Microsoft

AZ-800
Administer Windows Server Hybrid Core Infrastructure

© Copyright Microsoft Corporation. All rights reserved.

$12^{30} - 13^{30}$

$9^{10} - 15^{00}$ Theorie

$15^{15} - 17^{00}$ Labs

Agenda AZ-800

1 Deploy and manage identity infrastructure – Windows Server
2 Deploy and manage identity infrastructure – Hybrid

PIM P2

3 Administering Windows Server Hybrid Core Infrastructure – Windows Server ←
4 Administering Windows Server Hybrid Core Infrastructure – Hybrid

5 Manage virtualization and containers – Windows Server
6 Manage virtualization and containers – Hybrid

7 Implement and manage networking infrastructure – Windows Server
8 Implement and manage networking Infrastructure – Hybrid

9 Configure storage and file services – Windows Server
10 Configure storage and file services – Hybrid

© Copyright Microsoft Corporation. All rights reserved.

Windows Server Hybrid Core Infrastructure
(Windows Server administration)

- Perform Windows Server secure administration
- Windows Server administration tools
- Post-installation configuration of Windows Server
- Just Enough Administration in Windows Server
- Lab 03 – Managing Windows Server

MMC
Server Manager
PowerShell 7
5
Bicep → ARM
WAC
JEA PS Roles

© Copyright Microsoft Corporation. All rights reserved.

Perform Windows Server secure administration

© Copyright Microsoft Corporation. All rights reserved.

Learning Objectives – Windows Server secure administration

- Identify security principals
- Least privilege administrative models
- Implement delegated privilege
- Implement privileged access workstations (PAW)
- Implement jump servers
- Demonstration - Implementing delegated privileges
- Learning recap

© Copyright Microsoft Corporation. All rights reserved.

Define least privilege administration

Server ACLs xcacls

Azure
M365
Entra

RBAC

Owner

Global Admin

Least privilege is the concept of restricting access rights and permissions to only those rights permissions needed to perform a specific task or job role.

You can apply this principle to: *User accounts*, *Service accounts*, *Computing processes*.

TXT

You must then plan a less intrusive principle of least privilege

- Identify security principals.
- Modify group memberships.
- Determine currently assigned rights.
- Implement User Account Control.
- Implement Just Enough Administration.

.... @contoso.com

paul @az.trainig

@.... onmicrosoft.com

CAF 4

© Copyright Microsoft Corporation. All rights reserved.

Security Principals

Sensitive administrative groups:

Group	Description
Enterprise Admins	This global security group resides in the **Users** container of the forest root domain. Members can perform forest-wide administrative changes in Active Directory.
Domain Admins	The Domain Admins group is a member of the local Administrators group on all domain-joined computers by default. Members of the Domain Admins group have administrative rights on all domain-joined computers, allowing them to perform various administrative tasks without restrictions.
Schema Admins	This universal security group resides in the Users folder of the forest root domain. Members can modify the properties of the AD DS schema. Schema changes are infrequent, but very significant in their effect.
Administrators	This domain local security group resides in the Builtin folder in AD DS. The Administrators local group also exists in all computers in your AD DS forest.

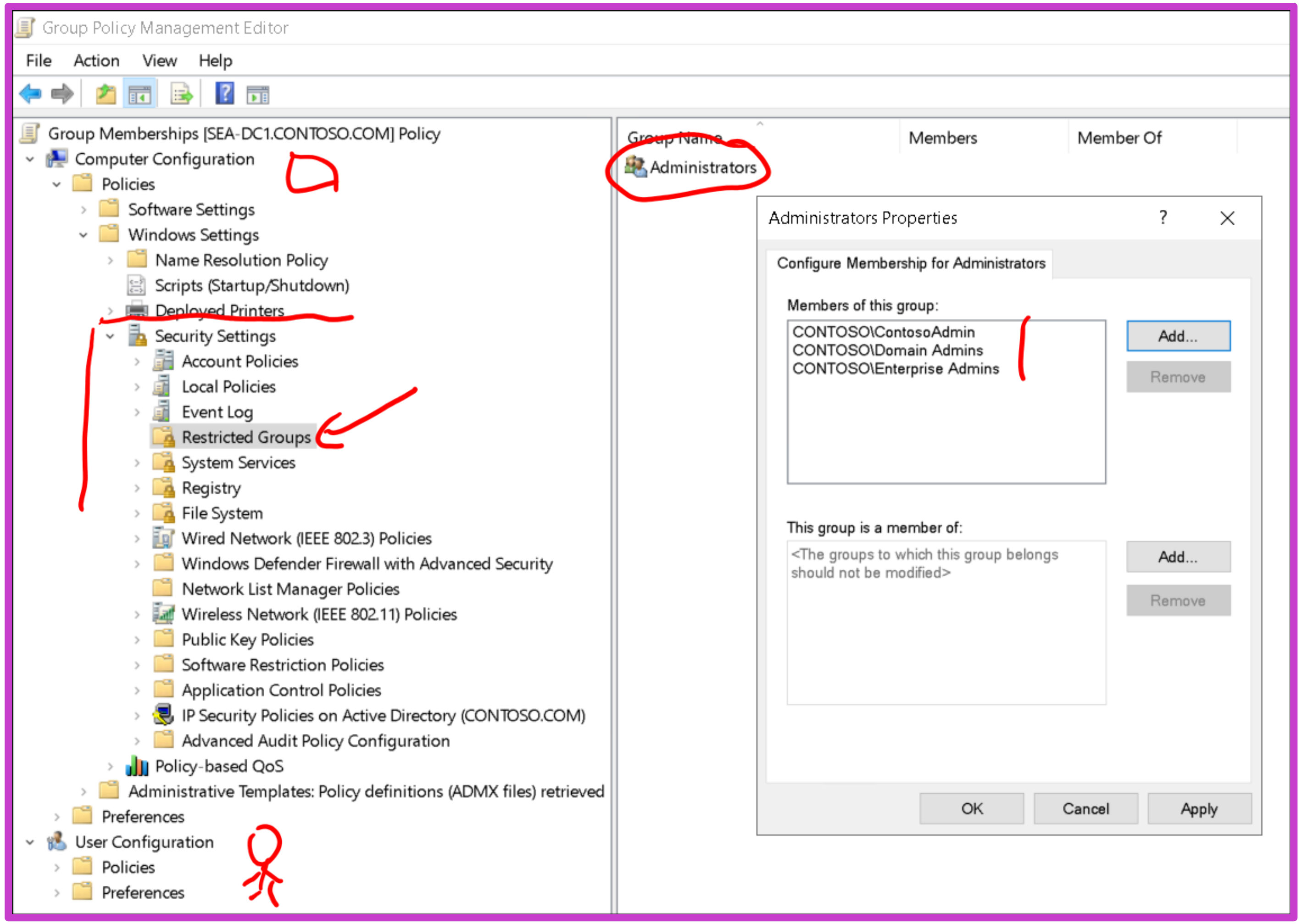
© Copyright Microsoft Corporation. All rights reserved.

Modify group memberships

How to modify group memberships?

Use the Restricted Groups feature:

- Open **Group Policy Management and** then create and link a GPO to the domain object.
- Open the **GPO** for editing.
- Locate **Computer Configuration, Policies, Windows Settings, Security Settings, Restricted Groups**.
- Right-click or activate the context menu for Restricted Groups and select Add Group.
- In the **Add Group** dialog box, add the required group.
- Add the members to the group or add the group to another group as a member.


Group Policy Management Editor
File
Action
View
Help
Group Memberships [SEA-DC1.CONTOSO.COM] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (CONTOSO.COM)
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX files) retrieved
Preferences
User Configuration
Policies
Preferences
Group Name
Members
Member Of
Administrators
Administrators Properties
?
Configure Membership for Administrators
Add...
Remove
Add...
Remove
OK
Cancel
Apply

Members of this group:

CONTOSO\ContosoAdmin
CONTOSO\Domain Admins
CONTOSO\Enterprise Admins

This group is a member of:

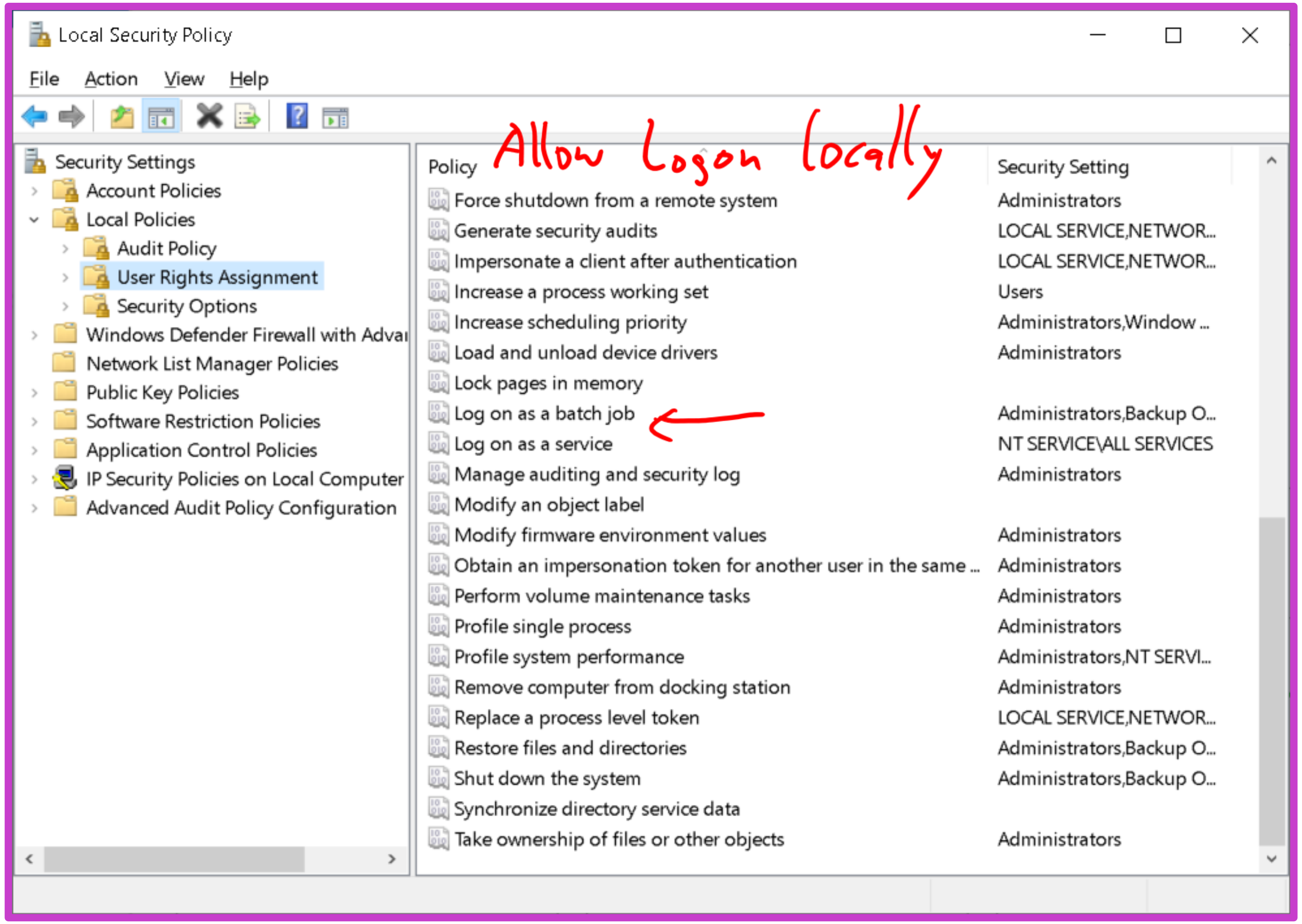
<The groups to which this group belongs should not be modified>

© Copyright Microsoft Corporation. All rights reserved.

Determine currently assigned rights

How to use the Local Security Policy console to determine what rights are assigned.

1. Select **Start**, and then select **Windows Administrative Tools**.
2. Select **Local Security Policy**.
3. In **Local Security Policy**, expand **Local Policies**, and then expand **User Rights Assignment**.
4. Review, and if necessary, edit the **Security Setting** value for each **Policy** listed.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Advai
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Allow Logon locally

Policy	Security Setting
Force shutdown from a remote system	Administrators
Generate security audits	LOCAL SERVICE,NETWOR...
Impersonate a client after authentication	LOCAL SERVICE,NETWOR...
Increase a process working set	Users
Increase scheduling priority	Administrators,Window ...
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	Administrators,Backup O...
Log on as a service	NT SERVICE\ALL SERVICES
Manage auditing and security log	Administrators
Modify an object label	
Modify firmware environment values	Administrators
Obtain an impersonation token for another user in the same ...	Administrators
Perform volume maintenance tasks	Administrators
Profile single process	Administrators
Profile system performance	Administrators,NT SERVI...
Remove computer from docking station	Administrators
Replace a process level token	LOCAL SERVICE,NETWOR...
Restore files and directories	Administrators,Backup O...
Shut down the system	Administrators,Backup O...
Synchronize directory service data	
Take ownership of files or other objects	Administrators

© Copyright Microsoft Corporation. All rights reserved.

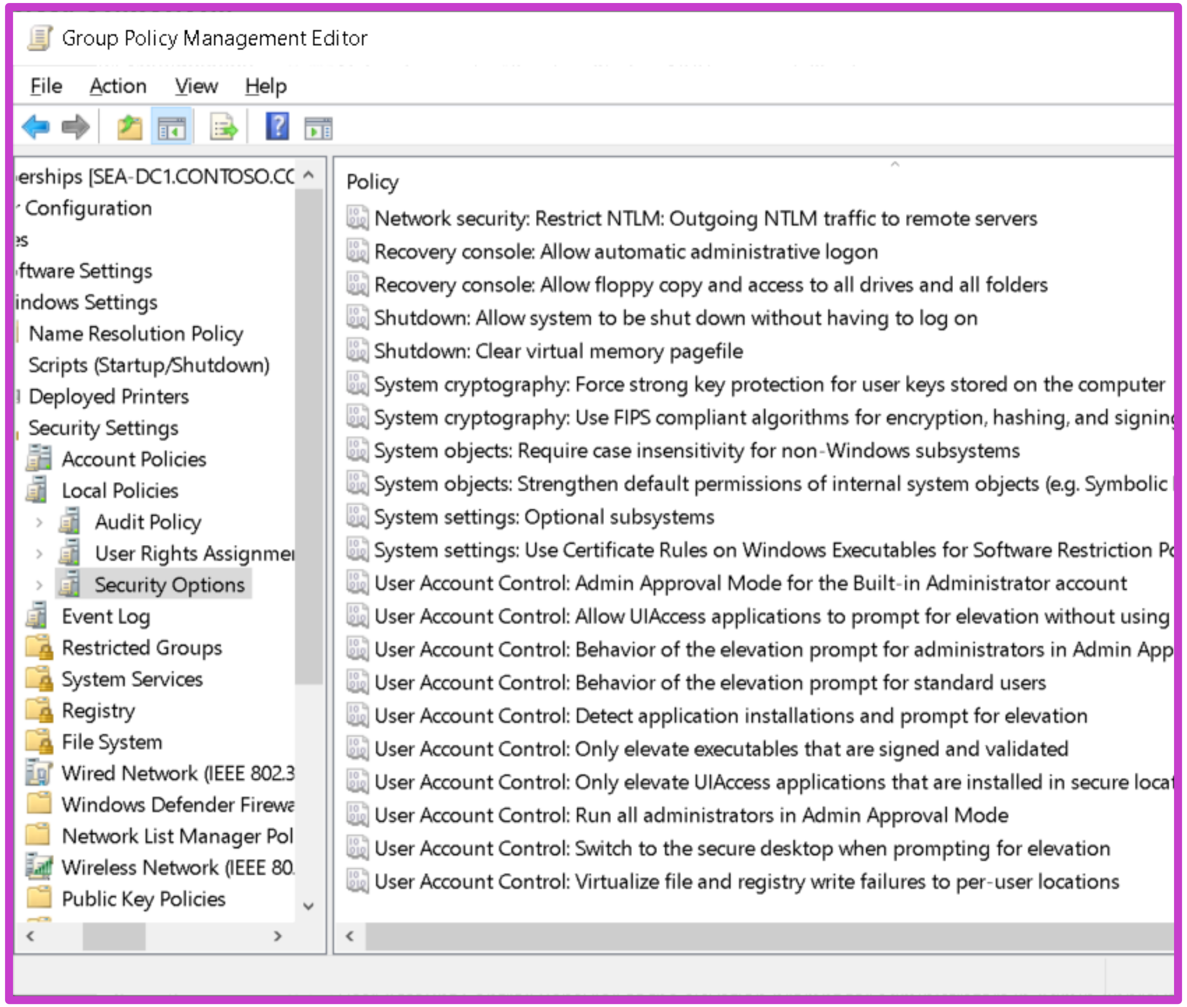
Implement User Account Control

How to control UAC prompts and behavior by using GPOs:

1. Open linked GPO: **Computer Configuration > Policies, Windows Settings > Security Settings > Local Policies, Security Options**.

2. Open **User Account Control: Behavior of the elevation prompt for administrators** setting, select **Define this policy setting**, and select the required setting.

3. Open **User Account Control: Behavior of the elevation prompt for standard users** setting, select **Define this policy setting**, and then select the required setting.



ɪerships [SEA-DC1.CONTOSO.CC
ʳ Configuration
ɪs
ɪftware Settings
indows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignmer
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3
Windows Defender Firewa
Network List Manager Pol
Wireless Network (IEEE 80.
Public Key Policies

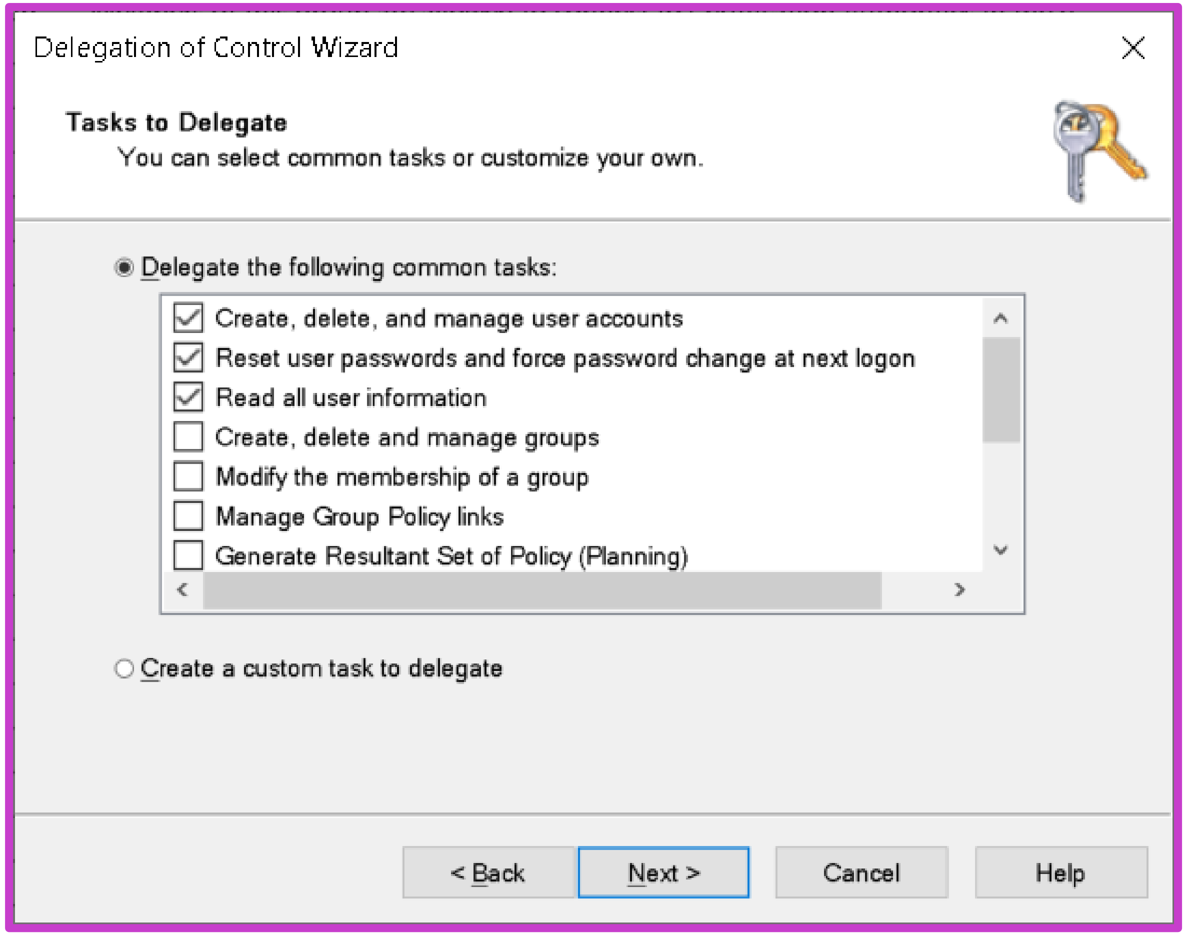
Policy
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers
Recovery console: Allow automatic administrative logon
Recovery console: Allow floppy copy and access to all drives and all folders
Shutdown: Allow system to be shut down without having to log on
Shutdown: Clear virtual memory pagefile
System cryptography: Force strong key protection for user keys stored on the computer
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing
System objects: Require case insensitivity for non-Windows subsystems
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic
System settings: Optional subsystems
System settings: Use Certificate Rules on Windows Executables for Software Restriction Po
User Account Control: Admin Approval Mode for the Built-in Administrator account
User Account Control: Allow UIAccess applications to prompt for elevation without using
User Account Control: Behavior of the elevation prompt for administrators in Admin App
User Account Control: Behavior of the elevation prompt for standard users
User Account Control: Detect application installations and prompt for elevation
User Account Control: Only elevate executables that are signed and validated
User Account Control: Only elevate UIAccess applications that are installed in secure loca
User Account Control: Run all administrators in Admin Approval Mode
User Account Control: Switch to the secure desktop when prompting for elevation
User Account Control: Virtualize file and registry write failures to per-user locations

© Copyright Microsoft Corporation. All rights reserved.

Implement delegated privileges

Use the Delegation of Control Wizard to limit administrative access

- You can delegate more granular privileges to users or groups
- You can also combine permissions to create and assign custom tasks



Delegation of Control Wizard

Tasks to Delegate
You can select common tasks or customize your own.

● Delegate the following common tasks:

☑ Create, delete, and manage user accounts
☑ Reset user passwords and force password change at next logon
☑ Read all user information
☐ Create, delete and manage groups
☐ Modify the membership of a group
☐ Manage Group Policy links
☐ Generate Resultant Set of Policy (Planning)

○ Create a custom task to delegate

© Copyright Microsoft Corporation. All rights reserved.

Demonstration – Implementing delegated privileges

- Open Active Directory Users and Computers
- Create a new group called Sales Managers in the Managers OU. Add a user to the Sales Managers group
- Run the Delegation of Control Wizard, targeting the Sales OU.
- Assign the Sales Managers group the Reset user passwords and force password change at next logon permission on the Sales OU.
- Assign the Sales Managers group the Reset user passwords and force password change at next logon permission on the Sales OU.

© Copyright Microsoft Corporation. All rights reserved.

Use privileged access workstations (1/2)

What is a privileged access workstation?

- A privileged access workstation (PAW) is a computer that you can use for performing tasks, such as the administration of:
  - Identity systems
  - Cloud services
  - Other sensitive services
- Never use PAW for web browsing, email, and other common end-user apps, and it should have strict application control.
- Microsoft recommends using **Windows 11 Enterprise** for your PAWs

© Copyright Microsoft Corporation. All rights reserved.

TS → RDS → AVD

Use privileged access workstations (2/2)

PAW hardware profiles

- Microsoft recommends using one of the following hardware profiles:
  - **Dedicated hardware**: Separate dedicated devices for user tasks versus administrative tasks
  - **Simultaneous use**: A single device that can run user tasks and administrative tasks concurrently by running two operating systems.
- To maintain security, administrator users should be provided with two workstations:
  - PAW
  - Single device for day-to-day tasks that don't require elevation

© Copyright Microsoft Corporation. All rights reserved.

What are jump servers?

A jump server is a hardened server used to access and manage devices in a different security zone

Jump servers are also known as bastion hosts. Azure Bastion is used for remote connectivity (RDP/SSH)

For medium-sized organizations, jump servers can provide a means to help enhance security in locations where physical security is more challenging

Jump servers do not typically have any sensitive data

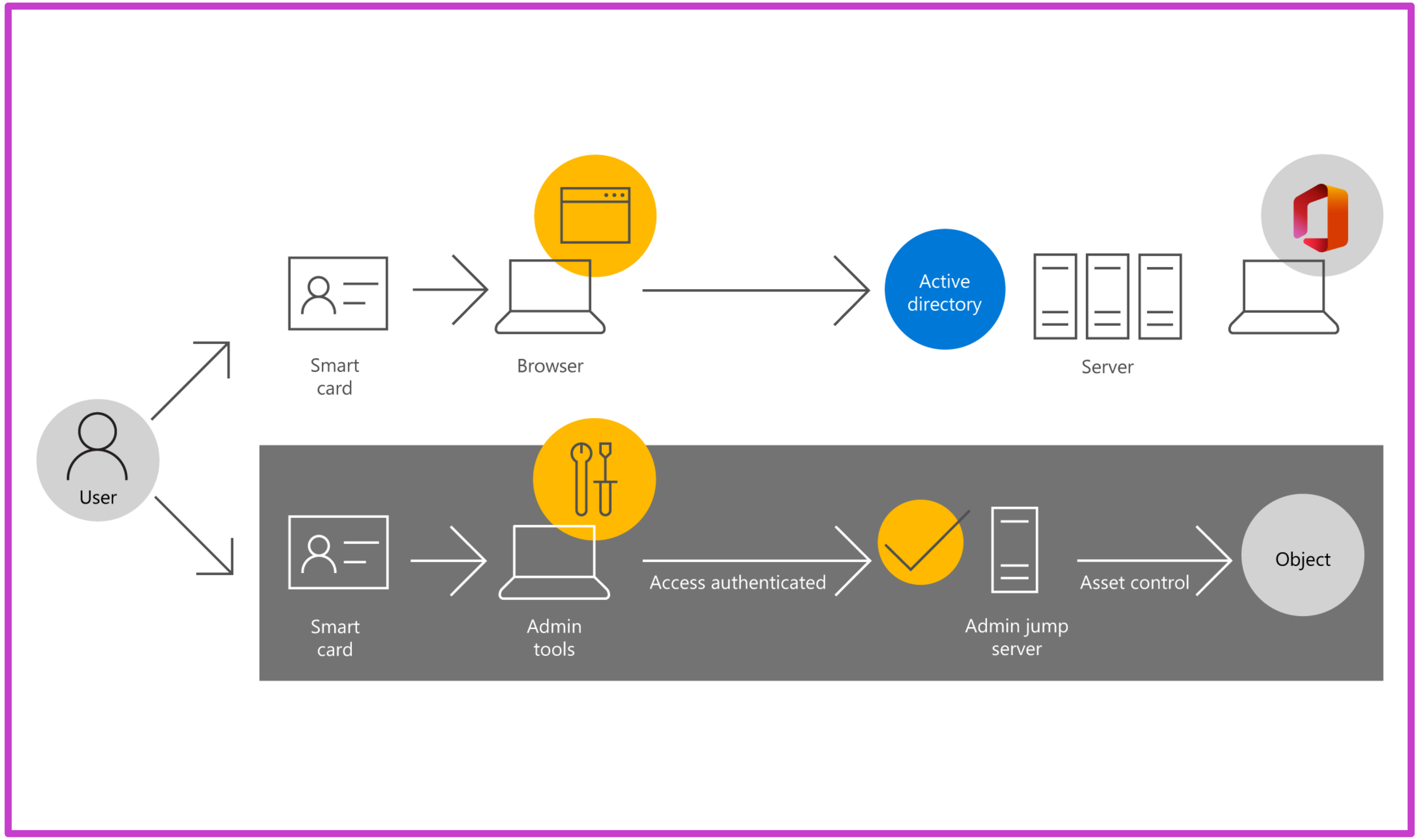
By using jump servers, either with or without PAWs, you can create logical security zones

© Copyright Microsoft Corporation. All rights reserved.

Use jump servers

Considerations for implementing jump servers include:

- Setup Remote Desktop Gateway to implement required restrictions
- Install Hyper-V to build VM for each admin
- Enable Server features: UEFI secure boot, Virtualization support, Signed Kernel mode drivers
- Install Remote administration tools.
- Require RDP connectivity to Admins VMs



© Copyright Microsoft Corporation. All rights reserved.

Learning recap – Windows Server secure administration

Module assessment

Microsoft Learn Modules (docs.microsoft.com/Learn)

Perform Windows Server secure administration

© Copyright Microsoft Corporation. All rights reserved.

Describe Windows Server Administration tools

© Copyright Microsoft Corporation. All rights reserved.

Learning Objectives – Windows Server administration tools

- Explore Windows Admin Center web
- Demonstration – Using Windows Admin Center
- Server Manager ✓ ADAC
- Use PowerShell to manage servers PS 7
- Use PowerShell to remotely administer a serve
- Demonstration – Manage a remote Windows Server
- Learning recap

© Copyright Microsoft Corporation. All rights reserved.

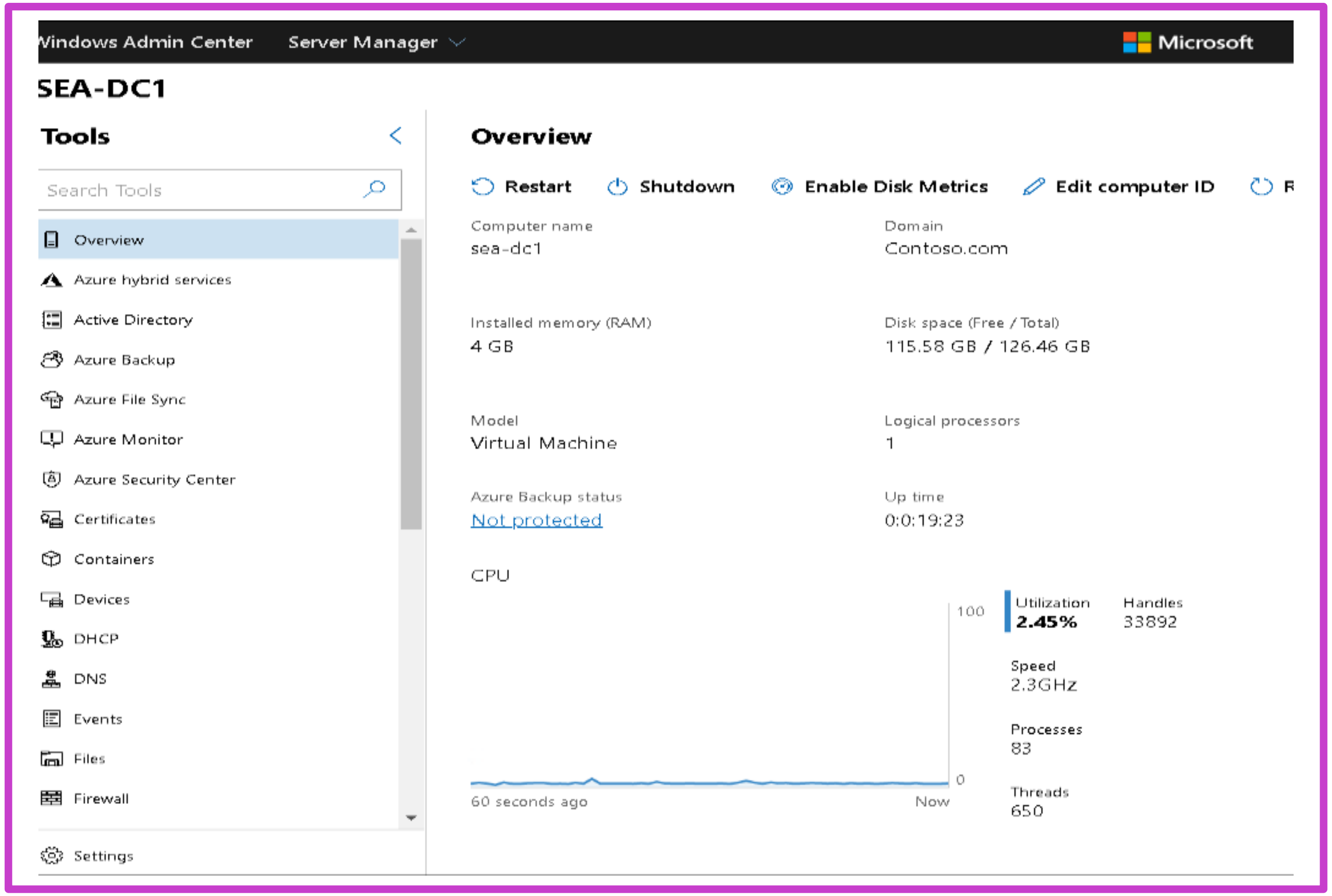
Explore Windows Admin Center

Windows Admin Center has two main components:

- **Gateway** to manage servers through PowerShell remoting and WMI
- **Web server** with UI to management station

Benefits of Windows Admin Center

- Easy to install and use
- Compliments existing solutions
- Manage from the internet
- Enhanced security
- Azure integration
- Extensibility
- No external dependencies



Computer name
sea-dc1

Domain
Contoso.com

Installed memory (RAM)
4 GB

Disk space (Free / Total)
115.58 GB / 126.46 GB

Model
Virtual Machine

Logical processors
1

Azure Backup status
Not protected

Up time
0:0:19:23

Utilization
2.45%

Handles
33892

Speed
2.3GHz

Processes
83

Threads
650

© Copyright Microsoft Corporation. All rights reserved.

Demonstration – Using Windows Admin Center

Install the Windows Admin Center from a downloadable .msi.

Verify that appropriate TCP port is configured during installation.

Add a domain controller to Windows Admin Center.

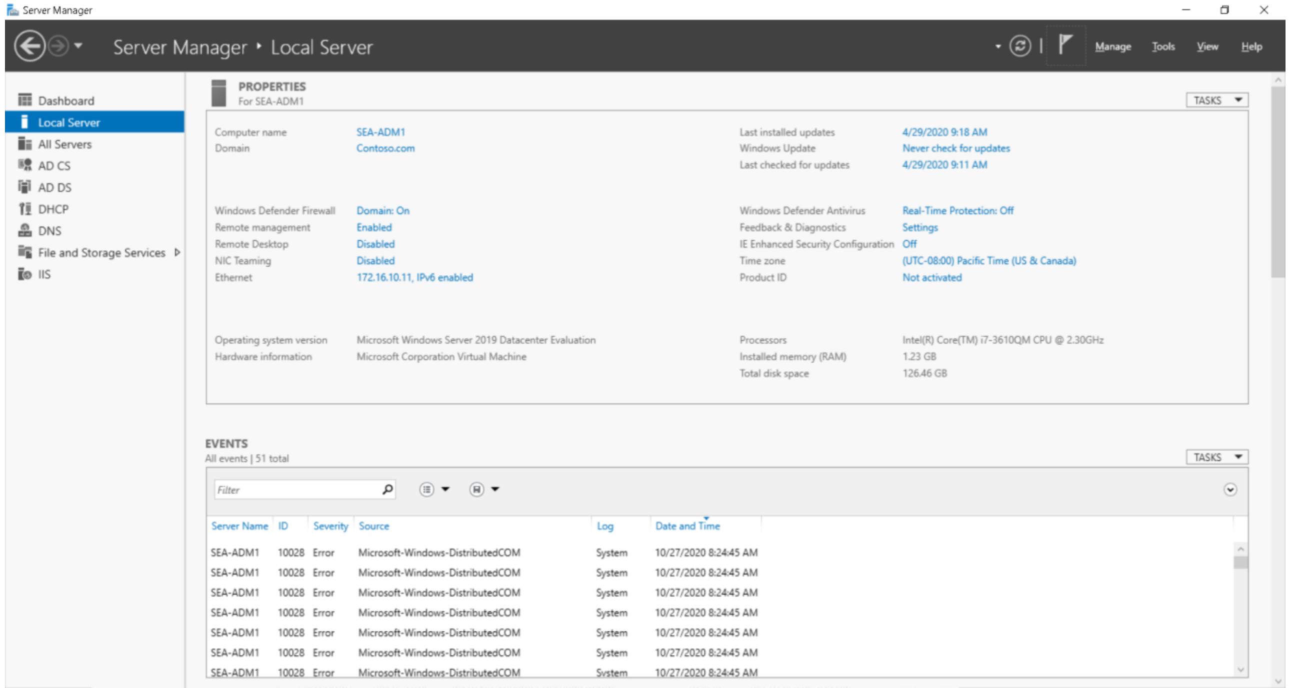
Review the options available on the **Overview** and **Tools** panes

Review certificates, Performance Monitoring, Processes, Registry, Roles & Features, Scheduled Tasks, and PowerShell

© Copyright Microsoft Corporation. All rights reserved.

Use Server Manager

- Server Manager can manage local server and remotely up to 100 additional servers
- Server Manager contains a dashboard for quick access to:
- Configuring the local server.
- Adding roles and features.
- Adding other servers to manage.
- Creating a server group.
- Connecting this server to cloud services.
- Provides basic information about the hardware:
- Operating system version
- Processor information
- Amount of memory
- Total disk space



PROPERTIES
For SEA-ADM1

Computer name SEA-ADM1
Domain Contoso.com

Windows Defender Firewall Domain: On
Remote management Enabled
Remote Desktop Disabled
NIC Teaming Disabled
Ethernet 172.16.10.11, IPv6 enabled

Operating system version Microsoft Windows Server 2019 Datacenter Evaluation
Hardware information Microsoft Corporation Virtual Machine

Last installed updates 4/29/2020 9:18 AM
Windows Update Never check for updates
Last checked for updates 4/29/2020 9:11 AM

Windows Defender Antivirus Real-Time Protection: Off
Feedback & Diagnostics Settings
IE Enhanced Security Configuration Off
Time zone (UTC-08:00) Pacific Time (US & Canada)
Product ID Not activated

Processors Intel(R) Core(TM) i7-3610QM CPU @ 2.30GHz
Installed memory (RAM) 1.23 GB
Total disk space 126.46 GB

EVENTS
All events | 51 total

Filter

Server Name	ID	Severity	Source	Log	Date and Time
SEA-ADM1	10028	Error	Microsoft-Windows-DistributedCOM	System	10/27/2020 8:24:45 AM
SEA-ADM1	10028	Error	Microsoft-Windows-DistributedCOM	System	10/27/2020 8:24:45 AM
SEA-ADM1	10028	Error	Microsoft-Windows-DistributedCOM	System	10/27/2020 8:24:45 AM
SEA-ADM1	10028	Error	Microsoft-Windows-DistributedCOM	System	10/27/2020 8:24:45 AM
SEA-ADM1	10028	Error	Microsoft-Windows-DistributedCOM	System	10/27/2020 8:24:45 AM
SEA-ADM1	10028	Error	Microsoft-Windows-DistributedCOM	System	10/27/2020 8:24:45 AM
SEA-ADM1	10028	Error	Microsoft-Windows-DistributedCOM	System	10/27/2020 8:24:45 AM

PS>

© Copyright Microsoft Corporation. All rights reserved.

List Remote Server Administration Tools

Part of available management tools of RSAT and their description

Tool	Description
Active Directory Certificate Services Tools	Includes Certification Authority, Certificate Templates, Enterprise PKI, and Online Responder Management snap-ins
DHCP Server Tools	Includes the DHCP Management Console, the DHCP Server cmdlet module for Windows PowerShell, and the Netsh command-line tool
DNS Server Tools	Includes the DNS Manager snap-in, the DNS module for Windows PowerShell, and the Ddnscmd.exe command-line tool
Shielded VM Tools	Includes Provisioning Data File Wizard and Template Disk Wizard

```
Install-Windows Feature Web-Server -IncludeManagemenTools
```

© Copyright Microsoft Corporation. All rights reserved.

List Remote Server Administration Tools (*cont.*)

Tool	Description
IP Address Management (IPAM) Tools	Includes tools for managing remote IPAM server
Remote Access Management Tools	Includes graphical and PowerShell tools for managing the Remote Access role
Network Load Balancing Tools	Includes the Network Load Balancing Manager, Network Load Balancing Windows PowerShell cmdlets, and the NLB.exe and WLBS.exe command-line tools
Windows Server Update Services Tools	Includes the Windows Server Update Services snap-in, WSUS.msc, and PowerShell cmdlets

© Copyright Microsoft Corporation. All rights reserved.

Use Windows PowerShell (1/2)

Cmdlet

Jeff Snover

Windows PowerShell commands and cmdlets

- Commands are building blocks that you piece together by using the Windows PowerShell scripting language
- Cmdlets are the fundamental components of commands

CloudShell

Bash PowerShell

Cmdlet verbs

- Get/Set/New/Add/Remove

Cmdlet nouns

- The noun portion of the cmdlet name indicates what kinds of resources or objects the cmdlet affects

```
Get-Service | Select-Object Name, Status | Export-CSV c:\service.csv
```

Parameter format

- Parameters modify the actions that a cmdlet performs
- Each cmdlet can have no parameters, one parameter, or many parameters. Parameter names begin with a dash (-)
- A space separates the value that you want to pass from the parameter name

© Copyright Microsoft Corporation. All rights reserved.

5

7

VS Code

Erich Gamma

Use Windows PowerShell (2/2)

Windows PowerShell ISE:

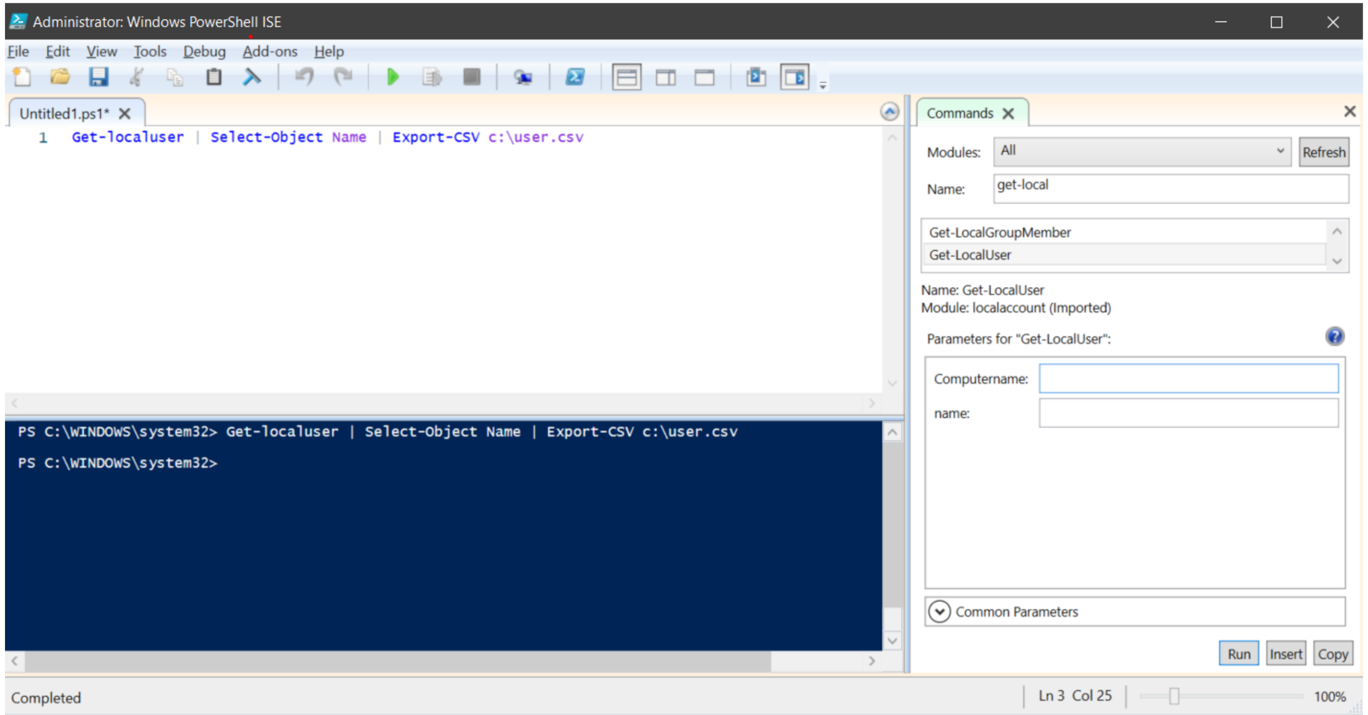
- The ISE is a fully graphical environment
- The ISE offers two main panes: a Script pane (or script editor) and the Console pane
- The ISE provides several ways to customize the view

Windows PowerShell remoting – three ways:

- One-to-One remoting
- One-to-Many remoting
- Many-to-One remoting

PowerShell Direct

- It enables you to run a Windows PowerShell cmdlet or script inside a VM



```
Get-localuser | Select-Object Name | Export-CSV c:\user.csv
```

```
PS C:\WINDOWS\system32> Get-localuser | Select-Object Name | Export-CSV c:\user.csv
PS C:\WINDOWS\system32>
```

Modules: All

Name: get-local

Name: Get-LocalUser
Module: localaccount (Imported)

Parameters for "Get-LocalUser":

Computername:

name:

Completed

Ln 3 Col 25

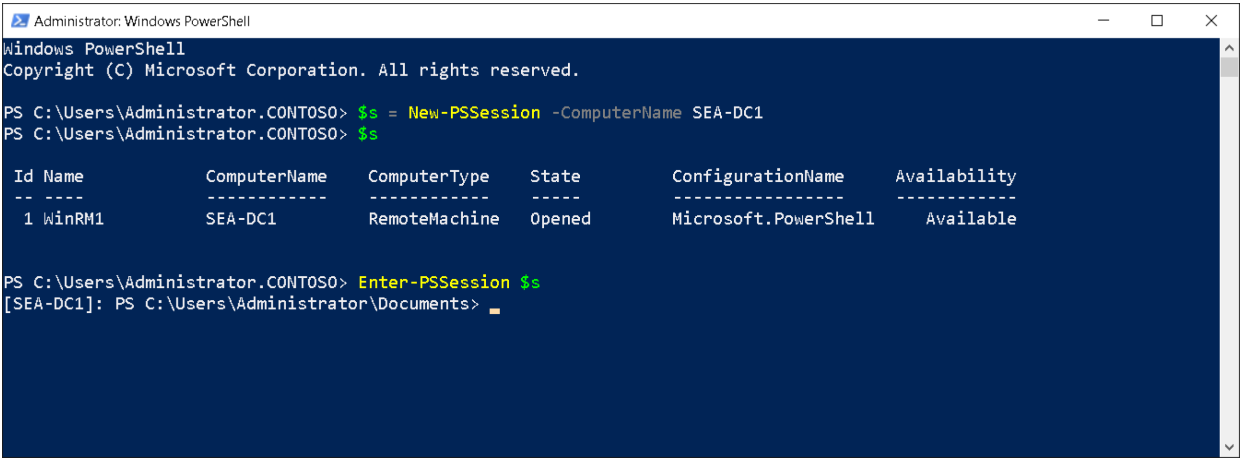
100%

© Copyright Microsoft Corporation. All rights reserved.

Use Windows PowerShell to remotely administer a server

Requirements for remoting

- PowerShell installed on your local computer
- Windows Remote Management enabled on any remote computers to connect
- PowerShell remoting must be enabled



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.CONTOSO> $s = New-PSSession -ComputerName SEA-DC1
PS C:\Users\Administrator.CONTOSO> $s

 Id Name            ComputerName    ComputerType    State         ConfigurationName     Availability
 -- ----            ------------    ------------    -----         -----------------     ------------
  1 WinRM1          SEA-DC1         RemoteMachine   Opened        Microsoft.PowerShell     Available


PS C:\Users\Administrator.CONTOSO> Enter-PSSession $s
[SEA-DC1]: PS C:\Users\Administrator\Documents> _
```

Run cmdlets against remote computers

- Processing remote commands
  - Create a temporary session by using the **Invoke-Command** cmdlet with the **–ComputerName** parameter
  - Create a persistent session by using the **New-PSSession** and **Enter-PSSession** cmdlet
  - Run remote commands on multiple computers

WS-Man
WinRM

:5985 AD
:5986 SSL

Run a script on remote computers

```
Invoke-Command -ComputerName SEA-DC1, SEA-SVR1 -FilePath C:\Test\Sample.ps1
```

{...}

© Copyright Microsoft Corporation. All rights reserved.

PowerShell remoting over SSH

:22

SSH is now available for Linux and Windows platform

- Allows true multi-platform PowerShell remoting
- Supports basic PowerShell session remoting between Windows and Linux computers
- To run SSH, PowerShell 7 or higher is recommended
- In Windows Server 2025, SSHD service is installed by default, and only needs to be enabled as a service

```
# Establish an SSH session to a remote computer
$session = New-PSSession –Hostname “SEA-SVR1” –Hostname “admin” –KeyFilePath
“C:\Users\admin\.ssh\id_rsa”

# Run a command on the remote computer
Invoke-Command -Session $session -ScriptBlock { Get-Process }

# Close the session
Remove-PSSession -Session $session
```

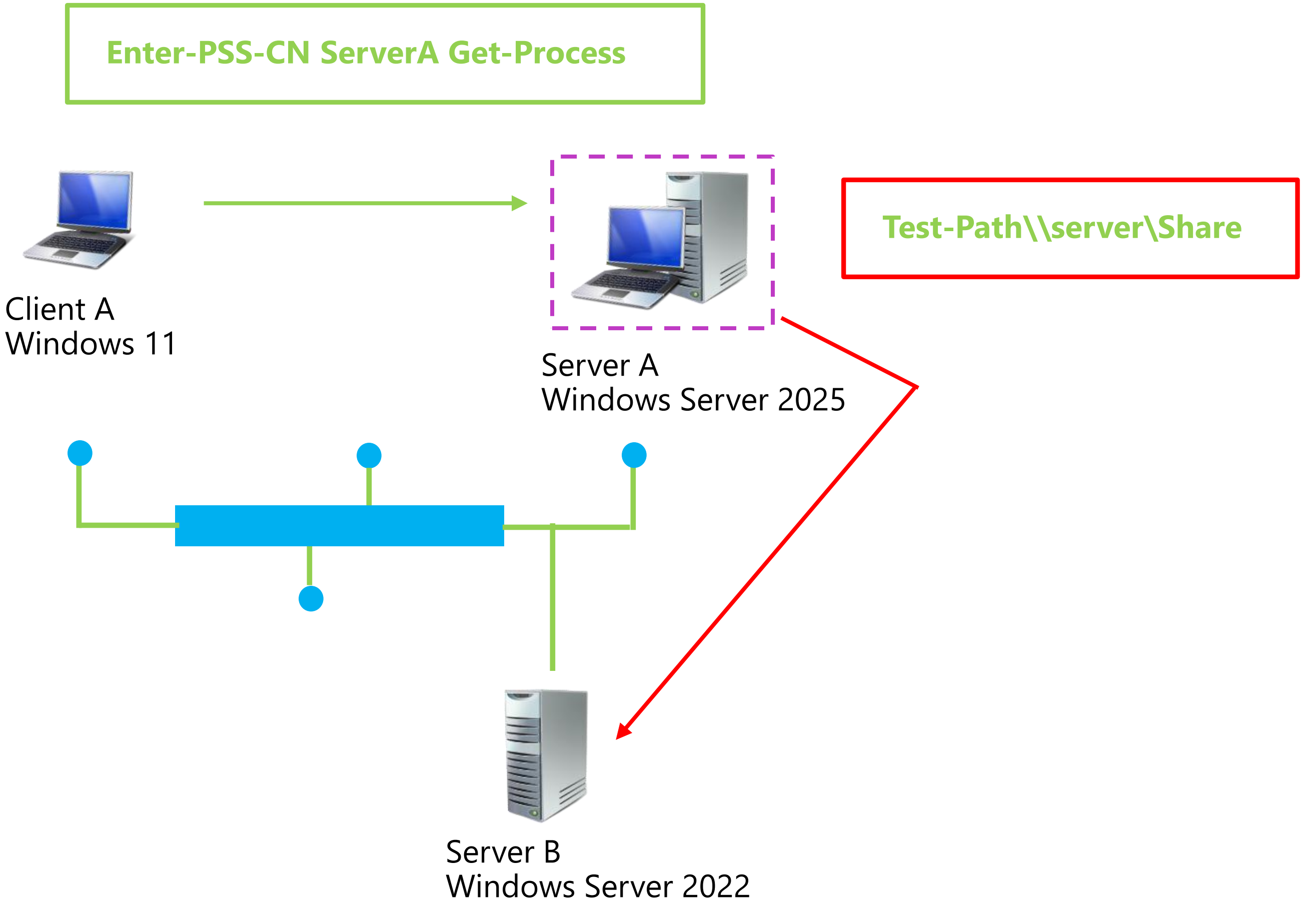
© Copyright Microsoft Corporation. All rights reserved.

Configure CredSSP or Kerberos Delegation for 2nd Hop Remoting

The following are the most recommended technologies to solve the second hop remoting problem:

- **CredSSP**: Credential Security Support Provider (CredSSP) – offers ease of use.

- **Kerberos Delegation**: This solution provides the following three options:
  - Resource-based Kerberos
  - Kerberos constrained delegation
  - Kerberos unconstrained delegation (*blocked by default in Windows Server 2025*)



```
Enter-PSS-CN ServerA Get-Process
```

```
Test-Path\\server\Share
```

© Copyright Microsoft Corporation. All rights reserved.

Demonstration – Manage a Remote Windows Server

Launch an elevated PowerShell prompt

Create a remoting session

```
Enter-PSSession -ComputerName SEA-DC1
```

Retrieve information about the server, such as name and IP address

```
Get-CimInstance -Class CIM_ComputerSystem | Select-Object *
```

Check status of IIS service and restart that service

```
Get-Service -Name IISAdmin | Restart-Service
```

© Copyright Microsoft Corporation. All rights reserved.

Learning recap – Describe Windows Server Administration Tools

Module assessment

Microsoft Learn Modules (docs.microsoft.com/Learn)

Describe Windows Server administration tools

© Copyright Microsoft Corporation. All rights reserved.

Perform post-installation Configuration of Windows Server

© Copyright Microsoft Corporation. All rights reserved.

Learning Objectives – Windows Server post-installation configuration

- Post-installation configuration
- Post-installation configuration tools
- Use Windows Admin Center for post-installation configuration
- Implement answer files to complete the configuration
- Demonstration - post installation configuration
- Learning recap

© Copyright Microsoft Corporation. All rights reserved.

Post-installation configuration

What must you configure?

Setting	Description
Computer name	The computer name is automatically generated. You'll need to change the name to something meaningful, and unique, within your organization.
Workgroup	The server is added to a workgroup called WORKGROUP.
Network settings	In the case of IPv4, a Dynamic Host Configuration Protocol (DHCP) configuration is assigned. For IPv6, stateless autoconfiguration is enabled. Both these defaults are probably suitable.
Time zone	The time zone defaults to the (UTC-08:00) Pacific Time (US & Canada) unless your installation media was based on a different locale. You'll need to change the time zone, and the computer's time and date.

© Copyright Microsoft Corporation. All rights reserved.

Post-installation configuration (*cont.*)

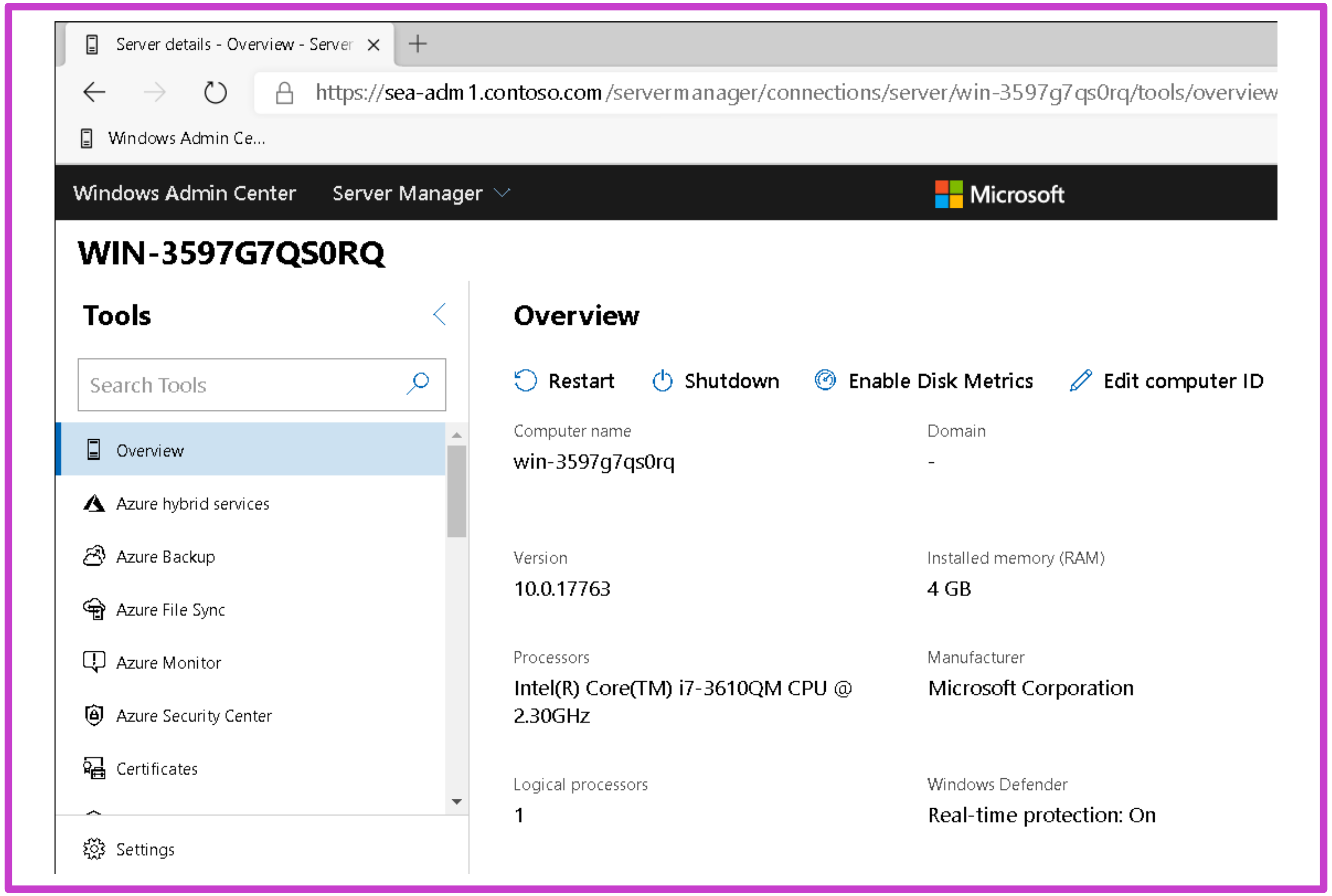
What must you configure?

Setting	Description
Locale and language settings	The initial values are specified during an interactive installation or are implied by the installation media locale. You'll need to update these settings to those which are appropriate for the server's physical location.
Roles and features	Very few roles or features are enabled by default in a standard installation. Typically, the Storage Services role service, and several features are enabled.
Firewall settings	The Windows Defender Firewall is enabled by default.
Activation	Typically, the server will not be activated.

© Copyright Microsoft Corporation. All rights reserved.

Available post-installation configuration tools

- **Server Manager** – Configure settings on the local server
- **Windows Admin Center** – Perform post-installation configuration
- **Answer files** – Created for automating the installation process by using Windows Assessment and Deployment Kit
- **ConfigMgr** - also widely used for post-installation tasks for Windows Server



https://sea-adm1.contoso.com/servermanager/connections/server/win-3597g7qs0rq/tools/overview

WIN-3597G7QS0RQ

Overview

Computer name
win-3597g7qs0rq

Domain
-

Version
10.0.17763

Installed memory (RAM)
4 GB

Processors
Intel(R) Core(TM) i7-3610QM CPU @ 2.30GHz

Manufacturer
Microsoft Corporation

Logical processors
1

Windows Defender
Real-time protection: On

© Copyright Microsoft Corporation. All rights reserved.

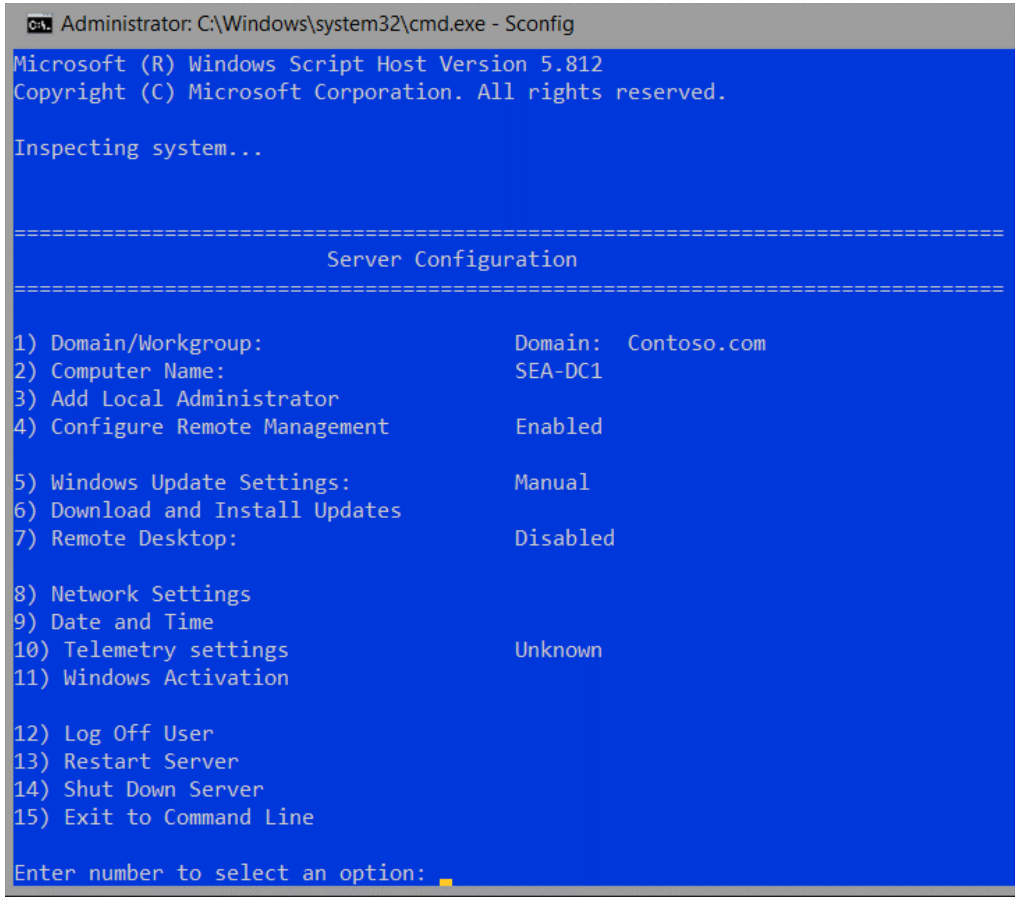
Configure Server Core using Sconfig

What is Sconfig?

- Text-based tool for basic configuration of Server Core and Windows Server Desktop.
- Perform the initial configuration directly after the installation completes.

Sconfig provides several options:

- Domain/Workgroup
- Computer Name
- Add Local Administrator
- Configure Remote Management
- Windows Update Settings
- Network settings
- Telemetry Settings
- Shut Down/Restart Server



```
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

Inspecting system...


===============================================================================
                         Server Configuration
===============================================================================

1) Domain/Workgroup:                    Domain:  Contoso.com
2) Computer Name:                       SEA-DC1
3) Add Local Administrator
4) Configure Remote Management          Enabled

5) Windows Update Settings:             Manual
6) Download and Install Updates
7) Remote Desktop:                      Disabled

8) Network Settings
9) Date and Time
10) Telemetry settings                  Unknown
11) Windows Activation

12) Log Off User
13) Restart Server
14) Shut Down Server
15) Exit to Command Line

Enter number to select an option:
```

© Copyright Microsoft Corporation. All rights reserved.

Demonstration – Post-installation configuration by Sconfig.exe

Run the Sconfig.exe command.

Review the available options.

Reconfigure the date and time.

Review the network settings

© Copyright Microsoft Corporation. All rights reserved.

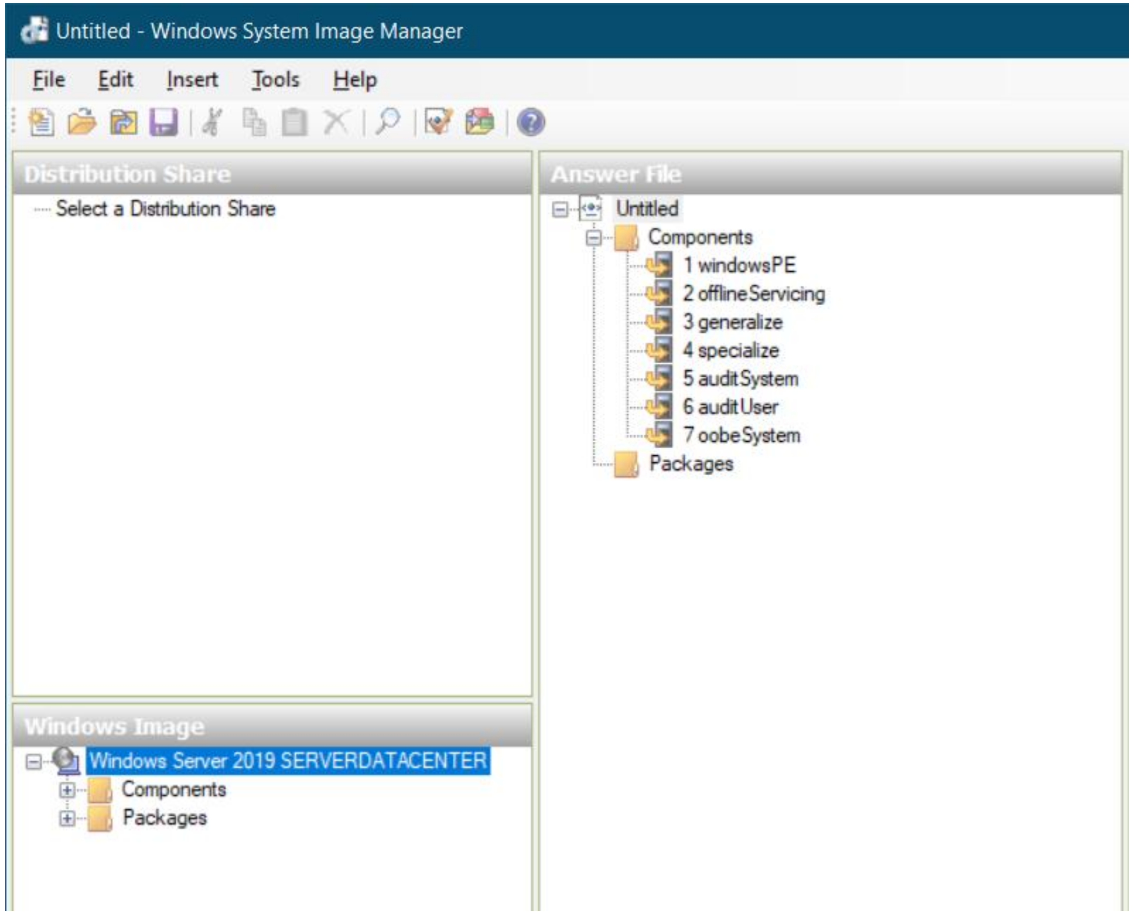
Configure a server with answer files (1/2)

What are answer files?

Text based .xml files that contain settings that enable you to customize and automate the deployment process of Windows.

Answer files are organized into two sections:

- **Components** – Contains all the component settings
- **Packages** – Contains packages for distribute updates and language packs, enable windows features.



© Copyright Microsoft Corporation. All rights reserved.

Configure a server with answer files (2/2)

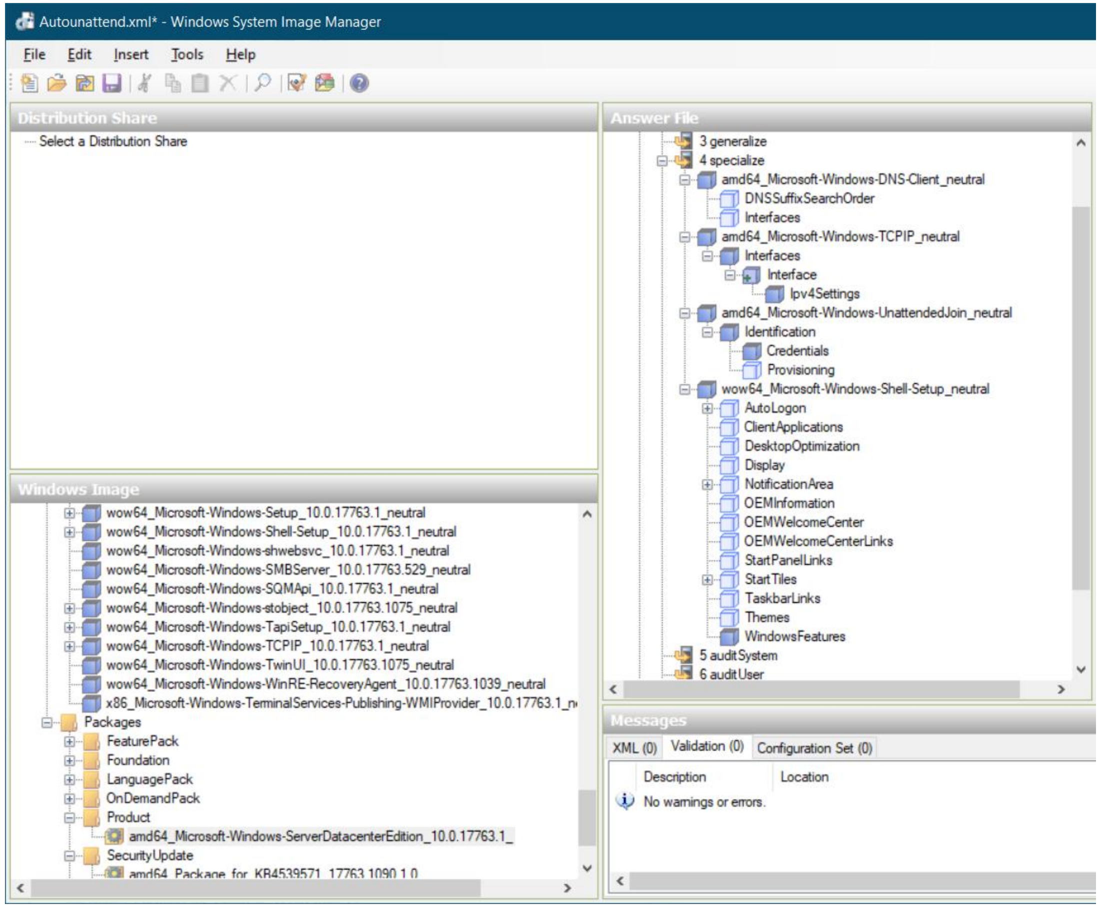
Create and distribute answer files

1. Download the Windows ADK and perform a custom installation
2. Create the catalog file.
3. Configure the answer file

Typical settings to include

In the **Components** node, some of the more common settings are:

- Microsoft-Windows-TCPIP.
- Microsoft-Windows-DNS-Client.
- Microsoft-Windows-UnattendedJoin.
- Microsoft-Windows-Shell-Setup.



```
Select a Distribution Share
```

```
wow64_Microsoft-Windows-Setup_10.0.17763.1_neutral
wow64_Microsoft-Windows-Shell-Setup_10.0.17763.1_neutral
wow64_Microsoft-Windows-shwebsvc_10.0.17763.1_neutral
wow64_Microsoft-Windows-SMBServer_10.0.17763.529_neutral
wow64_Microsoft-Windows-SQMApi_10.0.17763.1_neutral
wow64_Microsoft-Windows-stobject_10.0.17763.1075_neutral
wow64_Microsoft-Windows-TapiSetup_10.0.17763.1_neutral
wow64_Microsoft-Windows-TCPIP_10.0.17763.1_neutral
wow64_Microsoft-Windows-TwinUI_10.0.17763.1075_neutral
wow64_Microsoft-Windows-WinRE-RecoveryAgent_10.0.17763.1039_neutral
x86_Microsoft-Windows-TerminalServices-Publishing-WMIProvider_10.0.17763.1_n
Packages
  FeaturePack
  Foundation
  LanguagePack
  OnDemandPack
  Product
    amd64_Microsoft-Windows-ServerDatacenterEdition_10.0.17763.1_
  SecurityUpdate
    amd64_Package_for_KB4539571_17763.1090.1.0
```

```
3 generalize
4 specialize
  amd64_Microsoft-Windows-DNS-Client_neutral
    DNSSuffixSearchOrder
    Interfaces
  amd64_Microsoft-Windows-TCPIP_neutral
    Interfaces
      Interface
        Ipv4Settings
  amd64_Microsoft-Windows-UnattendedJoin_neutral
    Identification
      Credentials
      Provisioning
  wow64_Microsoft-Windows-Shell-Setup_neutral
    AutoLogon
    ClientApplications
    DesktopOptimization
    Display
    NotificationArea
    OEMInformation
    OEMWelcomeCenter
    OEMWelcomeCenterLinks
    StartPanelLinks
    StartTiles
    TaskbarLinks
    Themes
    WindowsFeatures
5 auditSystem
6 auditUser
```

XML (0) | Validation (0) | Configuration Set (0)

Description	Location
No warnings or errors.	

© Copyright Microsoft Corporation. All rights reserved.

Learning recap – Perform post-installation configuration of Windows Server

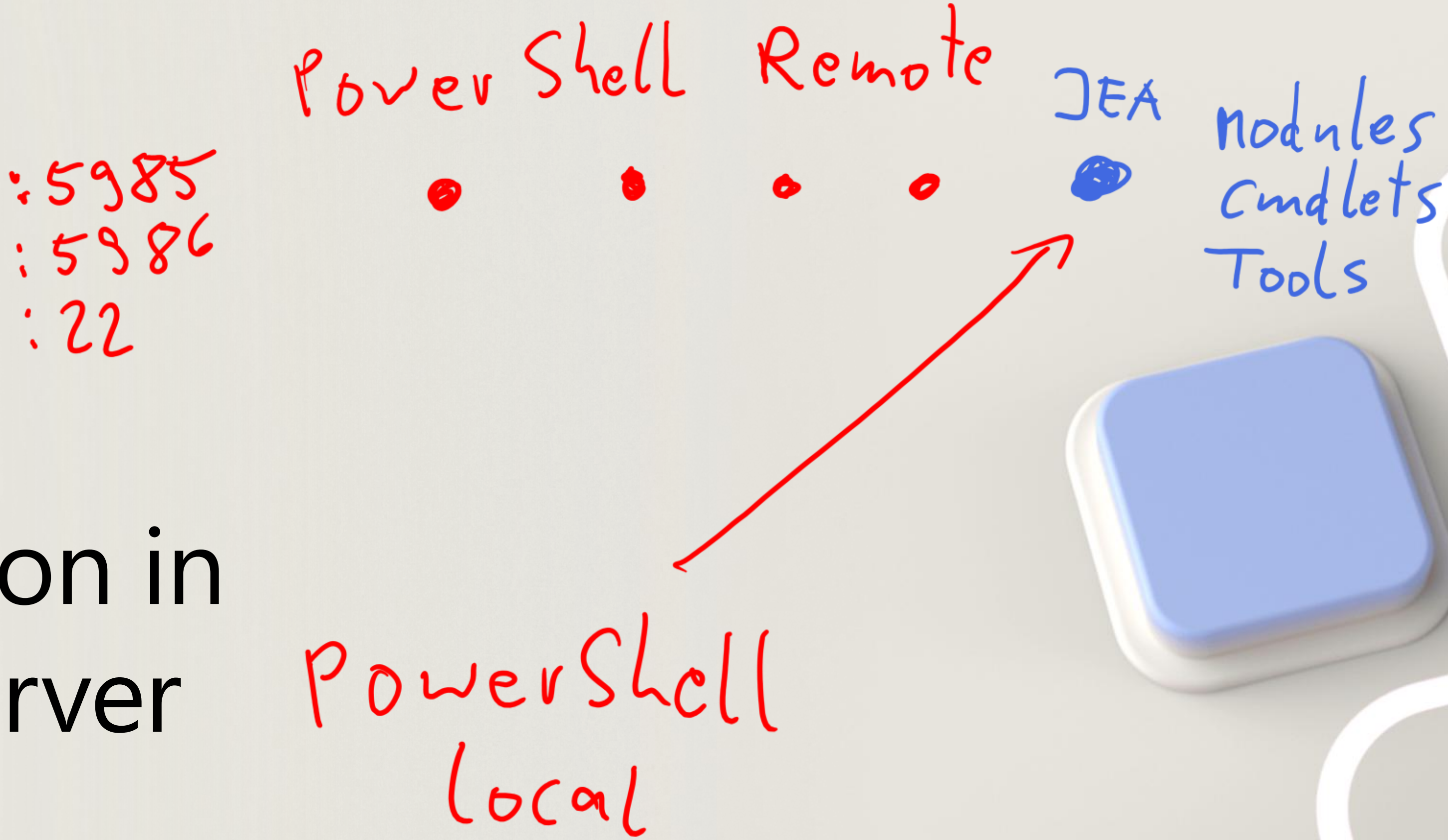
Module assessment

Microsoft Learn Modules (docs.microsoft.com/Learn)

Perform post-installation configuration of Windows Server

© Copyright Microsoft Corporation. All rights reserved.

Just Enough Administration in Windows Server



Power Shell Remote

JEA

modules
Cmdlets
Tools

:5985
:5986
:22

PowerShell
local

© Copyright Microsoft Corporation. All rights reserved.

Learning Objectives – Just Enough Administration

- Concept of Just Enough Administration
- Define role group capabilities
- Session configuration for a JEA session
- Create and connect to a JEA endpoint
- Demonstration - connect to JEA endpoints
- Learning recap

© Copyright Microsoft Corporation. All rights reserved.

Explain the concept of Just Enough Administration (JEA)

The concept of JEA

- Just Enough Administration (JEA) provides Windows operating systems with RBAC functionality built on Windows PowerShell remoting.
- When you configure JEA, an authorized user connects to a specially configured endpoint and uses a specific set of Windows PowerShell cmdlets, parameters, and parameter values.
- Configure a JEA endpoint to allow certain scripts and commands to be run, providing these commands run within a Windows PowerShell session.

JEA limitations

- For JEA role capabilities you must understand which cmdlets, parameters, aliases, and values required to perform administrative tasks.
- JEA is not suitable for tasks where the problem are not clearly defined
- JEA only works with Windows PowerShell sessions.
- JEA works only for Windows Server 2016 or later and Windows 10 or later

© Copyright Microsoft Corporation. All rights reserved.

Define role capabilities for a JEA endpoint

Role capability files help you specify what can be done in a Windows PowerShell session.

You can define the following limitations for the Windows PowerShell session in a role capability file:

- VisibleAliases
- VisibleCmdlets
- VisibleFunctions
- VisibleExternalCommands
- VisibleProviders

Example of generating role capability file allowing restart services

```
$roleParameters = @{
    Path = ".\Maintenance.psrc"
    Author = "User01"
    CompanyName = "Fabrikam Corporation"
    ModulesToImport =
    "Microsoft.PowerShell.Core"
    VisibleCmdlets = "Restart-Service", @{
        Name = "Restart-Computer"
        Parameters = @{ Name =
        "ComputerName"; ValidatePattern =
        "VDI\d+" } } }

New-PSRoleCapabilityFile @roleParameters
```

© Copyright Microsoft Corporation. All rights reserved.

Create a session configuration file to register a JEA endpoint

Session configuration files are used to register a JEA endpoint

Session configuration file is responsible for naming the JEA endpoint. It also controls:

- Who can access the JEA endpoint
- What roles the user is assigned
- Which identity is used by JEA's virtual account.

You can configure the following settings unique to session configure files:

- SessionType
- RoleDefinitions
- RunAsVirtualAccount
- TranscriptDirectory
- RunAsVirtualAccountGroup

© Copyright Microsoft Corporation. All rights reserved.

Describe how JEA endpoints work to limit access to a PowerShell session

Registering JEA on a single machine

- Creating JEA endpoints by **Register-PSSessionConfiguration** cmdlet
- Viewing existing JEA endpoints by **Get-PSSessionConfiguration** cmdlet
- You must have defined one or more roles, and the role capabilities file (or files)must be placed in the folder of a Windows PowerShell ***RoleCapabilities*** module.

Registering JEA on multiple machines

- You can register JEA on multiple machines by using Desired State Configuration (DSC)
- You can apply the DSC configuration using the Local Configuration Manager or by updating the pull server configuration.

© Copyright Microsoft Corporation. All rights reserved.

Create and connect to a JEA endpoint

Interactive JEA connections – To use JEA interactively, you need : **The remote computer name/The JEA endpoint name/An account with access to the desired endpoint**

```
Enter-PSSession -ComputerName localhost -ConfigurationName DNSOps
```

Implicit remoting and JEA

```
 $DNSOpssession = New-PSSession -ComputerName 'MyServer' -ConfigurationName 'DNSOps'
Import-PSSession -Session $DNSOpssession -Prefix 'DNSOps' Get-DNSOpsCommand
```

© Copyright Microsoft Corporation. All rights reserved.

Create and connect to a JEA endpoint (1 of 2)

Programmatic access to JEA

You can connect to JEA endpoints programmatically the same way you connect to other PowerShell endpoints programmatically.

JEA and PowerShell Direct

- PowerShell Direct allows Hyper-V administrators to connect to VMs from the Hyper-V host
- Whenever using JEA to manage VMs, you should create a dedicated JEA user account for the Hyper-V administrator, and the accounts' ability to sign-in locally to the VM.

© Copyright Microsoft Corporation. All rights reserved.

Demonstration – Connect to a JEA endpoint

Create a role capability file around DNS operations.

Create a session configuration file that allows members of a specific Active Directory group to use the privileges granted in the role capability file using a virtual account.

Testing that that JEA functions as expected by connecting using an unprivileged account to the JEA endpoint.

© Copyright Microsoft Corporation. All rights reserved.

Learning recap – Just Enough Administration in Windows Server

Module assessment

Microsoft Learn Modules (docs.microsoft.com/Learn)

Just Enough Administration in Windows Server

© Copyright Microsoft Corporation. All rights reserved.

Lab 03 – Managing Windows Server

© Copyright Microsoft Corporation. All rights reserved.

Lab 03: Managing Windows Server

Lab scenario

Contoso, Ltd. wants to implement several new servers in their environment, and they have decided to use Server Core. They also want to implement Windows Admin Center for remote management of both these servers and other servers in the organization. You will use Windows Admin Center for remote administration.

Objectives

Implement and configure Windows Admin Center

© Copyright Microsoft Corporation. All rights reserved.

End of presentation

© Copyright Microsoft Corporation. All rights reserved.