Welcome to the System Center Configuration Manager Overview

In this Video we will:

- Present an overview of Microsoft's System Center Configuration Manager.
- Describe the feature set for SCCM.
- At the end of this lecture, you will have a basic understanding of the capabilities of SCCM.

System Center Configuration Manager is the premier management solution from Microsoft.

So, what can SCCM do?

1. **Windows 10 Management** - Configuration Manager is designed to keep pace with Windows 10 updates and the current branch to provide support for new Windows features as they become available. Current Branch refers to security updates, bug fixes and new features published by Microsoft every few months. For example, the current Windows 10 branch is 1703 as of April 11th, 2017. When your clients reach the end of support for their current branch, alerts can be viewed.
2. **In-Console Software Updates** – Allows **centralized management** of Windows Security patches and updates. Products include Windows, Apple IOS, and Android. SCCM synchronizes with the Microsoft cloud to get updates that you can install within the console.
3. **Application Delivery** – Allows administrators to create one application that can be delivered to all user devices. Think of an application like a box. This box contains one or more sets of installation files for a software package known as a deployment type. A deployment type also contains rules that specify when and how the software is deployed. For example, the deployment type can be an msi installer package or an app package for a mobile device from the app store or an app package for an android device which you can deploy to devices or device collections.
4. **Device Management** – Provides a single administrative console for managing policies and asset compliance reporting across PCs and mobile devices using Microsoft Intune. With on-premises, windows 10 devices can now be managed. For example, one typical use for device management would be as follows. You have various devices that users wish to bring into the corporate environment. These devices (MAC, Windows, Unix and mobile devices must be registered with the corporate environment, data and applications must be secured. With device management, these devices can be considered "known" to your corporation.

5. **Endpoint Protection** – Provides security, antimalware protection, and firewall security.
6. **Compliance and Settings Management** - You create a baseline for security compliance and compare that baseline with the configuration of the clients that you manage. a **baseline** is a known state by which something is measured or compared.
7. **Software Update Management** – Configuration Manager, simplifies the complex task of delivering and managing updates to IT systems across the enterprise. IT administrators can deliver updates of Microsoft products, third-party applications, **hardware drivers, and system BIOS** to a variety of devices, including desktops, laptops, servers, and mobile devices.
8. **Client Power Management** – Works with the power management facilities built into the Windows O/S in a centralized environment. For example, you can apply different power settings during business hours and non-business hours. You can run reports that will evaluate power usage and power savings after you apply a power plan to computers.
9. **O/S Deployment** – Provides various methods for deploying operating systems to desktop's, servers, laptops, and mobile devices. Removes the problems associated with manually installing the operating systems by creating and deploying a consistent image of various operating systems.
10. **Client Health Monitoring** – Provides alerts if health statistics fall below the threshold of the baseline. Health statistics are based upon a list of status settings. For example, if the computer has not been connected to the network for a long period of time, client health could send an alert declaring the client has been inactive.
11. **Asset Intelligence** – Evaluates hardware and software assets and usage. Using generated reports administrators and managers can make informed purchasing decisions based upon usage and licensing requirements.
12. **Inventory – You can** use hardware inventory in System Center Configuration Manager to collect information about the hardware configuration of client devices in your organization. How often hardware data is gathered is based upon the client device settings schedule.
13. **Reporting** – Helps you gather information and create reports about the users, hardware and software inventory updates and applications in your organization. Reports are available on the local server or on-line web interface.

What can SCCM integrate with:

- Microsoft Intune to manage a wide variety of mobile device platforms.

- Windows Server Update Services (WSUS) to manage software updates.
- Certificate Services.
- Exchange Server and Exchange Online.
- Windows Group Policy.
- DNS.
-

SCCM also uses:

- Active Directory Domain Services for security, service location, configuration, and to discover the users and devices that you want to manage.
- Microsoft SQL Server as a distributed change management database—and integrates with SQL Server Reporting Services (SSRS) to produce reports to monitor and track management activities.
- Site system roles that extend management functionality and use the web services of Internet Information Services (IIS).
- Background Intelligent Transfer Service (BITS) and BranchCache to help manage the available network bandwidth.

In this Video

- We presented an overview of Microsoft's System Center Configuration Manager.
- We described the feature set for SCCM.
- You should now have a basic understanding of the capabilities of SCCM.