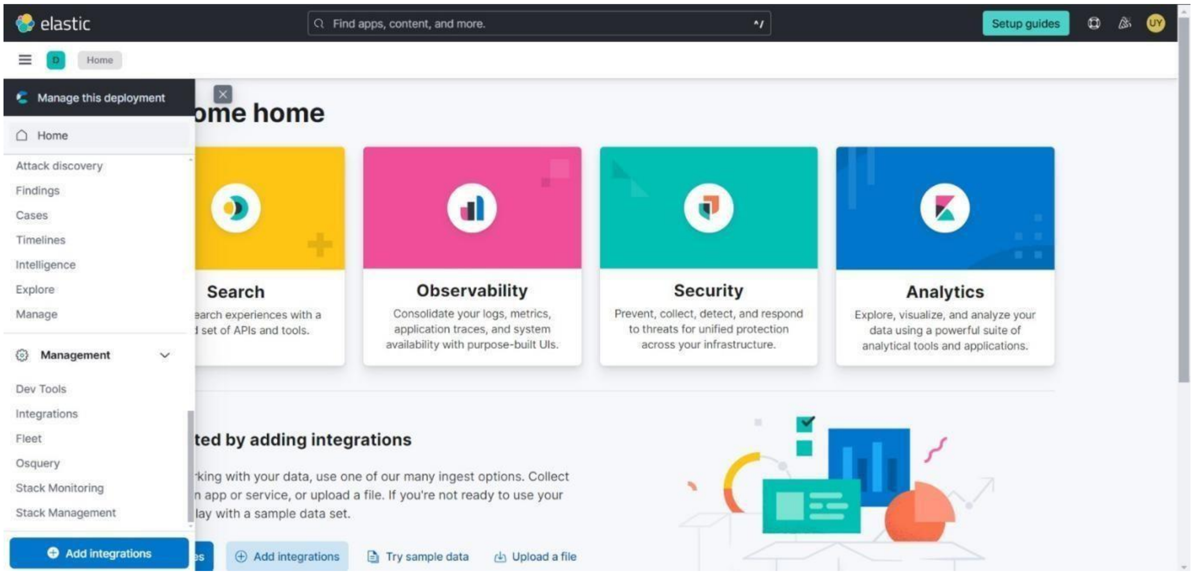
UI Assignment:



ome home

Search

earch experiences with a
l set of APIs and tools.

Observability

Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Security

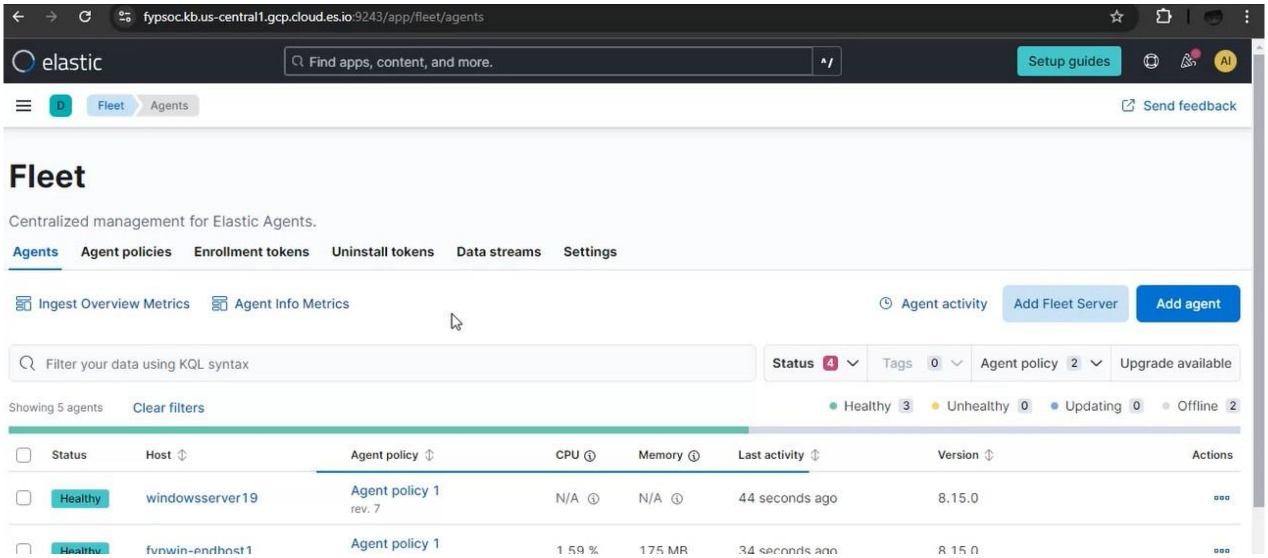
Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

Analytics

Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

ted by adding integrations

rking with your data, use one of our many ingest options. Collect
n app or service, or upload a file. If you're not ready to use your
lay with a sample data set.



fypsoc.kb.us-central1.gcp.cloud.es.io:9243/app/fleet/agents

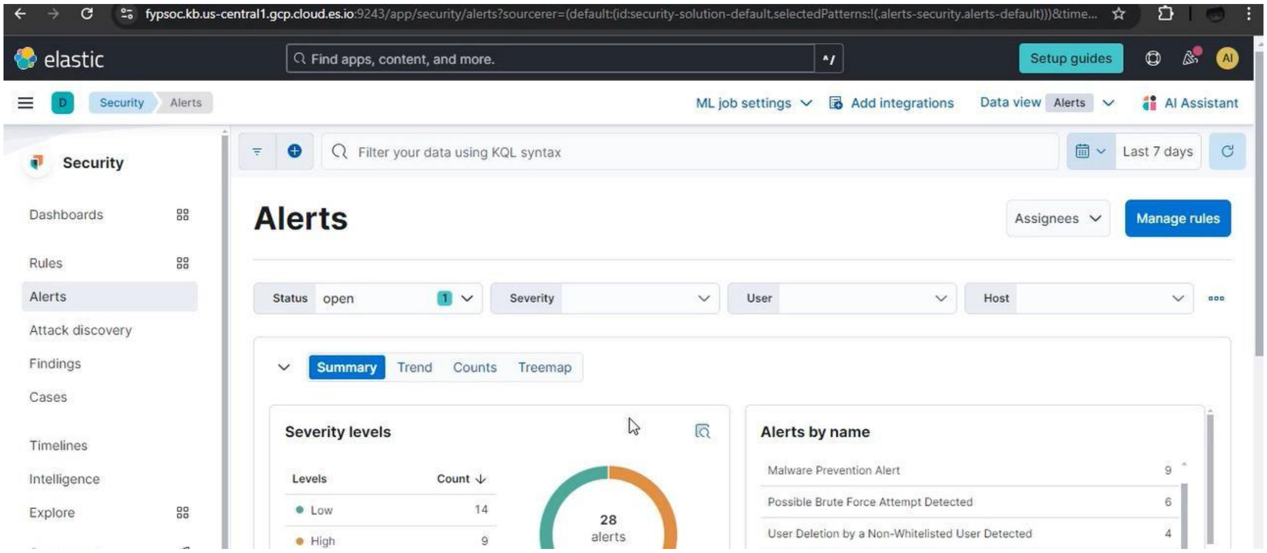
Fleet

Centralized management for Elastic Agents.

Showing 5 agents Clear filters

● Healthy 3 ● Unhealthy 0 ● Updating 0 ● Offline 2

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	windowsserver19	Agent policy 1 rev. 7	N/A	N/A	44 seconds ago	8.15.0	•••
Healthy	fypwin-endhost1	Agent policy 1	1.59 %	175 MB	34 seconds ago	8.15.0	•••



fypsoc.kb.us-central1.gcp.cloud.es.io:9243/app/security/alerts?sourcerer=(default:(id:security-solution-default,selectedPatterns:!(.alerts-security.alerts-default)))&time...

Alerts

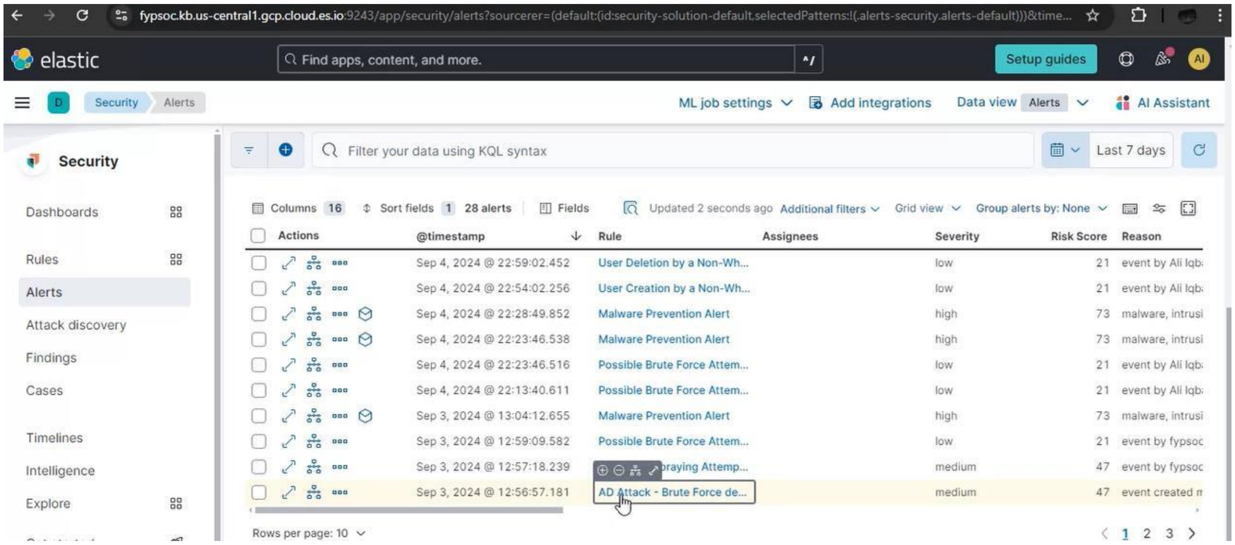
Severity levels

Levels	Count
● Low	14
● High	9

28 alerts

Alerts by name

Malware Prevention Alert	9
Possible Brute Force Attempt Detected	6
User Deletion by a Non-Whitelisted User Detected	4

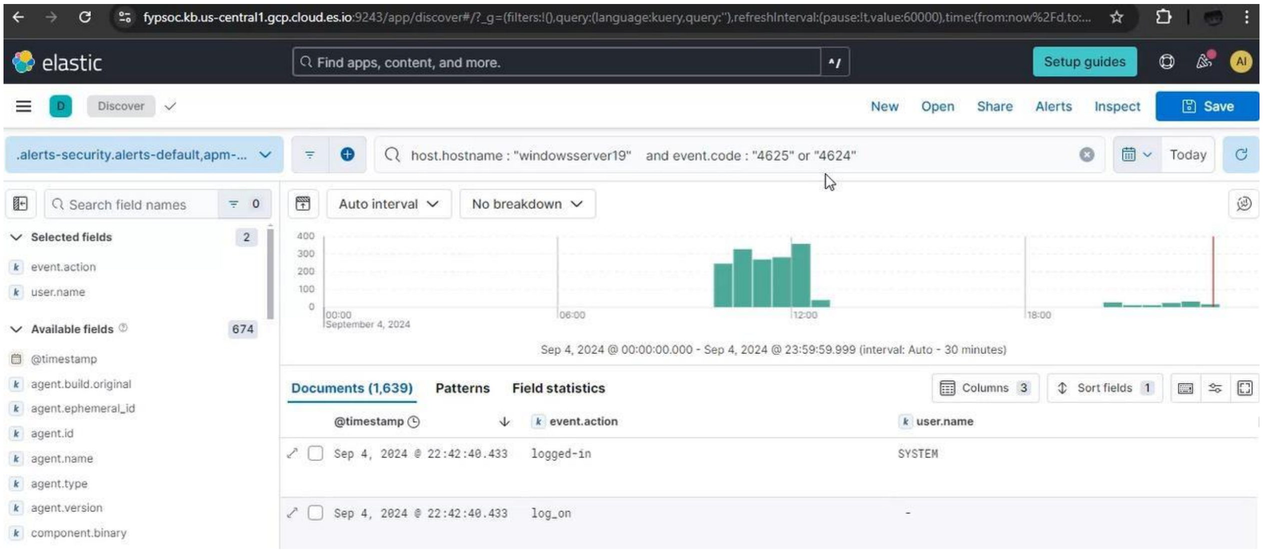


fypsoc.kb.us-central1.gcp.cloud.es.io:9243/app/security/alerts?sourcerer=(default:(id:security-solution-default,selectedPatterns:!(.alerts-security.alerts-default)))&time...

Columns 16 Sort fields 1 28 alerts Fields Updated 2 seconds ago Additional filters Grid view Group alerts by: None

Actions	@timestamp	Rule	Assignees	Severity	Risk Score	Reason
□	Sep 4, 2024 @ 22:59:02.452	User Deletion by a Non-Wh...		low	21	event by Ali Iqb
□	Sep 4, 2024 @ 22:54:02.256	User Creation by a Non-Wh...		low	21	event by Ali Iqb
□	Sep 4, 2024 @ 22:28:49.852	Malware Prevention Alert		high	73	malware, intrusi
□	Sep 4, 2024 @ 22:23:46.538	Malware Prevention Alert		high	73	malware, intrusi
□	Sep 4, 2024 @ 22:23:46.516	Possible Brute Force Attem...		low	21	event by Ali Iqb
□	Sep 4, 2024 @ 22:13:40.611	Possible Brute Force Attem...		low	21	event by Ali Iqb
□	Sep 3, 2024 @ 13:04:12.655	Malware Prevention Alert		high	73	malware, intrusi
□	Sep 3, 2024 @ 12:59:09.582	Possible Brute Force Attem...		low	21	event by fypsoc
□	Sep 3, 2024 @ 12:57:18.239	praying Attemp...		medium	47	event by fypsoc
□	Sep 3, 2024 @ 12:56:57.181	AD Attack - Brute Force de...		medium	47	event created n

Rows per page: 10 ‹ 1 2 3 ›



fypsoc.kb.us-central1.gcp.cloud.es.io:9243/app/discover#/?_g=(filters:!(),query:(language:kuery,query:''),refreshInterval:(pause:!t,value:60000),time:(from:now%2Fd,to:...

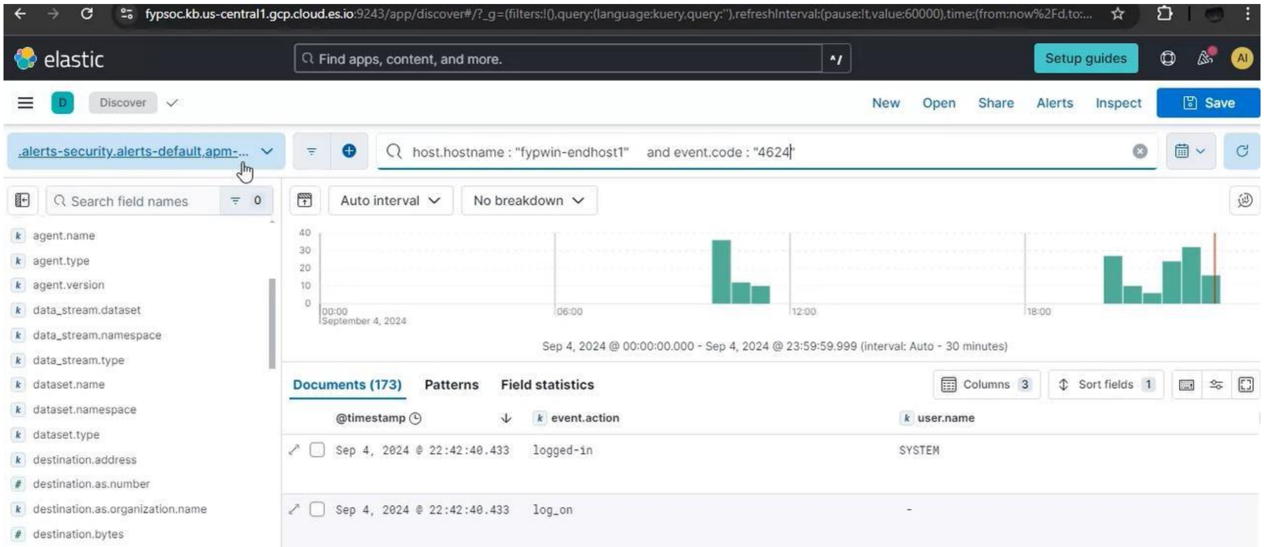
```
host.hostname : "windowsserver19"    and event.code : "4625" or "4624"
```

Selected fields 2
- event.action
- user.name

Available fields 674
- @timestamp
- agent.build.original
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- component.binary

Sep 4, 2024 @ 00:00:00.000 - Sep 4, 2024 @ 23:59:59.999 (interval: Auto - 30 minutes)

@timestamp	event.action	user.name
Sep 4, 2024 @ 22:42:40.433	logged-in	SYSTEM
Sep 4, 2024 @ 22:42:40.433	log_on	-



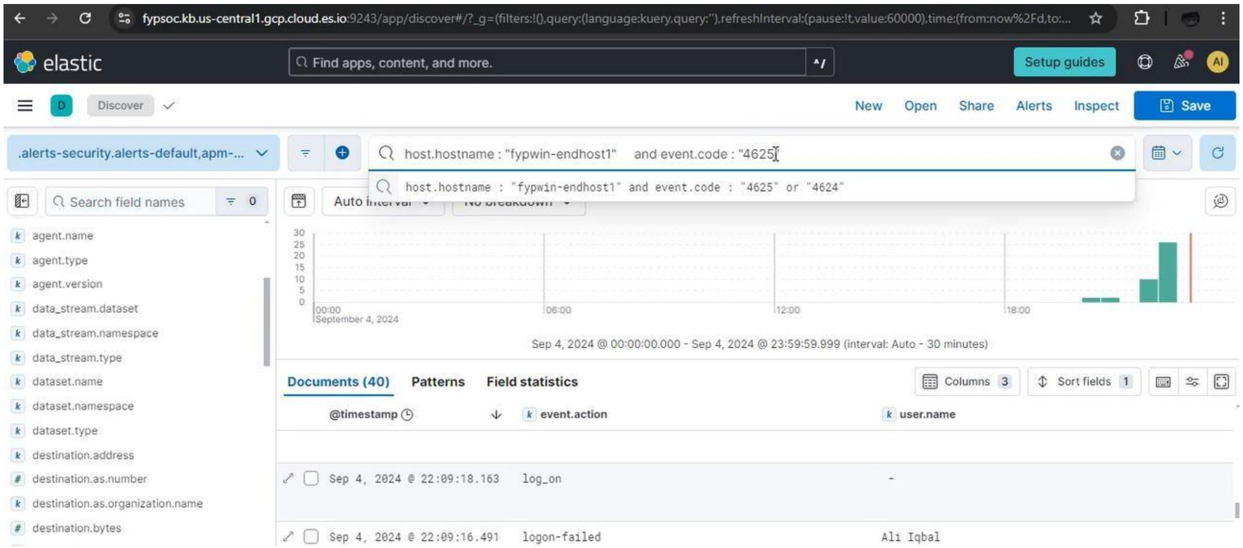
fypsoc.kb.us-central1.gcp.cloud.es.io:9243/app/discover#/?_g=(filters:!(),query:(language:kuery,query:''),refreshInterval:(pause:!t,value:60000),time:(from:now%2Fd,to:...

```
host.hostname : "fypwin-endhost1"    and event.code : "4624"
```

- agent.name
- agent.type
- agent.version
- data_stream.dataset
- data_stream.namespace
- data_stream.type
- dataset.name
- dataset.namespace
- dataset.type
- destination.address
- destination.as.number
- destination.as.organization.name
- destination.bytes

Sep 4, 2024 @ 00:00:00.000 - Sep 4, 2024 @ 23:59:59.999 (interval: Auto - 30 minutes)

@timestamp	event.action	user.name
Sep 4, 2024 @ 22:42:40.433	logged-in	SYSTEM
Sep 4, 2024 @ 22:42:40.433	log_on	-



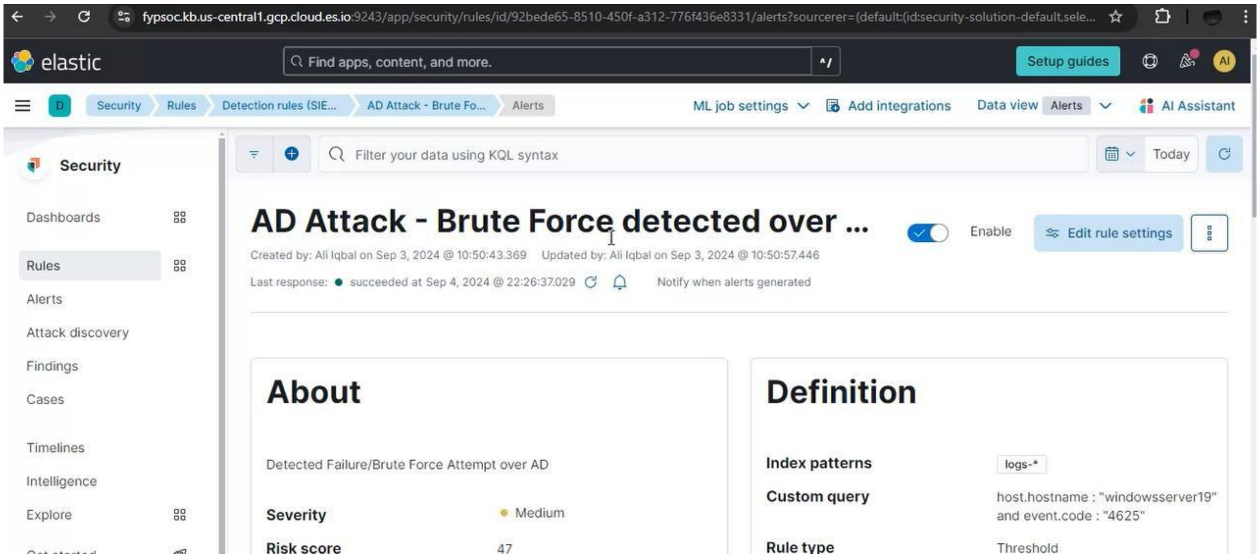
fypsoc.kb.us-central1.gcp.cloud.es.io:9243/app/discover#/?_g=(filters:!(),query:(language:kuery,query:''),refreshInterval:(pause:!t,value:60000),time:(from:now%2Fd,to:...

```
host.hostname : "fypwin-endhost1"    and event.code : "4625"
host.hostname : "fypwin-endhost1" and event.code : "4625" or "4624"
```

- agent.name
- agent.type
- agent.version
- data_stream.dataset
- data_stream.namespace
- data_stream.type
- dataset.name
- dataset.namespace
- dataset.type
- destination.address
- destination.as.number
- destination.as.organization.name
- destination.bytes

Sep 4, 2024 @ 00:00:00.000 - Sep 4, 2024 @ 23:59:59.999 (interval: Auto - 30 minutes)

@timestamp	event.action	user.name
Sep 4, 2024 @ 22:09:18.163	log_on	-
Sep 4, 2024 @ 22:09:16.491	logon-failed	Ali Iqbal



AD Attack - Brute Force detected over ...

Created by: Ali Iqbal on Sep 3, 2024 @ 10:50:43.369 Updated by: Ali Iqbal on Sep 3, 2024 @ 10:50:57.446

Last response: ● succeeded at Sep 4, 2024 @ 22:26:37.029 Notify when alerts generated

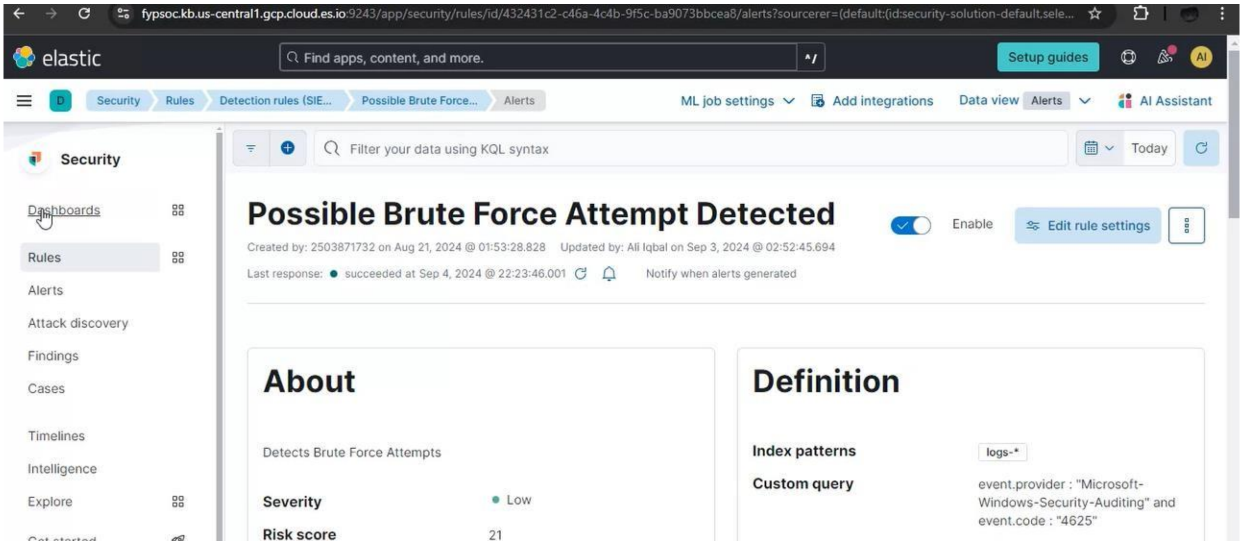
About

Detected Failure/Brute Force Attempt over AD

Severity	● Medium
Risk score	47

Definition

Index patterns	logs-*
Custom query	host.hostname : "windowsserver19" and event.code : "4625"
Rule type	Threshold



Possible Brute Force Attempt Detected

Created by: 2503871732 on Aug 21, 2024 @ 01:53:28.828 Updated by: Ali Iqbal on Sep 3, 2024 @ 02:52:45.694

Last response: ● succeeded at Sep 4, 2024 @ 22:23:46.001 Notify when alerts generated

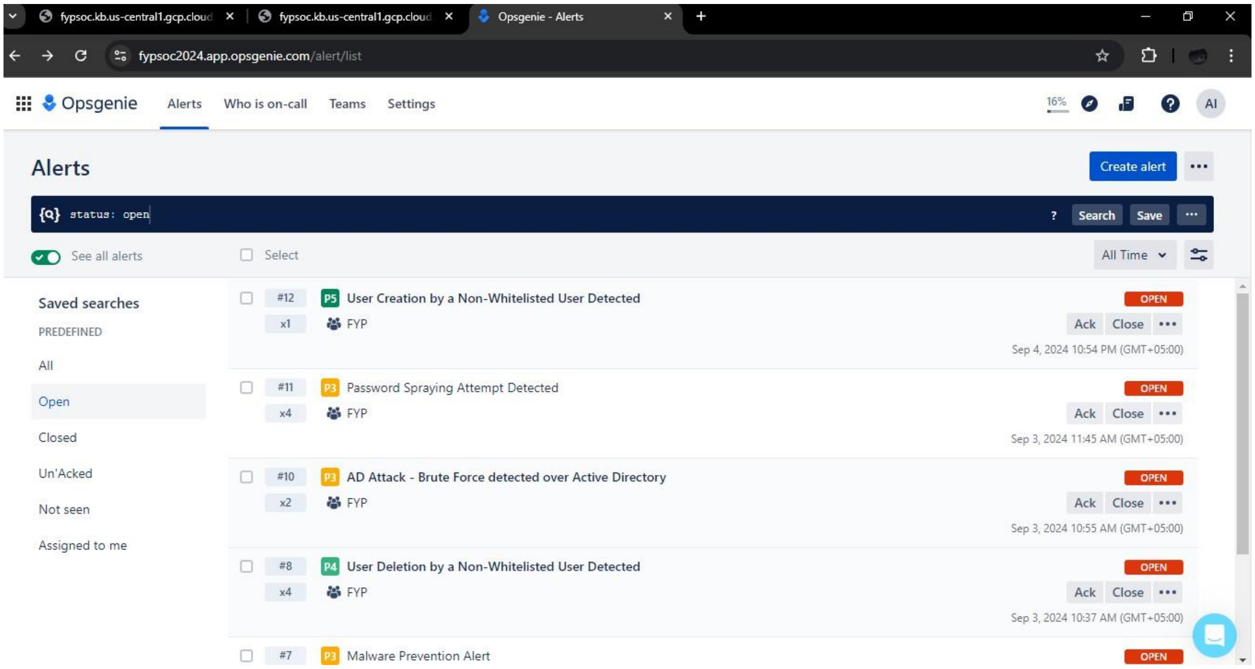
About

Detects Brute Force Attempts

Severity	● Low
Risk score	21

Definition

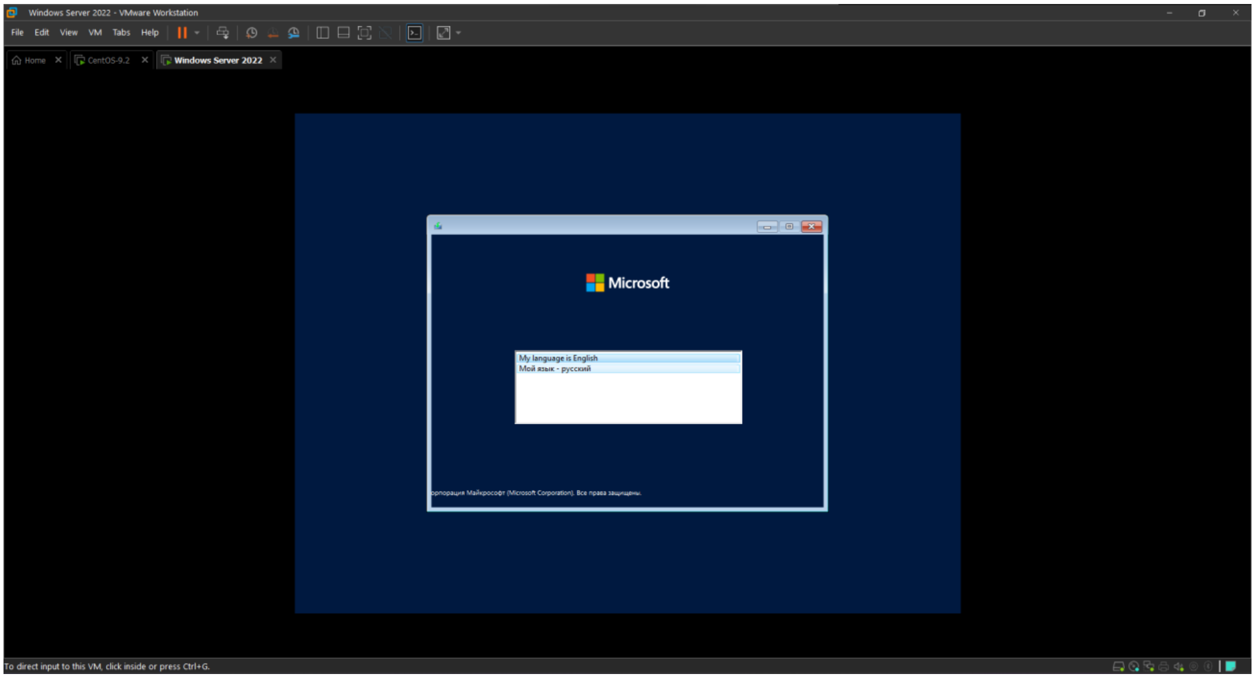
Index patterns	logs-*
Custom query	event.provider : "Microsoft-Windows-Security-Auditing" and event.code : "4625"



Alerts

status: open

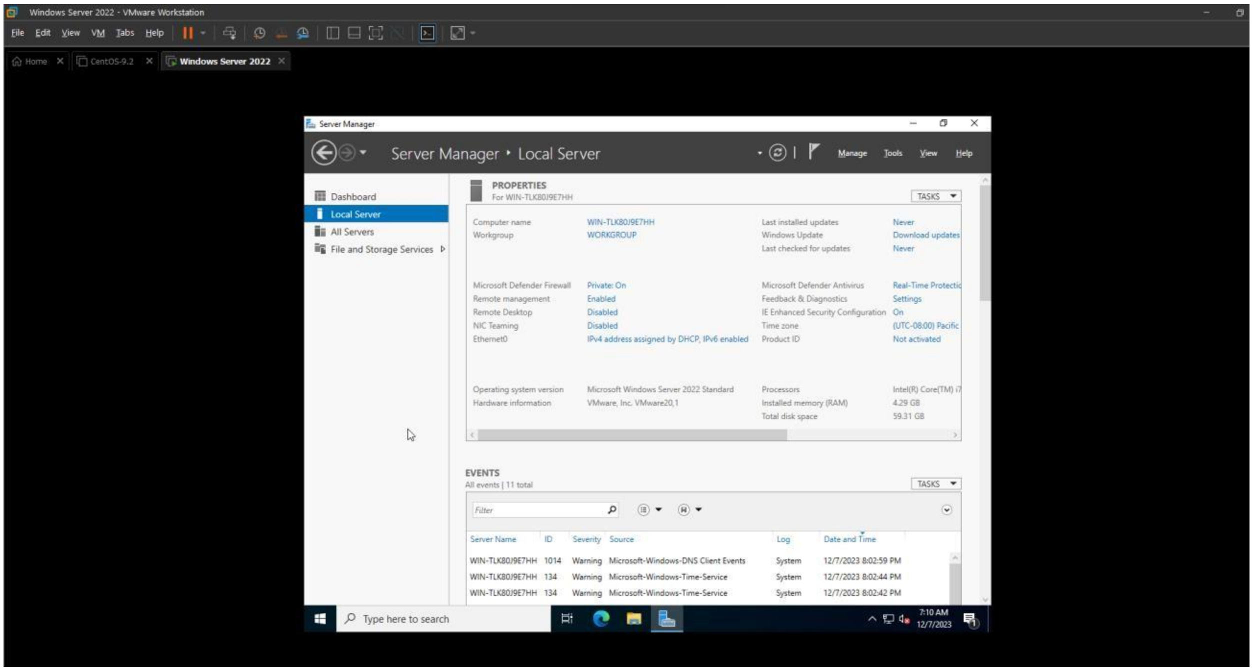
#12 x1	P5	User Creation by a Non-Whitelisted User Detected FYP	OPEN Ack Close Sep 4, 2024 10:54 PM (GMT+05:00)
#11 x4	P3	Password Spraying Attempt Detected FYP	OPEN Ack Close Sep 3, 2024 11:45 AM (GMT+05:00)
#10 x2	P3	AD Attack - Brute Force detected over Active Directory FYP	OPEN Ack Close Sep 3, 2024 10:55 AM (GMT+05:00)
#8 x4	P4	User Deletion by a Non-Whitelisted User Detected FYP	OPEN Ack Close Sep 3, 2024 10:37 AM (GMT+05:00)
#7	P3	Malware Prevention Alert	OPEN


Windows Server 2022 - VMware Workstation
File Edit View VM Tabs Help
Home
CentOS-9.2
Windows Server 2022
Microsoft

My language is English
Мой язык - русский

орпорация Майкрософт (Microsoft Corporation). Все права защищены.

To direct input to this VM, click inside or press Ctrl+G.

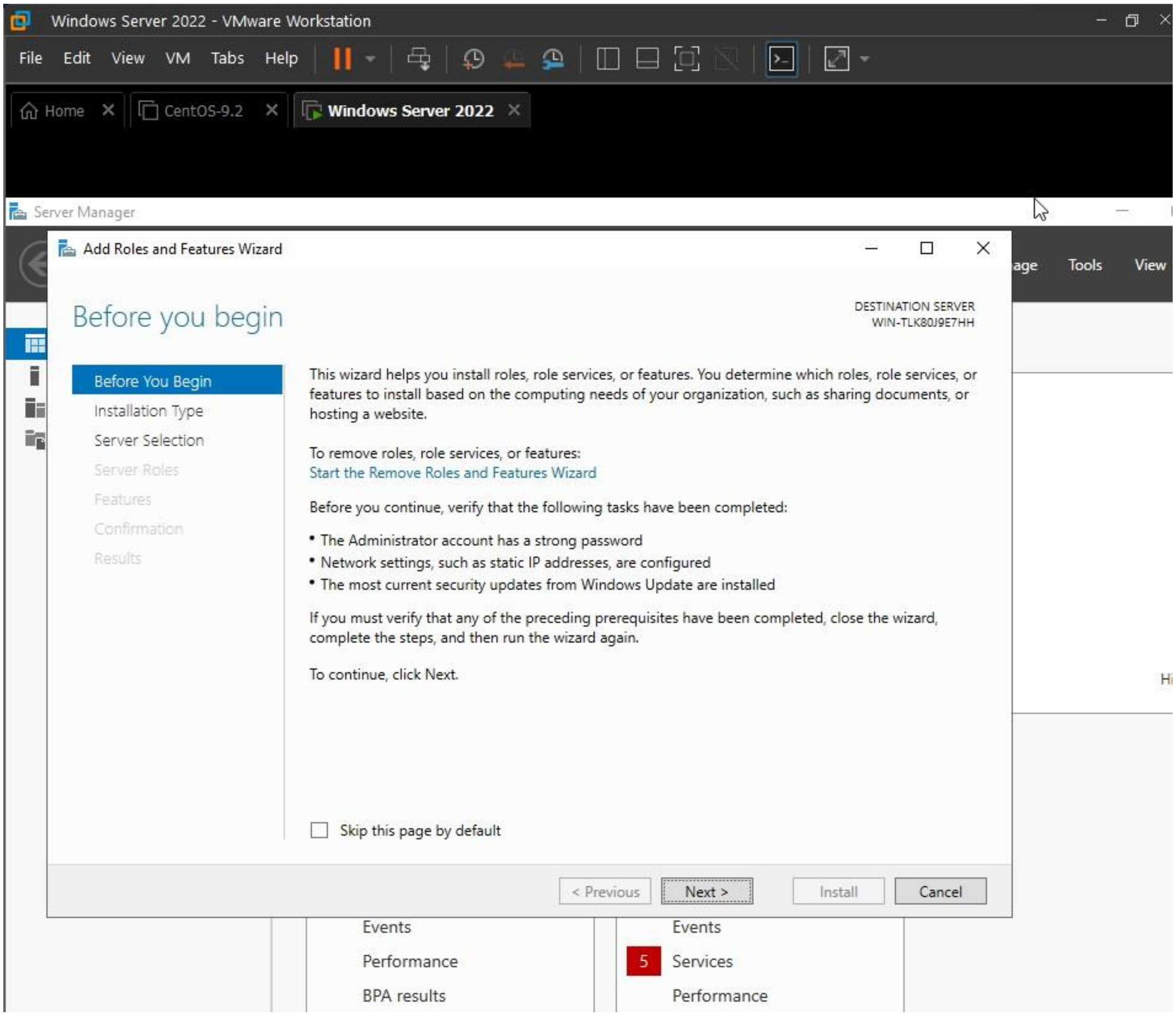


PROPERTIES
For WIN-TLK80J9E7HH

Computer name	WIN-TLK80J9E7HH	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Download updates
		Last checked for updates	Never
Microsoft Defender Firewall	Private: On	Microsoft Defender Antivirus	Real-Time Protectic
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:00) Pacific
Ethernet0	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	Not activated
Operating system version	Microsoft Windows Server 2022 Standard	Processors	Intel(R) Core(TM) i7
Hardware information	VMware, Inc. VMware20,1	Installed memory (RAM)	4.29 GB
		Total disk space	59.31 GB

EVENTS
All events | 11 total

Server Name	ID	Severity	Source	Log	Date and Time
WIN-TLK80J9E7HH	1014	Warning	Microsoft-Windows-DNS Client Events	System	12/7/2023 8:02:59 PM
WIN-TLK80J9E7HH	134	Warning	Microsoft-Windows-Time-Service	System	12/7/2023 8:02:44 PM
WIN-TLK80J9E7HH	134	Warning	Microsoft-Windows-Time-Service	System	12/7/2023 8:02:42 PM



Before you begin

DESTINATION SERVER
WIN-TLK80J9E7HH

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

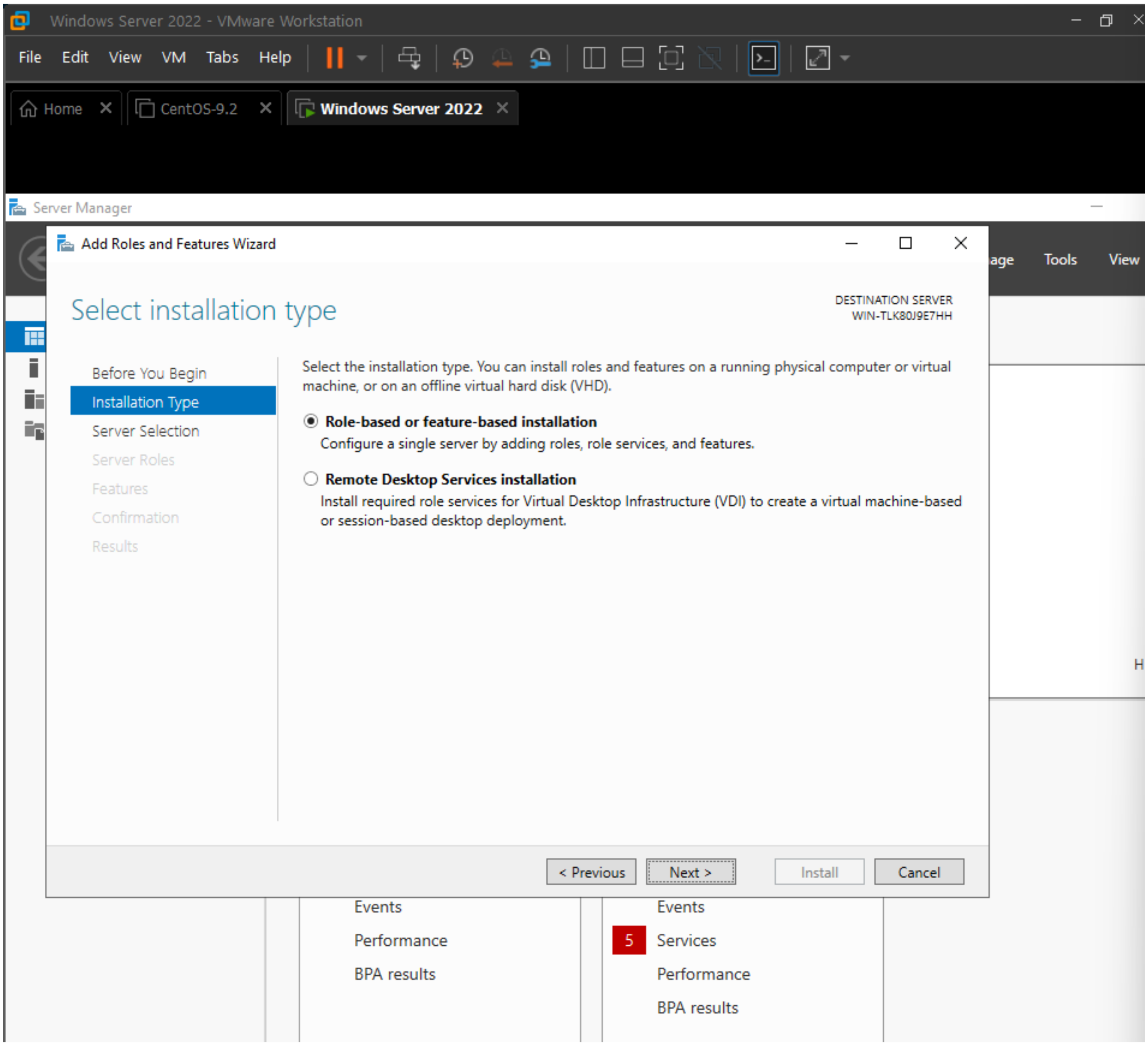
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

< Previous | Next > | Install | Cancel



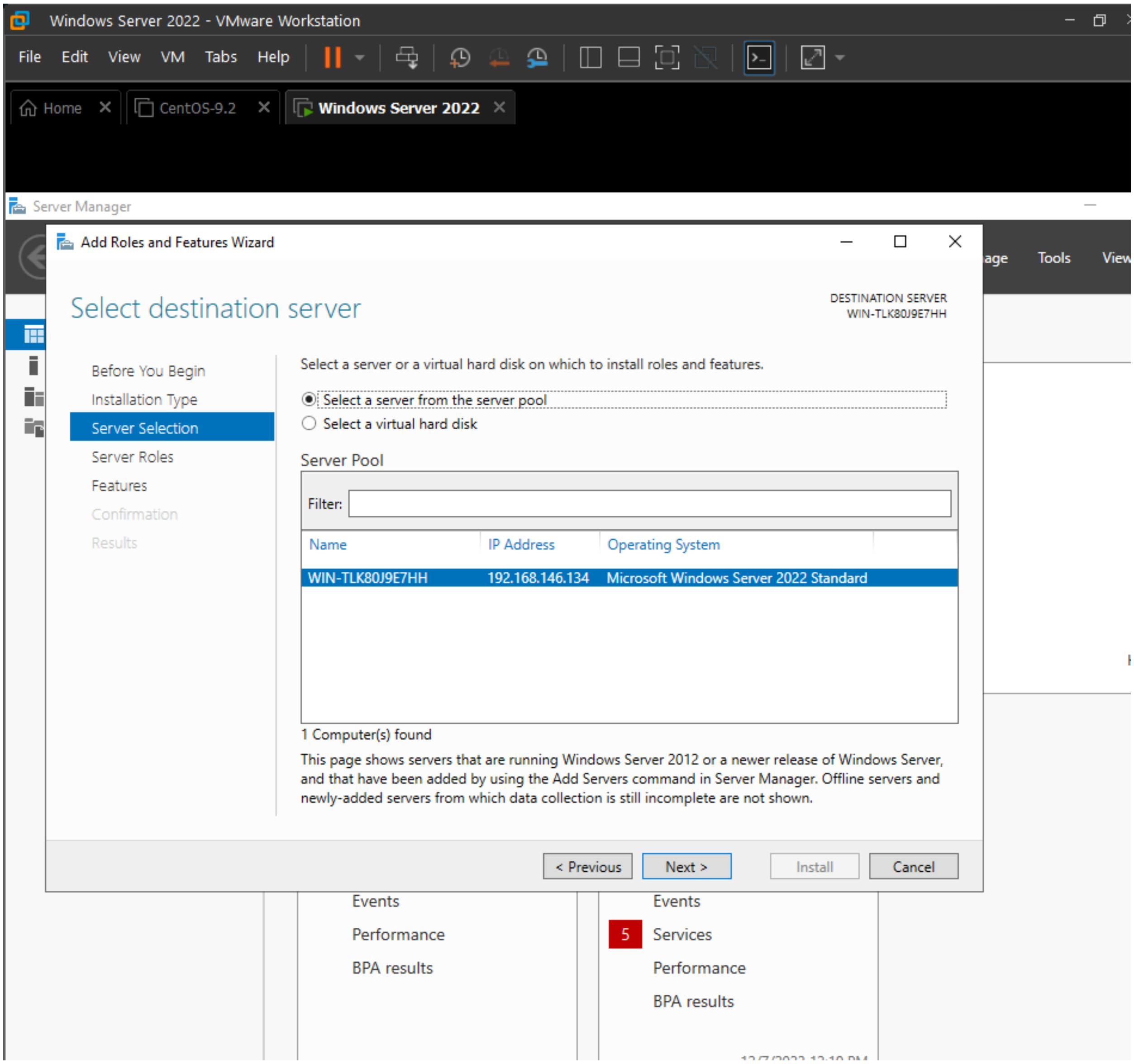
Select installation type

DESTINATION SERVER
WIN-TLK80J9E7HH

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.



Select destination server

DESTINATION SERVER
WIN-TLK80J9E7HH

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool

○ Select a virtual hard disk

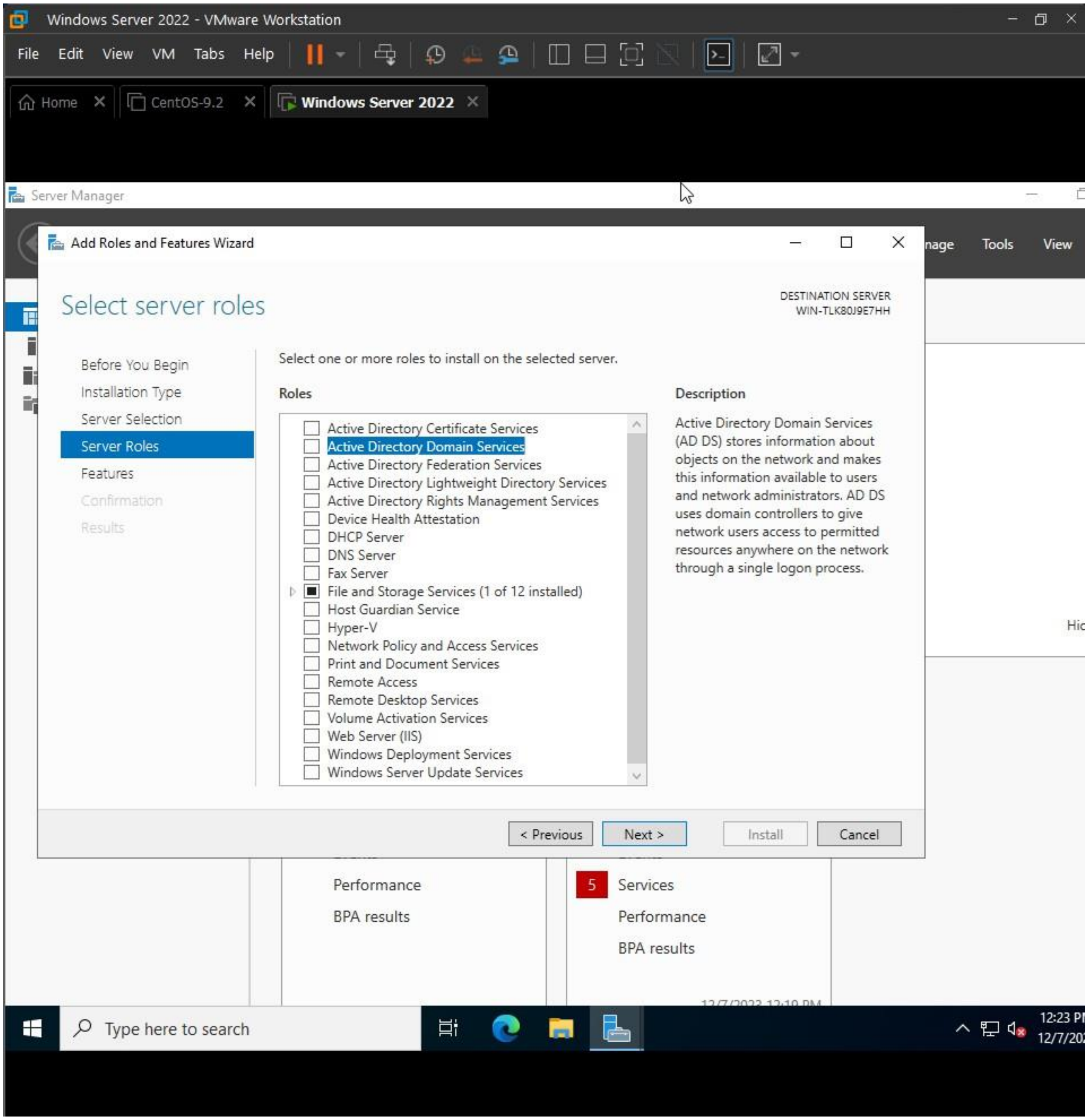
Server Pool

Filter:

Name	IP Address	Operating System
WIN-TLK80J9E7HH	192.168.146.134	Microsoft Windows Server 2022 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-TLK80J9E7HH

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select one or more roles to install on the selected server.

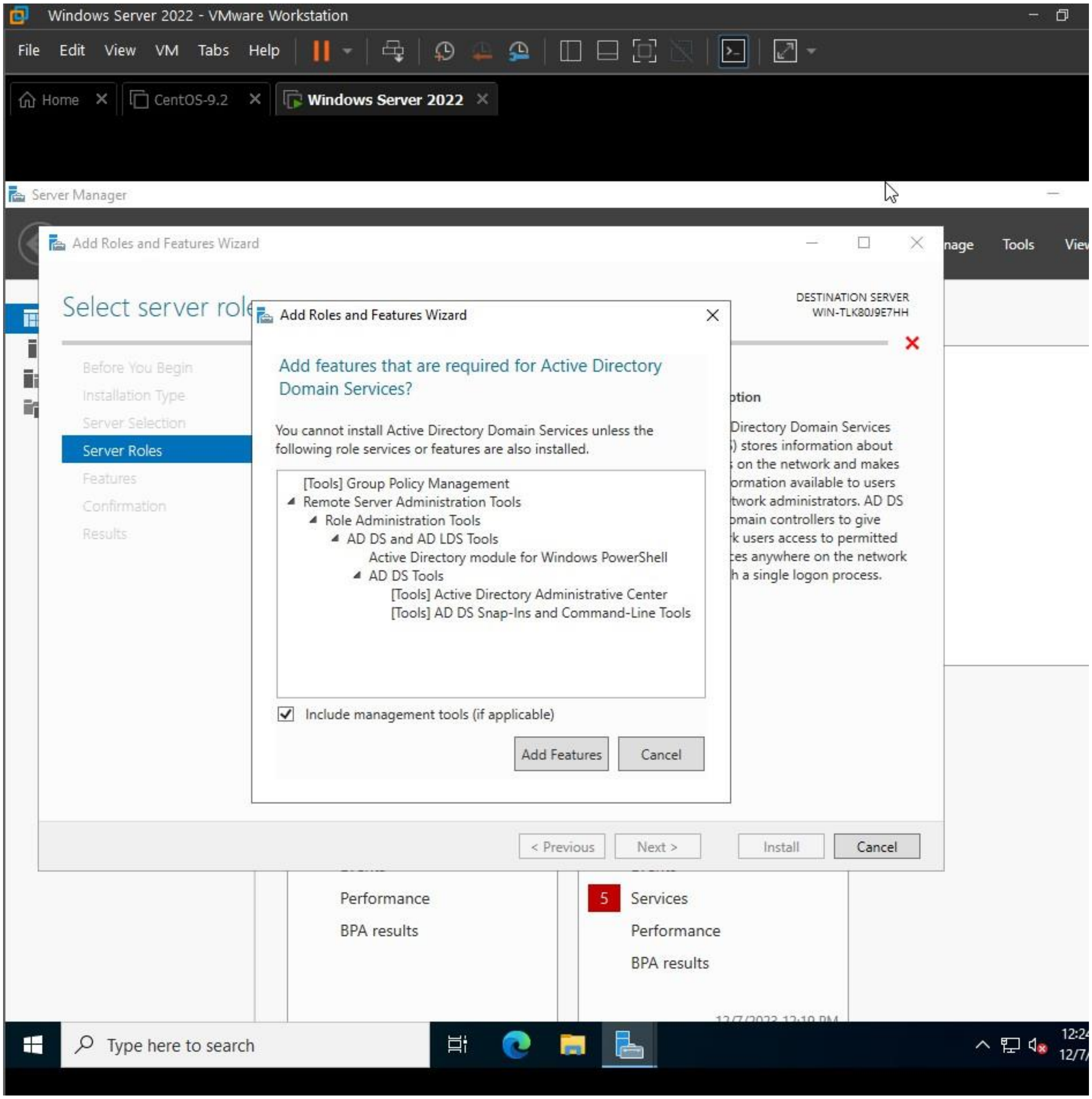
Roles

□ Active Directory Certificate Services
□ Active Directory Domain Services
□ Active Directory Federation Services
□ Active Directory Lightweight Directory Services
□ Active Directory Rights Management Services
□ Device Health Attestation
□ DHCP Server
□ DNS Server
□ Fax Server
■ File and Storage Services (1 of 12 installed)
□ Host Guardian Service
□ Hyper-V
□ Network Policy and Access Services
□ Print and Document Services
□ Remote Access
□ Remote Desktop Services
□ Volume Activation Services
□ Web Server (IIS)
□ Windows Deployment Services
□ Windows Server Update Services

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

< Previous | Next > | Install | Cancel



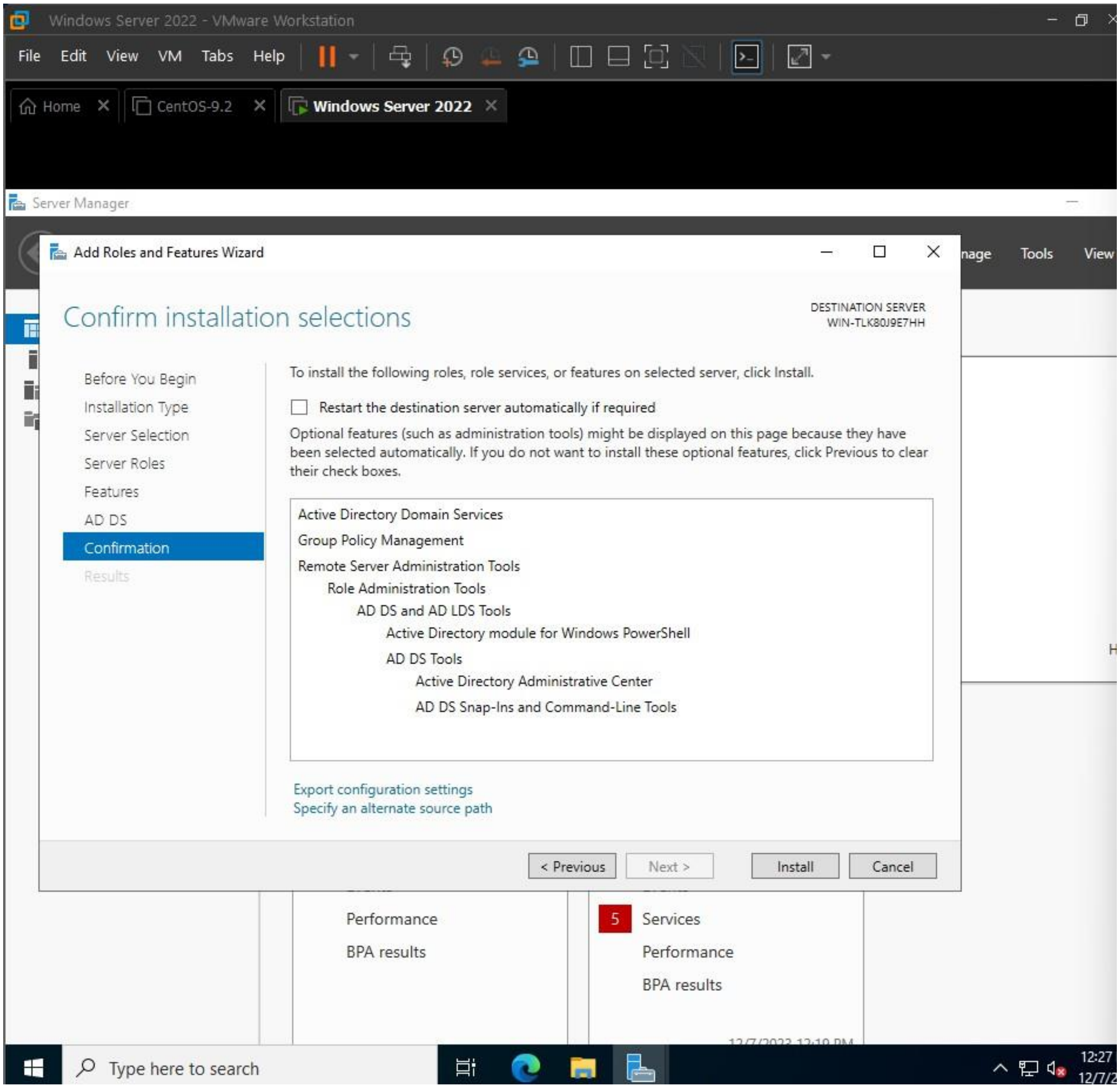
Add Roles and Features Wizard

Add features that are required for Active Directory Domain Services?

You cannot install Active Directory Domain Services unless the following role services or features are also installed.

```
[Tools] Group Policy Management
◢ Remote Server Administration Tools
  ◢ Role Administration Tools
    ◢ AD DS and AD LDS Tools
        Active Directory module for Windows PowerShell
      ◢ AD DS Tools
          [Tools] Active Directory Administrative Center
          [Tools] AD DS Snap-Ins and Command-Line Tools
```

☑ Include management tools (if applicable)


Windows Server 2022 - VMware Workstation
File Edit View VM Tabs Help
Home
CentOS-9.2
Windows Server 2022
Server Manager
nage Tools View

Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
WIN-TLK80J9E7HH

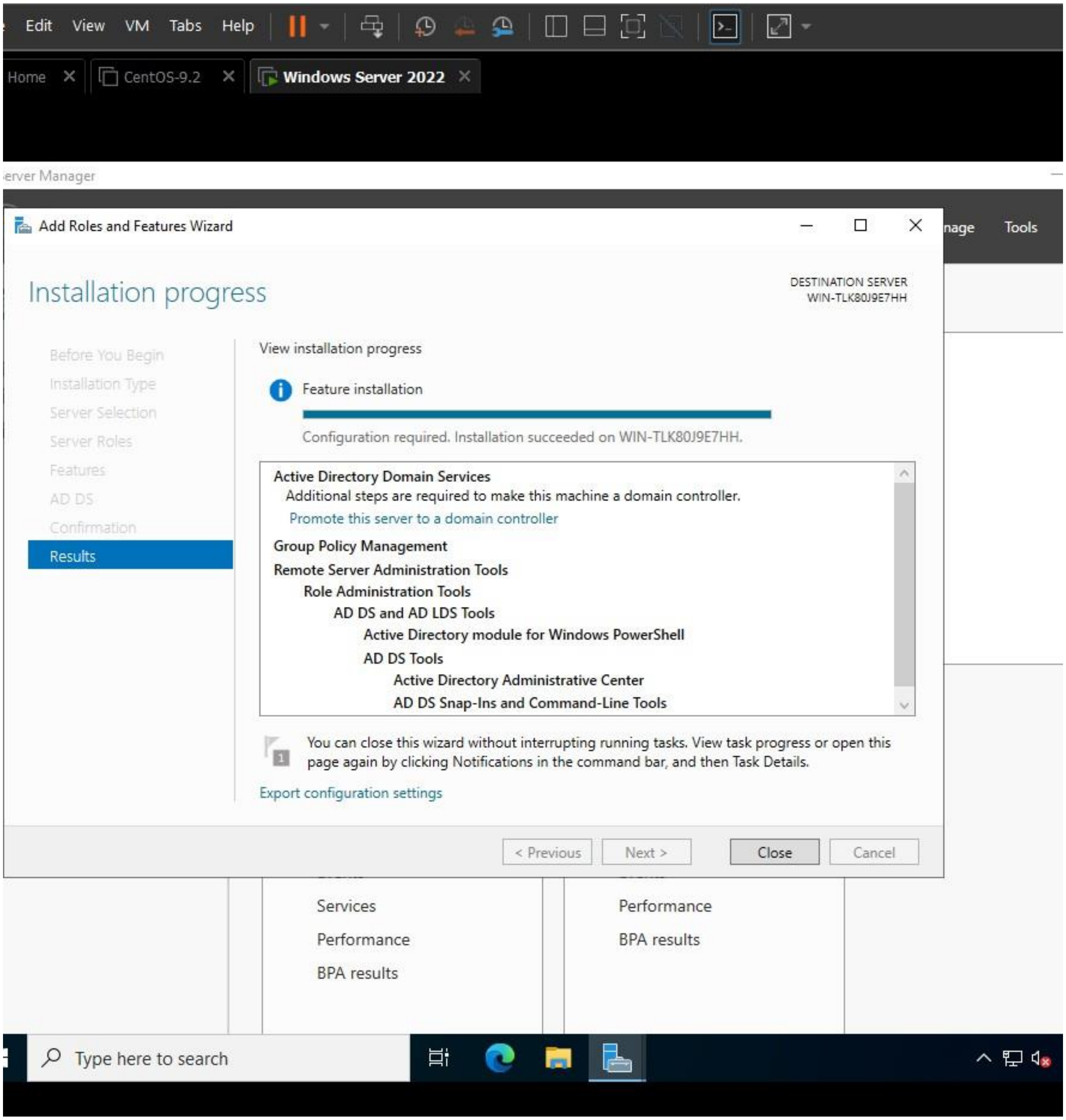
To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

```
Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
    Role Administration Tools
        AD DS and AD LDS Tools
            Active Directory module for Windows PowerShell
            AD DS Tools
                Active Directory Administrative Center
                AD DS Snap-Ins and Command-Line Tools
```

Export configuration settings
Specify an alternate source path



Installation progress

DESTINATION SERVER
WIN-TLK80J9E7HH

View installation progress

Feature installation

Configuration required. Installation succeeded on WIN-TLK80J9E7HH.

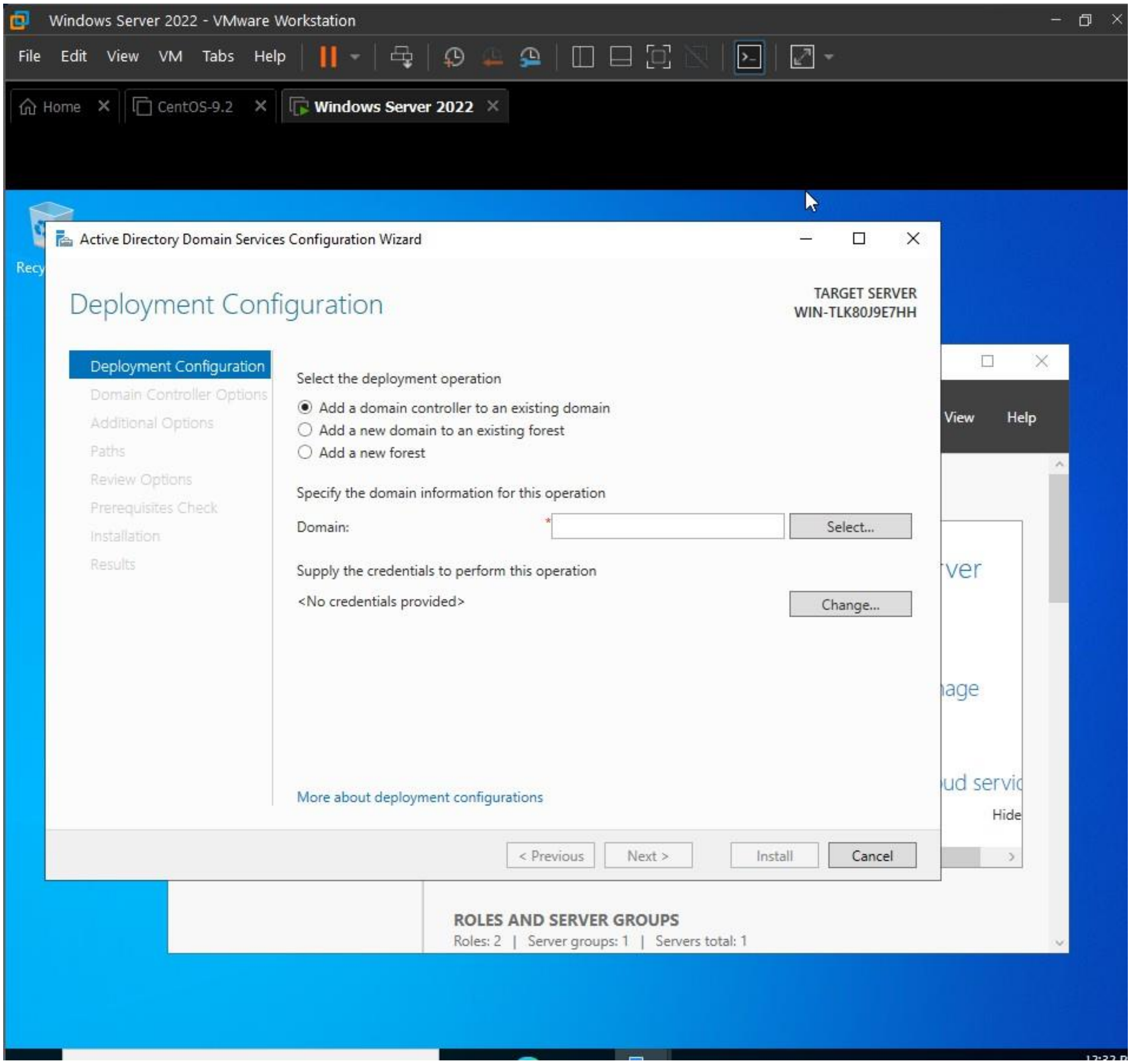
Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller

Group Policy Management

Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings



Deployment Configuration

TARGET SERVER
WIN-TLK80J9E7HH

Select the deployment operation

● Add a domain controller to an existing domain
○ Add a new domain to an existing forest
○ Add a new forest

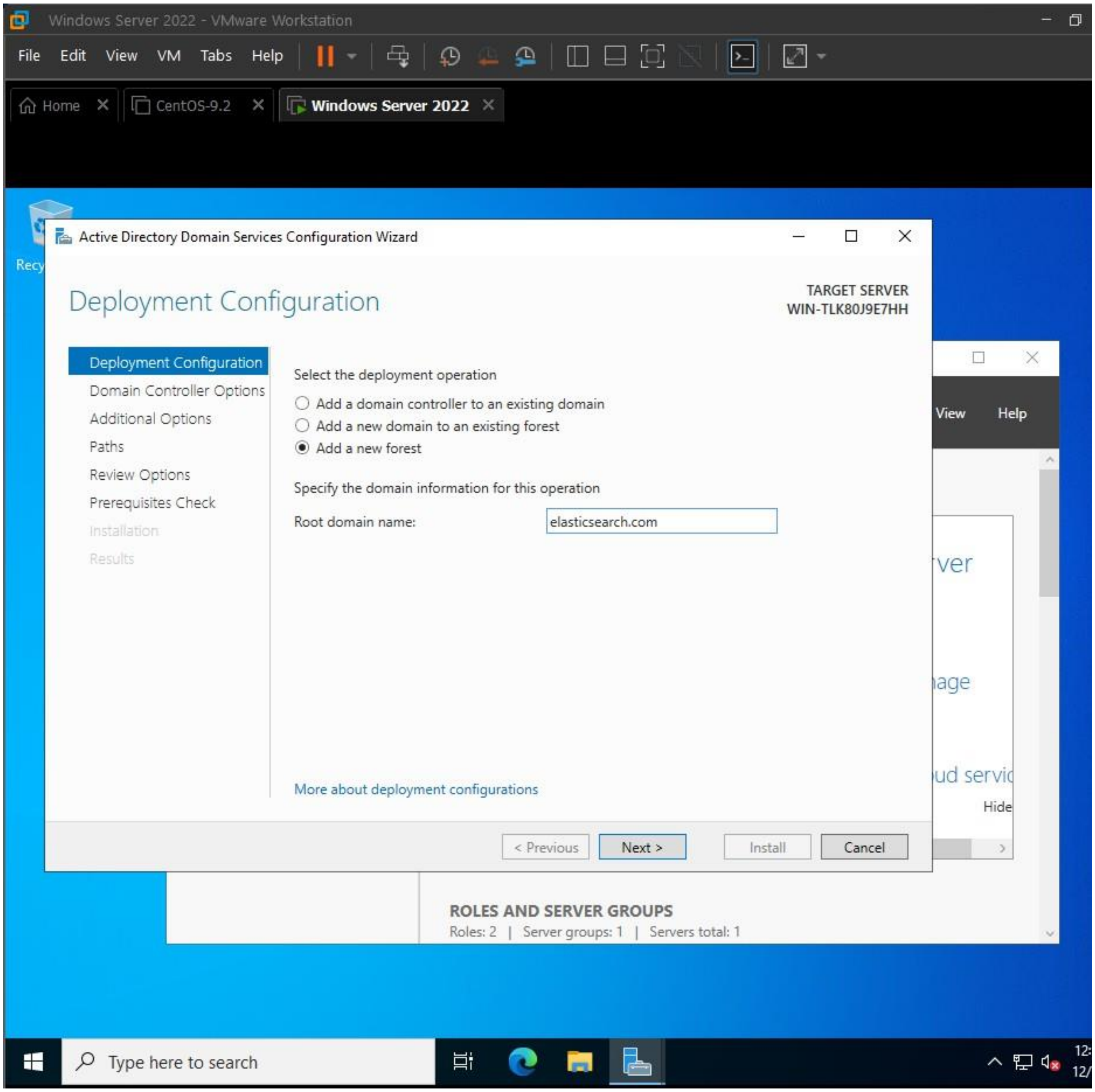
Specify the domain information for this operation

Domain: *

Supply the credentials to perform this operation

<No credentials provided>

ROLES AND SERVER GROUPS
Roles: 2 | Server groups: 1 | Servers total: 1



Deployment Configuration

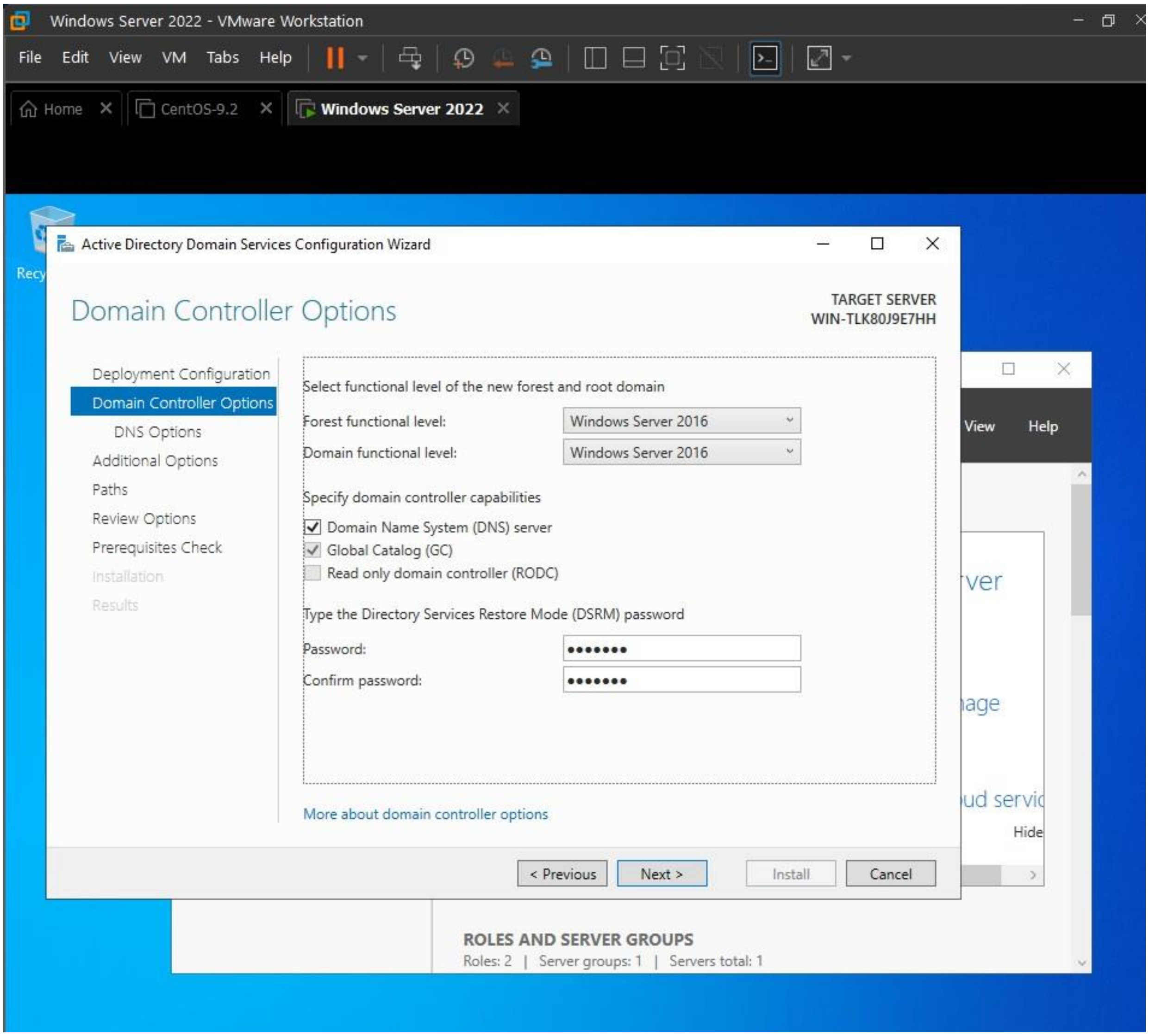
TARGET SERVER
WIN-TLK80J9E7HH

Select the deployment operation

○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

Specify the domain information for this operation

Root domain name: elasticsearch.com



Domain Controller Options

TARGET SERVER
WIN-TLK80J9E7HH

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

☑ Domain Name System (DNS) server

☑ Global Catalog (GC)

□ Read only domain controller (RODC)

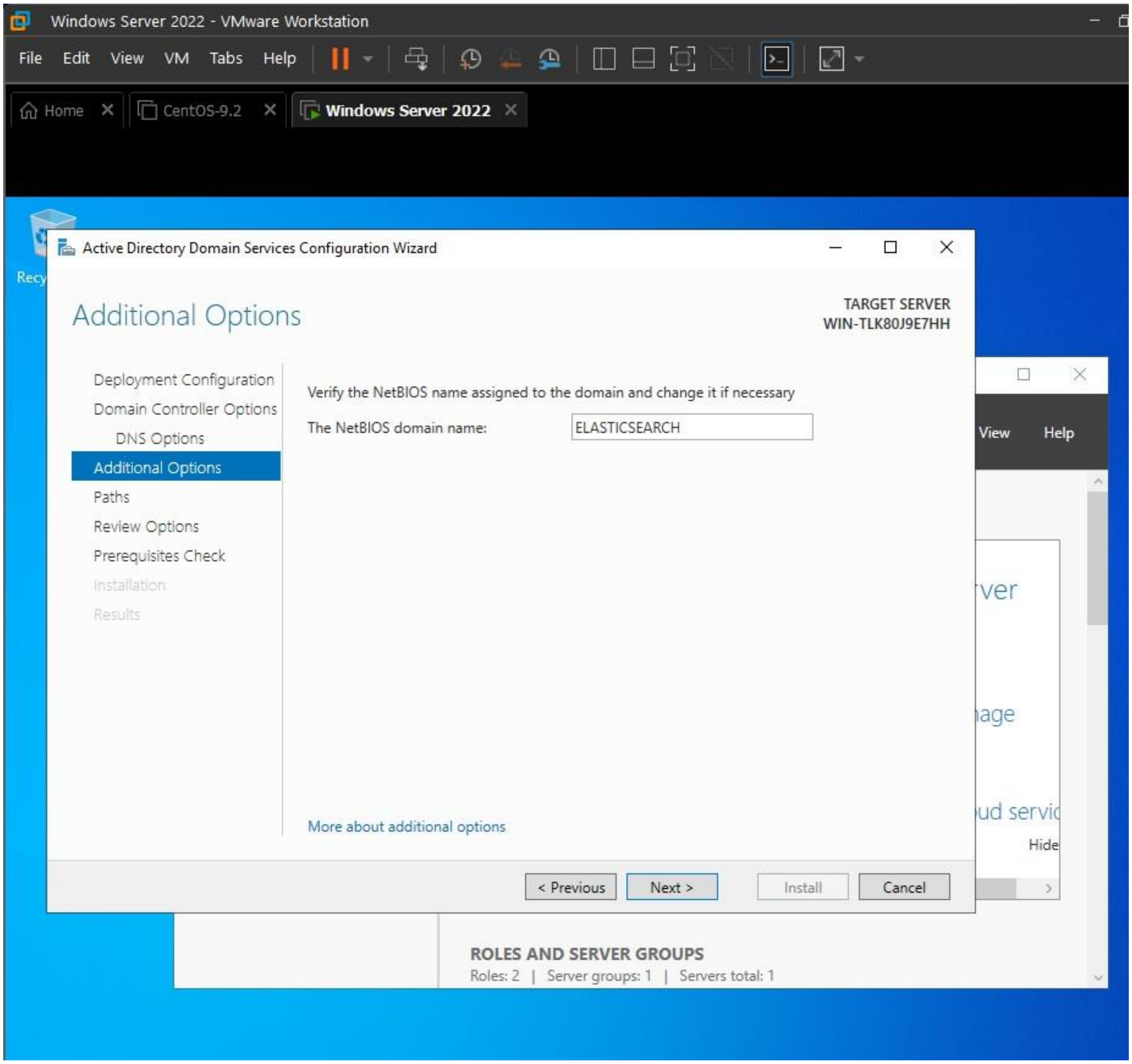
Type the Directory Services Restore Mode (DSRM) password

Password: •••••••

Confirm password: •••••••

More about domain controller options

ROLES AND SERVER GROUPS
Roles: 2 | Server groups: 1 | Servers total: 1



Windows Server 2022 - VMware Workstation
File Edit View VM Tabs Help
Home
CentOS-9.2
Windows Server 2022
Active Directory Domain Services Configuration Wizard

Additional Options

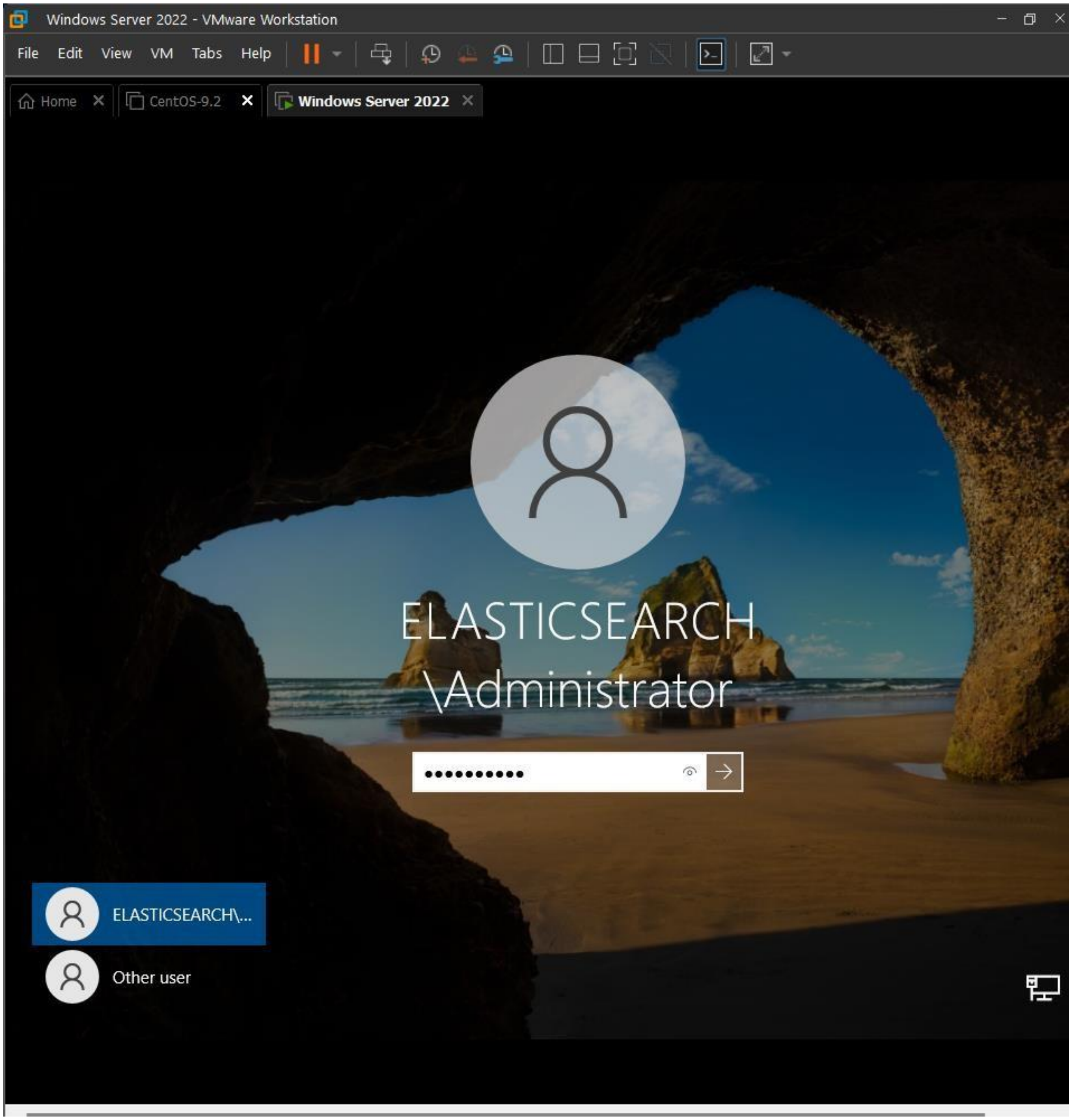
TARGET SERVER
WIN-TLK80J9E7HH

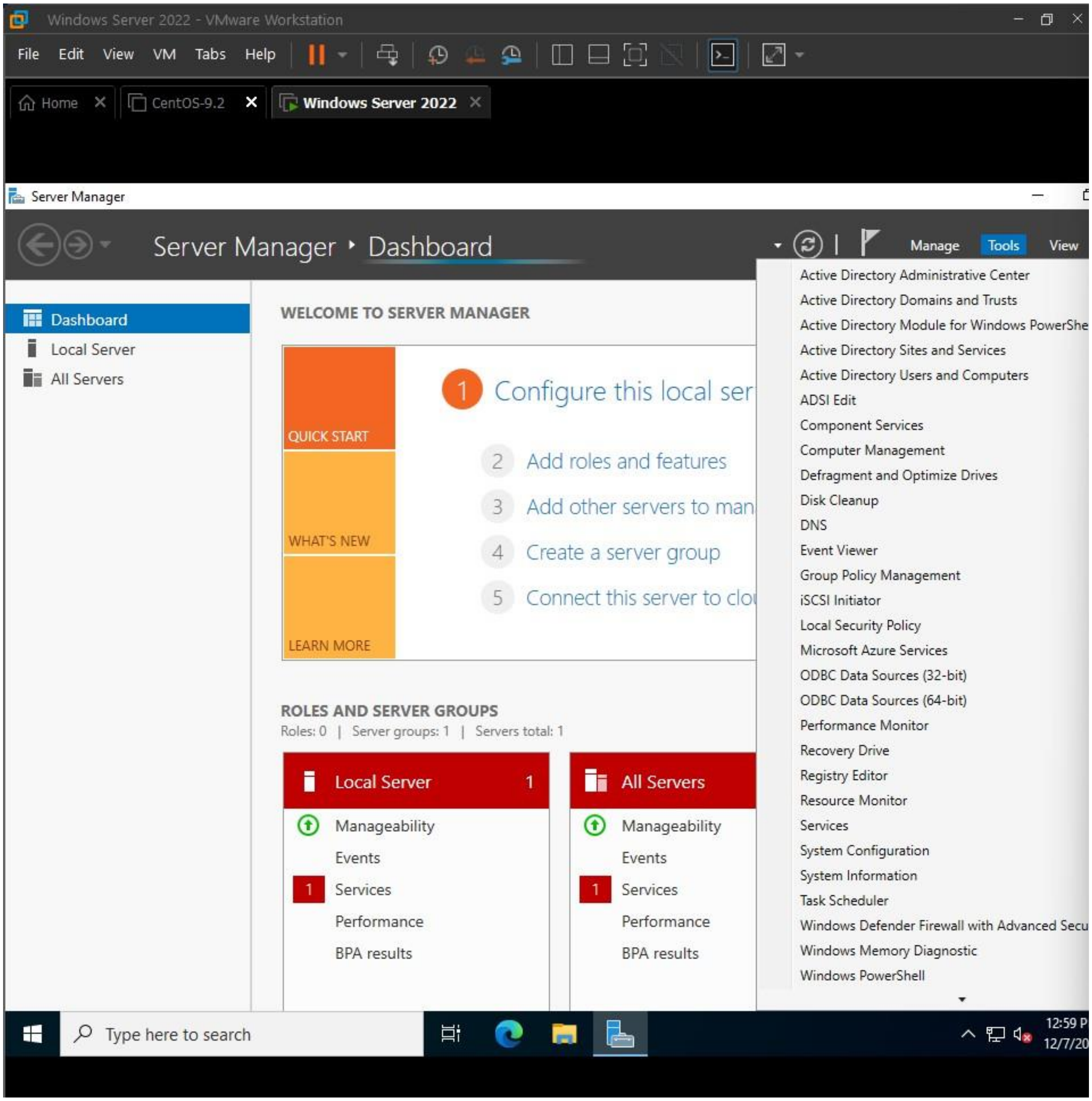
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

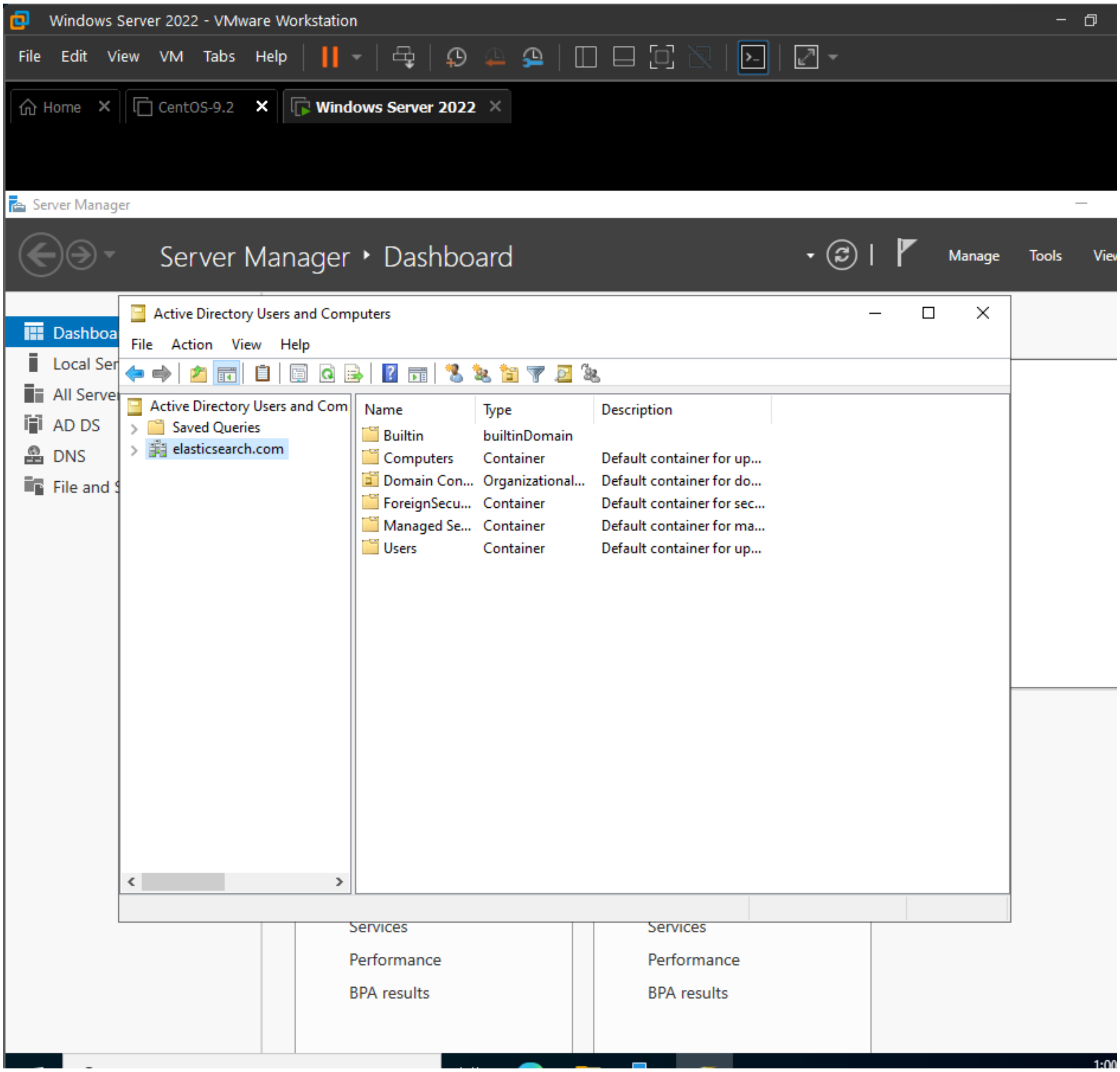
Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name: ELASTICSEARCH

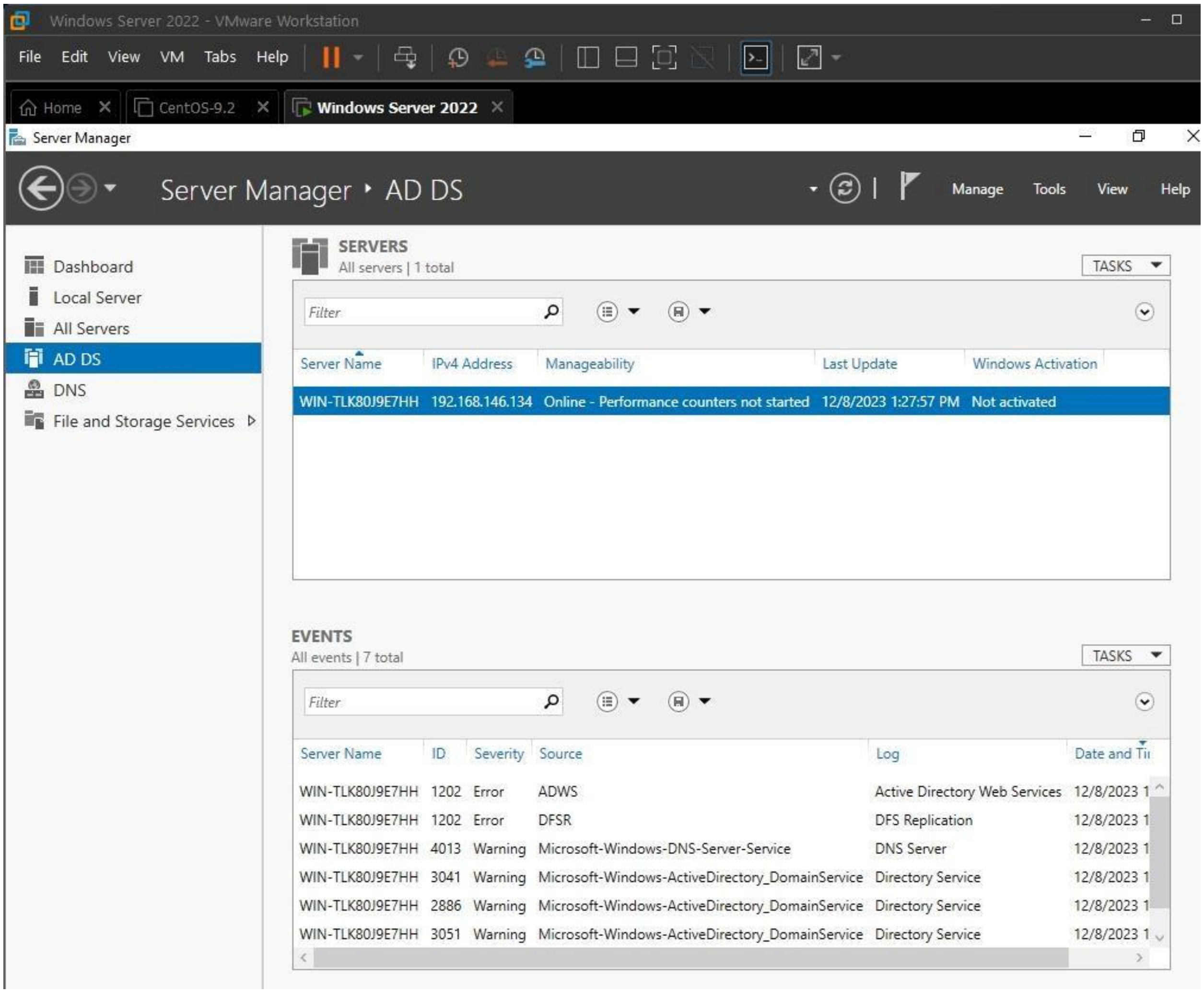
More about additional options
< Previous
Next >
Install
Cancel
View
Help
ROLES AND SERVER GROUPS
Roles: 2 | Server groups: 1 | Servers total: 1


Windows Server 2022 - VMware Workstation
File
Edit
View
VM
Tabs
Help
Home
CentOS-9.2
Windows Server 2022
ELASTICSEARCH
\Administrator
•••••••••••
ELASTICSEARCH\...
Other user


Windows Server 2022 - VMware Workstation
File
Edit
View
VM
Tabs
Help
Home
CentOS-9.2
Windows Server 2022
Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Dashboard
Local Server
All Servers
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local ser
2 Add roles and features
3 Add other servers to man
4 Create a server group
5 Connect this server to clo
ROLES AND SERVER GROUPS
Roles: 0 | Server groups: 1 | Servers total: 1
Local Server 1
Manageability
Events
1 Services
Performance
BPA results
All Servers
Manageability
Events
1 Services
Performance
BPA results
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShe
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Recovery Drive
Registry Editor
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Defender Firewall with Advanced Secu
Windows Memory Diagnostic
Windows PowerShell
Type here to search
12:59 P
12/7/20



Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
Users	Container	Default container for up...

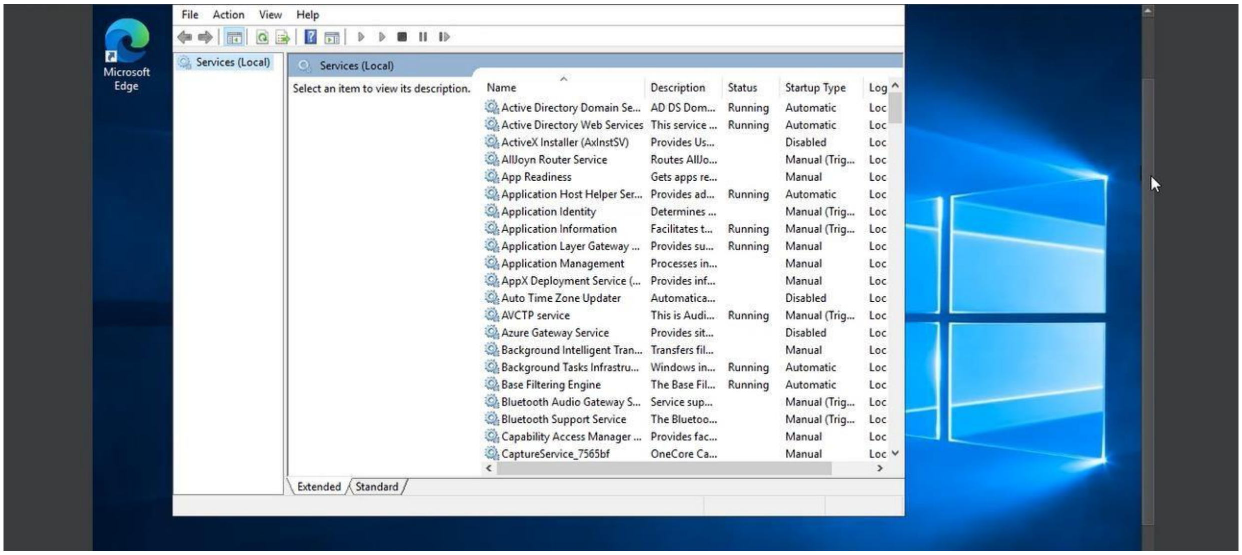


SERVERS
All servers | 1 total

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
WIN-TLK80J9E7HH	192.168.146.134	Online - Performance counters not started	12/8/2023 1:27:57 PM	Not activated

EVENTS
All events | 7 total

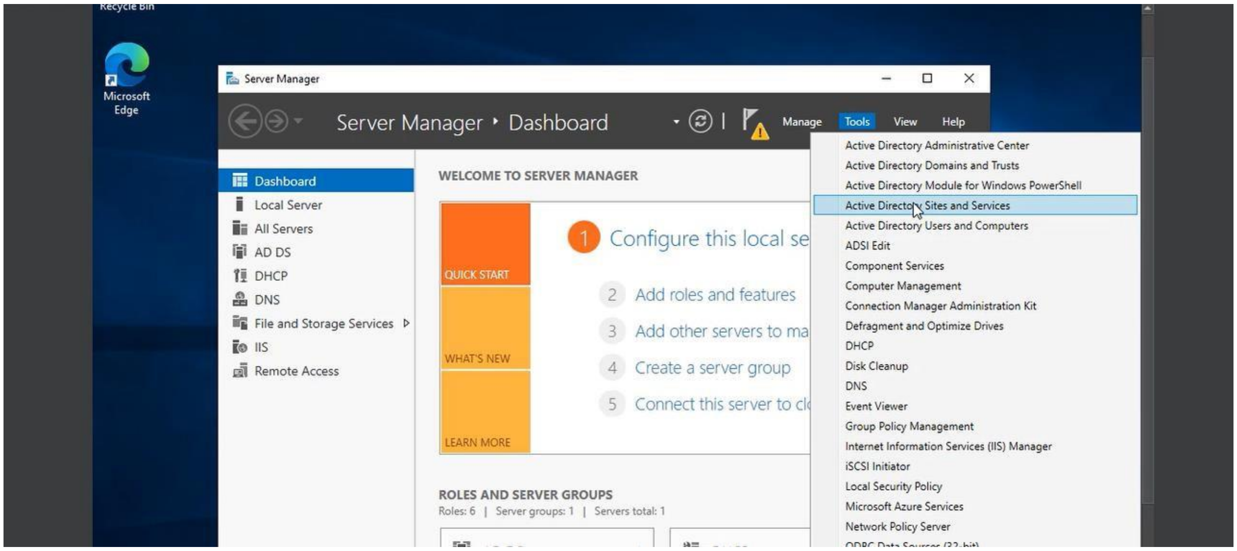
Server Name	ID	Severity	Source	Log	Date and Ti
WIN-TLK80J9E7HH	1202	Error	ADWS	Active Directory Web Services	12/8/2023 1
WIN-TLK80J9E7HH	1202	Error	DFSR	DFS Replication	12/8/2023 1
WIN-TLK80J9E7HH	4013	Warning	Microsoft-Windows-DNS-Server-Service	DNS Server	12/8/2023 1
WIN-TLK80J9E7HH	3041	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	12/8/2023 1
WIN-TLK80J9E7HH	2886	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	12/8/2023 1
WIN-TLK80J9E7HH	3051	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	12/8/2023 1



Services (Local)

Select an item to view its description.

Name	Description	Status	Startup Type	Log
Active Directory Domain Se...	AD DS Dom...	Running	Automatic	Loc
Active Directory Web Services	This service ...	Running	Automatic	Loc
ActiveX Installer (AxInstSV)	Provides Us...		Disabled	Loc
AllJoyn Router Service	Routes AllJo...		Manual (Trig...	Loc
App Readiness	Gets apps re...		Manual	Loc
Application Host Helper Ser...	Provides ad...	Running	Automatic	Loc
Application Identity	Determines ...		Manual (Trig...	Loc
Application Information	Facilitates t...	Running	Manual (Trig...	Loc
Application Layer Gateway ...	Provides su...	Running	Manual	Loc
Application Management	Processes in...		Manual	Loc
AppX Deployment Service (...	Provides inf...		Manual	Loc
Auto Time Zone Updater	Automatica...		Disabled	Loc
AVCTP service	This is Audi...	Running	Manual (Trig...	Loc
Azure Gateway Service	Provides sit...		Disabled	Loc
Background Intelligent Tran...	Transfers fil...		Manual	Loc
Background Tasks Infrastru...	Windows in...	Running	Automatic	Loc
Base Filtering Engine	The Base Fil...	Running	Automatic	Loc
Bluetooth Audio Gateway S...	Service sup...		Manual (Trig...	Loc
Bluetooth Support Service	The Bluetoo...		Manual (Trig...	Loc
Capability Access Manager ...	Provides fac...		Manual	Loc
CaptureService_7565bf	OneCore Ca...		Manual	Loc


Recycle Bin
Microsoft Edge
Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DHCP
DNS
File and Storage Services
IIS
Remote Access
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local se
2 Add roles and features
3 Add other servers to ma
4 Create a server group
5 Connect this server to cl
ROLES AND SERVER GROUPS
Roles: 6 | Server groups: 1 | Servers total: 1
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Connection Manager Administration Kit
Defragment and Optimize Drives
DHCP
Disk Cleanup
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
Network Policy Server
ODBC Data Sources (32-bit)