PowerON

DEPLOYMENT PRE-REQS

Checklist and Details

CONTENTS

Document Control

Version History

Version	Date	Change By	Comments
1.0	07/11/2019	Steve Beaumont	Initial Release
1.1	11/11/2019	Peter Egerton	Update
2.0	11/11/2019	Jennie Price	QA and release

Issue

Role	Name	Job Title
Author	Steve Beaumont	Chief Technology Officer
Reviewer / Approver	Peter Egerton	Principal Consultant

Related Documents

Document Name	Comments
ConfigMgr Design	

Team Involvement

Name	Company	Job Title
Steve Beaumont	PowerON	Chief Technology Officer
Peter Egerton	PowerON	Principal Consultant

1 Checklist

Prerequisite	Completion Status
Infrastructure: Setup required servers (Server 2016 only)	□
Infrastructure: Servers **Fully** Patched with Microsoft Updates	□
Infrastructure: Servers have Azure Resource Manager PowerShell Module	□
Infrastructure: ConfigMgr PS Servers Security Group is a local admin of all servers in scope	□
Software: Kamino: Run Setup Nodes PowerShell on all ConfigMgr Servers	□
Software: PowerON Kamino Installer executed on the Primary Site	
Active Directory: User Accounts Created	□
Active Directory: Group Accounts Created	□
Active Directory: Schema Extended	□
Networking: Anti-Virus Exclusions	□
Networking: Firewall/Proxy Exclusions	□

2 Consolidated Prerequisites

2.1 Software

Important information

PowerON FastTrack installation will be installed on Windows Server Standard 2016 with all current Windows Updates applied will be used for all servers in this design along with the following:

- Servers need Microsoft Azure Resource Manager PowerShell Module. (from an elevated PowerShell run: **Install-Module AzureRM**)
- PowerShell remoting enabled and firewall exception in place. From PowerShell run: **Enable-PSRemoting -Force**
- ConfigMgr Server security group must be added as an administrator to both servers.
- Servers should be given a final reboot prior to install starting to ensure pending file/reboot operations are cleared.

PowerON utilise an automated deployment platform based on Azure Desired State Configuration (DSC) to deploy Configuration Manager. This requires our installer to be installed on the servers to pull the required media from Azure and perform the installation.

A “Setup Nodes” PowerShell script will require executing on the 2 main primary servers in your main datacentre.
The script can be downloaded and assessed here:
https://kaminousstorage.blob.core.windows.net/ftkaminoinstaller/Setup-Nodes.ps1

2.2 Active Directory

2.2.1 Schema Change

Extend the AD Schema guide: https://kaminousstorage.blob.core.windows.net/ftconfigurationmanager/Guide-ExtendADSchema.pdf

2.2.2 Accounts

For normal operation of ConfigMgr, several Active Directory accounts are required. It is your organisation's responsibility to create the User Accounts and Groups.

The following table shows the accounts that are a requirement for the deployment and their purpose and the permissions recommendation. The tables column Account Names shows example names for the user accounts and security groups. It is up to your organisation if you want to change the Accounts Names. The Accounts Names and Passwords require populating into the Kamino Portal under the section System Credentials.

These Accounts require creating before the Deployment:

Note: Please do not put any of the following symbols within the passwords generated for use during deployment:

- $
- ,
- =

Account	Purpose	Permissions
<Domain>\CMAdmin	ConfigMgr Installation Account	• Local Admin rights to ConfigMgr Servers Can be disabled after installation but recommended to retain as heavily integrated into security model during installation.
<Domain>\SVC_CM_ADDisc	ConfigMgr Active Directory Forest Discovery Account An AD Discovery account will be required for each untrusted domain to be managed to access resources	• Read permissions to AD Forest/Domain • Write Permissions to the System Management container • Permissions to publish DNS records • Do not grant this account the right to join computers to the domain
<Domain>\SVC_CM_NA	ConfigMgr Network Access Account	• Requires "Access this computer from the network" right on the Distribution Points. • Minimum rights to access content on the Distribution Points. • Do not grant this account the right to join computers to the domain
<Domain>\SVC_CM_DJ	Domain Joining Account used within task sequences to join the OS to the domain.	• Do not grant the account interactive logon rights. Use Delegate Control in AD: Computer Objects - • Reset Password • Validated write to DNS host name • Validated write to service principal name • Read/Write Account Restrictions This object and all descendant objects - • Create/Delete Computer Objects
<Domain>\SVC_CM_CP	ConfigMgr Client Push Account	• Do not grant the account interactive logon rights. • Must be local admin on the target devices you push clients to. **N.B.** A client push account will be required for each domain to be managed to access resources
<Domain>\SVC_CM_RRA	ConfigMgr Reporting Service Point Account	• Account is granted rights if chosen as a new account during Reporting Point creation from the console.
<Domain>\SVC_CM_CAP	OS Deployment Image Capture Account	• Read and Write permissions to the network share specified to store the image capture

<Domain>\SVC_CM_SQLSvr	SQL Server Service Account	• Required to register the Service Principle Name (SPN) • Permission to log on as a service. • Sysadmin right on SQL database • Replace a process-level token • Bypass traverse checking • Adjust memory quotas for a process • Permission to start SQL Writer • Permission to read the Event Log service • Permission to read the Remote Procedure Call service •
<Domain>\SVC_CM_SQLAgt	SQL Agent Service Account	• Permission to log on as a service • Sysadmin right on SQL database • Replace a process-level token • Bypass traverse checking • Adjust memory quotas for a process
<Domain>\SVC_CM_SQLRS	SQL Reporting Service Account	• Permission to log on as a service. •

2.2.3 Groups

Group	Purpose
<Domain>\CM.Remote.Tools	Group containing rights to use the remote tools function
<Domain>\CM.Admins	Group containing all ConfigMgr Administrators (PowerON Tier 2 accounts)
<Domain>\CM.PSServers	Group containing all ConfigMgr Site Servers to grant security rights to the System Management Container
<Domain>\CM.DPServers	Group containing all ConfigMgr Distribution Point Servers
<Domain>\CM.SUPServers	Group containing all ConfigMgr WSUS Servers
<Domain>\CM.SQL.Admins	Group containing Admin accounts that require SQL Administrative permissions to the ConfigMgr SQL instance.

2.3 Servers

ConfigMgr Servers	RAM	CPU	HDD 1	HDD 2	HDD 3	HDD 4	HDD 5	HDD 6
Primary Site Server	32 GB	8	127 GB	50 GB	600GB	85 GB	22 GB	17GB
WSUS & DP	16 GB	4	127 GB	1 TB				

Important information

HDD 4,5 & 6 on Server 1 are SQL disks and must be formatted with 64k block allocation size

SQL Disk Sizes:
To calculate the SQL Disks sizes more accurately required for the ConfigMgr deployment please use the following spreadsheet:
https://kaminousstorage.blob.core.windows.net/ftconfigurationmanager/Pre-Requisite-ConfigMgr-Database-sizing.xlsx

2.3.1 Server Requirements

The server being used for the Configuration Manager Kamino Deployment require the following:

- Windows Server 2012 R2 or 2016 (preferred) as the Operating System
- If using 2012 R2, the Servers need patching with the latest Microsoft Security Updates. Patch KB2919355 and KB2919442 are mandatory installs. KB2919442 may not present itself as available please check manually. After the mandatory KBs are installed you will need to scan again for updates.
- Windows Management Framework (WMF) 5.1
- Servers need Microsoft Azure Resource Manager PowerShell Module. (after WMF 5 is install from PowerShell run: Install-Module AzureRM)
- PowerShell remoting enabled and firewall exception. From Powershell run: Enable-PSRemoting -Force
- ConfigMgr Server security group added as an administrator to both servers.

2.3.2 Server Node Setup

On all of the Server Nodes in scope, for example, the ConfigMgr Primary site and the WUD Server a setup script is required to be run.

Use the following link to download the setup nodes PowerShell Script:

https://kaminousstorage.blob.core.windows.net/ftkaminoinstaller/Setup-Nodes.ps1

Note: This should be run on Each Server from an Elevated (Administrator) PowerShell Console.

2.3.3 Kamino Installer

To enable PowerON to automate the deployment of ConfigMgr core infrastructure we need to be able to manage your Configuration Manager Primary site. Your organisation will receive a link to the PowerON Kamino installer via your Account Manager or Engagement Manager. The Kamino installer must run on the Microsoft Configuration Primary Site.

2.4 Anti-Virus Exclusions for Servers

2.4.1 Primary Site Servers

Location	File(s)
<driveletter>:\Program Files\Configuration Manager\	Install.map
<driveletter>:\Program Files\Configuration Manager\Inboxes	*.adc, *.box, *.ccr, *.cfg, *.cmn, *.ct0, *.ct1, *.ct2, *.dat, *.dc, *.ddr, *.i*, *.ins, *.ist, *.job, *.lkp, *.lo_, *.log, *.mif, *.mof, *.nal, *.ncf, *.nhm, *.ofn, *.ofr, *.p*, *.pcf, *.pck, *.pdf, *.pkg, *.pkn, *.rpl, *.rpt, *.sca, *.scd, *.scu, *.sha, *.sic, *.sid, *.srq, *.srs, *.ssu, *.svf, *.tmp, *.udc
<driveletter>:\Program Files\Configuration Manager\\Logs	*.log
<driveletter>:\Program Files\SMS_CCM\ServiceData	*.msg, *.que, *.xml
<driveletter>:\Program Files\SMS_CCM\Logs	*.log
SQL Data Directory	*.mdf
SQL Log Directory	*.ldf

2.5 Firewall Port Requirements

2.5.1 Kamino Ports

The following URLs must be whitelisted for proper Kamino communication during installation. 443 outbound only.

Description	TCP	Bypass HTTPS inspection

*.ods.opinsights.azure.com	443	Yes
*.oms.opinsights.azure.com	443	Yes
*.blob.core.windows.net	443	Yes
*.azure-automation.net	443	Yes

TABLE 1 – FIREWALL PORTS – KAMINO COMMUNICATION

!

Important Information Follows

If using a firewall solution which does not support DNS entries, here is a list for Microsoft's Datacentre IP's:
https://www.microsoft.com/download/details.aspx?id=41653

The regions which the Kamino service utilises are:

- US East
- US East 2
- UK West

These addresses are only required during installation and can be closed after.

2.5.2 ConfigMgr Ports

Servers/Roles referenced below are the two new servers to be created:

Source	Destination	Description	UDP	TCP
Server 1	Internet	Asset Intelligence Sync Point to Internet	--	443
All Workstations	Closest Distribution point or fallback DP	Client to Distribution Point	--	80 & 443
All Workstations	Closest Distribution point or fallback DP	Client to Distribution Point for PXE	67, 68, 69 & 4011	--
All Workstations	Server 2	Client to Fall-back Status Point	--	80
All Workstations	Server 1	Client to Management Point	--	80 & 443
PowerON Jumpbox	Server 1	ConfigMgr Admin Console to Site Server	135	135 & RPC Dynamic
All Distribution Points	Server 1	MP, DP & FSP to Site Server	--	135 & RPC Dynamic & 445
Server 2	Internet	Software Update Point to Internet	--	80
All Workstations	Server 2	Client to the Software Update Point	--	8530
Server 1	All Workstations	Management Point to Client	135	135, 445, RPC Dynamic, 10123, 80, 443
Server 1	Azure CMG	CMG Deployment & Fallback protocol to build CMG channel to only one VM instance		443
Server 1	Azure CMG	Preferred protocol to build CMG channel and use multiple VM Instances		10140-10155
All Workstations	Azure CMG	Only needed when outside of the network or on a specific		443

		LAN segment which is designated to use the CMG		

2.6 General Server and Client Internet access requirements

https://docs.microsoft.com/en-us/configmgr/core/plan-design/network/internet-endpoints

2.6.1 Server 1

- *.akamaiedge.net
- *.akamaitechnologies.com
- *.manage.microsoft.com
- go.microsoft.com
- *.blob.core.windows.net
- table.core.windows.net
- download.microsoft.com
- download.windowsupdate.com
- sccmconnected-a01.cloudapp.net
- configmgrbits.azureedge.net
- https://go.microsoft.com/fwlink/?LinkID=619849
- dl.delivery.mp.microsoft.com
- https://bspmts.mp.microsoft.com/V
- https://login.microsoftonline.com
- management.azure.com
- https://management.core.windows.net/
- https://graph.microsoft.com/
- officecdn.microsoft.com
- config.office.com

2.6.2 Server 2

- http://windowsupdate.microsoft.com
- http://*.windowsupdate.microsoft.com
- https://*.windowsupdate.microsoft.com
- http://*.update.microsoft.com
- https://*.update.microsoft.com
- http://*.windowsupdate.com
- http://download.windowsupdate.com
- http://download.microsoft.com
- http://*.download.windowsupdate.com
- http://test.stats.update.microsoft.com
- http://ntservicepack.microsoft.com

2.6.3 PowerON Jumpbox

- http://petrol.office.microsoft.com
- https://aka.ms
- https://raw.githubusercontent.com
- http://maps.bing.com

2.6.4 All Workstations

The list is too long for this document, please review this documentation from Microsoft.

https://docs.microsoft.com/en-GB/intune/fundamentals/intune-endpoints