Welcome to SCCM with Endpoint Protection

Server Prerequisites

- In this lecture, we will discuss the **features and benefits** of Endpoint Protection integration.
- Next, we will discuss the SCCM **server prerequisites**.
- Then we will demonstrate how Endpoint Protection is **integrated** into System Center Configuration Manager 2016.

I should point out that System Center Endpoint protection can be installed on a stand-alone system or it can be integrated together with Configuration Manager.

So, what are the **benefits** of integrating Endpoint Protection into SCCM?

- For example, if you have hundreds of computers in your organization that you want to protect with Endpoint Protection, instead of trying to manage them one at a time. With SCCM and Endpoint Protection working together you can automatically deploy updates and new antimalware file definitions to every computer in your organization.

SCCM Provides integration with Endpoint Protection by implementing:

- Centralized management with Endpoint Protection
- You can deploy updates to devices and device collections – In Configuration Manager You can consider a device collection as a group of computers.
- With Endpoint Protection, you can deploy Antimalware policies and Windows Firewall Policies to these collections
- SCCM allows us to configure Alerts and reports and send Email notifications when certain items are violated. Reports evaluate our malware situation.

SCCM Server Prerequisites

If you have been completed the labs in section two and three. You should have the following components already installed and configured in your lab.

- Server 2016
- Active Directory
- DNS for name resolution
- SQL – which stores inventory data and malware results in the SQL data base.
- SCCM 2016 with Endpoint Protection

Before we install Endpoint Protection I wanted to take a look at the integration capabilities of Endpoint Protection within the Configuration Manager console.

Integration of SCCM with Endpoint Protection

- Open the Configuration Manager and from the **Workspace** click **Assets and Compliance**. From the Navigation pane click Endpoint Protection and notice we can work with our
- Antimalware Policies
- Windows Firewall Policies
- Windows Defender ATP (Advanced Threat Protection)

From the **Workspace** Open **Software Library**

- Notice all Software updates, these are current file definitions for windows defender. These updates are available to be pushed to our Windows 10 clients.

From the workspace click Monitoring, from the Navigation Pane click security, open Endpoint Protection Status. Here Endpoint Protection displays our:

- Protection Status – Which shows the active clients in the collection
- The Malware remediation status of those clients.
- At the bottom, we have the Operational Status of clients that shows list the failure of Endpoint Protection installations and Antimalware policy application failure.
- As you can see there is a lot of integration with EP and SCCM

SCCM Server Configuration - There are a number of Server roles that will need to be configured in order to use EndPoint Protection

- Endpoint Protection point role – It must be installed on one site system server only and it must be installed at the top of the hierarchy.
- Software update point role – If you want to deliver updates. The SUP also allows Configuration Manager to use the WSUS catalog to scan EP clients.
- Reporting services point role – A site service role that provides integration with SQL server reporting services to create and manage reports for Configuration Manager. I installed this role because I wanted to run reports and have them available on the web.
- Configure an SMTP mail server if you want email notification to alert you.

Viewing the installed Servers Rolls - From the Workspace click Administration, from the Navigation Pane click Site configuration/Servers and Site System Roles – I can view the installed Roles.

- Here we see the Endpoint Protection point role
- The Software update point role
- Reporting services point role

- If the desired role is not there just right click on the server, add site system roles, click next, then next again. On the right is the remaining system roles that have not been installed. If one of the required roles is not installed just check the box and run the wizard.

Please note that the WSUS server role will need to be installed in this case on our ITFSCCM01 server. All four Server Roles installations will be demonstrated in the Endpoint Protection Installation Lecture.

Congratulations you have completed this lecture. Thanks for watching and we will see you in the next lecture.