ADMINISTRATION OF OPERATING SYSTEMS

Windows Server installation and administration

Lesson 1: Overview of Windows Server administration principles and tools

Overview of Windows Admin Center (1 of 2)

- Windows Admin Center consolidates multiple admin tools into a single console that can be easily deployed and accessed through a web interface
- Windows Admin Center is a modular web application comprised of the following four modules:
  - Server manager
  - Failover clusters
  - Hyper-converged clusters
  - Windows 10 clients
- Windows Admin Center has two main components:
  - Gateway
  - Web server

Overview of Windows Admin Center (2 of 2)

- Windows Admin Center offers the following benefits:
  - Familiar functionality
  - Easy to install and use
  - Complements existing solutions
  - Manageable from the internet
  - Enhanced security
  - Azure integration
  - Extensibility
  - No external dependencies

Demonstration: Use Windows Admin Center

- Install Windows Admin Center
- Add servers for remote administration
- Browse through the various admin sections

Server Manager

- **Server Manager** allows server administrators to:
  - Manage the local server and remotely manage multiple servers
  - Configure the local server
  - Get basic information about installed hardware
  - Query event logs
  - Monitor status of services
  - Perform best practice analysis
  - Check performance monitors
- **Server Manager** initially opens to the dashboard, which provides quick access to:
  - Add roles and features
  - Add other servers to manage
  - Create a server group
  - Connect this server to cloud services

Remote Server Administration Tools

- To enable IT administrators to remotely manage roles and features in Windows Server from a computer that is running Windows 10 or Windows 8.1, use **RSAT**
- **RSAT** include:
  - Active Directory Domain Services tools
  - DHCP server tools
  - DNS server tools
  - Failover clustering tools
  - File services tools
  - Group Policy management tools
  - Windows Server Update Services tools

Windows PowerShell (1 of 2)

- Windows PowerShell is a command line shell and scripting language that allows task automation and configuration management
- Windows PowerShell cmdlets execute at a Windows PowerShell command prompt or combine into Windows PowerShell scripts
- Cmdlets:
  - Are small commands that perform specific functions
  - Can be combined to perform multiple tasks
  - Can be piped together to perform multiple operations
- Modules:
  - Cmdlets specific to a product are packaged together and installed as modules
  - Some are installed with the product and some need to be added manually

Windows PowerShell (2 of 2)

- PowerShell Integrated Scripting Environment is a graphical user interface–based tool that allows you to:
  - Run commands and create, modify, debug, and test scripts
  - Test the script while in development
- Windows PowerShell remote management:
  - Allows Windows PowerShell to remotely run cmdlets on other Windows systems
  - Depends on the Windows Remote Management service running on the target systems
- PowerShell Direct:
  - Enables you to run a Windows PowerShell cmdlet or script inside a virtual machine from the host operating system

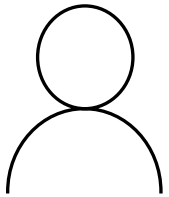
Demonstration: Manage servers remotely

- Enable PowerShell remote on the Server Core machine and use PowerShell remote to restart a service

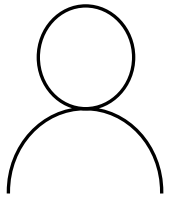
Overview of the least-privilege administration concept

- Most security breaches or data loss incidents are the result of human error, malicious activity, or a combination of both. Least privilege is the concept of restricting access rights for users, service accounts, and computing processes to only those resources absolutely required to perform their job roles.

The principle states that all users should log on with a user account that has the absolute minimum permissions necessary to complete the current task and nothing more. Doing so provides protection against malicious code, among other attacks. This principle applies to computers and the users of those computers.



Day to day standard user account for IT admins



Full admin account only used to perform administration functions

Delegated privileges

- Accounts that are members of high-privilege groups such as **Enterprise Admins** and **Domain Admins** need to be guarded, but occasionally non-admins need rights to perform certain functions, such as resetting passwords or modifying group memberships.
- Built-in groups with pre-defined admin rights exist to allow users to perform specific admin tasks. If those groups do not suit your needs, you can delegate more granular permissions by using the **Delegation of Control Wizard**.
  - The wizard has pre-defined tasks that can be assigned to users or groups, or custom permissions can be assigned.

Demonstration: Delegate privileges

- Create a group for sales managers and add a user
- Use the **Delegation of Control Wizard** to allow the sales managers group to reset passwords for users in the sales organizational unit
- Test the delegation

Privileged Access Workstations

- A PAW is a computer that is used for performing only administration tasks
  - Protected from the Internet and locked down so that only the required administration apps can run
- Microsoft recommends using Windows 10 Enterprise in one of these profiles:
  - Dedicated hardware
  - Simultaneous use

Credential guard	Device guard
• Secure Boot • Virtual Secure Mode • Isolated LSA (LSAIso)	• Secure Boot • Configurable CI • Virtual Secure Mode • HVCI & Protected KMCI

Jump servers

- A jump server is a hardened server used to access and manage devices in a different security zone, such as between an internal network and a perimeter network
- A jump server would typically be accessed by a PAW to ensure secure access
- This server will run on dedicated hardware that supports both hardware and software-based security features such as:
  - **Credential Guard** to encrypt the domain credentials in memory
  - **Remote Credential Guard** to prevent remote credentials from being sent to the jump server, instead using Kerberos protocol version 5 single sign-on tickets
  - **Device Guard**: HVCI to leverage Virtualization-based security to enforce kernel mode components to comply with the code integrity policy
  - **Device Guard**: Config code integrity to allow admins to create a custom code integrity policy, and specify trusted software

Lesson 2: Introducing Windows Server 2022

Windows Server 2022 editions

- Windows Server 2022 is released in four editions:
  - Windows Server 2022 **Essential**
  - Windows Server 2022 **Standard**
  - Windows Server 2022 **Datacenter**
  - Windows Server Core

Windows Server 2022 Edition	Ideal for	Licensing model	CAL requirements[1]	Suggested Retail Price (MSRP)[4]
Datacenter[2]	Highly virtualized datacenters and cloud environments	Core-based	Windows Server CAL	$6,155
Standard[2]	Physical or minimally virtualized environments	Core-based	Windows Server CAL	$1069
Essentials	Small businesses with up to 25 users and 50 devices	Specialty servers (server license)[3]	No CAL required	$501

- [1] CALs are required for every user or device accessing a server. See the Product Use Rights for details.
- [2] Datacenter and Standard edition pricing is for 16 core licenses.
- [3] Up to 10 cores and 1 VM on single-socket servers. Windows Server Essentials is available through our OEM Server Hardware partners.
- [4] Pricing is shown in USD and may vary from country to country. Please contact your Microsoft representative for a quote.

Hardware requirements for Windows Server 2022

- Hardware requirements will vary depending on:
  - Job role
  - Workload

Minimum hardware requirements for Windows Server 2022:

Component	Requirement
Processor architecture	64 bit
Processor speed	1.4 gigahertz (GHz)
RAM	512 MB
Hard drive space	32 GB

Overview of deployment options (1 of 2)

- Traditionally, new server versions always offered clean install. Windows Server 2022 also provides the option for an in-place upgrade.
  - Clean install:
    - Boot the machine or VM from the Windows Server 2022 media
    - Choose the installation language, time and currency formats, and keyboard layout
    - Choose the architecture (either Standard or Datacenter) with or without Desktop Experience
    - Accept the license
    - Choose custom installation
    - Choose the volume that will host the installation

Overview of deployment options (2 of 2)

- In-place upgrade
  - Insert the disk or mount the ISO of Windows Server 2022 media and then run **Setup.exe**
  - Respond to the prompt to download updates, drivers, and optional features
  - Choose the architecture (either **Standard** or **Datacenter**) with or without **Desktop Experience**
  - Accept the license
  - Choose what to keep: personal files and apps, or nothing

Deployment accelerators (1 of 2)

- Microsoft provides free solution accelerators that provide guidance and content to help you design and plan your Windows Server deployment. Solution accelerator scenarios focus on security and compliance, management and infrastructure, and communication and collaboration.
  - MDT:
    - Lightweight tool for automated server and desktop deployments
    - Deploys standardized images
    - Automates the deployment process by configuring unattended setup files
    - Complements Windows Deployment Services and System Center Configuration Manager

Deployment accelerators (2 of 2)

- Microsoft Assessment and Planning Toolkit
  - Analyzes the inventory of an organization
  - Assists in Hyper-V server planning
  - Assesses the environment for Microsoft 365 and Office 2022
  - Creates reports to use for upgrade and migration plans

Servicing channels for Windows Server

- You can use servicing channels to choose whether new features and functionality will be delivered regularly during a server's production lifespan, or when to move to a new server version
  - There are two release channels:
    - Long-Term Servicing Channel
      - A major version of Windows Server will be released every two or three years
      - Normal security updates and Windows updates will be delivered on a regular basis
    - Semi-Annual Channel
      - New features will be delivered semi-annually, in the spring and the fall
      - Normal security updates and Windows updates will be delivered on a regular basis
      - Semi-annual releases can be identified by their version number, which is a combination of the year and month that the features were released

Licensing and activation models for Windows Server (1 of 2)

- Licensing for Windows Server **Standard** and **Datacenter** is based on the number of cores, not processors
  - Each Windows Server has the following minimum license requirement:
    - All physical cores must be licensed
    - There must be 8 core licenses per processor
    - There must be 16 core licenses per server
  - Client access licenses are required for each user or device that connects to the server for any purpose

Licensing and activation models for Windows Server (2 of 2)

- To ensure that your organization has the proper licenses, and to receive notices for product updates, you must activate every copy of Windows Server that you install
- Windows Server activation methods:
  - Manual activation requires a product key
  - Automatic activation options:
    - Key Management Services
    - Volume Activation Services server role
    - Active Directory-based activation
    - Volume Activation Management Tool
    - Multiple Activation Key
    - Automatic virtual machine activation

What's new in Windows Server 2019? (1 of 2)

- Windows Server 2019 is designed to easily link your on-premises infrastructure with Microsoft Azure. The new features it offers include the following:

Feature	Description
Windows Admin Center	Manages Windows servers, clusters, hyper-converged infrastructure, as well as Windows 10 PCs
Deduplication for ReFS volumes	Windows Server 2019 fully supports deduplication of the ReFS file system
Cluster Sets	Allow you to create large scale-out clusters

What's new in Windows Server 2019? (2 of 2)

Feature	Description
Windows Defender Advanced Threat Protection and **Windows Defender Exploit Guard**	A new set of host intrusion prevention such as attack detection and zero-day exploits (previously only available for Windows 10 platforms)
Server Core App Compatibility	An optional feature that improves app compatibility of the Windows Server Core by including a subset of binaries and packages from Windows Server with Desktop Experience
Shielded VMs for Linux	Protects Linux VMs from attacks and rogue administrators

What’s new in Windows Server 2022? (1 of 3)

- Security
  - Secured-core server
  - Hardware root-of-trust
  - Firmware protection
  - UEFI secure boot
  - Virtualization-based security (VBS)

What’s new in Windows Server 2022? (2 of 3)

- Secure connectivity
  - HTTPS/TLS1.3 enabled by default
  - Secure DNS (Encrypted DNS name resolution, DNS-over-HTTPS
  - SMB AES-256 encryption
  - SMB East-West SMB encryption controls for cluster communication
  - SMB Direct and RDMA encryption
  - SMB over QUIC

What’s new in Windows Server 2022? (3 of 3)

- Other key features
  - Networking:
    - TCP and UDP performance improvements
    - Hyper-V virtual switch improvements
  - Storage:
    - Storage Migration Service
    - Adjustable storage repair speed
    - Faster repair and sync
    - Storage bus cache with Storage Spaces
    - ReFS file-level snapshots
    - SMB compression

Lesson 3: Overview of Windows Server Core

Server Core vs. Windows Server with Desktop Experience

- The following table lists the major advantages and disadvantages of Server Core

Advantages	Disadvantages
Small footprint that uses fewer server resources and less disk space, as little as 5 GB for a basic installation	You cannot install several applications on Server Core.
Because Server Core installs fewer components, there are fewer software updates. This reduces the number of monthly restarts required and the time required for you to service Server Core.	Several roles and role services are not available.
The small attack surface makes Server Core much less vulnerable to exploits.	You cannot install many vendor lines of business applications on Server Core, but the **App Compatibility** FOD can help to mitigate that in some cases.

Server Core installation and post-installation tasks

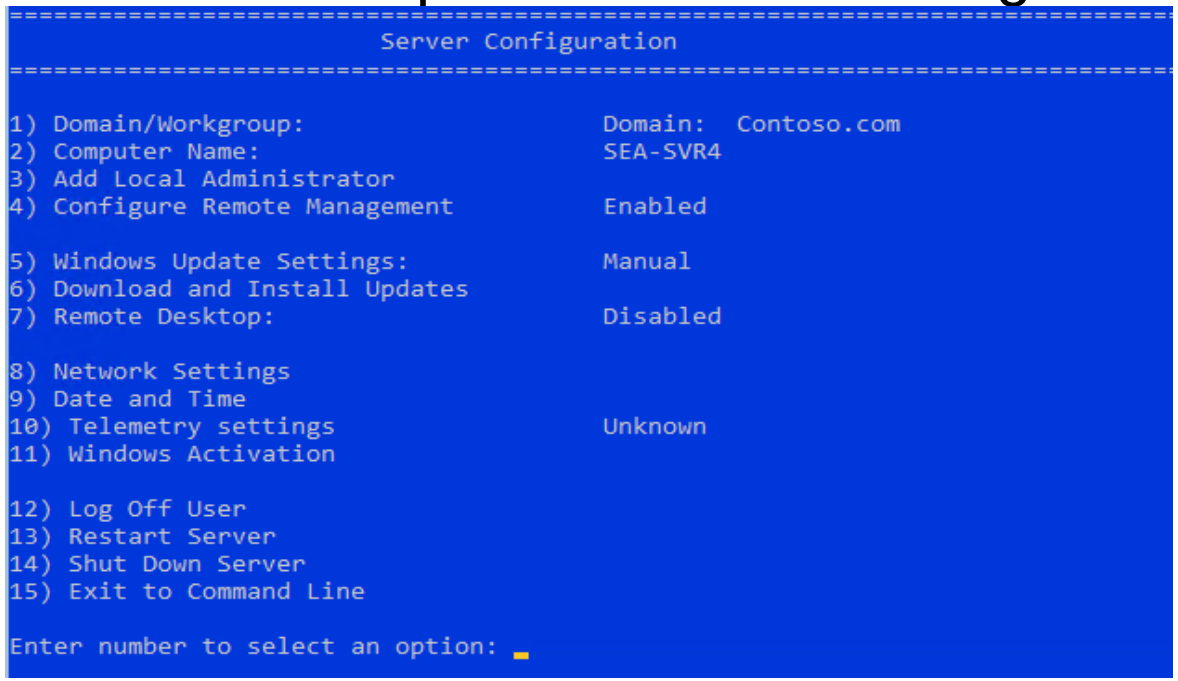
- To install Server Core:
  - Connect to the installation source
  - Choose:
    - Language
    - Time and currency
    - Keyboard
  - Select the operating system to install
- Accept license
  - Choose installation type
    - Upgrade
    - Custom
  - Choose install disk
  - Provide admin password

Install Features on Demand

- Server Core **App Compatibility** FOD installs binaries and packages from the Desktop Experience, making it possible to install applications that might otherwise fail due to missing dependencies
- The FOD can be installed two ways:
  - Directly through Windows Update by using PowerShell
  - By downloading the ISO to a network share and mounting the image

Use the sconfig tool in Server Core

- Sconfig is a text-based utility that allows you configure Server Core to prepare it for use in your production environment
- Sconfig provides 15 different options for initial configuration



Demonstration: Configure Server Core

- Use the sconfig utility to perform basic configuration tasks

References

For more information, refer to the following links:

- Microsoft Assessment and Planning Toolkit
- Windows Server servicing channels: LTSC and SAC
- Roles, Role Services, and Features not in Windows Server - Server Core
- Roles, Role Services, and Features included in Windows Server - Server Core
- Implementing Least-Privilege Administrative Models
- Active Directory Security Groups
- Privileged Access Workstations
- Windows Server servicing channels: LTSC and SAC
- Review and Select Activation Methods

Hvala na pažnji!