VMO NOTES - BLOCK 3

Contents

- Insights
- L1 - Vulnerability Remediation Overview
- L2 - ARAD Overview
- L3 - ARAD Hierarchy
- L4 - MECM Overview
- L5 - MECM Hierarchy
- L6 - MECM Administration Basic: Site System Roles
- L7 - MECM Administration Basic: Administration
- L8 - MECM Collections
- L9 - MECM Role-based Administration
- L10 - MECM Host Client
- L11 - MECM Maintenance Windows
- L12 - MECM Discovery
- L13 - MECM Querying
- L14 - MECM Querying
- L15 - MECM Reporting
- L16 - MECM Report Distribution
- L18 - Monitoring MECM
- L20 - MECM Compliance
- L21 - Non-Client Deployment Overview within MECM
- L22 - MECM Content Management: Application / Package
- L24 - MECM Application Management
- L25 - MECM Software Update Management Process
- L26 - MECM Self-Diagnosis

Insights

> - "Software" = Microsoft, "Application" = everything else

L1 - Vulnerability Remediation Overview

> - Goals
> - Explain concept of Vulnerability Remediation
> - Discuss Capabilities of Vulnerability Remediation Tools
> - Discuss Roles of Vulnerability Remediation Tools

> - Vulnerability Remediation
> - *"The patching or fixing of cybersecurity weaknesses that are detected in enterprise assets, networks, and applications"*
> - Formerly a manual process, now more automated
> - Data science, threat intelligence, and predictive algorithms now help determine which vulnerabilities should be remediated first
> - The number of CVEs observed in devices has tripled since 2020, according to the National Vulnerability Database
> - Vulnerability remediation is mandated by the AFI, MPTO, and AFMAN government regulations, and the NIST industry standard
> 1. Does a VMO have to remediate all Vulnerabilities?
> 2. How can you determine which vulnerabilities are likely to be exploited by hackers and malware?
> 3. How can you effeciently remediate those vulnerabilities?
> 4. How do you set realistic remediation deadlines?
> - Prioritize remediation based on vulnerability severity and potential CIA impact on the vulnerable system or data
> - Severity is determined by the NIST CVSS rating
> - NOS/COSs meet a 95% remediation threshold; remaining assets are the responsibility of the local base, PMO, or other responsible entity
> - Base CFPs are assist NOS/COSs with remediation that enterprise automated tools cannot do
> - Base CFP/CSs will alert their servicing NOS/COSs when unmanaged assets rise above 10%
> - Asset numbers are determined by cross-referencing their ACAS NAD with AD, ARAD, and MECM
> - Base NCC/CFPs will populate NOS/COS patch testing groups with at least 3% of their base's total assets, to include a representitive sample of every configuration at the base and systems from each mission set
> - Base NCC/CFPs will identify information systems controlled by a PMO within their respective AOR
> - PMO systems will be patched only upon approval of the PMO or system owner
> - To be consider a PMO system, the system must be registered in DITPR and have Interim Approval to Operate, Approval to Operate/Connect in eMASS through the DoD RMF

- Capabilities of Remediation Tools
    - VMOs will implement Advertise Only Server Maintenance Windows
        - The Advertise Only group is primarily for mission-essential servers, where a sysadmin must log into the server and run installs
            - ex. Core service or Mission Critical servers that often need ASI for updates and reboots
        - ASIs are used to communicate scheduled outages affecting AFIN operations, and must be approved prior to any changes or modifications
        - Servers not in a required maintenance window will default into the Advertise Only group
    - VMOs will implement a process for users to customize an install schedule when mission requirements call for a client system to remain uninterrupted
        - Implementation deadlines shall restrict the users' ability to delay updates for an unreasonable amount of time, determined at the discretion of the implementation authority and VMO
    - Plans of Action and Milestones (POA&Ms) are required when the date for certain orders or requirements cannot be met and will only be granted when additional time is required to bring systems into compliance
        - A POA&M identifies specific actions with completion dates, but does not extend the date for those orders or requirements; they will not be considered met until systems are brought into compliance
        - A POA&M doesn't grant the requesting agency the authority to accept vulnerabilities or risks identified in the orders/requirements, but is instead an acknowledgment of the risks for the specified period based on an Operation Risk Management decision
        - Non-compliant systems without an approved POA&M are subject to quarantine or disconnection orders
    - Prioritization Model (3 Tiers)
        - *"690 NSS/AMAC will direct NOS/COS, NCC/CFP, and PMO through the orders management system to implement Normal Vulnerability remediation actions via the three-tiered prioritization model. 616 OC will direct tasking Priority and Emergency remediation actions to NOS/COSs via that same three-tiered prioritization model."*

        1. Normal (11 Days)
            - NOS/COS VMOs will implement a phased patch testing approach
                - Issues discovered turing testing phases will be reported to the responsible party per issued orders

                1. Patches will be tested on a local testing environment for 24-72 hours
                2. Patches will be issued to the AFIN 3% test group for 3-5 days
                3. If no issues are discovered, as determined by the CSCS functional lead for Vulnerability Management, VMOs will issue patches AFIN-wide until the orders are rescinded, the patch is superseded, or the 95% threshold is reached

        2. Priority (3 Days)
            - VMO Patch Management technicians will test patch for 24-48 hours
            - VMO Patch Management team will have 24 hours to deploy to enterprise, to a minimum 80% compliance of machines with remediation clients installed

after 5 days
        - If 80% minimum compliance is not met, NOS/COS Crew will report to 616 OC via MISREP for action to re-task or send another unit for remediation
        - If 80% minimum compliance is met, then a persistent deployment will be created
    3. Emergency (24 hours)
        - VMOs will forgo all testing
        - Upon notification to CSCS Crew Commander, the NOS/COS Patch Management Team will release enterprise patch within 24 hours, with a mandated minimum 70% compliance within 72 hours
        - If 70% minimum compliance is not met, NOS/COS Crew will report to 616 OC via MISREP for action to re-task or send another unit for remediation
        - If 70% minimum compliance is met, then a persistent deployment will be created

- Roles of Remediation Tools
    - "*VMOs will execute vulnerability remediation to reduce AFIN risk through the implementation of approved countermeasures*"
    - Countermeasures must be tasked by approved order; examples below
        - Configuration changes to systems and registries
        - Installation of software patches
        - Removal of non-approved software
        - Searching for and removing malicious files
        - Upgrading applications
        - Reinstalling OS
        - Correction of system configuration deviations against approved guidlines
    - Vulnerability management features for a variety of enterprise security needs
        - Continuous monitoring and scanning for vulnerabilities
        - Monitoring profile and rule system (as determined by IT)
        - Ability to set notification rules
        - Attack surface visualization
        - Attack vector analytics and modeling
        - Risk-scoring (CVSS)
        - Patch management (MECM)
        - Automated updates and patching (MECM)
        - Network access path analysis to identify problematic routes and suggest redirection
        - Reachability analysis for endpoints and secured assets
        - Customizable reporting
        - Automatic remediation (ARAD)
    - Vulnerability management software takes a proactive approach, compared to reactive cybersecurity tools like firewalls and antivirus software which manage attacks as they occur
        - They are designed to proactively look for weaknesses by scanning and identifying vulnerabilities and providing remediation
    - Some vulnerability management tools can assign threat levels to weaknesses (CVSS), allowing IT teams to prioritize the most significant issues, or even automatically applying patches or fixes

    - Paid enterprise vulnerability management software can save technicians time that a free tool would require, paying for itself in both data breaches and staff time

---

L2 - ARAD Overview

- Goals
    - Explain ARAD capabilities and limitations
    - Differentiate Questions vs Actions with ARAD

- Automated Remediation Asset Discovery (ARAD)
    - Automated, near real-time remediation solution, individually utilized on AF Enterprise networks
    - Implemented on the AFNet with both manual and automated plain language queries and packages
        - Packages can be any executable or action to be accomplished as device administrator on a managed endpoint

- ARAD Capabilities
    - Provide a near real-time, standardized, simplified architecture/solution for rapid and automated DoDIN Ops and DCO
    - (CSCS), (ACD), (CDA), and (CVA/H) weapon systems
    - Enforce Enterprise-wide security standards on managed end-points
    - Conduct defensive missions on managed end-points
        - Maintain enterprise-level situational awareness about managed end-points
    - ARAD Servers are installed at Scott AFB Area Processing Center (APC) and Wright-Patterson AFB to operate as a "single source"
    - Architecture provides a high-availability and redundant solution to prevent diminished capability due to system or network prolems
    - Servers are placed as close to the boundary as practical and postured for implementation within the Integrated Management Suite (IMS) for out-of-band-managememeng (OOBM)
    - Mission Effectiveness Criteria
        - Situational Awareness
            - Provide complete and accurate situational awareness of the operational environment within 15 minutes for any issued query for all managed endpoints
        - Defensive Posture and Response
            - Automate crafted/known malicious activity queries and alert within 15 seconds of detection
            - Automate elements of existing SOPs/TTPs allowing operators to focus on analysis and operational response
    - DISA-developed STIGs for Tanium (the ARAD soulution) will be applied/followed
        - If unable to implement in whole or part, the PMO will document POA&M and obtain approval until STIGs can be app
    - Speed

        - Provides near real-time AFNet Response and Situational Awareness within seconds to minutes
    - Root-level access on each machine
        - The Current Branch clients for ARAD and MECM will be added as permanent elements of all current and future SDC and SSC operational baselines
            - Built-in 2-person integrity (TPI)
            - Centralized, remote removal of unapproved software AFNet-wide
            - Maneuver and engage adversary activity
    - Multiple supported OS vendors for endpoints
        - Windows, MacOS, Linux, AIX, Solaris

- ARAD Limitations
    - No opearational deployments
    - Client based; No client, no management
    - Time to live - 10 minutes
        - Only recieve answers from cliented systems that are currently online

- ARAD Questions
    - Tanium questions are queies that are issued from the Tanium server to managed endpoints
        - Questions have a "get clause" that specifies the information to retrieve and "from clause" that specifies the target endpoints
    - Question Categories
        - Dynamic question
            - Create and issue through the Explore Data or Question Builder features
        - Saved question
            - Configuration object that enables reissuing a question without reconstructing it
    - Methods for Dynamic Question creation
        - Explore Data
            - Suggests a number of queries based on natural language parsing
        - Question Builder
            - Guided method for dynamic question creation; has form fields for completing the get statement and from clause, including any filters

- ARAD Actions
    - After using Tanium Interact to issue a question, analyze the question results, and determine which endpoints require administrative action, one can deploy a package to those endpoints so that the Tanium Client can run the associated action
    - Actions include using the Patch module to manage operating system patching across the entire enterprise
    - Workflows and schedule patches can be based on rules or exceptions built around patch lists, block lists, and maintenance windows
    - The Patch module generates reports and returns current patch applicability results from every endpoint
        - Details provided

        - Patch details, such as severity, release date, applicable CVE, files, and links to knowledge base articles
        - Patch status, split out by computer group
        - Assigned patch lists or block lists for the patch
    - The patch module provides a baseline reporting patch list for each supported OS, patch and block lists must also be created
        - A patch list contains patches that can be applied
        - A block list contains patches that must be excluded
        - Lists can be determined by any detail included in the patch information

---

L3 - ARAD Hierarchy

- Goals
    - Explain ARAD Hierarchy
    - Explain Linear Chain as used by ARAD

- ARAD Linear Chain
    - ARAD uses a linear chain system where devices dynamically organize into neighorhood groups
        - These groups in turn gather data in a serial motion where the last machine submits the whole group's findings to the central server
        - ARAD is built on 2 server stacks located at Wright-Patterson and Scott APCs
    - Backward Leader
        - First member of the chain, answers the question and passes the question and answer down the chain
    - Forward Leader
        - Last member of the chain, sends results back to the Tanium server; all answers are hashed
    - The systems one can query is based on the level of your security group
        - Base-level ARAD groups will only see systems at one base, while MAJCOM-level gtoups would see an entire MAJCOM's system
        - The AORs are currently tied to OUs
        - There are over 900 sensors built in to Tanium by default, and ARAD administrators may add more as necessary
    - Tanium clients will scan their systems once every 24 hours for STIG changes

---

L4 - MECM Overview

- Goals
    - Explain MECM capabilities and limitations
    - Explain hierarchies of sites within MECM
    - Differentiate management capabilities of Central Administration Site (CAS) vs Primary Site vs Secondary Site and roles within MECM

    - Discuss collection replication within MECM
    - Discuss purpose of Windows Server Update Services (WSUS) integration with MECM

- MECM Capability
    - *"MECM is a cromprehensive management system developed by Microsoft that manages, maintains, and patches hundreds of thousands of AF networked systems each day."*
    - Capabilities
        - Centralized Application Deployment
        - Software Updates
        - Operating System Deployment (OSD)
        - System Management "STIGs & Registry Keys"
        - Reporting
        - Root level access

- MECM Limitations
    - Client-based
        - Some clientless devices are supported, but this is mostly limited to MDM devices
    - Windwos OS-based
        - Some MacOS and MDM devices are supported, but this is limited

- MECM Hierarchy of Sites
    - A Configuration Management deployment **must** be installed in an Active Directory domain
        - The foundation of this deployment includes one or more Configuration Manager sites that form a hierarchy of sites
        - Type and location of sites one installs provide the ability to scale up a deployment when necessary, and deliver key services to users and devices
        - Top-tier site is at the top of the hierarchy of sites, and is initially the first site to be deployed
    - Central Administration Site (CAS)
        - Suitable for large-scale deployments, provides centralized administration, and provides the flexibility to support globally distributed devices
        - If deployed, must be the top-tier site, with at least 1 child primary site
        - Doesn't directly support management of devices
    - Primary Site
        - Used to directly manage devices, and to control network bandwidth when managed devices are in different geographical locations
        - If a primary site is the top-tier site (stand-alone primary), it must be the only primary site in the deployment
        - If there are more than one primary site in a deployment, they must be children of a CAS
    - Secondary Site
        - Can only be installed as a child to a primary site
        - Extends the reach of a primary site to manage devices (secondary site does not manage the clients, but does have clients assigned to it)
        - Useful in locations with a slow network connection to the primary site

        - Provides support by compressing and managing the transfer of information across the network
    - Hierarchy Tiers
        - Tier 0
            - Top-level site
            - CAS or Stand-alone Primary
        - Tier 1
            - Child Primary or Child Secondary to a Stand-alone Primary
        - Tier 2
            - Child Secondary to Child Primary
        - Managed Devices
            - PCs, Servers, Mobile, and others

- Collection Replication
    - Collections organize resources into manageable units
        - Used to perform operations on multiple resources at once
        - Contains devices or users
    - Replication types
        - File-based Replication
            - Transfers file-based data between sites in the hierarchy, including applications and packages for deployment to distribution points in child sites
        - Database Replication
            - Uses SQL Server to transfer data; merges changes in its site database with information from the database at other sites in hierarchy
            - When a secondary site is attached to a primary site, the sites use database
    - Configuration Manager primarily classifies the data that it replicates as either global data or site data
        - Global Data
            - Transfers to a parent or child site
            - Includes
                - Software Deployments
                - Software Updates
                - Collection Definitions
                - Role-based administration security scopes
        - Site data
            - Transfer only to parent site
            - Includes
                - Hardware inventory
                - Status messages
                - Alerts

- WSUS Integration
    - "*Configuration Manager integrates with Windows Server Update Services (WSUS) to manage software updates*"

L5 - MECM Hierarchy

- Goals
  - Discuss purpose of the MECM host client

- Host Client
  - *"The Configuration Manager site accepts data from devices that run the Configuration Manager client. This behavior introduces the risk that the clients could attack the site. Deploy the Configuration Manager client only to devices that you trust."*
  - Client Status Information types (Refer to L18 for detailed information)
    - Client online status
    - Client Activity
      - Requested policy update
      - Sent a heartbeat message
      - Sent hardware inventory
    - Client Check
    - Decommissioned
    - Obsolete

L6 - MECM Administration Basic: Site System Roles

- Goals
  - List site system roles within MECM

- Site System Roles
  - Configuration Manager site server
  - Configuration Manager site system
  - Configuration Manager component site system role
  - Configuration Manager site database server
  - SMS Provider
  - Asset Intelligence synchronization point
  - Certificate registration point
  - Cloud management gateway connection point
  - Data warehouse service point
  - Distribution point
  - Endpoint Protection point
  - Enrollment point
  - Enrollment proxy point
  - Exchange Server connector
  - Fallback status point
  - Management point
  - Reporting services point
  - Service connection point
  - Software update point
  - State migration point

L7 - MECM Administration Basic: Administration

- Goals
  - Describe function of management point role
  - Describe function of Configuration Manager site database server role within MECM
  - Describe function of roles
    - SMS Provider
    - Distribution point
    - Software update point
    - Reporting services point
    - Fallback status point
  - Discuss impact of database replicas for management
  - Discuss impact of extending Active Directory discovery regarding MECM and site information publishing
  - Explain impact of MECM integration with Windows Server Update Services (WSUS)
  - Explain impact of Software Center installation alongside MECM client on host

- Role Support
Site System Role	CAS	Pri	Sec
Component server	Yes	Yes	Yes
Distribution Point		Yes	Yes
Management Point		Yes	Yes
Site Database Server	Yes	Yes	Yes
Site Server	Yes	Yes	Yes
Site System	Yes	Yes	Yes
System Health Validator point	Yes	Yes	
State Migration point		Yes	Yes
Fallback Status point		Yes	
Out of Band Service point		Yes	
SMS Provider	Yes	Yes	
Reporting Services point	Yes	Yes	
Application Catalog web service point		Yes	
Application Catalog website point		Yes	
Mobile Device Enrollment proxy point		Yes	
Mobile Device and AMT Enrollment point		Yes	
Asset Intelligence Synchronization point	Yes		

Site System Role	CAS	Pri	Sec
Endpoint Protection point	Yes		
Software Update point	Yes	Yes	Yes
Windows Intune Connector	Yes	Yes	
Certificate Registration point	Yes	Yes	

- Management Point Role
  - A site system role provides policy and service location information to clients, and receives configuration from clients
  - By default, this role installs on the site server when you install a new primary or secondary site
  - Primary sites support multiple instances of the role, Secondary sites support only 1
  - Also referred to as a proxy management point, this role on a Secondary site provides a local point of contact for clients to get computer and user policies
  - Set up to support HTTP or HTTPS
  - Use database replicas for management points to reduce processing load on the site database server
  - Each client independently identifies a management point as its default when it first assigns to a primary site
    - Becomes the client's assigned management point
    - Client selects a management point based on client's network location and boundary group configurations
    - Client may not use the assigned management point
  - Preferred management points are from a client's assigned site, associated with a boundary group that the client uses to find site system servers
    - Association is similar to how distrution and state migration points are associated with a boundary group
    - If enabled, clients will try to use a preferred manage point before others from its assigned site
  - When a client needs to contact a management point, it first checks the MP list, created when the client installs and updated periodically with details about each MP in the hierarchy
  - When the client can't find a valid MP in the list, it searches the service location sources in order until it finds a point it can use
    1. Management Point (MP)
    2. Active Directory Domain Services (AD DS)
    3. DNS
    - When the client locates and contacts a management point, it updates its MP list.
  - Clients communicate with MPs to
    - Download information about other MPs and build a list of known MPs for future service location cycles (MP list)
    - Upload configuration details, like inventory and status
    - Download a policy that sets configurations on the client, informs it of software to install, and other related tasks

        - Request information about other site system roles that provide services the client can use
            - ex. Distribution points for software or software update points

- Database Server Role
    - The site assigns this role to site system servers that hold an instance of the site dataase
    - Only move by running setup to modify the site to use a different instance of SQL Server to host the site database

- SMS Provider Role
    - Assigned to each computer that hosts an instance of the SMS Provider
    - The interface between a Configuration Manager console and the site database
    - By default, role automatically installs on the site server of a central administration site and primary sites
    - Install additional instances at each site to provide access to additional administrative users, and for redundancy
    - To install additional providers, run Configuration Manager setup to manage the SMS provider, then install additional providers on additional computers
        - Only install one instance per computer, which must be in the same domain as the site server

- Distribution Point Role
    - Contains source files for clients to download
        - Examples
            - Application content
            - Software packages
            - Software updates
            - OS images
            - Boot images
    - By default, installs on the site server when one installs a new primary or secondary site
    - Not supported on a CAS
    - Install multiple instances at a supported site, and at multiple sites in the same hierarchy
    - All distribution points host the client source files
    - Clients find the nearest distribution point to download source files during client deployment or update
        - If the site doesn't have a distribution point, clients downlaod source files from their management point

- Software Update Point Role
    - Integrates with Windows Server Update Services (WSUS) to provide software updates to Configuration Manager Clients
    - Supported at all sites
        - Install this site system at the CAS to synch with WSUS
        - Set up each instance at child primary sites to synch with the CAS
        - When network data transfer is slow, consider installing a software update point in secondary sites
    - Number of supported clients depends on WSUS version and on whether the software update point site system role coexists with other site system roles

- Reporting Services Point Role
  - Site system role that integrates with SSRS to create and manage reports for CM
    - Supported at Primary sites and CAS
    - Can install multiple instances on a site
    - Some client deployment reports require clients are assigned a fallback status point

- Fallback Status Point Role
  - Site system role that helps monitor client isntallation
    - Identifies unmanaged clients because they can't communicate with their management point
    - Supported only at Primary sites
    - Can install multiple instances on a site
    - Optional, but recommended for client deployment
    - Tracks client deployment and enables computers in the CM site to send state messages when they can't communicate with a management point
    - Always communicates with clients of HTTP
      - Uses unauthenticated connections and sends data in clear text
      - Vulnerable to attack, particularly when used with internet-based client management
      - To reduce attack surface, always dedicate a server to running the fallback status point
    - Don't install other site system roles on the same server
    - Don't install if the security risks of running a website with unauthenticated connections and clear text transfers outweigh the benefits of identifying client communication problems

- Impact of Database Replicas
  - CM primary sites can use a database replica to reduce the CPU load placed on a database server
  - Regularly monitor the site database and replicas to ensure they sync up

- Extending AD Discovery and Site Information Publishing MECM
  - After extending the AD schema for CM, VMO can publish CM sites to AD DS; this lets AD computers securely retrieve site information from a trusted source
  - Publishing site information to AD DS is not required for CM functionality, but it can reduce administrative overhead
  - When a site is configured to publish to AD DS, CM clients can automatically find management points through AD publishing
  - When a site doesn't publish to AD DS, clients must have an alternative mechanism to locate their default management point

- Impact Software Center Installation
  - Software Center is installed when the CM client is installed on a Windows device
  - Users use Software Center to request and install software that VMO deploy
  - Software Center lets users browse and install applications, software updates, and new OS versions, view their software request history, and view device compliance against organization policies

    - Organization IT admin uses Software Center to install applications, software updates, and upgrade Windows
        - VMO may disable some aspects of Software Center
        - If multiple users are using a device at the same time, only the user with the lowest session ID will see all available deployments in Software Center

---

L8 - MECM Collections

- Goals
    - Define Collections within MECM
    - Differentiate types of rules used to configure members of a collection

- Collections
    - Groupings of users or devices
        - Can only contain one or other
    - Used for tasks like managing applications, deploying compliance settings, or installing software updates
        - Can also be used to manage groups of client settings or with role-based administration to specify resources an administrative user can access

- Configure Rules Collection Members
    - Built-in collections (cannot be modified)

Group	Description
All User Groups	Contains user groups discovered by Active Directory Security Group Discovery
All Users	Contains users discovered by Active Directory User Discovery
All Users and User Groups	Contains All User Groups and All Users; contains the largest scope of user and user group resources
All Desktop and Server Clients	Contains the server and desktop devices that have the Configuration Manager client installed; membership maintained by Heartbeat Discovery
All Mobile Devices	Contains mobile devices managed by Configuration Manager; membership restricted to mobile devices successfully assigned to a site or discovered by the Exchange Server connector
All Unknown Computers	Contains generic computer records for multiple computer platforms; one can use this to deploy an OS by using a task sequence and PXE boot, bootable media, or pre-staged media

Group	Description
All Systems	Contains All Desktop and Server Clients, All Mobile Devices, and All Unknown Computers, as well as all mobile devices enrolled by Microsoft Intune; contains the largest scope of device resources

- Custom Collections
  - Created in Configuration Manager
  - Membership determined by collection rules
Rule	Function
Direct Rule	Choose the users or computers that you want to add; requires more administrative overhead. Resources must be discovered or imported before adding; removing resources also removes it from the rule
Query Rule	Dynamically update collection membership based on a query running on a schedule
Include Collection Rule	Includes the members of another collection; can include multiple collections and updates run on a schedule
Exclude Collection Rule	Excludes the members of another collection; can exclude multiple collections and updates run on a schedule; takes priority over Include if the two rules conflict

L9 - MECM Role-based Administration

- Goals
  - Describe role-based administration within MECM

- Role-Based Administration/Access Control (RBAC)
  - With Configuration Manager, one uses role-based administration to secure the access that administrative users need
    - Also secures access to objects being managed, like collections, deployments, and sites
  - "*The role-based administration model centrally defines and manages hierarchy-wide security access.*"
  - This model is implemented for all sites and site settings by using these items
    - Security roles are assigned to admins to give them permissions for Configuration Manager objects; ex. permission to create or change client settings
    - Security scopes are used to group specific instances of objects that an admin is responsible to manage; ex. an application that installs the Configuration Manager console
    - Collections are used to specify groups of users and devices that the administrative user can manage in Configuration Manager

    - The combination of roles, scopes, and collections allow one to segregate administrative assignments that meet organization requirements
        - This combination defines the scope of a user
        - Administrative scope controls the objects that an admin views in the Configuration Manager console, and controls the permissions that a user has on those objects
    - All security assignments are replicated and available through the hierarchy
    - Role-based administration configurations replicate to each site in the hierarchy as global data and applied to all administrative connections

- Security Roles
    - Used to grant security permissions to admins
    - *"Security roles are groups of security permissions that you assign to administrative users so that they can do their administrative tasks."*
    - These security permissions define the actions that an admin can do and the permissions that are granted for specific object types
        - As a security best practice, assign the security roles that provide the least permissions required for the task (Principle of Least Privilege)
    - Configuration Manager has several built-in security roles to support typical groupings of administrative tasks
        - Built-in roles cannot be modified, other than to add users
        - Built-in roles can be copied, and these copies can be modified like any other custom security roles
    - You can make custom security roles, or import roles created in a seperate environment; ex. roles created in a testing environment
    - Each security role has specific role permissions for different object types

- Security Scopes
    - Used to provide admins with access to securable objects
    - *"A security scope is a named set of securable objects that are assigned to administrator users as a group."*
    - All securable objects are assigned to one or more security scopes
    - Built-in Security Scopes
        - All: Grants access to all scopes; objects cannot be assigned to this scope
        - Default: Used for all objects by default; Configuration manager assigns all objects to this scope upon installation
    - Create security scopes to restrict objects that admins can see and manage
    - Security scopes cannot be nested
    - Some objecs cannot be included in security scopes because they are only secured by security roles; administrative access to these objects cannot be limited to a subset of the available objects

---

L10 - MECM Host Client

- Goals
    - Define MECM client

    - Differentiate methods to deploy clients to hosts within MECM
    - Discuss settings and options for the MECM console from the Client Settings node in the Administration workspace

- MECM Client
    - Configuration Manager can manage 2 broad categories of devices
        - Clients
            - Devices like workstations, laptops, servers, and mobile devices where you install the MECM client software
            - Client software is required for some management functions, like hardware inventory
        - Managed Devices
            - Can include clients, but typically includes mobile devices where the CM client software isn't installed; these devices are manged using the built-in on-premises mobile device management (MDM) in CM
    - Devices can also be grouped and identified based on user rather than client type
    - There are 2 ways to use Configuration Manager client software to mange a device
        1. Discover the device on the network, deploy client software
        2. Manually install client software on the device, then have it join the site
    - To discover devices that don't have the client software installed, run one or more of the built-in discovery methods
        - When a device is discovered, use one of several methods to install client software

- Clients to Hosts Deployment Methods
    1. Client Push Installation
        - 3 main ways to use
            - Configure client push installation for a site; automatically runs on devices the site discovers; method is dependent on boundary groups
            - Run the Client Push Installation Wizard for a specific collection or resource
            - Run the Client Push Installation Wizard for client installation to query the result; the installation will only succeed if the query returns the proper result
        - Advantages
            - Can be used to install the client on a single computer, a collection of computers, or to the results of a query
            - Can be used to automatically install on all discovered computers
            - Automatically uses client installation properties defined on the Client tab in the Client Push Installation Properties dialog box
        - Disadvantages
            - Can cause high network traffic when pushing to large collections
            - Can only be used on computers that have been discovered by Configuration Manager
            - Cannot install clients on an AD workgroup member, only AD domain members
            - A client push installation account must be specified that has administrative rights to the intended client computer
            - Windows Firewall must be configured with exceptions on client computers
            - You can't cancel client push installation

        - Configuration Manager tries to install the client on all discovered resources, and retries any failures for up to 7 days
2. Software Update Point-based Installation
    - Publishes the client (or update) to a software update point as a software update
    - Advantages
        - Can existing software update infrastructure to manage the client software
        - Can automatically install the client software on new computers if WSUS and AD DS are configured to enable it
        - Doesn't require computers to be discovered before the client can be installed
        - Computers can read client installation properties that have been published to AD DS
        - If the client is removed, this method reinstalls it
        - Doesn't require you to configure and maintain an installation account for the intended client computer
    - Disadvantages
        - Requires functioning software updates infrastructure
        - Must use the same server for client installation and software updates; this server must reside in a primary site
        - To install new clients, a group policy object must be configured in AD DS with the client's active software update point and port
        - If the Active Directory schema isn't extended for CM, group policy settings must be used to provision computers with client installation properties
3. Group Policy Instillation
    - Use Group Policy in Active Directory Domain Services to publish or assign the CM client
        - Client installs when the computer starts and client appears in Add or Remove Programs in Control Panel, where the user can install it; accessing client installation files requires administrator permissions
    - Advantages
        - Doesn't require computers to be discovered before the client can be installed
        - Can be used for new client installations for upgrades
        - Computers can read client installation properties that have been published to AD DS
        - Doesn't require configuring and maintaining an installation account for the intended client computer
    - Disadvantages
        - If a large number of clients are being installed, it can cause high network traffic
        - If the Active Directory schema isn't extended for Configuration Manager, group policy settings must be used to add client installation properties to computers in the site
4. Manual Installation
    - Manually install the client software using CCMSetup.exe, found in the {Configuration Manager installation folder}\Client on the site server; accessing client installation files requires administrator permissions
    - Advantages

        - Doesn't require computers to be discovered
        - Can be useful for testing
        - Supports using command-line properties for CCMSetup
        - Additionally supports non-windows client platforms (macOS X)
    - Disadvantages
        - No automation; time-consuming
5. Longon Script Installation
    - Configuration Manager supports using logon scripts to install the client using the CCMSetup.exe; uses the same methods as Manual Installation
    - Advantages
        - Doesn't require computers to be discovered
        - Supports using command-line properties for CCMSetup
    - Disadvantages
        - If a large number of clients are being installed, it can cause high network traffic
        - If users don't frequently log on to the network, it can take a long time to install on all computers
6. Microsoft Intune MDM Installation
    - Deploys the CM client to devices that are enrolled with Microsoft Intune
    - Advantages
        - Doesn't require computers to be discovered
        - Doesn't require configuring and maintaining an installation account for the intended client computer
        - Can use modern authentication with Azure Active Discovery
        - Can install and assign computers on the internet
        - Can automate with Windows AutoPilot and Microsoft Intune for co-management
    - Disadvantages
        - Requires additional technologies outside of CM
        - Requires the device have internet access, even if not internet-based

---

L11 - MECM Maintenance Windows

- Goals
    - Describe function of Maintenance Windows in MECM
    - List tasks that support Maintenance Windows in MECM
    - Discuss timing considerations for scheduling maintenance windows
    - Discuss considerations for overlapping maintenance windows
    - Differentiate maintenance window and service window

- Functions of Maintenance Windows
    - *"Use maintenance windows to define when Configuration Manager can run impacting tasks on devices."*
    - Maintenance windows help make sure client configuration changes occur during times that don't effect productivity

    - With Software Center, users can see the device's nex maintenance window in the Installation status tab
    - When users install applications from software center, the client starts it immediately, prioritizing user intent over admin intent
    - When an application deployment needs to reach an installation deadline during non-business hours defined in Software center, the client installs the application, prioritizing admin intent over user intent

- Tasks - Maintenance Windows
    - 4 tasks that support maintenance windows
        - Application and package deployments
        - Software update deployments
        - Compliance settings deployment/evaluation
        - OS and custom task sequence deployments

- Scheduling Maintenance Windows
    - Configure maintenance windows with an effective date, start and end time, and recurrence pattern
        - Maximum duration must be less than 24 hours
    - By default, computer restarts caused by a deployment aren't allowed outside of a maintenance window, but this can be overridden
    - Maintenance windows affect only the time the deployment runs
        - Deployments configured to download and run locally can download content outside of the window
    - Deployment will only run if its maximum allowed runtime doesn't exceed the duration of the maintenance window
    - If a deployment fails, the client generates an alert, then reruns the deployment during the next maintenance window that has available time

- Overlapping Maintenance Windows
    - If maintenance windows overlap, clients treat them as a single window for the entire time of both windows
    - By default, in the case of overlapping maintenance windows, the client only installs software updates during Software Update type windows, ignoring All-deployments windows unless they're the only type
        - This behavior can be configured with Software Update client settings

- Maintenance Window vs Service Window
    - Maintenance windows are for clients
    - Service windows are for site servers
        - Site servers can be serviced individually while others still operate, impacting global or site performance based on the server experiencing downtime

---

L12 - MECM Discovery

- Goals

    - Explain endpoint discovery within MECM
    - Differentiate Discovery methods
    - Define Discovery Data Records (DDRs)
    - Discuss DDR replication across the site hierarchy

- Discovery
    - Used to find device and user resources, and identify network infrastructure
    - Most discovery methods require enabling them at the site and setting them up to serach specific network or Active Directory locations
        - When they run, they query the location for information on devices and users CM can manage
    - Discovery can create high traffic, and Discovery Data Records can use significant CPU resources during processing
        - Use only discovery methods required to meet goals

- Discovery Methods
    - Available Discovery Methods
        - Active Directory Forest Discovery
        - Active Directory Group Discovery
        - Active Directory System Discovery
        - Active Directory User Discovery
        - Heartbeat Discovery
        - Network Discovery
        - Server Discovery
    - Active Directory (AD) Forest Discovery
        - Does not discover resources that can be managed
        - Discovers network locations that are configured in AD, and can convert these locations into boundaries for use in the hierarchy
        - Searches local AD Forest, trusted forests, and each additional forest configured in the AD Forests node of CM
        - Use to
            - Discovery AD sites and subnets, and create CM boundaries
            - Identify supernets assigned to an AD site, and convert each supernet into an IP address range boundary
            - Publish to Active Directory Domain Services (AD DS) in a forest when publishing is enabled; the specified AD Forest account must have permissions to that forest
    - Active Directory Group Discovery
        - Used to search AD DS for
            - Local, global, and universal security groups
            - The membership of groups
            - Limited information about a group's member computers and users, even when another discovery method hasn't discovered those computers and users
        - Intended to identify groups and group relationships of members
        - Security groups by default, can also find membership of distribution groups

        - Doesn't support extended AD attributes identified using AD System Discovery or AD User Discovery
        - Not optimized to discover computer and user resources; run after System and User Discovery
            - Creates a full DDR for groups, but only a limited DDR for members of groups
    - Active Directory System Discovery
        - Used to search AD DS locations for computer resources that can be used to create collections and queries
        - Can install the CM on discovered devices via client push installation
        - Discovers basic computer information
            - Computer Name
            - OS and version
            - AD container name
            - IP address
            - Active Directory site
            - Time stamp of last login
        - To create a DDR for a computer, AD System Discovery must be able to identify a computer's account and resolve the computer name to an IP address
    - Active Directory User Discovery
        - Used to search AD DS to identify user accounts and associated attribute
        - Discovers basic user account information
            - Username
            - Unique username, includes domain name
            - Domain
            - AD container names
    - Heartbeat Discovery
        - Enabled by default, and runs on clients to create a DDR instead of site server
            - For mobile clients, the DDR is created by the management point of the device
        - Maintains database record of CM clients
            - Can also force discovery of a computer as a new resource record
        - Runs every 7 days by default
            - If this is modified, one must ensure it runs more frequently than the site maintenance task Delete Aged Discovery Data, which deletes inactive client records from the site database
            - Delete Aged Discovery Data can be configured only for primary sites
        - Can also be manually invoked on a specific client
            - Run the Discovery Data Collection Cycle action on a client's CM control panel
        - When run, Heartbeat Discovery creates a DDR with the client's current information, a small file (~1KB) which the client then copies to a management point so that a primary site can process it; file information includes:
            - Network location
            - NetBIOS name
            - Version of the client agent
            - Operational status details

        - The only discovery method that provides details about client installation status, which it achieves by updating the system resource client attribute to set a value equal to Yes
    - Network Discovery
        - Used to discover topology of a network and discover devices on the network with an IP address
        - Searches the network for IP-enabled resources by querying the following entities
            - Servers that run a Microsoft implementation of DHCP
            - Address Resolution Protocol (ARP) caches in network routers
            - SNMP-enabled devices
            - Active Directory domains
        - The level of discovery must be specified before running Network Discovery
            - One or more discovery mechinisms must also be configured that enable Network Discovery to query for network segments or devices
            - Additional settings help control discovery actions on the network
            - Lastly, one or more schedules are defined for when the Network Discovery runs
        - To successfully discover a resource, Network Discovery must identify its IP address and subnet mask, using the following methods
            - Router ARP cache
                - Network Discovery queries the ARP cache of a router to find subnet information
                - Due to the short time-to-live of ARP cache data, the cache may not have information on the requested object
            - DHCP
                - Network Discovery queries each DHCP specified to discover devices for which they provided a lease
                - Supports only the Microsoft implementation of DHCP
            - SNMP
                - Network Discovery directly queries an SNMP device
                - Device must have a local SNMP agent installed
                - Network Discovery must be configured to use the community name used by the SNMP agent
        - When an IP-addressable object with a known subnet mask is discovered, Network Discovery creates a DDR for that object
        - Because it works by exploring the network directly, Network Discovery discovers resources that don't support the CM client; ex. printers and routers
        - Returned Attributes
            - NetBIOS name
            - IP addresses
            - Resource domain
            - System roles
            - SNMP community name
            - MAC addresses
        - Discovery Levels
            - Topology

            - Discovers routers and subnets, but not subnet masks
        - Topology and Client
            - Also discovers potential clients and resources (ex. computers and printers)
            - Tries to identify the subnet mask of found objects
        - Topology, client, and client operating system
            - Also tries to discover computer OS and version
            - Uses Windows Browser and Windows Networking calls
    - Complex networks and low-bandwidth connections can cause Network Discovery to run slowly and generate significant network traffic
    - Best practice is to run Network Discovery only when the other discovery methods cannot find the resources one must discover
        - Ex. Other methods do not discover workgroup computers
- Server Discovery
    - "*Creates resource records for computers that are site systems, like a computer that is configured as a management point*"
    - Not user configurable
- Common Features of AD Group/System/User Discovery
    - Similar in configuration and operation
    - Discovers computers, users, and information about group membership of resources stored in AD DS
    - Discovery process managed by a discovery agent that runs on the site server at each site where discovery is configured to run
    - Can all be configured to search one or more Active Directory locations as location instances in the local forest or remote forests
    - Individual search options can be configured for each location, like enabling a recursive search of its AD child containers
    - A unique account can be configured to use when it searches a location, providing flexibility in configuring a discovery method at one site to search multiple AD locations across multiple forests, without configuring a single account that has permissions to all locations
    - When the methods run at a specific site, the CM site server at that site contacts the nearest domain controller in the specified AD Forest to locate AD resources
        - The account assigned to each location must have Read access permissions to the specified AD locations
    - Discovery searches the specified location for objects and tries to collect information about those objects, then a DDR is created when sufficient information about a resource can be identified
        - Required information varies depending on the discovery method being used
    - The same discovery method can be configured to run at different CM sites to take advantage of querying local AD servers, allowing the operator to configure each site with a unique set of discovery options
    - Discovery data is shared with each site in the hierarchy, so it is best to avoid overlap between configurations to discover each resource a single time

- Discovery Data Recors (DDR)

    - *"When a discovery method successfully finds information about a resource, it puts that information into a file called a Discovery Data Record (DDR)"*
        - The file is then processed by a primary site or CAS
        - Processing a DDR creates a new record in the site database for newly discovered resources or updates existing records
    - Some discovery methods can generate a large volume of network traffic, and processing DDRs can produce can result in a significant use of CPU resources

- DDR Replication - Site Hierarchy
    - DDRs are files created by a discovery method, containing information about a resource that can be managed by CM, including computers, users, and occasionally network infrastructure
        - They are processed at a primary site or CAS
        - After the processed information is entered into the database, the DDR is deleted and the information replicates as global data to all sites inhe hierarchy
        - Information is shared regardless of where the data was processed, which can save network bandwidth by allowing a discovery method to run at only a single site, reducing duplicate discovery
    - The site at which a DDR is processed depends on the information it contains
        - Newly discovered resources are processed at the top-level site, which creates a new resource record and assignes it a unique identifier
            - DDRs transfer by file-based replication until they reach the top-level site
        - Previously discovered objects are processed at primary sites
            - Child primary sites do not transfer DDRs to the CAS when the DDR contains information the CAS already has
        - Secondary sites do not process DDRs, and always transfer them by file-based replication to their parent primary site
    - DDR files use the .ddr extension and have a file size of about 1KB

L13 - MECM Querying

- Goals
    - Descibe function of a query within MECM

- Query Functions
    - Queries can be created and run to locate objects in a Configuration Manager Hierarchy that match query criteria
    - Can return most types of CM objects, including sites, collections, applications, and inventory data
    - Must specify 2 parameters minimum: where to search, what to search for
        - When a VMO creates an initial query, they can specify additional query criteria; ex.
            - Can specify that query results include only computers that are assigned to a specified site
            - Change how results are displayed so VMO can view the results in an order that's meaningful to VMO

        - Specify that the results are sorted by the amount of free hard drive space, in ascending/descending order

---

L14 - MECM Querying

- Goals
    - Discuss WMI Query Language (WQL) regarding MECM queries
    - Discuss importing a query into MECM

- WMI Query Language (WQL)
    - A subset of the American National Standards Institute Structured Query Language (ANSI SQL) with minor semantic changes to support WMI

- Query Configuration
    - A query must specify at least 2 parameters: where to search, and what to search for (FROM, SELECT)
    - Queries can specify additional criteria that filter results to include only objects meeting specific parameters (WHERE)
    - Queries are stored by CM and are displayed in the Queries node in the Monitoring workspace

---

L15 - MECM Reporting

- Goals
    - Differentiate SQL Server Reporting Services (SSRS) and Power BI (Business Intelligence)
    - Describe SSRS regarding MECM Reporting
    - Describe Power BI Reporting Server

- SQL Server Reporting Services (SSRS) vs Power BI (Business Intelligence)
    - The reporting services point can be integrated with either SSRS or Power BI Report Server
        - One of them must be installed on a site before installing the reporting services point
        - CM uses SSRS as its primary reporting solution
    - Power BI Report features are a superset of SSRS; it can do everything SSRS can, adding support for Power BI reports

- SQL Server Reporting Services (SSRS)
    - "*Server-based reporting platform that provides comprehensive reporting functionality for different kinds of data sources*"
    - SSRS provides ready-to-use tools to create, deploy, and manage reports
    - Programming features to extend and customize reporting functionality
    - Advantages
        - Industry standard reporting system to query the CM database

        - Displays reports using CM Report Viewer or Report Manager, a web-based connection to the report
        - Provides high performance, availability, and scalability
        - Provides subscriptions to reports
        - Exports reports in multiple formats (refer to ACAS formats)

- Power BI (Business Intelligence) Report Server
    - On-premises report server with a web portal to display and manage reports and key performance indicators, including tools to create reports
        - User can access the reports via web brower, mobile, or email

---

L16 - MECM Report Distribution

- Goals
    - Recall reporting services points within MECM reporting
    - Discuss scope of reports
    - Discuss the list of reports
    - Discuss how report prompts and parameters impact report data in SSRS
    - Discuss usage of report links to relate data sets in SSRS
    - Duscuss usage of report subscriptions to automate report delivery in SSRS

- Reporting Services Points
    - *"The reporting services point is a site system role that you add on a server that runs Microsoft SQL Server Reporting Services"*
    - Functions
        - Copies CM report definitions to Reporting Services
        - Creates report folders based on report categories
        - Sets security policy on the report folders and reports
            - Policies are based on role-based permissions for CM admins
            - In a 10-minute interval, the reporting services point connects to Reporting Services to reapply the security policy if it's been changed

- Scope of Reports
    - Admins can only run and modify reports for which they have the appropriate security rights
    - When selecting a site to install the reporting services point, users who will access the reports must be in the same security scope as the site where the role is installed
    - When installing a reporting services point, specify a Reporting services point account; for users from a different domain to run a report, create a two-way trust between domains, otherwise the report will fail to run

- List of Reports
    - CM provides report definitions for over 400 reports in over 50 report folders
    - Reports don't propagate up or down the CM hierarchy; they only run against the database of the site in which they're created

    - When a report retrieves data from a site database, it has access to site data for the current site and its children, and global data for every site in the hierarchy
    - Admins must have the appropriate permissions to run or modify reports
        - Run Report and Modify Report permissions
    - 2 types of reports
        - Model-based report; interactively select items to include
        - SQL-based report; retrieve data based on a report SQL statement

- Report Prompts and Parameters
    - A report prompt or parameter can be configured when a report is created or modified
    - Create report promps to limit or target data
        - A report can contain multiple prompts
        - Prompt names must be unique and contain only alphanumeric characters that conform to the SQL Server rules for identifiers
    - When a report is run, the prompt requests a value for a required parameter
        - Based on the parameter value, it retrieves the report data

- Usage of Report Links
    - Report links in CM are used in a source report to provide easy access to other data
        - ex. link to more detailed information to each item in the report
    - If the destination report requires 1 or more prompts to run, the source report must contain a column with the appropriate values for each prompt
    - The link needs to specify the column number with the calue for the prompt
    - If a destination report is moved to a different report folder, the location for the destination report changes
        - CM doesn't automatically update the report link in the source report with the new location, and links to the destination report will stop working

- Report Subscriptions
    - *"A report subscription in SSRS is a recurring request to deliver a report at a specific time or in response to an event."*
        - Subscriptions provide an alternative to running a report on demand, which requries that a viewer actively selects the report each time they want to view it
    - Subscriptions are specified in an application file format
    - Report subscriptions can be managed in the CM console
    - Subscriptions are processed by the report server, distributing them using delivery extensions deployed on the server
    - By default, subscriptions can send reports to a shared folder or to an email address

---

L18 - Monitoring MECM

- Goals
    - Differentiate client status information types provided by the MECM console
    - Discuss customization options for the Client Health Dashboard
    - Differentiate the checks and remediation run by the MECM client health check

- Client Status Information Types
  - Types
    - Client Online Status
      - Device considered online if it's connected to its assigned management point
      - Indicated by the client with ping-like messages sent to the management point
        - If client doesn't ping for 5 minutes, the site considers it offline
    - Client Activity
      - Device considered active if it's communicated with CM in the past 7 days
      - Considered inactive if it hasn't done the following actions for 7 days
        - Requested policy update
        - Sent a heartbeat message
        - Sent hardware inventory
    - Client Check
      - State of the periodic evaluation that the CM client runs on the device
      - Evaluation checks the device and can remediate some of the problems it finds
      - On Windows 7, client checks run as a scheduled task; newer OS versions run checks automatically during the Windows maintenance window
  - Remediation can be configured not to run on specific devices, like a business-critical server
  - CM compliance settings can be used to monitor additional configurations
  - Record Statuses
    - Decommissioned
      - Site has marked device record for deletion
      - Happens when a new registration for the same device assigns to the same or a different primary site in a hierarchy
      - Site deletes decommissioned devices the next time it runs the site maintenance task Delete Aged Discovery Data
    - Obsolete
      - Site has discovered a new device record with the same hardware ID, so it marks the old record as obsolete
      - Reports don't count obsolete records of the same device multiple times
      - Policies can still target obsolete devices
      - If a site doesn't get a heartbeat for an obsolete record after 90 days of inactivity, it removes the obsolete device when it runs the site maintenance task Delete Aged Discovery Data

- Client Health Dashboard
  - Data Display Filters
    - "*Client health for clients in the following collections*"
      - Defaults to All Systems
    - "*Client activity in last number of days*"
      - Defaults to 3
    - "*Include client health for offline clients*"
      - Defaults to only online clients
      - Client notification channel updates online status every 5 minutes

        - *"Only show un-healthy client details"*
            - Only view devices reporting client health failure
    - Healthy CM client properties
        - Online
        - Actively sending data
        - Passes all client health evaluation checks
    - Core Health Scenarios
        - Client policy
        - Heatbeat discovery
        - Hardware inventory
        - Software inventory
        - Status messages
        - Combined (All)
            - Combination of all scenarios (AND)
        - Combined (Any)
            - At least one of the scenarios (OR)

- Checks and Remediation Run
    - Client check runs a series of checks with remediation actions
    - There are a variety of remidation actions, and some checks don't feature automatic remediation
        - Remediation actions involve starting or resetting services

---

L20 - MECM Compliance

- Goals
    - Discuss compliance configuration for devices managed with and without the MECM client
    - Define configuration item regarding compliance management
    - Define configuration baseline regarding compliance management

- Compliance Configuration
    - Compliance settings manage the configuration and compliance of clients in an organization
    - Configuration Items fall into 2 main categories
        - Settings for devices managed wtih the CM client
        - Settings for devices managed without the CM client
            - Typically devices managed with Microsoft Intune, or CM on-premises device management

- Configuration Items
    - *"A configuration item is a container that stores specific information"*
    - Information configured depends on the configuration item type
    - Configuration item information
        - Detection method information
            - Only for Windows configuration items that contain application settings

            - Detects whether an application is installed using the Windows installer file for the application or a custom script
        - Settings
            - Represents the business or technical conditions to assess compliance on cleint devices
            - Configure new settings or brows existing settings on a reference computer
        - Compiance rules
            - Specify the conditions that define the compliance of a configuration item setting
            - Before the client evaluates a setting for compliance, it must have at least one compliance rule
            - Some settings remediate noncomplient values
        - Supported Platforms
            - Device platforms on which the client evaluates compliance of the configuration item
            - Configuration items can be deployed to platforms they don't support, but the client won't perform the evaluation for them

- Configuration Baseline - Compliance Management
    - "*Client devices evaluate their compliance against each deployed configuration baseline and immediately report the results to the site by using state messages and status messages*"
        - If a device is disconnected from the network, but downloaded the configuration baseline, it still evaluates compliance of the configuration items and sends the compliance information when it reconnects
    - Configuration baselines include 1 or more configuration items
        - Essentially, a baseline is a rule book, and items are rules
    - Configuration baselines are deployed to user and device collections for client self-evaulation, run on a schedule
        - Multiple baselines can be deployed to a single device

---

L21 - Non-Client Deployment Overview within MECM

- Goals
    - Recall functions of distribution points within MECM
    - Recall Software Center integration with MECM
    - Discuss basics of content deployment
    - Discuss basics of application deployment
    - Discuss basics of software update deployment

- Distribution Points
    - "*Distribution point groups provide a logical grouping of distribution points for content distribution*"
    - Used to to manaage and monitor content from a central location for distribution points that span multiple sites
    - Distribution point groups are collections of distribution points

    - Considerations
        - Add 1 or more distribution points from any site in the hierarchy to a distribution point group
        - Add a distribution point to more than one distribution point group
        - CM distributes content to all distribution points that are a member of the group
        - When adding a new distribution point to a group after an inititial content distribution, CM automatically distributes the content to the new member
        - Associate a collection with a distribution point group
            - When distributing content to that collection, CM determines which groups are associated with the collection

- Software Center - MECM
    - Used to request and install software VMO deploys
    - Installed when the CM client is installed
    - Software Center User Actions
        - Browse for and install applications, software updates, and OS updates
        - View software request history
        - View device compliance against organization policies
    - Features custom tabs to meet additional business requirements

- Content Deployment
    - After installing distribution points for CM, content can be deployed to them
    - Typlically, content transfers to distributin points across the network
    - After content transfers to a distribution, it can be updated, redistributed, removed, and validated

- Application Deployment
    - Application and Deployment Type
        - In CM, an application is a "box" that contains 1 or more sets of installation for a software package (known as deployment types), and instructions on how to deploy the software
        - An application requires at least one deployment type, which determines how to install an app (don't send an empty box)
        - Use more than one deployment type to configrue different content and installation for the same application
    - Requirements
        - In previous versions of CM, applications would be deployed to a device collection
            - Use requirements to specify more detailed criteria for an application deployment
        - CM evaluates requirements to determine whether it installs an application and any of its deployment types, then determines the correct deployment type to use
        - Every 7 days by default, the CM client reevaluates requirement rules to determine compliance
    - Global Conditions
        - A library of predefined requirements used with any application and deployment type
        - CM includes a set of built-in global conditions and custome ones can be created

    - Simulated Deployment
        - Evaluates the requirements, detection method, and dependencies for an application; results reported by the client without installing the application
    - Supersedence
        - CM lets VMO upgrade or replace existing applications user a superscedence relationship
        - Supercedence specifies a new deployment type to replace the old type of the superseded application
        - Superseded application can be uninstalled or upgrade

- Software Update Deployment
    - Steps of Synchronization at a Top-Level Site
        1. Software update synchronization starts
        2. WSUS Synchronization Manager requests the WSUS instance on the default SUP to start synchronization with its source
        3. Software update metadata is synched from the source; changes updated in the WSUS database
        4. When finished, WSUS Synchronization Manager synchs the metadata from the WSUS database to the CM database, stored in the database as a configuration item
        5. Configuration items sent to any existing child sites via database replication
        6. Upon successful snychronization, WSUS Synch manager creates a status message (6702)
        7. WSUS Synch Manager sends a synch request to any existing child sites
        8. WSUS Synch Manager sents requests one at a time to the WSUS instance running on each SUP at the top-level site
    - Steps of Synchronization at Child Sites
        1. The WSUS Synch Manager recieves a synch request from its parent site
        2. Requests the WSUS instance running on the default SUP to start synch
        3. Requests the WSUS instance running on the default SUP to start synch
        4. The WSUS instance on the SUP of the child site synchs software update metadata from the WSUS instance on the parent site
        5. Upon successful snychronization, WSUS Synch manager creates a status message (6702)
        6. WSUS Synch Manager sends a synch request to any existing child sites
        7. WSUS Synch Manager sents requests one at a time to the WSUS instance running on each SUP at the top-level site
    - Software Update Compliance Assessment
        - Before deploying updates to clients in CM, scan for software update compliance
        - For each software update, a state message is created that contains the compliance state for the update
        - State messages sent in bulk to the management point and site server, compliance state inserted into site database, displays in CM Console
    - Compliance States
        - Required
            - Update is applicable and required on the client computer
            - Conditions
                - Update was not deployed to client

            - Update installed on client, but most recent state message wasn't insterted into site server database
            - Update installs but requires a restart
            - Update was deployed but not yet installed
        - Not Required
            - Update is not applicable
        - Installed
            - Update installed
        - Unknown
            - No state message recieved from client
                - The client didn't successfully scan for software update compliance
                - Scan finished successfully, but state message hasn't been processed on the site server
                - Scan finished successfully, but state message hasn't been recieved from child site
                - Scan finished successfully, but state message was corrupted and couldn't be processed

---

L22 - MECM Content Management: Application / Package

- Goals
    - Discuss basics of distribution for content deployment within MECM
    - Differentiate content types managed in the Software Library workspace within the MECM console
    - Describe the function of pre-staged content for application management
    - Discuss considerations for distributing pre-staged content
    - Differentiate options for managing content that has been transferred to a MECM distribution point
    - Recall function of maintenance windows within MECM

- Distribution for Content Deployment
    - Once uploaded, patch packages are available to the entire AFIN
    - Locally created patches must be thoroughly tested and recieve approval through the Change Management process
    - Typically, VMO distributes content to distribution points so that it's available to clients
        - Exception is when VMO use on-demand content distribution
    - When distributing content, CM stores content files in a package, then distributes it to the distribution point
        - Package content pulled from the site server's content library
    - When a package contains source files, the site it's created on becomes the site owner for the content source
        - CM copies the source files from the path specified for the object to the content lobrary on the site server that owns it, then CM replicates it to additional sites

- Software Library

    - CM Software Library Workspace Objects / Content Types
        - Applications
        - Packages
        - Software Update Deployment Packages
        - Driver Packages
        - OS Images
        - OS Upgrade Packages
        - Boot Images
        - Task Sequence
            - Doesn't contain content; has associated content references

- Application Management Pre-staged Content
    - A compressed file that contains the content files and associated metadata for a content type
    - Can be manually imported to another site server, secondary site, or distribution point
        - When importing pre-staged content files on a site server, the content files are added to its content library, then registers the content in the site server database
        - When importing pre-staged content files on a distribution point, the content files are added to its content library, then it sends a status message to the site server

- Distributing Pre-staged Content
    - Limitations and Considerations
        - When the distribution point is located on the site server, don't enable the distribution point for pre-staged content
        - When the distribution point is configured as a pull-distribution point, don't enable it for pre-staged content; this will override the pull-distribution point configuration
        - Before pre-staging content to the distribution point, create the content library on the server and distribute content over the network at least once to prepare the content library
        - When pre-staging content for objects with a long package source path (>140 characters), the Extract Content command-line tool might fail

- Managing Content Options - Distribution Point
    - Options for managing content
        - Update content
            - Update content files on distribution points
            - Site copies content from original package source location to the content library on the site that owns the content source
        - Update content on schedule
        - Redistribute Content
        - Remove content
            - When content is associated with another package distributed to the same distribution point, it can't be removed
        - Validate content
            - Verifies integrity of content files on distribution points

- Maintenance Windows
    - Used to define when CM can run impacting tasks on devices

    - Helps make sure that client configuration changes occur during times that don't affect productivity
    - Users can see the device's next maintenance windows on Software Center

---

L24 - MECM Application Management

- Goals
    - Discuss application types that can be deployed utilizing MECM
    - Discuss deployment settings regarding application management

- Application Types Deployment
    - CM Application Types
        - Windows Installer
            - (msi)
        - Windows App Package and App Bundles
            - (appx, appxbundle, msix, msixbundle)
        - Windows App Package in the Microsoft Store
        - Script installer for third-party installers and script wrappers
        - Microsoft App-V v4 and v5
        - macOS
        - A non-OS deployment task sequence for complex apps
    - App types managed by non-client device management via on-premises device management
        - Windows Phone app package (xap)
        - Windows Phone app package in the Microsoft Store
        - Windows Installer through MDM (msi)
        - Web application

- Deployment Settings - Application Management
    - Create or simulate a deployment of an application to a device or user collection in CM; this deployment gives instructions to the CM client on how and when to install or uninstall the software
    - Before deploying an application, create at least one deployment type for it
    - Alternatate Features to Consider
        - If several applications need to deploy together, instead of creating multiple deployments, create an application group, which can be sent to a user or device collection as a single deployment
        - For more complex deployments, first test it with a simulated deployment, which tests teh applicability of a deployment without installing or uninstalling the application
            - A simulated deployment evaluates the detection method, requirements, and dependencies for a deployment type and reports the results in the Deployments node of the CM Monitoring workspace
            - Can only simulate the deployment of required applications, not packages or software updates

        - On-premises MDM-enrolled devices don't support simulated deployments, user experience, or scheduling settings
    - Phased deployments allow one to orchestrate a coordinated, sequenced rollout of software based on customizable criteria and groups

---

L25 - MECM Software Update Management Process

- Goals
    - Summarize impact of binary differential replication (BDR) on software update deployment packages within MECM

- Binary Differential Replication (BDR)
    - CM uses BDR to update content that was previously distributed to other sites or remote distribution points
    - BDR minimizes the network bandwidth used to send updates for distributed content
        - Resends only new or changed content instead of the entire set of content source files
        - To support BDR's reduction of bandwidth usage, install the Remote Differential Compression feature on distribution points
    - When BDR is used, CM identifies changes to source files for each set of content previously distributed
        - When files in the source content change, the site creates a new incremental version of the content and replicates only the changed files to destination sites and distribution points
            - A file is considered changed if it's been renamed or moved, or if the content changes
        - CM supports up to 5 incremental versions of a content set before it resends the entire content set; the next change causes the site to create a new version of the content set, which is distributed to replace the previous set and its incremental versions
    - BDR is supported between each parent and child site in a hierarchy, and within a site between its server and its regular distribution points
    - BDR is not supported on pull-distribution points and content-enabled cloud management gateways
        - Pull-distribution points support file-level deltas and transfering new files, but not blocks within a file
    - Applications always use binary differential replication
    - BDR is optional for packages and not enabled by default
        - Configured when creating or editing a package
        - Always enabled for applications
    - Summary of BDR
        - CM's term for Windows Remote Differential Compression
        - Block-level differences
        - Always enabled for apps
        - Optional on legacy packages

        - If a file already exists on the distribution point, and there's a achange, the site uses BDR to replicated block-level change instead of the entire file; this behavior only applies when object uses BDR
    - Summary of Delta Replication
        - File-level differences
        - On by default, not configurable
        - When a package changes, the site checks for changes to individual files instead of the entire package
        - If a file changes, uses BDR to do the work
        - If there's a new file, copy the new file

- New Software Update Deployment
    - "*A software update deployment package is the vehicle used to download software updates to a network shared folder, and copy the software update source files to the content library on site servers and on distribution points that are defined in the deployment*"
    - The SMS Provider computer account and the admin who downloads the software updates both require write permissions to the package source
        - Restricting access to package source reduces risk of an attacker tampering with software update source files
    - When a deployment package is created, the content version is 1, and when the software update files are downloaded using the package, the content version increments to 2, so all new deployment packages start with a content version of 2
        - When the content of a deployment package changes the content version increments by 1
    - Clients install softtware updates in a deployment by using any distribution point that has the software updates available, regardless of the deployment package
        - Even if a package is deleted, clients can still install software updates in the deployment as long as each update was downloaded to another deployment package and is available on a distribution point the client can access
            - When the last deployment that contains a software update is deleted, clients cannot retrieve the software update

- Configure Software Update Deployment
    - After deploying software updates or when an automatic deployment rule runs and deploys updates, a deployment assignment policy is added to the machine policy for the site
    - Software Update Download->Distribution Point Flow
        1. Software updates are downloaded from a download location, the internet, or a network shared folder to the package source
        2. Copied from the package source to the content library on the site server
        3. Copied to the content library on the distribution point
    - When a client computer computer in the target collection for the deployment recieves the machine policy
        1. Software Update Client Agent starts an evaluation scan
        2. The client downloads the content for required software updates from a distribution point to the local client cache at the Software Available time set for the deployment
        3. The software updates are then available to install

        - Software updates in optional deployments (deployments without a deadline) are not downloaded until a user manually installs

---

L26 - MECM Self-Diagnosis

- Goals
    - Describe Configuration Manager Health Evaluation within MECM
    - Explain Management Point communication within MECM
    - Explain CMTrace functionality regarding MECM logs
    - Describe function of MECM logs
    - Describe CcmEval.exe Components within MECM
    - Explain usage of Reports for self-diagnostics

- Configuration Manager Health Evaluation
    - "*The task for Configuration Manager Health Evaluation is ccmeval.exe; it can be used in addition to the Client Health Dashboard to assist in evaluating and remediating client health*"
    - ccmeval performs multiple client health checks, and can verify key areas
        - If needed, it will remediate issues, repaire WMI, or reinstall the client
        - Set to run daily for each client

- Management Point Communication
    - "*Proper communication between the client and the management point must take place for the client to receive policy for Applications, updates for the Windows OS as well existing Microsoft and 3rd Party Software*"

- CMTrace
    - A CM tool that allows the user to view and monitor log files
    - Helps to analyze log files by highlighting, filtering, and providing error lookup
    - Log File types
        - Log files in CM or Client Component Manger (CCM) format
        - Plain ASCII or Unicode text files, suck as Windows Installer logs

- MECM Logs
    - "*In Configuration Manager, client and site server components record process information in individual log files*"

- Usage of Reports
    - "*Reports help you gather, organize, and present information about users, hardware and software inventory, software updates, applications, site status, and other Configuration Manager operations in your organization*"
    - Reports in CM are stored in SSRS
    - Reports can be accesed in the Monitoring Tab of the CM console or by using Report Manager