Capability Architecture



System Center Configuration Manager

Prepared for

[Type Customer Name Here]

2/7/2017

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](#_Toc474245959)

[2 Current Infrastructure 9](#_Toc474245960)

[2.1 Core 9](#_Toc474245961)

[2.2 Device Management 10](#_Toc474245962)

[2.3 Application Management 10](#_Toc474245963)

[2.4 Servicing 11](#_Toc474245964)

[2.5 Platform Delivery 12](#_Toc474245965)

[2.6 Upgrade or Migration 15](#_Toc474245966)

[3 Core 16](#_Toc474245967)

[3.1 Usage Scenario 17](#_Toc474245968)

[3.2 Infrastructure Requirements 17](#_Toc474245969)

[3.3 Features 20](#_Toc474245970)

[4 Core Upgrade 24](#_Toc474245971)

[4.1 Usage Scenario 24](#_Toc474245972)

[4.2 Infrastructure Requirements 24](#_Toc474245973)

[4.3 Features 25](#_Toc474245974)

[5 Device Management 27](#_Toc474245975)

[5.1 Usage Scenario 27](#_Toc474245976)

[5.2 Infrastructure Requirements 27](#_Toc474245977)

[5.3 Features 29](#_Toc474245978)

[6 Application Management 31](#_Toc474245979)

[6.1 Usage Scenario 31](#_Toc474245980)

[6.2 Infrastructure Requirements 32](#_Toc474245981)

[6.3 Features 33](#_Toc474245982)

[7 Servicing 35](#_Toc474245983)

[7.1 Usage Scenario 35](#_Toc474245984)

[7.2 Infrastructure Requirements 35](#_Toc474245985)

[7.3 Features 37](#_Toc474245986)

[8 Platform Delivery 38](#_Toc474245987)

[8.1 Usage Scenario 38](#_Toc474245988)

[8.2 Infrastructure Requirements 39](#_Toc474245989)

[8.3 Features 40](#_Toc474245990)

[9 Migration 44](#_Toc474245991)

[9.1 Usage Scenario 44](#_Toc474245992)

[9.2 Infrastructure Requirements 44](#_Toc474245993)

[9.3 Features 46](#_Toc474245994)

[10 Gap Analysis 48](#_Toc474245995)

[11 Recommendation 50](#_Toc474245996)

[11.1 Core 50](#_Toc474245997)

[11.2 Core Upgrade 50](#_Toc474245998)

[11.3 Device Management 51](#_Toc474245999)

[11.4 Application Management 51](#_Toc474246000)

[11.5 Servicing 52](#_Toc474246001)

[11.6 Platform Delivery 52](#_Toc474246002)

[11.7 Migration 52](#_Toc474246003)

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

Consultant: This section should be completed last in the document. The section should include text to address the following items:

1. Customer decision on which capability option will be implemented
2. Why this option is selected
3. Complete the table to also indicate why other options were excluded.

|  |  |  |
| --- | --- | --- |
| Capability | Acceptance Rationale | Rejection Rationale |
| The Core Infrastructure capability is designed to size infrastructure required to support the capabilities identified and ensure future growth can be accommodated. Additionally, the capability will support software inventory, hardware inventory and remote support to devices in the production environment | The capabilities that the platform will provide are understood and growth estimates are available to enable the infrastructure to be designed for scalability | Capabilities that the platform will provide are not required; growth estimates are not available. The customer will retain existing inventory and support tooling to provide these services |
| The Core Infrastructure Upgrade capability is designed to support an upgrade of the existing platform if supported. | Existing infrastructure in the production environment can support the in-place upgrade process | Infrastructure is not capable of supporting in-place upgrade to the new version |
| The Device Management capability is designed to support on-premises and mobile devices and apply a consistent policy baseline per customer requirements. | Devices in the environment require the flexibility to be managed on and off customer premises | The customer will retain existing tooling to support mobile devices |
| The Application Management capability is designed for a user centric approach for the installation of applications on client devices | User centric application delivery complies with the application delivery strategy and minimizes device dependencies | Infrastructure in the production environment does not support user-based deployment [User-based application deployment is not part of the IT strategy] |
| The Servicing capability is designed to support client devices using updates and upgrades, Windows 10 devices using the Windows as a Service model and updates to the System Center Configuration Manager infrastructure | Devices and platform infrastructure in the environment require updates and upgrades to be applied in a standardized and automated manner that meet business service level agreements | Windows Update for Business or a 3rd Party infrastructure management tool will manage the servicing capability |
| The Platform Delivery capability is designed for a Zero Touch Installation (ZTI) method for the deployment of a supported customer reference image | Existing infrastructure in the production environment can support Zero Touch Installation of the customer reference image | Infrastructure in the production environment is not capable of supporting Zero Touch Installation of the customer reference image |
| The Migration capability is designed to support the transfer content and configuration from the existing infrastructure management platform to the new environment. | Existing infrastructure in the production environment is capable of supporting migration to the new environment, and content / configuration has been identified that requires migration | Infrastructure is not capable of supporting migration to the new environment, and/or content / configuration does not require an automated transfer approach |

1. Current Infrastructure

Document the current infrastructure that the customer has implemented. This section should be completed after the Infrastructure requirements sections is finished.

The following sections document the current infrastructure implemented in the production environment, which is used to understand what gaps (if any) exist and require remediation ahead of the introduction of System Center Configuration Manager in the production environment.

* 1. Core

The following table provides background information on the supporting infrastructure in the production environment:

|  |  |
| --- | --- |
| Active Directory Version | Click or tap here to enter text. |
| Active Directory Schema extended to support System Center Configuration Manager 2007 or System Center 2012 Configuration Manager |  |
| Internet connectivity available to servers in production environment |  |
| Supported versions of SQL in production environment | Click or tap here to enter text. |
| Supported Server OS’s in production environment | Click or tap here to enter text. |
| Supported Client OS’s in production environment | Click or tap here to enter text. |
| Number of users to support | Click or tap here to enter text. |
| Number of devices to support | Click or tap here to enter text. |
| PXE Network Boot capability utilized for Platform Delivery | Click or tap here to enter text. |
| Software Inventory used in environment |  |
| Software Metering used in environment |  |
| Hardware Inventory used in environment |  |
| Custom hardware inventory used in environment |  |
| Remote support technology used in production environment | Click or tap here to enter text. |
| Power management used in environment |  |
| Support teams provide solicited remote assistance to users |  |
| Support teams provide unsolicited remote assistance to users |  |
| Support teams are permitted to remote control user devices with user permission |  |
| Support teams are permitted to remote control users devices without user permission |  |

Information provided and confirmed by the customer in no more than two paragraphs.

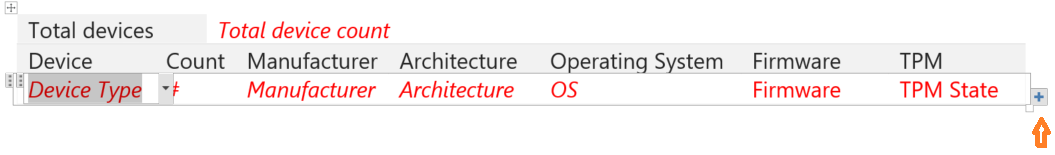
* 1. Device Management

To review the suitability of devices with System Center Configuration Manager, an assessment of the devices that are in the estate will be performed, and the current infrastructure that manages devices will be assessed.

**Device Assessment**

The current device portfolio comprises the following:

Consultant: Add entries by completing information in the starter row. To add more rows, click the “**+**” at the end of the row as shown in the illustration below.



|  |
| --- |
| Total devices |
| Device | | Count | Operating System |
| *Device Type* | | *#* | *OS* |

* 1. Application Management

Desktop applications, often referred to as Win32 apps after the programming interface used, form the major part of any enterprise application portfolio, and often include critical line-of-business applications. The following will be considered priority applications to be imported into System Center Configuration Manager for use by devices in the production environment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Application | App-V Sequenced | Product Name | Version | Comment |
| *Click or tap here to enter text.* |  | *Click or tap here to enter text.* | *Click or tap here to enter text.* | *Click or tap here to enter text.* |

The following table provides background information on the tools and processes used to deploy and access applications in the existing Operating System platform in the production environment:

|  |  |
| --- | --- |
| Application delivery toolset | *Click or tap here to enter text.* |
| Primary application deployment method (Device or User) | *Click or tap here to enter text.* |
| Users can obtain applications through a self-service portal |  |
| Windows Store for Business implemented? |  |
| Applications are deployed to domain joined devices |  |
| Applications are deployed to mobile devices |  |

|  |  |
| --- | --- |
| Applications are categorized for enterprise, role based and individual deployment |  |
| Currently use Windows Universal Applications |  |
| Number of line-of-business Universal apps | *Click or tap here to enter text.* |
| Applications are already Universal apps |  |
| Office suites are currently in use |  |
| Number of Office installations | *Click or tap here to enter text*. |
| Language Packs are required |  |
| Number of Language Packs | *Click or tap here to enter text.* |
| Preferred installation method (MSI vs C2R) | *Click or tap here to enter text.* |
| Preferred activation technology | *Click or tap here to enter text.* |

Add information provided and confirmed by the customer in no more than two paragraphs.

* 1. Servicing

To review the current Servicing infrastructure, an assessment of the products that will be supported will be performed, and the current infrastructure that performs the Servicing capability will be assessed.

**Supported Software Products**

|  |  |
| --- | --- |
| Supported Microsoft Products | Click or tap here to enter text. |
| Supported Product Classifications | Click or tap here to enter text. |
| 3rd Party Products | Click or tap here to enter text. |

**Servicing Infrastructure**

|  |  |
| --- | --- |
| WSUS Version | Click or tap here to enter text. |
| WSUS KB3095113 applied? |  |
| WSUS Server in DMZ? |  |
| Windows Update used by client devices? |  |
| Windows Update for Business implemented? |  |
| 3rd Party Servicing Infrastructure? |  |
| Group Policy configured to point clients to servicing infrastructure? | Click or tap here to enter text. |
| SLA for applying OS updates to client devices | Click or tap here to enter text. |
| SLA for applying OS service packs to client devices | Click or tap here to enter text. |
| SLA for applying OS updates to server devices | Click or tap here to enter text. |
| SLA for applying OS service packs to server devices | Click or tap here to enter text. |

Add information provided and confirmed by the customer in no more than two paragraphs.

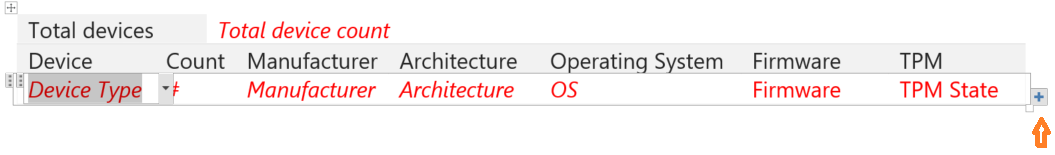
* 1. Platform Delivery

To review the current Platform Delivery infrastructure, an assessment of the devices that will run Windows Operating Systems will be performed, and the current infrastructure that performs the Platform Delivery capability will be assessed.

**Device Assessment**

The most recent refresh of devices in the production environment was performed in Year. The current device portfolio comprises the following:

Consultant: Add entries by completing information in the starter row. To add more rows, click the “**+**” at the end of the row as shown in the illustration below.



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Total devices | | *Total device count* | | | | | |
| Device | Count | | Manufacturer | Architecture | Operating System | Firmware | TPM |
| *Device Type* | *#* | | *Manufacturer* | *Architecture* | *OS* | Firmware | TPM State |

The Unified Extensible Firmware Interface (UEFI) 2.3.1 or later is used by recently released Operating Systems to verify the pre-boot process through the Trusted Boot feature. Devices that use the Basic Input/Output System firmware (BIOS), or incompatible UEFI versions are unable to configure this feature. Trusted Boot is a pre-requisite for the Device Guard feature in Windows 10.

A Trusted Platform Module (TPM) is a cryptographic co-processor attached to the system board of the device. This device is used to generate, and securely store, secrets used in key exchanges. Windows features and applications use TPM 2.0 to store or generate secrets using Credential Guard in Windows 10. Windows BitLocker uses the TPM 1.2 or higher to store secrets associated with an encrypted drive.

System Center Configuration Manager devices:

**are/are not** compliant with UEFI 2.3.1.

**are/are not** installed with a TPM chip that supports version 1.2 or above

**do / do not** support TPM 2.0 where a TPM chip is installed

Use **BIOS / UEFI** to boot the existing Operating System

**Supporting Infrastructure Assessment**

A supporting infrastructure is required to support bare metal and device rebuild scenarios. The following table provides background information on the tools and processes used to deploy the existing Operating System platform in the production environment:

|  |  |
| --- | --- |
| Primary identity repository e.g. Active Directory | *Click or tap here to enter text.* |
| Schema Version | *Click or tap here to enter text.* |
| Users authenticate to published services using this identity |  |
| Identity is synchronized to a cloud service |  |
| Synchronization method/tool and version | *Click or tap here to enter text.* |
| Personal identities are permitted e.g. Microsoft Account |  |
| Certificates are used for identity |  |
| Last Active Directory Health Check | *Click or tap to enter a date.* |

|  |  |
| --- | --- |
| Completion of last major deployment | *Click or tap to enter a date.* |
| Previous operating system | *Choose an OS* |
| Duration of last deployment (incl. engineering time) | *Click or tap here to enter text.* |
| Primary deployment method | *Click or tap here to enter text.* |
| Secondary deployment method | *Click or tap here to enter text.* |
| New devices are deployed using | *Click or tap here to enter text.* |
| Remote devices are deployed using | *Click or tap here to enter text.* |
| Device procurement cycle (years) | *Click or tap here to enter text.* |
| Number of custom partitions when deployed | Click or tap here to enter text. |
| Disk partition structure maintained for Windows 10 |  |

|  |  |
| --- | --- |
| Domain systems managed with (include version) | Click or tap here to enter text. |
| WMI scripting currently used | Click or tap here to enter text. |
| AppLocker currently in use | Click or tap here to enter text. |
| PowerShell currently used | Click or tap here to enter text. |
| MDOP currently used (product and version) | Click or tap here to enter text. |
| Are there dedicated devices for Administrators | Click or tap here to enter text. |
| Workgroup Windows devices are used |  |
| Number of workgroup Windows devices | Click or tap here to enter text. |
| Workgroup devices are managed using | Click or tap here to enter text. |
| Mobile Device Management products (vendor & version) | Click or tap here to enter text. |

Information provided and confirmed by the customer in no more than two paragraphs.

* 1. Upgrade or Migration

In supported scenarios, the existing infrastructure management platform can be connected to System Center Configuration Manager to provide an automated capability to migrate content and configuration. The following table provides background information on the capabilities implemented by the existing infrastructure management platform in the production environment:

Record the list of capabilities used by the existing infrastructure management platform:

|  |  |
| --- | --- |
| System Center Configuration Manager Version | *Click or tap here to enter text*. |
| Active Directory Schema Extended |  |
| Software Distribution Feature |  |
| Software Update Feature |  |
| Software Metering Feature |  |
| Mobile Device Management Feature |  |
| Operating System Deployment Feature |  |
| Desired Configuration Management (Settings Management) Feature |  |
| Remote Tools Feature |  |
| Network Access Protection Feature |  |
| Wake on LAN Feature |  |
| Out of Band Management Feature |  |
| Reporting Feature |  |
| Power Management Feature |  |

Add information provided and confirmed by the customer in no more than two paragraphs.

1. Core

This section discusses the Core architecture of the platform. The capability provides the design of the hierarchy per customer technical and business requirements, and includes changes to the core infrastructure to accommodate features and functionality required from the output of device management, platform delivery, application management and asset management and support capability workshops. The following service inputs are applicable to the Core architecture, which are discussed below:

* **Stakeholder Input** – Customer participants that contribute to defining the requirements during the Core architecture workshop. This input is used to design the hierarchy of the platform and the infrastructure required to support the core features and solution capabilities defined in previous workshops.
* **Users and Devices** – Information that can be shared about the size of the company in terms of supported users and devices will assist in shaping the design per customer requirements.
* **Capacity Planning** – Guidance regarding future changes to the size of the company, including number of supported users and geography can assist to size core infrastructure for scalability
* **Standards and Compliance** - An understanding of corporate standards and compliance that impact the infrastructure management platform is required to ensure that any parameters can be met in the design.
* **Constraints** - An understanding of business or technical constrains that may impact the approach to the design of the core infrastructure is required to ensure that constraints can be accommodated in the design.
* **Service Level Agreements and Resiliency** - An understanding of any Service Level Agreements or resiliency requirements are needed as service inputs for capabilities offered by the solution. This will assist in the design of the core infrastructure
* **Hardware Inventory Customization** – Windows Management Instrumentation (WMI), Managed Object Files (MOF) or Management Information Files (MIF) can be used to extend existing Hardware Inventory capabilities.
* **Current Recommended Practice** - The design principles presented in this document for Core architecture follow Microsoft’s current recommended practice for designing a System Center Configuration Manager hierarchy
  1. Usage Scenario

List the scenarios for which the technical component is recommended.

The Core architecture capability is used to:

* Create an infrastructure management hierarchy that meets both business and technical requirements of the organization
* Determine if the solution will manage mobile devices
* Scale the solution to accommodate for planned capacity increases
* Define a baseline of configuration settings for devices that will be managed by the solution
* Monitor devices in the estate to provide compliance and inventory information
* Design the infrastructure to support the capabilities defined in the capability workshops
  1. Infrastructure Requirements

Infrastructure requirements for the Core architecture capability is categorized as follows:

* Infrastructure required to support the Core architecture capability;
* Networking requirements to ensure the core architecture can operate.

The following infrastructure is required to support the Core architecture capability

|  |  |  |
| --- | --- | --- |
| Requirement | Specification | Comments |
| Active Directory | * A supported version of Active Directory is required for authentication and authorization of client devices. * A change to the Active Directory Schema is recommended to allow clients to retrieve many types of information related to Configuration Manager from a trusted source. | The Active Directory schema extensions for System Center Configuration Manager are unchanged from those used by System Center Configuration Manager 2007. If the schema is already extended in the production environment, this action does not need to be performed again. |
| Networking | * DNS to support name resolution and communication between devices * Firewall configuration to support remote control and remote assistance capabilities * DHCP to provide a network address to the device * (OPTIONAL) Internet connectivity to support platform capabilities | The Core infrastructure should be designed to support devices across slow network links, if required. |
| (OPTIONAL) Central Administration Site Infrastructure | * Required to support multiple primary sites in the production environment * Required for customers with over 175,000 devices in the environment | * The Central Administration Site is the top-level site in a hierarchy * Clients cannot be assigned to the Central Administration Site |
| Primary Site Infrastructure | * A single Primary Site is suitable for customers with less than 175,000 devices in the environment. * Each primary site can support up to 250 secondary sites * (OPTIONAL) Asset Intelligence Synchronization Point * (OPTIONAL) Reporting Point | The primary site system server should be appropriately sized to accommodate customer size, future scalability requirements and all features identified for use in the production environment. A Reporting Point is required to report on information collected. An additional site system role is required to support Asset Intelligence. |
| (OPTIONAL) Secondary Site | Use secondary sites to manage the transfer of deployment content and client data across low-bandwidth networks. | Consider using Windows BranchCache or distribution points that are enabled for bandwidth control and scheduling to reduce infrastructure investments |
| Database Infrastructure | * SQL Server 2008 R2, 2012, 2014 and 2016 are supported with specific Service Packs and Cumulative Updates for each version * The hierarchy chosen and number of supported devices determines whether SQL Standard or Enterprise edition is best. | The SQL Server instance can be co-located with the site system server, or on a remote computer. The decision to locate the database on a separate server provides the option for increased scalability to accommodate future growth. |
| Management Point Infrastructure | * Each primary site supports up to 15 management points * Allocate at least one management point for every 25,000 clients | The number of devices that a management point supports depends on the type of site where the management point is located, and the type and numbers of clients that might use the management point |
| Distribution Point Infrastructure | * Each primary and secondary site supports up to 250 distribution points. * Each primary and secondary site supports up to 2000 additional distribution points configured as pull-distribution points * Each distribution point supports up to 4000 devices | Devices that use the platform delivery and application management capability leverage distribution point to obtain content. The site system roles should be appropriately sized to accommodate customer platform delivery and application management requirements. |
| Device Management Infrastructure | * (OPTIONAL) The Service Connection Point and Microsoft Intune subscription is required to provide a Hybrid Mobile Device Management Capability | * Management Point infrastructure should be scaled accordingly to support the transfer of policy to client devices |
| Platform Delivery Infrastructure | * (OPTIONAL) The State Migration Point Role can be configured to support a User State Migration capability for replace deployment scenarios | * Distribution Point infrastructure should be scaled accordingly to support the transfer of OS, application, and configuration content to client devices |
| Application Management Infrastructure | * (OPTIONAL)The Application Catalog Website Point and Application Catalog Web Service Point can be configured to provide a Self-Service Application capability * (OPTIONAL) A Software Update Point can be configured to update Microsoft products that exist in the production environment | * Distribution Point infrastructure should be scaled accordingly to support the transfer of OS, application, and configuration content to client devices * Windows Server 2012 R2 is recommended to run the Software Update Point to ensure the Windows 10 servicing approach can be accommodated in future releases of the product. |
| Asset Management & Support Infrastructure | * (OPTIONAL) Asset Intelligence Synchronization Point is required to connect Configuration Manager sites to System Center Online to synchronize Asset Intelligence catalog information * Firewall configuration to support remote control and remote assistance capabilities | * Out of band management is out of scope for the System Center Configuration Manager project. * Internet connectivity is required to support the Asset Intelligence Synchronization Point * Management Point infrastructure should be scaled accordingly to support the transfer of policy to client devices |
| Secure Communication Infrastructure | * Public Key Infrastructure required to support a secure communication solution | * Secure communication is out of scope for the System Center Configuration Manager project. * It is recommended to validate the operation of the solution without the use of secure communication as a first step, before implementing a secure communication solution. |

* 1. Features

The following features are available for use with the Core infrastructure capability.

|  |  |  |
| --- | --- | --- |
| Feature | Description | Usage Scenario |
| Application Management | Provides a set of tools and resources that can help you create, manage, deploy, and monitor applications in the enterprise | * Design the infrastructure to support the capabilities defined in the capability workshops |
| Company Resource Access | Provides a set of tools and resources that enable users to access data and applications from remote locations. These tools include Email profiles and Windows Hello for Business | * Design the infrastructure to support the capabilities defined in the capability workshops |
| Compliance Settings | Provides a set of tools and resources that can assess, track, and remediate the configuration compliance of client devices in the environment. | * Design the infrastructure to support the capabilities defined in the capability workshops |
| Endpoint Protection | Provides security, antimalware, and Windows Firewall management for devices in the environment | * Define a baseline of configuration settings for devices that will be managed by the solution |
| Inventory | Provides a set of tools to help identify and monitor assets:   * Hardware inventory: Collects detailed information about the hardware of devices in the environment * Software inventory: Collects and reports information about the files that are stored on devices * Asset Intelligence: Provides tools to collect inventory data and to monitor software license | * Design the infrastructure to support the capabilities defined in the capability workshops |
| Operating System Deployment | Provides a tool to deploy operating systems to devices that are managed by Configuration Manager and to unmanaged computers, by using PXE boot or bootable media such as a CD set, DVD, or USB flash drives. | * Design the infrastructure to support the capabilities defined in the capability workshops |
| Power Management | Provides a set of tools and resources that you can use to manage and monitor the power consumption of client computers in the enterprise. | * Define a baseline of configuration settings for devices that will be managed by the solution |
| Queries | Provides a tool to retrieve information about resources in your hierarchy and information about inventory data and status messages. You can then use this information for reporting or for defining collections of devices or users for software deployment and configuration settings. | * Monitor devices in the estate to provide compliance and inventory information |
| Remote Connection Profiles | Provides a set of tools and resources to help create, deploy, and monitor remote connection settings to devices in the environment. By deploying these settings, end-user effort required to connect to the device on the corporate network is minimized. | * Design the infrastructure to support the capabilities defined in the capability workshops |
| Remote Control | Provides tools to remotely administer client devices from the Configuration Manager console. | * Design the infrastructure to support the capabilities defined in the capability workshops |
| Reporting | * Provides a set of tools and resources that help use the advanced reporting capabilities of SQL Server Reporting Services from the Configuration Manager console. * Integrate with PowerBI to deliver rich visual dashboards | * Design the infrastructure to support the capabilities defined in the capability workshops |
| Software Metering | Provides tools to monitor and collect software usage data from Configuration Manager clients. | * Design the infrastructure to support the capabilities defined in the capability workshops |
| Software Updates | Provides a set of tools and resources that can help manage, deploy, and monitor software updates in the environment. | * Design the infrastructure to support the capabilities defined in the capability workshops |
| Microsoft Intune Management | * This feature can be used to manage iOS, Android (including Samsung KNOX), Windows Phone and Windows devices using the Microsoft Intune service over the Internet. * Although the Microsoft Intune service is used, the Service Connection Point site system role (available through the Configuration Manager console) completes management tasks. | * Design the infrastructure to support the capabilities defined in the capability workshops * Determine if the solution will manage mobile devices |
| Servicing | Provides the capability to service Windows 10 client devices and the System Center Configuration Manager platform | * Design the infrastructure to support the capabilities defined in the capability workshops |

1. Core Upgrade

This section discusses the capabilities enabled by the upgrade from the existing infrastructure management platform. The Core Upgrade capability is used to upgrade from a supported version of System Center Configuration Manager. The following service inputs are applicable to the migration capability, which are discussed below:

* **Stakeholder Input** – Customer participants that contribute to defining the requirements during the upgrade workshop. This input is used to determine what components will be retained after the upgrade to the latest System Center Configuration Manager platform.
* **Content** – Required content from the existing platform that supports capabilities in the production environment.
* **Configuration** – Required configuration from the existing platform that supports capabilities in the production environment.
* **Current Recommended Practice** - The design principles and default configurations in this document comply with Microsoft’s current recommended practice for upgrading to the latest System Center Configuration Manager platform.
  1. Usage Scenario

List the scenarios for which the technical component is recommended.

The Core Upgrade capability is used to:

* Design and architect an upgrade strategy form the existing infrastructure management platform.
* Ensure content and configuration can be delivered to the production environment in a repeatable and reliable manner to reduce administrative overhead and defects associated with manual processes.
  1. Infrastructure Requirements

Infrastructure requirements for the Core Upgrade capability are considered in the following categories:

* Requirements for the existing System Center Configuration Manager environment;
* Networking and storage requirements for the infrastructure management platforms.

The following infrastructure is required to support core upgrade capability:

|  |  |  |
| --- | --- | --- |
| Requirement | Specification | Comments |
| Existing Infrastructure | * The existing infrastructure management platform must meet the minimum requirements of System Center 2012 Configuration Manager SP1 * The System Center Configuration Manager environment must exist in the production environment and has no unresolved issues * The following roles must be uninstalled * Out of Band Management Point * Service Health Validator Point | System Center Configuration Manager 2007 R2 or R3 on the source site are not a consideration. |
| Networking | Domain Name Resolution (DNS) to support name resolution and communication | The existing infrastructure management platform must be able to communicate with the System Center Configuration Manager environment. |

* 1. Features

The following features are required to support Migration:

|  |  |  |
| --- | --- | --- |
| Feature | Description | Usage Scenario |
| Application Management Content & Configuration | All existing customer selected application and software update artefacts/configuration that must be upgraded to the new platform | * Ensure users have the applications they need to perform their role or function * Ensure content and configuration can be delivered to the production environment in a repeatable and reliable manner to reduce administrative overhead and defects associated with manual processes. |
| Platform Delivery Content & Configuration | Existing selected content & configuration and that may contain Reference images, drivers, task sequences and boot images | * Ensure content and configuration can be delivered to the production environment in a repeatable and reliable manner to reduce administrative overhead and defects associated with manual processes. |
| Device Management Configuration | Existing selected compliance configuration that must be migrated to the new platform | * Apply a consistent settings management baseline to devices across both infrastructure management platforms * Ensure content and configuration can be delivered to the production environment in a repeatable and reliable manner to reduce administrative overhead and defects associated with manual processes. |
| Asset Management & Support Configuration | Existing selected asset intelligence and software metering configuration that must be migrated to the new platform | * Ensure content and configuration can be delivered to the production environment in a repeatable and reliable manner to reduce administrative overhead and defects associated with manual processes. |
| Core Infrastructure Configuration | Existing selected boundary and collection configuration information that must be upgraded to the new platform | * Ensure content and configuration can be delivered to the production environment in a repeatable and reliable manner to reduce administrative overhead and defects associated with manual processes. |

1. Device Management

This section discusses the capabilities enabled by Device Management. The device management policies created by the <PROJECTNAME> ensures supported device types are managed per customer requirements, comply with corporate compliance settings, are protected by an anti-malware solution, and have a defined power management configuration applied. These settings are applied per the specification outlined in the Device Management technical guide. The following service inputs are applicable to the device management architecture, which are discussed below:

* **Stakeholder Input** – Customer participants that contribute to defining the requirements during the Device Management workshop. This input is used to design and configure the device management system that meets the requirements of the production environment.
* **Management Tools** – To enable mobile device management as part of the project, the appropriate products and subscriptions are required to ensure connectivity between the solution and a supported device type can be achieved.
* **Current Recommended Practice** - The design principles presented in this document for Device Management follow Microsoft’s current recommended practice
  1. Usage Scenario

List the scenarios for which the technical component is recommended.

Device Management is used to:

* Determine which supported device types the solution will manage
* Enable devices to access company resources in a secure manner
* Ensure devices meet a specified compliance baseline
* Protect corporate data against potential data leakage
* Protect supported devices using a solution to reduce malware infection risk
* Configure and manage the power settings of supported device types
  1. Infrastructure Requirements

Infrastructure requirements for Device Management can be categorized as follows:

* Infrastructure required to support the management of on-premises devices
* Infrastructure required to support the management of mobile devices
* Networking required to support the delivery of large volumes of data reliably to one or more systems during a deployment.
* Devices that are supported by and can be managed by the solution

The following infrastructure is required to support Device Management

|  |  |  |
| --- | --- | --- |
| Requirement | Specification | Comments |
| On-premises device management infrastructure | The following roles must be configured to support Device Management in System Center Configuration Manager:   * Primary Site * Management Point * (OPTIONAL) Central Administration Site | Devices that use the device management capability leverage the management point to authenticate and obtain configuration information. The management point site system role should be appropriately sized and scaled to accommodate customer device management requirements. |
| Hybrid device management infrastructure | The following roles must be configured to support Device Management in System Center Configuration Manager:   * Primary Site * Management Point * Service Connection Point * (OPTIONAL) Central Administration Site | * A Microsoft Intune subscription is required to enable the Hybrid device management infrastructure. * On-premises devices use the device management capability leverage the management point to authenticate and obtain configuration information. Mobile devices use Microsoft Intune and obtain configuration information from System Center Configuration Manager using the Service Connection Point. Site system roles should be appropriately sized and scaled to accommodate customer device management requirements. |
| Networking | * DNS to support name resolution and communication between devices and the management infrastructure * DHCP to provide a network address to the device to enable communication in the customer environment * Internet connectivity for mobile devices to communicate to Microsoft Intune. | The Device Management infrastructure should be designed to support devices across slow network links |
| Supported Devices | * The device management product must support devices to be managed | Refer to <https://technet.microsoft.com/en-US/library/mt589738.aspx#bkmk_ClientOS> for a list of supported devices for System Center Configuration Manager and Microsoft Intune |

* 1. Features

The following features are required to support Device Management:

|  |  |  |
| --- | --- | --- |
| Feature | Description | Usage Scenario |
| Company Resource Access | * Provisions authentication certificates for managed devices * E-mail profiles * Windows Hello for Business * Secure services on devices that are enrolled in Microsoft Intune based on conditions that enforce company policy | * Enable devices to access company resources in a secure manner |
| Compliance Settings | * Used to manage configuration (includes Windows Information Protection) and compliance of Windows and non-windows devices, including mobile devices | * Ensure devices meet a specified compliance baseline |
| Endpoint Protection | * Provides an antimalware and security solution for the Microsoft platform, including: * Alert configuration * Antimalware policy configuration * Windows firewall configuration | * Protect supported devices using a solution to reduce malware infection risk |
| Power Management | * Allows the configuration of Peak and Non-Peak plans for hardware with appropriate power capabilities * Collects information through Hardware Inventory related to the consumption of power | * Configure and manage the power settings of supported device types |

1. Application Management

This section discusses the capabilities enabled by Application Management. The capability is defined by the supported application types, deployment mechanisms and application targeting approach per the specification outlined in the Application Management technical guide. The following service inputs are applicable to the application management architecture, which are discussed below:

* **Stakeholder Input** – Customer participants that contribute to defining the requirements during the Application Management workshop. This input is used to design and configure the application deployment system that meets the requirements of the production environment
* **Application Inventory** – Used to determine which applications are to be imported into the System Center Configuration Manager environment
* **Application Source** – Application media is available and can be used without modification
* **Application Settings** – Configures the installation of applications, and application settings, during the delivery process
* **Current Recommended Practice** - The design principles presented in this document for the Application Management capability follow Microsoft’s current recommended practice for deploying applications to a device in a device or user centric fashion
  1. Usage Scenario

List the scenarios for which the technical component is recommended.

Application Management is used to:

* Ensure that users have the required applications to perform a job function
* Target applications efficiently to devices, groups of devices & users, or individuals
* Install essential corporate applications to devices for use at first logon
* Install role based applications to users or devices through a direct association or via group membership
* Expedite application installation and availability for use
* Support a user centric application delivery approach that provides the user with an application type suitable for the device being used
* Provide a self-service capability for users to install applications they require without the need to raise a service desk request
* Utilize application deployment types that are de-coupled from the operating system and minimize the footprint of the application on the device
  1. Infrastructure Requirements

Infrastructure requirements for Application Management can be considered in the following categories:

* Infrastructure required to support user-centric and device-centric application delivery models
* Networking and storage requirements to manage application delivery in the production environment.

The following infrastructure is required to support Application Management

|  |  |  |
| --- | --- | --- |
| Requirement | Specification | Comments |
| Application Management Infrastructure | The capability must meet the minimum requirements for the following roles in System Center Configuration Manager:   * Primary Site * Management Point * (OPTIONAL) Central Administration Site * (OPTIONAL) Secondary Site * Distribution Point * (OPTIONAL) Software Update Point * Application Catalog web service point (for Self Service Application Delivery) * Application Catalog website point (for Self Service Application Delivery) | Application Management infrastructure can provide a mixture of administrative application delivery and a self-service capability for users to select and install approved applications.  User centric application delivery and App-V application delivery is supported on System Center Configuration Manager. |
| Networking | * DNS to support name resolution and communication between Windows devices, the customer Active Directory domain, and the update infrastructure * DHCP to provide a network address to the Windows 10 device to enable communication in the customer environment * (OPTIONAL) Internet Connectivity to support access to the Universal Application deep link application type with a dedicated Application Management infrastructure and Windows Store for Business integration | The Application Management infrastructure should be designed to support devices across slow network links and the use of Application Virtualization deployment types, if required. |

* 1. Features

The following features are required to support Application Management:

|  |  |  |
| --- | --- | --- |
| Feature | Description | Usage Scenario |
| Device Centric Application Delivery | * Applications and devices have a direct relationship * Users must locate devices with required applications installed | * Ensure users have the applications they need to perform their role or function * Deliver essential corporate applications to devices for use at first logon * Deliver role based applications to users or devices through a direct association or via group membership |
| User Centric Application Delivery | * Applications are delivered to user devices wherever they login, as defined by an administrator * Users can select applications to be installed to their device from a self-service portal | * Ensure users have the applications they need to perform their role or function * Deliver role based applications to users or devices through a direct association or via group membership * Reduce the time a user must wait for an application to be installed * Support a user centric application delivery approach that provides the user with an application type suitable for the device being used * Provide a self-service capability for users to install applications they require without the need to raise a service desk request |
| Application Categorization | Provides a method of delivering applications to devices and users in a standardized manner | Understand the most efficient way to target applications to devices, groups of devices & users, or individuals |
| Definitive Media Library | Source repository for all customer application installation media. | Ensure users have the applications they need to perform their role or function |
| Universal Application Delivery | Support customer developed Universal Applications and Universal applications downloaded from the Windows Store | Utilize application deployment types that are de-coupled from the Operating System and minimize the footprint of the application on the device |
| App-V Application Delivery | Supports previous investments in application virtualization in the environment and take advantage of the benefits of this application type | * Utilize application deployment types that are de-coupled from the Operating System and minimize the footprint of the application on the device * Support existing corporate applications on selected Operating System platforms |
| Win32 Application Delivery | Supports previous investments in Win32 applications in the environment and take advantage of the benefits of this application type | Support existing corporate applications on selected Operating System platforms |

1. Servicing

This section discusses the capabilities enabled by Servicing. The supported software products, operating systems, and platform update approach define the capability per the specification outlined in the Servicing technical guide. The following service inputs are applicable to the servicing architecture, which are discussed below:

* **Stakeholder Input** – Customer participants that contribute to defining the requirements during the servicing workshop. This input is used to design and configure the servicing approach that meets the requirements of the production environment
* **Software Products** – Used to determine which applications are to be supported by the System Center Configuration Manager environment
* **Software Classifications** – Used to determine what types of updates should be applied to the supported software products in the System Center Configuration Manager environment
* **Current Recommended Practice** - The design principles presented in this document for the Servicing capability follow Microsoft’s current recommended practice for updating applications or operating systems on a device
  1. Usage Scenario

List the scenarios for which the technical component is recommended.

The Servicing capability may be used to:

* Ensure devices are updated with security and feature improvements
* Keep all managed devices in a supported state
* Support existing corporate applications on selected Operating System platforms
* Support Windows 10 devices using the Windows as a Service model
* Maintain platform infrastructure using in-console platform updates
  1. Infrastructure Requirements

Infrastructure requirements for Servicing can be considered in the following categories:

* Infrastructure required to support software update management, Windows 10 servicing and infrastructure platform servicing models
* Networking and storage requirements to manage the servicing capability in the production environment.

The following infrastructure is required to support Servicing:

|  |  |  |
| --- | --- | --- |
| Requirement | Specification | Comments |
| Servicing Infrastructure | The capability must meet the minimum requirements for the following roles in System Center Configuration Manager:   * Primary Site * Management Point * (OPTIONAL) Central Administration Site * (OPTIONAL) Secondary Site * Distribution Point * Software Update Point * Service Connection Point | Servicing infrastructure can provide a mixture of updates and upgrades for devices and platform infrastructure  In-console servicing for Windows 10 and platform updates is supported on System Center Configuration Manager. |
| Networking | * DNS to support name resolution and communication between Windows devices, the customer Active Directory domain, and the update infrastructure * DHCP to provide a network address to the Windows 10 device to enable communication in the customer environment * Internet Connectivity to support access to Windows Update, to obtain System Center Configuration Manager platform updates and integrate with Upgrade Analytics | The Servicing infrastructure should be designed to support devices across slow network links to ensure Operating System updates and upgrades can be delivered and installed per corporate requirements |

* 1. Features

The following features are required to support Servicing:

|  |  |  |
| --- | --- | --- |
| Feature | Description | Usage Scenario |
| In-console platform updates | * Updates are downloaded via the internet and are available for administrators to apply to site servers | * Deliver new platform features and improvements to existing features * Ongoing platform support for Windows 10 current branch and current branch for business |
| Software Update Management | * Provides software updates for Microsoft products including (but not limited to) Microsoft Operating Systems and productivity tools such as Office 365 | * Deliver essential updates to products to meet corporate SLA’s |
| Windows as a Service | * Provides an update and upgrade approach to service Windows 10 devices in the production environment * Visualize Windows 10 Upgrade readiness in the environment through Upgrade Analytics | * Ensure devices are grouped into servicing ‘rings’ to receive feature and security improvements per their level of importance/criticality to the business * Deliver essential updates to products to meet corporate SLA’s |

1. Platform Delivery

This section discusses the delivery capabilities enabled by the Platform Delivery capability. The <PROJECTNAME> platform delivery task sequence ensures a customer created reference image, applications, and configuration can be delivered per the Platform Delivery technical guide specification. The following service inputs are applicable to the platform delivery architecture, which are discussed below:

* **Stakeholder Input** – Customer participants that contribute to defining the requirements during the Platform Delivery workshop. This input is used to design and configure the deployment system that meets the requirements of the production environment.
* **Windows System Image** – A reference image created by the customer that is supported for deployment by platform.
* **Deployment Components** – Components required to support the automation of operating system deployment to corporate standards in the environment
* **Deployment Tools** – Products chosen to support the deployment methods of the Operating System in the environment
* **Deployment Methods** – Includes in-scope deployment methods that enable delivery of Operating Systems, applications, and relevant configuration to a device
* **Current Recommended Practice** - The design principles presented in this document for the Platform Delivery capability follow Microsoft’s current recommended practice for deploying a reference image, applications, and configuration to a device.
  1. Usage Scenario

List the scenarios for which the technical component is recommended.

The Platform Delivery capability may be used to:

* Upgrade existing supported devices to a new Operating System
* Install an Operating System on supported new devices
* Retain existing user data and settings on the device during the deployment or upgrade process
* Automate the deployment of the reference image with varying level of required interaction intervention.
* Deploy the corporate image dynamically to multiple device types, architectures and form factors
* Reduce adoption cycle of a new version of the reference system image
* Deliver essential corporate applications to devices for use at first logon
* Reduce configuration error and subsequent investigation and troubleshooting
* Provide a facility to re-build devices in case of configuration error or hardware failure
  1. Infrastructure Requirements

Infrastructure requirements for the Platform Delivery capability are considered in the following categories:

* Infrastructure required to support the deployment of an Operating System to new and existing devices;
* Networking required to support the delivery of large volumes of data reliably to one or more systems during a deployment.

The following infrastructure is required to support the Platform Delivery capability

|  |  |  |
| --- | --- | --- |
| Requirement | Specification | Comments |
| Zero Touch Operating System Deployment Infrastructure (Primary and Remote site) | The following roles must be configured to support Platform Delivery in System Center Configuration Manager:   * Primary Site * Management Point * Distribution Point * (OPTIONAL) Central Administration Site * (OPTIONAL) Secondary Site * (OPTIONAL) State Migration Point | Devices that use the platform delivery capability leverage the management point to authenticate and obtain configuration information, and the distribution point to obtain content. Both site system roles should be appropriately sized to accommodate customer platform delivery requirements. |
| Networking | * DNS to support name resolution and communication between devices and the OSD infrastructure * DHCP to provide a network address to the device to enable communication in the customer environment * PXE to support network boot of devices to deploy a customer selected reference image, applications, and configuration | Zero-Touch deployment tools support Multicast deployment functionality. However, multicast is beyond the scope of this offering. |
| User Devices | * Devices must meet the minimum requirements to run the operating system. | Additional hardware requirements may be required to use certain Operating System features |

* 1. Features

The following features are required to support the Platform Delivery capability:

|  |  |  |
| --- | --- | --- |
| Feature | Description | Usage Scenario |
| Zero Touch Installation Deployment Method | * A Zero Touch Installation (ZTI) is a fully automated deployment initiated by an IT administrator. * Suitable for traditional deployments with well-connected client devices. * Provides an enterprise deployment process with corporate investment in the infrastructure management tooling. * User interaction not required to complete each deployment. * Provides application delivery and device management capabilities after the Operating System has been deployed | * Automate the deployment of an Operating System with no user/administrative intervention. * Deploy an Operating System dynamically to multiple device types, architectures and form factors * Increase adoption rates by accelerating deployment * Deliver essential corporate applications to devices for use at first logon |
| Reference Image Repository | Stores Operating System reference images for use in deployment task sequences | Deploy an Operating System dynamically to multiple device types, architectures and form factors |
| Out-of-Box Driver Repository | Stores and applies any drivers dynamically during the deployment process | Deploy an Operating System dynamically to multiple device types, architectures and form factors |
| Task Sequence Repository | A Task Sequence is used to deploy the customer reference image, applications, and configuration. | Deploy an Operating System dynamically to multiple device types, architectures and form factors |
| New Deployment Scenario | * Familiar with enterprises * Required for new (bare metal) or devices that do not require the any existing data to be retained | * Upgrade existing devices in the customer estate to a new Operating System * Install an Operating System on new devices to corporate standards |
| Refresh Deployment Scenario | * Familiar with enterprises * Required for fleet standardization or issue resolution scenarios * Administrator to configure preservation of existing apps, settings, and drivers | Provide a facility to re-build devices in case of configuration error or hardware failure |
| In-Place Upgrade Deployment Scenario | * Can drastically reduce the time and cost to migrate to Windows 10 * Uses the standard Windows 10 image * Automatically preserves existing apps, settings, and drivers * Supported with Windows 7, Windows 8, and Windows 8.1 * Use System Center Configuration Manager or Microsoft Deployment Toolkit for managing the process * May not provide full application compatibility picture – use new device or refresh scenarios for full application testing | * Retain existing user state on the device as part of the deployment or upgrade process * Reduce wait times to have a functional device available for use in the customer environment |
| State Migration | * Used to retain user state data when transitioning from an existing operating system to a new operating system. * State migration can be performed using the refresh or replace deployment scenario * Infrastructure (State Migration Point) is required to support the transfer user state configuration and content when the replace scenario is used * Hard link migrations using the refresh scenario have no infrastructure dependency – all data remains on the device, which is not formatted as part of the Operating System deployment process | Retain existing user data and settings on the device during the deployment or upgrade process |
| Boot Image(s) | Used to boot the device that will be used to create the image from the network (in conjunction with Windows Deployment Services) and connect it to the server running lite touch or zero touch infrastructure to apply the task sequence configuration and deploy an Operating System to the device. | Automate the deployment of an Operating System with limited or no user/administrative intervention. |
| Network Boot Service | Windows Deployment Services is a feature of Windows Server 2012 R2 that will be enabled and configured to allow a device to boot from the network, so that it can be used to boot the end user device to initiate the Operating System Deployment | Automate the deployment of an Operating System with limited or no user/administrative intervention. |

1. Migration

This section discusses the capabilities enabled by the migration of artefacts from the existing infrastructure management platform. The Migration capability is used to automate the transfer of content and configuration from a supported version of System Center Configuration Manager. The following service inputs are applicable to the migration capability, which are discussed below:

* **Stakeholder Input** – Customer participants that contribute to defining the requirements during the migration workshop. This input is used to determine how artefacts will be moved to the System Center Configuration Manager platform.
* **Content** – Required content from the existing platform that supports capabilities in the production environment.
* **Configuration** – Required configuration from the existing platform that supports capabilities in the production environment.
* **Current Recommended Practice** - The design principles and default configurations in this document comply with Microsoft’s current recommended practice for migrating artefacts to the System Center Configuration Manager platform.
  1. Usage Scenario

List the scenarios for which the technical component is recommended.

The Migration capability is used to:

* Design and architect a migration strategy form the existing infrastructure management platform.
* Ensure content and configuration can be delivered to the production environment in a repeatable and reliable manner to reduce administrative overhead and defects associated with manual processes.
* Reduce the amount of infrastructure required to migrate between the infrastructure management platforms.
  1. Infrastructure Requirements

Infrastructure requirements for the Migration capability are considered in the following categories:

* Requirements for the content and configuration that must be transferred to the System Center Configuration Manager environment;
* Networking and storage requirements to transfer artefacts between infrastructure management platforms.

The following infrastructure is required to support migration capability:

|  |  |  |
| --- | --- | --- |
| Requirement | Specification | Comments |
| Migration Infrastructure | * The existing infrastructure management platform must meet the minimum requirements of System Center Configuration Manager 2007 * The System Center Configuration Manager environment must exist in the production environment to enable the migration to occur | For migration, System Center Configuration Manager 2007 R2 or R3 on the source site are not a consideration. |
| (OPTIONAL) Shared Distribution Point Infrastructure | * To share a distribution point, at least one primary site or the central administration site in the destination hierarchy must use the same port numbers for client requests as the source site * A FQDN must be configured on distribution points in the existing infrastructure management platform to enable it for use as a shared distribution point | Shared distribution points reduce infrastructure requirements during the migration of content, but can limit features and functionality of the new System Center Configuration Manager environment during the migration. |
| (OPTIONAL) Software Update Infrastructure | A Software Update Point must be configured in the new System Center Configuration Manager environment before software updates can be migrated. | The System Center Configuration Manager environment must be appropriately configured to ensue software updates can be migrated. |
| Networking | Domain Name Resolution (DNS) to support name resolution and communication between site systems | The existing infrastructure management platform must be able to communicate with the System Center Configuration Manager environment. |

* 1. Features

The following features are required to support Migration:

|  |  |  |
| --- | --- | --- |
| Feature | Description | Usage Scenario |
| Application Management Content & Configuration | All customer selected application and software update artefacts/configuration that must be migrated to the new platform | * Ensure users have the applications they need to perform their role or function * Ensure content and configuration can be delivered to the production environment in a repeatable and reliable manner to reduce administrative overhead and defects associated with manual processes. |
| Platform Delivery Content & Configuration | Customer selected content & configuration and that may contain Reference images, drivers, task sequences and boot images | * Ensure content and configuration can be delivered to the production environment in a repeatable and reliable manner to reduce administrative overhead and defects associated with manual processes. |
| Device Management Configuration | All customer selected compliance configuration that must be migrated to the new platform | * Apply a consistent settings management baseline to devices across both infrastructure management platforms * Ensure content and configuration can be delivered to the production environment in a repeatable and reliable manner to reduce administrative overhead and defects associated with manual processes. |
| Asset Management & Support Configuration | All customer selected asset intelligence and software metering configuration that must be migrated to the new platform | * Ensure content and configuration can be delivered to the production environment in a repeatable and reliable manner to reduce administrative overhead and defects associated with manual processes. |
| Core Infrastructure Configuration | All customer selected boundary and collection configuration information that must be migrated to the new platform | * Ensure content and configuration can be delivered to the production environment in a repeatable and reliable manner to reduce administrative overhead and defects associated with manual processes. |

1. Gap Analysis

Document the gap between the Current Infrastructure and each of the Technical Components. This will assist in developing a recommendation in the next section. the table below contains examples. Modify these examples and augment depending on the gap identified in Section 2.

|  |  |  |  |
| --- | --- | --- | --- |
| Capability | Current Infrastructure | Requirement | Proposed Remediation |
| Core | Remote support is de-centralized | All remote support events are to be centralized using the Configuration Manager Console | Develop criteria for administrators that are permitted to remotely control user devices for support and troubleshooting purposes. |
| Core | Primary Site & Multiple Secondary Site Hierarchy | Simplify the hierarchy to reduce administrative effort to maintain and manage the environment | Identify devices in the environment that can be used as distribution points to reduce the requirement for dedicated secondary site infrastructure. |
| Device Management | Supports on-premises domain joined devices | Mobile device management support for Windows Phone, iOS, and Android devices | Prepare the environment to support a hybrid device management model by connecting System Center Configuration Manager to Microsoft Intune to enable the management of mobile devices. |
| Application Management | Device centric application management approach | User centric application management approach | Evaluate which Line of Business applications are to be made available for user self-service installation, and identify which applications will be targeted for conversion to the application model to support user centric delivery |
| Servicing | Windows 10 devices are upgraded via task sequence | Windows 10 device upgrades are automated | Enable support for Windows 10 upgrades by moving the Windows Server Update Services instance to a host running Windows Server 2012 (and above) and installing [KB3095113](https://support.microsoft.com/en-us/kb/3095113) to provide upgrade functionality |
| Platform Delivery | Supports network boot for bare metal deployment scenarios | Requirement to retain network boot support for bare metal scenarios on new infrastructure platform | Consider an approach to transition the network boot functionality from the existing infrastructure management platform to the new platform as part of the transition |
| Migration | System Center Configuration Manager 2007 | Migration to System Center Configuration Manager | Apply a patch to System Center Configuration Manager 2007 to Service Pack 2 to support migration |

1. Recommendation

Use the Gap analysis to provide a formal recommendation on which technical component should be used for the capability.

The following sections define the steps that should be taken across each capability of the System Center Configuration Manager environment to prepare for implementation.

* 1. Core

Based on the information provided during the workshop, it is recommended that the customer consider embarking on the following activities to prepare for the implementation of System Center Configuration Manager in the production environment.

Consultant: Remove recommendations that should not be made for the customer. Augment the recommendations as required based on new information obtained during the workshops.

* Review and update existing network and Active Directory design diagrams (where required) to ensure the core hierarchy design can be validated for accuracy
* Update the Active Directory schema to support the System Center Configuration Manager platform
* Plan a deployment approach to implement the core design throughout the production environment
* Modify firewall rules to support core configuration and feature capability requirements implemented by the System Center Configuration Manager platform
* Consider implementing a Role Based Administration strategy to define roles and responsibilities for administrators that use the System Center Configuration Manager platform
* Define criteria to allow administrators to remotely connect to devices through the System Center Configuration Manager platform
* Identify custom hardware inventory requirements that are to be supported by the new platform
* Determine which Line of Business Applications criteria should be identified for software metering
  1. Core Upgrade

Based on the information provided during the workshop, it is recommended that the customer consider embarking on the following activities to prepare for the core upgrade.

Consultant: Remove recommendations that should not be made for the customer. Augment the recommendations as required based on new information obtained during the workshops.

* Upgrade the existing System Center Configuration Manager platform to a supported level that can leverage the core upgrade capability
  1. Device Management

Based on the information provided during the workshop, it is recommended that the customer consider embarking on the following activities to prepare for migration.

Consultant: Remove recommendations that should not be made for the customer. Augment the recommendations as required based on new information obtained during the workshops.

* Define the devices that will be supported in the environment
* Evaluate the use of Microsoft Intune to support mobile device management capabilities with System Center Configuration Manager
* Work with security and end user teams to understand configuration requirements for devices that will be managed by the platform
  1. Application Management

Based on the information provided during the workshop, it is recommended that the customer consider embarking on the following activities to prepare for application management to Windows 10 devices.

Consultant: Remove recommendations that should not be made for the customer. Augment the recommendations as required based on new information obtained during the workshops.

* Design a plan to rationalize the existing application portfolio to reduce migration effort when importing applications to the new platform
* Consider remediation of applications that have used shimming as a mitigation technology
* Evaluate the use of application virtualization to sequence applications for delivery to corporate, domain-joined devices
* Evaluate the use of universal applications for use
* Plan and commence an upgrade to Internet Explorer 11 to ensure existing Internet Explorer browser platforms remain in a supported state
* Perform the discovery of corporate web-based sites using the Site Discovery Toolkit for Internet Explorer
* Initiate the testing of web-based applications for compatibility with Internet Explorer 11
* Evaluate the use of Enterprise Mode in Internet Explorer 11
* Evaluate the Windows Store for Business as corporate application store
  1. Servicing

Based on the information provided during the workshop, it is recommended that the customer consider embarking on the following activities to prepare for Servicing with System Center Configuration Manager

Consultant: Remove recommendations that should not be made for the customer. Augment the recommendations as required based on new information obtained during the workshops.

* Ensure the Service Connection Point role can connect to the internet to obtain Platform Updates for System Center Configuration Manager
* Expand on the work undertaken in the capability workshop to define Windows 10 Servicing rings for the organization to enable System Center Configuration Manager to support Windows 10 updates and upgrades per corporate requirements
* Define all the products that will be supported by the Servicing capability
* Consider configuring and deploying Upgrade Analytics to provide Windows 10 upgrade readiness data
  1. Platform Delivery

Based on the information provided during the workshop, it is recommended that the customer consider embarking on the following activities to prepare for Platform Delivery with System Center Configuration Manager.

Consultant: Remove recommendations that should not be made for the customer. Augment the recommendations as required based on new information obtained during the workshops.

* Test existing script investments for Windows PE, DISM and USMT
* Determine all reference images, Operating Systems and architectures that will be supported by Platform Delivery
* Define the deployment methods that will be used to deploy reference images using the new platform delivery infrastructure
* Consider the requirement for user state migration as part of the Platform Delivery capability in the new environment
* Evaluate and update Microsoft Deployment Toolkit to the appropriate version to provide support for new Operating Systems
* Determine all systems that require a change from BIOS to UEFI
  1. Migration

Based on the information provided during the workshop, it is recommended that the customer consider embarking on the following activities to prepare for migration.

Consultant: Remove recommendations that should not be made for the customer. Augment the recommendations as required based on new information obtained during the workshops.

* Upgrade the existing System Center Configuration Manager platform to a supported level that can leverage the migration capability
* Determine suitability criteria to migrate existing content and configuration artefacts
* Establish a roadmap for migration and decommissioning of the existing infrastructure management platform