hardware Inventory in the production environment, which can be performed using the steps below.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Configure Hardware Inventory Client Settings | To configures the default client settings for hardware inventory which will apply to all the clients in your hierarchy. If you want these settings to apply to only some clients, create a custom device client setting and assign it to a collection that contains the devices that you want to use hardware inventory. | * Refer to the Technical Planning Spreadsheet (CORE-HWINV) to determine how Hardware Inventory should be configured in the production environment * Refer to TechNet article for configuration instructions: <https://technet.microsoft.com/en-us/library/mt488791.aspx> |
| Enable or Disable Existing Inventory classes | To enable or disable the default inventory classes used by Configuration Manager or to create custom client settings that allows to collect different hardware inventory classes from specified collections of clients. | * Refer to the Technical Planning Spreadsheet (CORE-HWINV) to determine how Hardware Inventory should be configured in the production environment * Refer to TechNet article for configuration instructions: <https://technet.microsoft.com/en-us/library/mt488791.aspx> |
| Add new inventory class | Extend Hardware inventory by adding a new inventory class from the WMI namespace of another device. | * Refer to the Technical Planning Spreadsheet (CORE-HWINV) to determine how Hardware Inventory should be configured in the production environment * Refer to TechNet article for configuration instructions: <https://technet.microsoft.com/en-us/library/mt488791.aspx> |
| MIF to Extend Hardware Inventory | Use Management Information Format (MIF) files to extend hardware inventory information collected from clients by Configuration Manager. | * Refer to the Technical Planning Spreadsheet (CORE-HWINV) to determine how Hardware Inventory should be configured in the production environment * Refer to TechNet article for configuration instructions: <https://technet.microsoft.com/en-us/library/mt488791.aspx> |
| Configure Hardware inventory for mobile devices | To configure Hardware inventory for mobile devices enrolled by Microsoft Intune and Configuration manager | Refer to TechNet article for configuration instructions   * <https://technet.microsoft.com/en-us/library/mt488787.aspx> |
| Configure Maintenance Tasks | To alter the age, schedule, and deletion of Inventory Data for Hardware Inventory | Refer to TechNet article for configuration instructions   * <https://technet.microsoft.com/en-us/library/mt488786.aspx> |

Table 19: Hardware Inventory Implementation Steps

* 1. Power BI Dashboard

The installation of the Power BI Dashboard is required in the environment, which can be performed using the steps below.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Configure Power BI Dashboard | The Power BI template allows you to do things like:   * Compare key System Center Configuration Manager metrics to personalize targets and see how they trend over time * Identify trouble spots and get the information you need to understand what needs to be done | Refer to the GitHub article for configuration instructions:   * <https://github.com/Microsoft/Business-platform-solution-templates/tree/master/Template/Microsoft-SCCMTemplate> |

* 1. Remote Administration

The environment must be prepared to support Remote Administration in the production environment, which can be performed using the steps below.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Configure Client Settings for Remote Administration | To configure the default client settings for remote control which applies to all computers in the hierarchy. If you want these settings to apply to only some computers, create a custom device client setting and assign it to a collection that contains the computers that you want to use in a remote-control session. | * Refer to the Technical Planning Spreadsheet (CORE-RA) to determine how Remote Administration should be configured in the production environment * Refer to TechNet article for configuration instructions: <https://technet.microsoft.com/en-us/library/mt629361.aspx> |

Table 20: Remote Administration Implementation Steps

1. Test Plan

This section details the test plan for the core infrastructure component developed for the production environment. The following tests are needed:

|  |  |
| --- | --- |
| Section | Activity |
| 4.1 | Infrastructure Validation |
| 4.2 | Site Communication |
| 4.3 | Policy Configuration |
| 4.4 | Reporting |
| 4.5 | Access Control |
| 4.6 | Hardware Inventory |
| 4.7 | Software Inventory |
| 4.8 | Remote Administration |

Table 21: List of tasks to test for Core Infrastructure

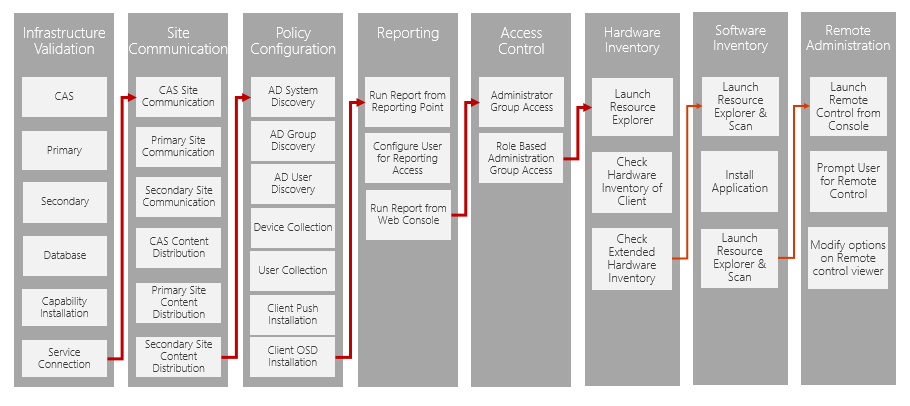


Figure 5: Core Infrastructure Test Scenario

The following sections define the description of how testing should start, pause, and stop for each test scenario. These are key quality metrics to be used in ensuring the items under test are ready to progress to the next stage in the testing process.

* 1. Infrastructure Validation

List of tasks to perform to validate platform infrastructure:

|  |  |  |
| --- | --- | --- |
| Task ID | Description | Pass / Fail |
| 1 | Confirm Central Administration Site installed correctly   * Installation - Check C:\ConfigMgrSetup.log on CAS Server * Roles and Services - Open Console – Monitoring – Sites Status to confirm all services installed and report OK | Choose an item. |
| 2 | Confirm Primary Site installed correctly   * Installation - Check C:\ConfigMgrSetup.log on CAS Server * Roles and Services - Open Console – Monitoring – Sites Status to confirm all services installed and report OK | Choose an item. |
| 3 | Confirm Secondary Site installed correctly   * Installation - Check C:\ConfigMgrSetup.log on CAS Server * Roles and Services - Open Console – Monitoring – Sites Status to confirm all services installed and report OK * Distribution Point – Open Console – Administration – Site Configuration – Secondary Server – Check Distribution Point Role enabled | Choose an item. |
| 4 | Confirm Database installed correctly   * Installation - - Database Server - Open SQL Server Management Studio, Connect to Server (Windows Authentication), Expand databases, Confirm SMS DB listed * Data and Log File Paths – Right Click SMS DB and confirm Path of Data and Log files is correct. | Choose an item. |
| 5 | Confirm Infrastructure Capabilities Installed   * CAS - Logon to server console and confirm required capabilities are installed * Primary - Logon to server console and confirm required capabilities are installed | Choose an item. |
| 6 | Confirm Service Connection Point is configured with selected Diagnostics & Usage Data configuration, and can obtain updates to the System Center Configuration Manager platform   * Online – Confirm Service connection point can download 1602 update * Offline – Confirm 1602 update can be obtained offline | Choose an item. |

Table 22: Infrastructure Validation Test Criteria

* 1. Site Communication

List of tasks to perform to validate site communication:

|  |  |  |
| --- | --- | --- |
| Task ID | Description | Pass / Fail |
| 1 | CAS Site Communication - Verify information is replicating to other sites   * Add new device to primary site, confirm device is present in all systems collection on CAS Site Server. | Choose an item. |
| 2 | Primary Site Communication - Verify information is replicating to other sites   * Add new device to secondary site, confirm device is present in all systems collection on CAS and Primary Site Server. | Choose an item. |
| 3 | Secondary Site Communication – Verify information is replicating to Primary Site   * Add new device to secondary site, confirm device is present in all systems collection on Primary Site Server. | Choose an item. |
| 4 | CAS Content Distribution – Distribute Package to all Distribution Points   * Open System Center Configuration Manager Console, Create Software Package, Deploy to all distribution points. Verify the package has been distributed by selecting the Package status folder. Review all DPs listed to confirm the Targeted and Installed columns are the same. | Choose an item. |
| 5 | Primary Site Content Distribution - Distribute Package to all Distribution Points   * Open System Center Configuration Manager Console, Create Software Package, Deploy to all distribution points. Verify the package has been distributed by selecting the Package status folder. Review all DPs listed to confirm the Targeted and Installed columns are the same. | Choose an item. |
| 6 | Secondary Site Content Distribution - Push Content to Distribution Point   * Open System Center Configuration Manager Console, Create Software Package, Deploy to all distribution points. Verify the package has been distributed by selecting the Package status folder. Review all DPs listed to confirm the Targeted and Installed columns are the same. | Choose an item. |

Table 23: Site Communication Test Criteria

* 1. Policy Configuration

List of tasks to perform to validate policy configuration:

|  |  |  |
| --- | --- | --- |
| Task ID | Description | Pass / Fail |
| 1 | Validate Active Directory System Discovery Functionality   * Add a computer to an Active Directory OU targeted by Active Directory System Discovery, manually trigger Active Directory System Discovery, Check the AdSysDis.log to confirm resource discovery command completed successfully, update collection membership of the All Systems Collection to confirm new resource added. | Choose an item. |
| 2 | Validate Active Directory System Group Discovery Functionality   * Add a group to an Active Directory OU targeted by Active Directory Group Discovery, manually trigger Active Directory Group Discovery, Check the AdSysGrp.log to confirm resource discovery command completed successfully, update collection membership of the All Systems Collection to confirm new resource added. | Choose an item. |
| 3 | Validate Active Directory User Discovery Functionality   * Add a user to an Active Directory OU targeted by Active Directory User Discovery, manually trigger Active Directory User Discovery, Check the AdUsrDis.log to confirm resource discovery command completed successfully, update collection membership of the All Systems Collection to confirm new resource added. | Choose an item. |
| 4 | Validate Device Collection Functionality   * Open the System Center Configuration Manager Console – Assets and Compliance – Create a Device Collection with a membership rule based on an Active Directory OU, devices are members of the collection. Collection should be replicated to all the primary sites and secondary. | Choose an item. |
| 5 | Validate User Collection Functionality   * Open the System Center Configuration Manager Console – Assets and Compliance – Create a User Collection with a membership rule based on an Active Directory OU, users are members of the collection. Collection should be replicated to all the primary sites and secondary. | Choose an item. |
| 6 | Validate Client Push Installation Functionality   * Configure Client Push installation, define systems that client push should be distributed to, confirm after discovery and assignment a client agent should be automatically installed and the correct site code assigned | Choose an item. |
| 7 | Validate Client OSD Installation Functionality   * Deploy a device from the Platform Delivery task sequence, confirm the client appears in System Center Configuration Manager Console and the correct site code is assigned | Choose an item. |

Table 24: Policy Configuration Test Criteria

* 1. Reporting

List of tasks to perform to validate reporting for core features:

|  |  |  |
| --- | --- | --- |
| Task ID | Description | Pass / Fail |
| 1 | Validate reports run as expected from Reporting Point   * Open the System Center Configuration Manager Console on the site server, go to Monitoring – Reporting – Reports. Reports should run from console and reflect accurate data e.g. Software Updates and Inventory information | Choose an item. |
| 2 | Configure User with Reporting Access   * Add a user to a role that has read only access to reports and attempt to view reports using a browser on a workstation. Attempt to access the System Center Configuration Manager console. User should be able to run reports and should not be able to see any data in the System Center Configuration Manager console. | Choose an item. |
| 3 | Validate reports run as expected from Reporting Service Point   * Reports should run and reflect accurate data e.g. Software Updates and Inventory information | Choose an item. |
| 4 | Validate data is shown in the Power BI Dashboard   * Data should be populated and reflect accurate data in the Power BI Dashboard | Choose an item. |

Table 25: Reporting Test Criteria

* 1. Access Control

List of tasks to perform access control validation:

|  |  |  |
| --- | --- | --- |
| Task ID | Description | Pass / Fail |
| 1 | Validate Administrators Group for site servers in hierarchy   * Login as Global Administrator, browse through site settings, run discovery, run reports | Choose an item. |
| 2 | Validate Role Based Administration Group   * Logon as a user in a Role Based Administration Group, confirm RBAC user has full control over their own functions, cannot modify settings or see collections from other sites/regions, cannot run reports from other sites/regions | Choose an item. |

Table 26: Access Control Test Criteria

* 1. Hardware Inventory

List of tasks to perform to check hardware inventory for a device:

|  |  |  |
| --- | --- | --- |
| Task ID | Description | Pass / Fail |
| 1 | Click the computer containing the inventory that you want to view and then, in the **Home** tab, in the **Devices** group, click **Start** and then click **Resource Explorer**. | Choose an item. |
| 2 | Right-click any item in the right-pane of the **Resource Explorer** window and then click **Properties** to open the <item name> Properties dialog box which can help you to view the collected inventory information in a more readable format. | Choose an item. |
| 3 | Check for extended inventory items are collected in the properties | Choose an item. |

Table 27: Hardware Inventory Test Criteria

* 1. Software Inventory

List of tasks to perform to check software inventory for a device:

|  |  |  |
| --- | --- | --- |
| Task ID | Description | Pass / Fail |
| 1 | Right-click the computer containing the inventory that you want to view and then, start **Resource Explorer** and then select **Software Scan** and check the **Last Scan Date**. | Choose an item. |
| 2 | Install an MSI based application on the client computer. Create a test folder under program files and copy an .exe file into the folder. Start the client, open the System Center 2012 R2 Configuration Manager applet in Control Panel. On the Actions tab, run a **Software Inventory Cycle**. On the Primary site, right-click the client and start **Resource Explorer**. Confirm that the .exe file has been inventoried. Confirm that the MSI has been inventoried under Product Details. | Choose an item. |

Table 28: Software Inventory Test Criteria

* 1. Remote Administration

List of tasks to perform to use the remote-control capability from the System Center Configuration Manager console:

|  |  |  |
| --- | --- | --- |
| Task ID | Description | Pass / Fail |
| RM-01 | Click the computer containing the inventory that you want to view and then, in the **Home** tab, in the **Devices** group, click **Start** and then click **Remote Control**. | Choose an item. |
| RM-02 | The Connection should not initiate until the user at remote computer agrees to the remote-control prompt.  Note: If the client setting **Prompt user for Remote Control** permission is set to **True** | Choose an item. |
| RM-03 | Click options like **View – Scale to Fit** or **Action – Send CTRL+Alt+Del key** | Choose an item. |

Table 29: Remote Administration Test Criteria

1. Component Operation

This section details the operation of the service as implemented in the production environment.

|  |  |  |
| --- | --- | --- |
| Scenario | Outcome | Tasks |
| Configure Alerts | Administrators are notified of configured service alert thresholds. | Configure the database server alert threshold - <https://technet.microsoft.com/en-us/library/mt605239.aspx> |
| Backup Platform | Ensure the platform can be backed up on a schedule that can meet customer defined service level agreements, recovery point objectives or return to operation requirements. | * Schedule the site backup maintenance task * Verify site backup maintenance task completes successfully * Perform supplemental backup tasks including the backup of custom reporting, content, custom software updates, user state migration data |
| Restore Platform | Ensure the platform can be restored that can meet customer defined service level agreements, recovery point objectives or return to operation requirements. | Restore the site server using an existing backup or recovery media downloaded by System Center Configuration Manager.  Refer to the following link for more information: <https://technet.microsoft.com/en-us/library/mt605292.aspx#bkmk_Cdlatest> |
| Update Platform | Ensure the platform is kept current to maintain supportability and add new features / functionality | If the version installed is older than current version available on the internet, initiate a controlled process to upgrade the installed version. Refer to the Servicing technical guide for more information. |
| View Software Inventory | Use Resource Explorer in System Center Configuration Manager to view information about software inventory that has been collected from devices in the hierarchy | Refer to TechNet Article for more information: <https://technet.microsoft.com/en-us/library/mt488908.aspx> |
| Monitor Software Metering | Software metering in System Center Configuration Manager includes several built-in reports which allow administrators to monitor information about software metering operations. These reports have the report category of **Software Metering**. | Refer to TechNet Article for more information: <https://technet.microsoft.com/en-us/library/mt627957.aspx> |
| View Asset Intelligence Information | The **Asset Intelligence** home page displays a summary dashboard for Asset Intelligence catalog information. On the home page, you can view information about catalog synchronization and inventoried software status. | Refer to TechNet Article for more information: <https://technet.microsoft.com/en-us/library/mt488912.aspx> |
| View Hardware Inventory | Use Resource Explorer in System Center Configuration Manager to view information about hardware inventory that has been collected from devices in the hierarchy. | Refer to TechNet Article for more information: <https://technet.microsoft.com/en-us/library/mt488791.aspx> |
| Remote Administration | Remotely administer a supported device in System Center Configuration Manager.  Use System Center 2012 Configuration Manager reports to view audit information for remote control. | Refer to TechNet Article for more information: <https://technet.microsoft.com/en-us/library/mt629361.aspx> |

Table 30: Component Operation