# Fundamentals of sites and hierarchies for Configuration Manager

## ❖ Hierarchies of sites

When you install Configuration Manager for the first time, the first Configuration Manager site that you install determines the scope of your hierarchy. The first Configuration Manager site is the foundation from which you will manage devices and users in your enterprise. This first site must be either a central administration site or a stand-alone primary site.

- A Central Administration Site (CAS) is used for large organizations.
- It acts as a central control point but does not manage devices directly.
- Instead, it requires child Primary Sites to manage devices in different locations.
- These Primary Sites handle client management and help optimize network bandwidth across distributed environments.

After setting up your first site in Configuration Manager, you can add more sites to expand management.

- If you start with a Central Administration Site (CAS), you can add child-primary sites to manage devices.
- After adding a primary site (stand-alone or child), you can add secondary sites beneath it.
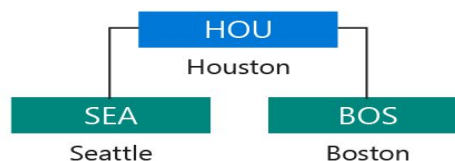
A Secondary Site:

- Can only be added under a Primary Site.
- Is used for remote locations with slow network connections.
- Helps by compressing data and managing the flow of client communication, but the Primary Site still manages the clients directly.
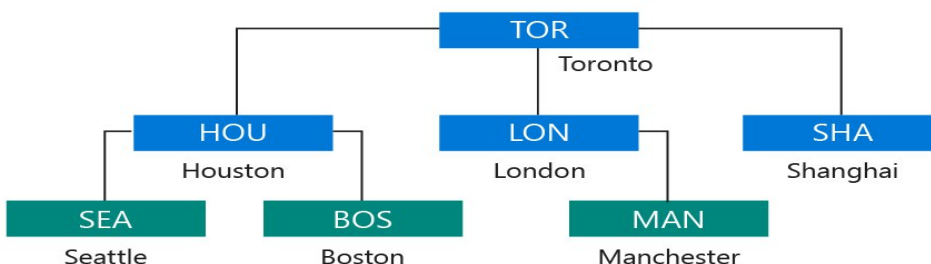
Example: Stand-alone site

HOU
Houston

Example hierarchy: Primary site with secondary sites

HOU
Houston

SEA
Seattle

BOS
Boston

Example hierarchy: Central administration site with primary sites and secondary sites

TOR
Toronto

HOU
Houston

LON
London

SHA
Shanghai

SEA
Seattle

BOS
Boston

MAN
Manchester

## ❖ Site system servers and site system roles

Each Configuration Manager site installs *site system roles* that support management operations. The following roles are installed by default when you install a site:

The site server role is assigned to the computer where you install the site.

The site database server role is assigned to the SQL Server that hosts the site database.

**Site system roles** in Configuration Manager are optional and provide specific features (like software updates, reporting, etc.).

Any computer hosting a role is called a **site system server**.

- In **small deployments**, all roles can run on the **main site server**.
- As the environment grows, you can add **more site system servers** to host roles separately, improving performance and scalability.

## ❖ Publishing site information to Active Directory Domain Services

To make Configuration Manager easier to manage, you can extend the Active Directory (AD) schema so that sites can publish important info (like site and server details) to Active Directory Domain Services (AD DS).

Managed computers can then safely retrieve site info from AD.

This process is done once per forest, and includes creating a System Management container in each domain.

It helps improve security and reduces manual setup, but it's optional for basic functionality.

## Features and capabilities of Configuration Manager

Configuration Manager (part of Microsoft Endpoint Manager) helps IT teams manage devices, apps, and updates across on-premises and cloud environments.

- **Co-management**: Manage Windows devices with both Configuration Manager and Microsoft Intune.
- **Cloud-attached management**: Use services like Cloud Management Gateway and Microsoft Entra ID for internet-based client management.
- **Real-time management**: Use CMPivot and PowerShell to instantly manage and gather data from online devices.
- **Application management**: Deploy and monitor apps, including Microsoft 365 Apps and Store apps.
- **OS deployment**: Automate Windows deployment and imaging (PXE, media, or Autopilot).
- **Software updates**: Deploy and manage system updates while optimizing network use.
- **Company resource access**: Configure access to VPN, Wi-Fi, email, and certificates.

- **Compliance settings**: Enforce and monitor security and configuration compliance.
- **Endpoint Protection**: Manage antivirus, firewall, and Defender security tools.
- **Inventory**: Collect hardware and software data, and manage software licensing with Asset Intelligence.
- **On-premises mobile device management**: Manage mobile devices using internal infrastructure.
- **Power management**: Optimize energy use and support off-hours maintenance with Wake-on-LAN.
- **Remote control**: Remotely support and troubleshoot client machines.
- **Reporting**: Use built-in and custom reports via SQL Server Reporting Services.
- **Software metering**: Track software usage to assess licensing needs.

These capabilities help organizations streamline IT management, enhance security, and improve productivity.