System Center 2012 – Configuration Manager

Executive Summary

Management and consistent availability of servers and endpoints in a business means higher productivity. Period. When employees no longer have to be concerned with the availability of a given resource, productivity and longevity improves and administration costs go down.

One of the most mature components of System Center is Configuration Manager (Formally known as SMS). System Center Configuration Manager (SCCM), offers a complete management solution that includes deployment, patching, and inventory for Windows desktops and servers in addition to management and deployment and inventory capabilities for iOS, Android, Linux, Mac OS, and Windows RT. We will explore key capabilities of Configuration Manager, some best practices on its use and deployment, and how Configuration Manager is more than just a tool for desktops.

We at Managed Solutions strongly believe we are able to provide custom solutions to meet many, if not all of a business's technology needs.

"Like its namesake, System Center Configuration Manager's (SCCM) job is to manage the Configuration of endpoints."

Configuration Manager

Like its namesake, System Center Configuration Manager's main proficiency is to manage the Configuration of endpoints. In the following sections to come, you will be introduced to some of the major areas of concentration that comprise System Center 2012 Configuration Manager.

Network Access Protection (NAP)

Network Access Protection (NAP) is SCCM's first line of defense against allowing systems onto the corporate network that may potentially comprise a threat to security and integrity. When NAP is enabled, Configuration Manager clients can assess whether they are compliant or not with the software updates that you select. Configuration Manager

Contents

Microsoft System Center

clients send this information in a statement of health (SoH). This is presented to the Configuration Manager System Health Validator that resides on the System Health Validator point site system role.

The System Health Validator point is installed on a computer that is running Windows Server 2008 or later, with the Network Policy Server role. It validates whether the client computer is compliant or noncompliant and passes the health state of that computer to the Windows Network Policy Server (may be installed on the same system).

The Windows Network Policy Server is configured to use policies that determine the action for computers that are known to be compliant or noncompliant. If the health state of a client cannot be determined, then this is considered an error condition. By default, all error conditions are mapped to a noncompliant state. However, they are split into five categories and each category can be configured to map to either compliant or noncompliant.

The actions that the Network Policy Server can take based on computer health states include the following: Restrict computers from accessing the full network provide full access to the network but for a limited period provide full access to the network indefinitely remediate noncompliant computers to bring them into compliance with policies Be aware that the Configuration Manager administrative user cannot control the action that will be taken because of a computer health state that it passes to the Network Policy Server. However, if the Network Policy Server is configured to enforce compliance through remediation, Configuration Manager Services are then used to deliver the software updates that are required to bring noncompliant clients into compliance. When compliance is successfully remediated, clients reassess their statement of health, which then changes from noncompliant to compliant, and their health state is updated to compliant.

Operating System Deployment

One of the core-competencies of SCCM performs is an automated Operating System Deployment

"One of the primary *Tools* is, simply put, a change in philosophies and viewpoints from *Device Centric Management,* to *User Centric Management."*

(OSD) via Task Sequences. These Task Sequences automate in either a Lite-Touch (LTI) or Zero-Touch (ZTI) manner to replicate a known successful image many, many times over. In addition, these Task Sequences (TS) can include nearly every manual, time-consuming step required to deploy an operating system to an endpoint. This very much may include deploying Web Shortcuts to our

System Health Validator

Windows Network Policy Server

Operating System Deployment (OSD)

previously mentioned Web-based Applications, App-V and Med-V instances as well as providing a consistent installation of other applications.

USMT/State Migration Point

OSD can also leverage the User State Migration Tool (USMT) to capture user's data and settings on their assigned endpoints. This data may be either copied from the system to a State Migration Point (Server with a role to hold Migration Data) or "Hard linked" (Data remains on the local system and literally, a new operating system is deployed around the old data).

User-Centric Application Delivery System Center 2012

Configuration Manager makes it easy to establish a user-centric application delivery model. IT administrators can use Configuration Manager to deploy full Office installations to desktops and App-V versions of applications to virtualized desktops. Configuration Manager uses variables such as user identity, application dependencies, and network and device characteristics to dynamically determine the appropriate deployment type for a specific device.

A user-centric approach lets IT administrators deploy an application to a user, regardless of the devices used. When a user brings a new device into the enterprise, Configuration Manager can help deploy the appropriate applications to that device without requiring an administrator to manually push those applications.

Application Catalogue

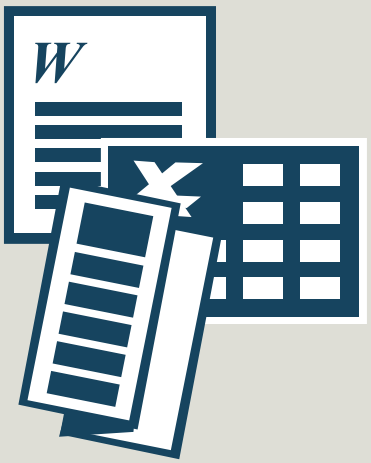
Applications and other self-service tasks may also be installed via the Application Catalogue. This applet is installed with the SCCM client. Apps and other jobs may also be pushed via SCCM by administrators to perform silent, background installations as employees perform their daily tasks.

Unified Asset Inventory

One of the biggest concerns facing administrators is the need to capture and analyze all assets

"One of the biggest concerns facing administrators is the need to capture and analyze all assets connected to corporate resources."

connected to corporate resources. Configuration Manager provides IT administrators with a comprehensive view to identify and inventory mobile, physical, and virtual assets. This improves your ability to map devices to users, which aides in implementing user-centric policies and deploying applications to users. It also delivers an advantage over other solutions



Microsoft System Center

User-Centric Application Delivery System Center 2012 Configuration Manager

that might offer information on mobile devices and virtual and physical assets, but through different management consoles that make it more difficult to get the complete picture.

To bring mobile-device asset inventory into the same console, Configuration Manager uses Microsoft Exchange ActiveSync (EAS) to automatically pull data from Exchange when users log on to check email. Information such as the device's hardware ID and operating system and the user ID is delivered through EAS, recorded, and available in the same standardized reports used for traditional desktop and laptop inventories. This gives administrators the ability to see the complete collection of devices used by particular users, from their smartphones and laptops to tablets and desktop PCs. The result is a single platform that administrators can use to inventory Windows, iOS, Android, and other EAS-compliant devices.

Configuration Manager is also "virtualization aware," so administrators can conduct inventories on virtual desktops and virtual sessions. The improved virtualization support in Configuration Manager helps you to consistently treat virtualized environments in a dedicated manner without "ghost asset" issues and duplication that can plague non-virtualization–aware management solutions.

Configuration Manager remains a useful tool for pulling hardware and software inventory information from traditional devices, like laptops and desktops. More advanced capabilities, such as licensing information and software metering, are also available to help you track usage of applications within the organization.

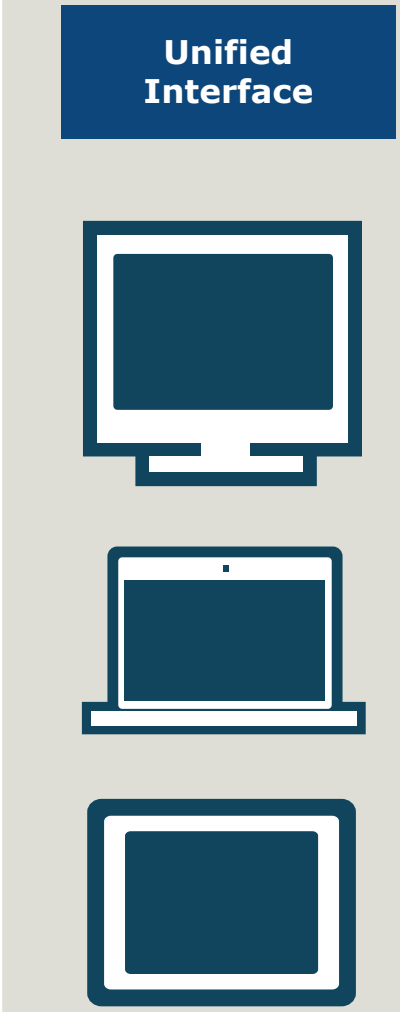
Unified Settings Management

Configuration Manager allows consistent settings across a diverse range of devices. Configuration Manager provides a unified interface that helps IT administrators manage the configuration and compliance of a full range of enterprise devices, including servers, laptops, desktop PCs, and mobile devices.

The compliance settings tool in Configuration Manager helps

"The compliance settings tool in Configuration Manager helps administrators assess the compliance of users and client devices in relation to any number of configurations."

administrators assess the compliance of users and client devices in relation to any number of configurations. For example, determine whether the correct Windows operating system versions are installed and configured appropriately, whether required applications are installed



and configured correctly, and if a user has installed prohibited applications. Administrators can also check to see if laptops are in compliance with software updates and security settings.

Configuration Manager, using EAS, also lets administrators push basic policies such as PIN/password and remote wipe to specific user devices. Because Configuration Manager is virtualization aware, it is possible to deploy policies that either exempt or specifically target virtual desktops. This is important to prevent issues such as overloading physical hardware with synchronized policy tasks, also known as VDI storms. Configuration Manager automatically randomizes tasks to prevent overloading of physical hardware in a virtual environment.

Another tool to assist with unified settings management is Microsoft Advanced Group Policy Management (AGPM), part of the Microsoft Desktop Optimization Pack (MDOP). With AGPM, administrators can access functions such as policy versioning, rollback, and views of resulting policy changes to help manage enterprise devices more efficiently through Active Directory Domain Services.

Microsoft Advanced Group Policy Management (AGPM)

System Integrity and Device Encryption

Configuration Manager can be used to deploy operating systems with Microsoft BitLocker Drive Encryption, a data protection feature available in enterprise editions of Windows Vista and Windows 7 that reduces the threat of data exposure due to lost, stolen, or inappropriately decommissioned computers. With Bitlocker installed on a device, Microsoft BitLocker Administration and Monitoring (MBAM), part of MDOP, can be used for provisioning, deploying, and recovering BitLocker-enabled mobile and remote devices running Windows.

Microsoft BitLocker Drive Encryption

For devices with Windows and third-party devices, administrators can use Configuration Manager and EAS to enforce encryption of devices using EAS. Some EAS-compliant platforms also provide the ability to encrypt devices for an added level of security. This is especially important on mobile devices, which are more prone to loss or theft.

Anti-malware Software

There are a variety of tools available to protect the organization against malware. Windows Defender is built into consumer and enterprise editions of Windows. Microsoft also provides Microsoft Security Essentials, a free security software product geared for consumers and small businesses to help secure devices running Windows against the threat of malware.

In a corporate environment, System Center 2012 Endpoint Protection provides antimalware protection for laptops, desktops, and virtualized

environments. It helps protect devices running Windows against the threat of malware with the added benefit of cost savings through reduced infrastructure. Eliminating the duplicate infrastructure for antimalware software and systems management can save thousands of dollars each year, depending on organization size.

Having management and security functionality in the same console provides a number of benefits, such as a better correlation between malware protection and the update state of a specific machine. Because device infections are often a result of user computing habits, Configuration Manager and Endpoint Protection help IT administrators to easily determine which users are most prone to malware and target those users with additional training to help reduce the likelihood of infection.

On-Prem, Off-Prem – No Worries

Functionality does not change if the endpoint is off-prem. As long as basic Internet connectivity is established, the client may continue full functionality over the Internet. In fact, distribution points may be fully cloud-centric to provide secured caches of content without the requirement for traversal back to the main SCCM infrastructure.