# SCCM Lab Setup Guide

In this project, I established a comprehensive SCCM (System Center Configuration Manager) lab environment to facilitate advanced software deployment, management, and reporting. The setup involved configuring SCCM on both Microsoft Azure and a local machine using Proxmox VMs, ensuring a robust and scalable test environment.

Key Tasks Included:

- **Deployment and Configuration:** Installed and configured SCCM, deploying essential software packages, applications, Office 365, PowerShell scripts, and Windows updates.
- **Infrastructure Setup:** Created boundary groups, users, and device collections to streamline management and deployment processes.
- **Reporting and Analysis:** Developed custom reports and queries, utilizing SQL Management Studio for in-depth reporting and analysis.
- **Advanced Configurations:** Created task sequences to automate deployment tasks and implemented PXE boot to facilitate network-based installations.

This project demonstrated my ability to design and implement a scalable SCCM environment, leveraging both cloud and local resources to enhance software management and deployment capabilities.

**Lab Architecture:**

- Domain Server: DC, DNS, DHCP
- MECM/SCCM Server: Database, MP (management point), DP (Distribution Point), SMS Provider, and SCP (Service Connection Provider)
- Client PC: Windows 10

This series of pages outlines the complete setup of an SCCM (System Center Configuration Manager) or MECM lab environment.

Click Set up a Configuration Manager lab for detailed setup instructions and access to all necessary download links for the lab.

- Create a Virtual Internal VS with NAT Network in Hyper-V
- Initial VM Configuration

# Create a Virtual Internal VS with NAT Network in Hyper-V

## Step-by-Step Instructions

This guide walks you through creating a **Hyper-V Internal Virtual Switch** with NAT support for use in labs or test environments — useful for setting up isolated virtual networks.

### ? 1. Open PowerShell as Administrator

All commands below require elevated privileges.

---

### ? 2. Create a New Virtual Switch (Internal)

```
New-VMSwitch -SwitchName "LabSwitch" -SwitchType Internal
```

- This creates an **Internal** Hyper-V virtual switch named `LabSwitch`.
- The internal switch allows communication between host and virtual machines but **not** to the internet directly.

---

### ? 3. Get the Interface Index of the New Adapter

```
Get-NetAdapter
```

- Find the newly created **LabSwitch** interface.
- **Note the** `InterfaceIndex` assigned to it (e.g., `49`).
- This value will be used in the next step.

---

### ? 4. Assign a Static IP Address to LabSwitch

```
New-NetIPAddress -IPAddress 10.0.0.1 -PrefixLength 24 -InterfaceIndex 49
```

- Replace `49` with the actual **InterfaceIndex** from step 3.
- You can use any **private IP subnet** (e.g., `192.168.100.1/24`, `172.16.0.1/24`, etc.).

---

### ? 5. Create a NAT Network

```
New-NetNat -Name "NatSwitch" -InternalIPInterfaceAddressPrefix 10.0.0.0/24
```

- This enables NAT for the subnet attached to the virtual switch.
- You can name the NAT (`NatSwitch`) anything you like.
- Make sure the `AddressPrefix` matches the range you used in the previous step.

# ? Optional: Remove Network Components

## ? Remove the Virtual Switch

```
Remove-VMSwitch "LabSwitch"
```

## ? Remove NAT Object(s)

```
Get-NetNat          # List all existing NATs
Remove-NetNat -Name "NatSwitch"
```

---

> ◫ Tips
>
> - Attach virtual machines to the **LabSwitch** virtual adapter to place them on the internal NAT network.
> - VMs will use `10.0.0.1` as their **gateway** for internet access via NAT.
> - Use DHCP manually or statically assign IPs in the same subnet ( `10.0.0.x/24` ).

# Initial VM Configuration

**Steps after Virtual Machine Installation:**

1. Rename all virtual machines
2. Configure each server:
   - Open **Server Manager > Local Server**
     - Disable IPv6
     - Rename the server
     - Disable IE Enhanced Security Configuration
     - Disable Windows Update:

       ```
       Run > sconfig > Choose option 5 (Windows Update) > Set to Manual
       ```

# Domain Controller Setup

**Install AD DS and DNS:**

- Go to **Server Manager > Manage > Add Roles and Features**
- Add "Active Directory Domain Services" and "DNS Server"
- Promote the server to a Domain Controller:
  - Choose **"Add a new forest"**, name it (e.g., `lab.com`)

**Optional: Network Configuration for All VMs (If you are using Hyper-V):**

- Attach each VM to the **LabSwitch** network
- Assign static IP addresses:
  - On each VM:
    - Go to **Network Adapter Properties > IPv4 > Properties**
    - e.g.:
      - IP Address: 10.0.1.X
      - Subnet: 255.255.255.0
      - Gateway: 10.0.1.1
      - DNS:
        - For DC: `127.0.0.1`, and `1.1.1.1`
        - All other VMs: `IP of DC`, and `1.1.1.1`

**Join All Machines to the Domain**

# Firewall Configuration via GPO

On the Domain Controller:

1. Open **Group Policy Management**
2. Create new GPO: `SCCM Firewall Policy`
3. Edit the GPO:
   - Allow RDP:
     - Computer Config > Policies > Admin Templates > Windows Components > Remote Desktop Services > RD Session Host > Connection: Enable remote desktop
     - Security: Enable user authentication
   - Add inbound rules (ports: **80, 443, 1433, 4022, 8530, 8531, 3389**)
   - Add predefined rules:
     - File and Printer Sharing (inbound & outbound)
     - Windows Management Instrumentation (WMI)

# Prepare AD for SCCM Publishing

**Click Set up a Configuration Manager lab for detailed setup instructions and access to all necessary download links for the lab.**

1. **Extend the AD Schema**
   - run: `extadsch.exe`
   - Check `C:\extadsch.log` for success
2. **Create System Management Container**
   - Use **ADSI Edit**
     - Connect to CN=System
     - Right-click > New > Object > Container > Name: `System Management`
3. **Delegate Full Control** to the SCCM server:
   - Open **AD Users and Computers > Advanced View**
   - Right-click System Management > Delegate Control
   - Add SCCM Server (e.g. SCCMSRV) > Full Control

> The **extadsch.exe** tool is in the **SMSSETUP\BIN\X64** folder on the Configuration Manager installation media. Run this tool from a command line to view feedback while it runs.

# SCCM Server Prerequisites

**Click Set up a Configuration Manager lab for detailed setup instructions and access to all necessary download links for the lab.**

**Install Required Features:**

- IIS, .NET 3.5, .NET 4.7, BITS, RDC, WSUS, Windows Auth, ASP.NET 3.5, IIS 6 WMI Compatibility, IIS Management Scripts
- When prompted for source files, use Windows ISO:
  - Path: `X:\Sources\SXS`

**Install SQL Server:**

- Choose a new stand-alone instance
- Instance Features: Database Engine Services only
- Set collation: `SQL_Latin1_General_CP1_CI_AS`
- Add the current user for admin access

**Install SQL Server Management Studio (SSMS)**

- Add the SCCM Server to the local Administrators group
- Configure SQL Memory (min 8192MB, max 10240MB)

**Install SQL Reporting Services:**

- Run `sqlreportingservices.exe`
- Configure Web URL, Database, and Portal URL with defaults

# WADK, WinPE & Admin Console

**Click Set up a Configuration Manager lab for detailed setup instructions and access to all necessary download links for the lab.**

**Install:**

- Windows ADK: Deployment Tools, USMT only
- WinPE Addon
- SCCM Admin Center

## To download and install Configuration Manager:

1. Navigate to the Evaluation Center page to download the newest evaluation version of Configuration Manager.
2. Decompress the download media into your predefined location.
3. Follow the installation procedure listed at Install a site using the Configuration Manager Setup Wizard. Within that procedure, you'll input the following:

| Step in site installation procedure | Selection |
|---|---|
| Step 4: the **Product Key** page | Select **Evaluation**. |
| Step 7: **Prerequisite Downloads** | Select **Download required files** and specify your predefined location. |
| Step 10: **Site and Installation Settings** | - **Site code: e.g. LAB**<br>- **Site name: e.g. Mylab**<br>- **Installation folder:** specify your predefined location. |
| Step 11: **Primary Site Installation** | Select **Install the primary site as a stand-alone site**, then click **Next**. |
| Step 12: **Database Installation** | - **SQL Server name (FQDN):** input your FQDN here.<br>- **Instance name:** leave this blank, as you'll use the default instance of SQL Server that you previously installed.<br>- **Service Broker Port:** leave as default port of 4022. |

| Step in site installation procedure | Selection |
| --- | --- |
| Step 13: **Database Installation** | Leave these settings as default. |
| Step 14: **SMS Provider** | Leave these settings as default. |
| Step 15: **Client Communication Settings** | Confirm that **All site system roles accept only HTTPS communication from clients** isn't selected |
| Step 16: **Site System Roles** | Input your FQDN and confirm that your selection of **All site system roles accept only HTTPS communication from clients** is still deselected. |

## Enable publishing for the Configuration Manager site

Each Configuration Manager site publishes its own site-specific information to the System Management container within its domain partition in the Active Directory schema. Bidirectional channels for communication between Active Directory and Configuration Manager must be opened to handle this traffic. You'll also additionally enable Forest Discovery to determine certain components of your Active Directory and network infrastructure.

## To configure Active Directory forests for publishing:

1. In the bottom-left corner of the Configuration Manager console, click **Administration**.
2. In the **Administration** workspace, expand **Hierarchy Configuration**, then click **Discovery Methods**.
3. Select **Active Directory Forest Discovery** and click **Properties**.
4. In the **Properties** dialog box, select **Enable Active Directory Forest Discovery**. Once this is active, select **Automatically create Active Directory site boundaries when they are discovered**. A dialog box will appear that states **Do you want to run full discovery as soon as possible?** Click **Yes**.
5. In the **Discovery Method** group at the top of the screen, click **Run Forest Discovery Now**, then navigate to **Active Directory Forests** in the sidebar. Your Active Directory forest should be shown in the list of discovered forests.
6. Navigate to the top of the screen, to the **General** tab.
7. In the **Administration** workspace, expand **Hierarchy Configuration**, then click **Active Directory Forests**.

## To enable a Configuration Manager site to publish site information to your Active Directory forest:

1. In the Configuration Manager console, click **Administration**.
2. You'll configure a new forest that hasn't yet been discovered.
3. In the **Administration** workspace, click **Active Directory Forests**.

4. On the **Publishing** tab of the site properties, select your connected forest, then click **Ok** to save the configuration.

# Post-Installation Tasks

**Click Set up a Configuration Manager lab for detailed setup instructions and access to all necessary download links for the lab.**

**A. Discover Resources:**

- Enable all AD Discovery Methods (Forest, Group, System, User)
- Disable Network Discovery (not needed)
- Logs:
  - `C:\Program Files\Microsoft Configuration Manager\Logs`
  - `C:\Program Files\SMS_CCM\Logs`

**B. Create Boundaries & Groups:**

- Example:
  - IP Range: 10.0.1.2 – 10.0.1.50
  - Boundary Group: Assign site and enable site assignment

**C. Client Push Setup:**

- Site Config > Sites > Client Push Installation > Enable
- Add domain admin account
- Deploy client to discovered devices manually if needed

**Client Install Verification:**

- Folder: `C:\Windows\ccmsetup\`
- Log: `ClientIDManagerStartup.log`
- Check: "SMS Agent Host" service, "Configuration Manager" in Control Panel

**D. Create Custom Client Settings:**

- Example Name: "Client Settings for LAB"
- Customize:
  - Cache: 10240MB
  - Policy polling: 3 mins
  - Hardware Inventory: 1 hr, configure classes
  - Software Inventory: scan *.exe, *.msi, *.mp4, etc.
  - Enable Remote Tools, Software Center, Restart behavior

**Deploy Client Settings:**

- Right-click > Deploy > Select Collection

**Force Policy:**

- Right-click Collection > Client Notification > Download Device Policy

**E. Create Collections:**

- **Direct Rule:** Add specific devices
- **Query Rule:** Example: OS Caption contains "Windows 11"
- Enable incremental updates