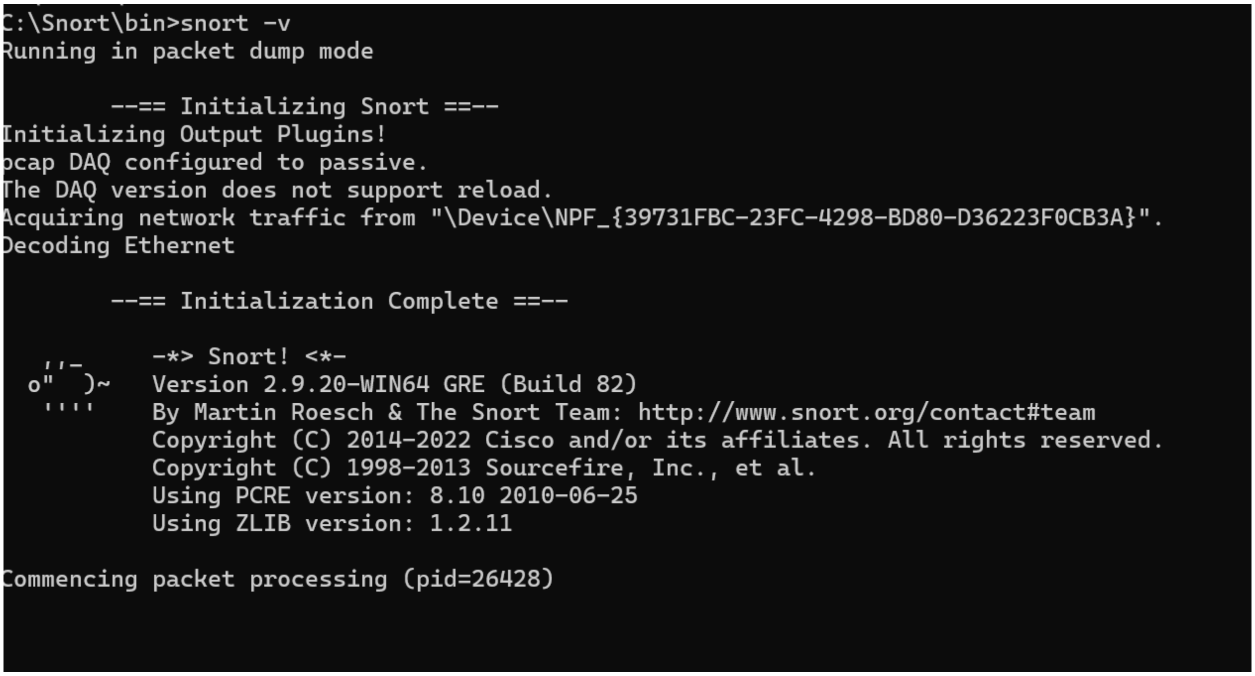
NIYIGABA CLAUDE   24RP14647   BTECH IT   RP MUSANZE

Assignment 2

Q. In summary, with examples of screenshots from snort and RBAC/window server, describe the best practices measures to implement for protection of information.

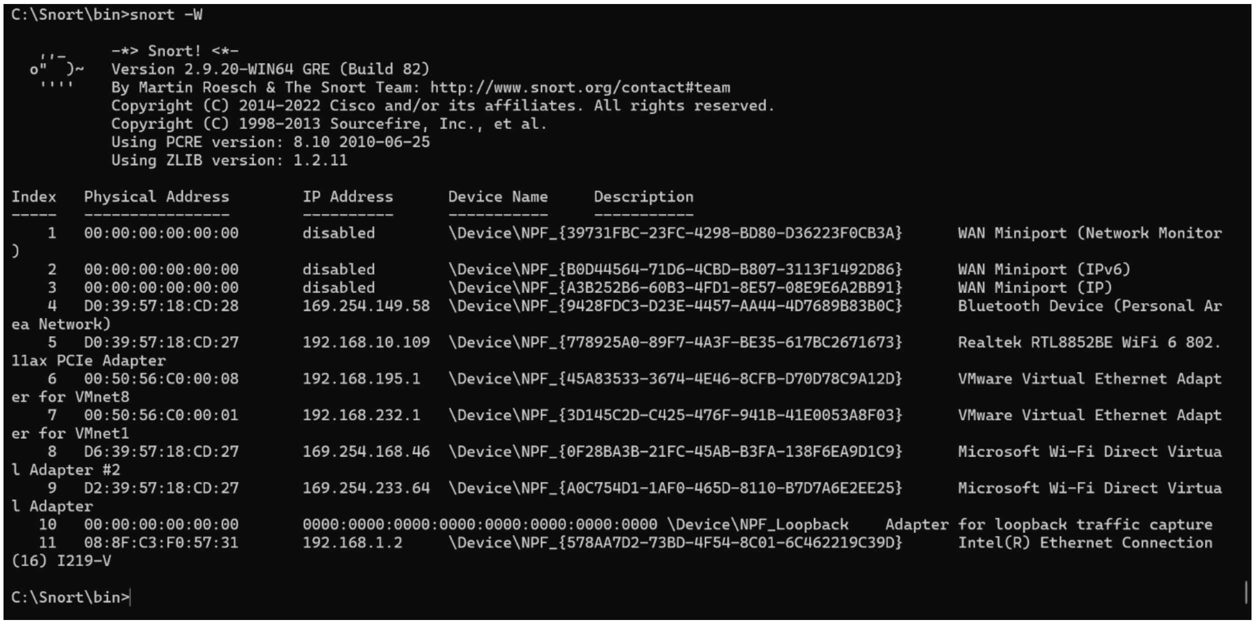
I. with examples of screenshots from snort

1. Snort –v



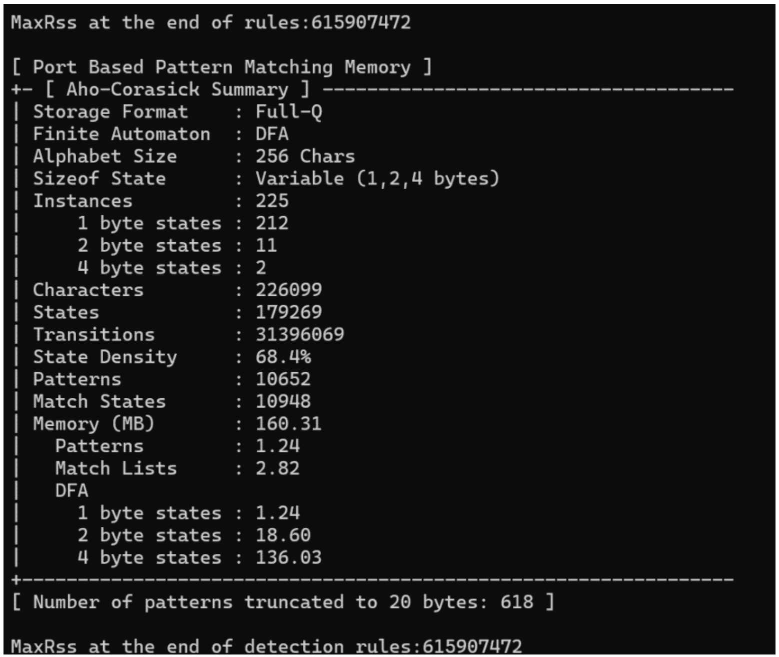
```
C:\Snort\bin>snort -v
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{39731FBC-23FC-4298-BD80-D36223F0CB3A}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

ommencing packet processing (pid=26428)
```

2. Cmd snort/bin > snort -W   / show interfaces

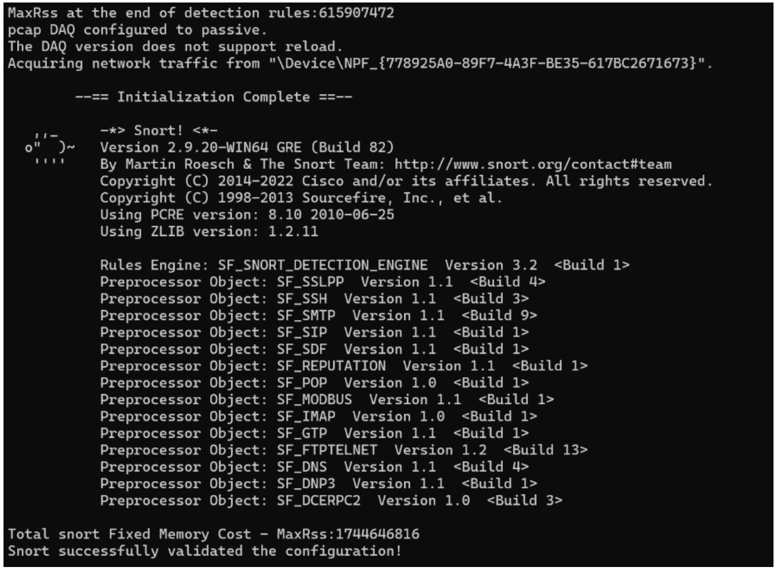


```
C:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       disabled        \Device\NPF_{39731FBC-23FC-4298-BD80-D36223F0CB3A}      WAN Miniport (Network Monitor
)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{B0D44564-71D6-4CBD-B807-3113F1492D86}      WAN Miniport (IPv6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{A3B252B6-60B3-4FD1-8E57-08E9E6A2BB91}      WAN Miniport (IP)
    4   D0:39:57:18:CD:28       169.254.149.58  \Device\NPF_{9428FDC3-D23E-4457-AA44-4D7689B83B0C}      Bluetooth Device (Personal Ar
ea Network)
    5   D0:39:57:18:CD:27       192.168.10.109  \Device\NPF_{778925A0-89F7-4A3F-BE35-617BC2671673}      Realtek RTL8852BE WiFi 6 802.
11ax PCIe Adapter
    6   00:50:56:C0:00:08       192.168.195.1   \Device\NPF_{45A83533-3674-4E46-8CFB-D70D78C9A12D}      VMware Virtual Ethernet Adapt
er for VMnet8
    7   00:50:56:C0:00:01       192.168.232.1   \Device\NPF_{3D145C2D-C425-476F-941B-41E0053A8F03}      VMware Virtual Ethernet Adapt
er for VMnet1
    8   D6:39:57:18:CD:27       169.254.168.46  \Device\NPF_{0F28BA3B-21FC-45AB-B3FA-138F6EA9D1C9}      Microsoft Wi-Fi Direct Virtua
l Adapter #2
    9   D2:39:57:18:CD:27       169.254.233.64  \Device\NPF_{A0C754D1-1AF0-465D-8110-B7D7A6E2EE25}      Microsoft Wi-Fi Direct Virtua
l Adapter
   10   00:00:00:00:00:00       0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback    Adapter for loopback traffic capture
   11   08:8F:C3:F0:57:31       192.168.1.2     \Device\NPF_{578AA7D2-73BD-4F54-8C01-6C462219C39D}      Intel(R) Ethernet Connection
(16) I219-V

C:\Snort\bin>
```

3. Snort -I 4 -c c:\snort\etc\snort.conf -T   for checking error

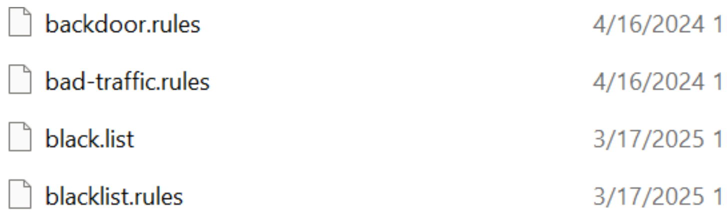


```
MaxRss at the end of rules:615907472

[ Port Based Pattern Matching Memory ]
+- [ Aho-Corasick Summary ] -------------------------------------
| Storage Format    : Full-Q
| Finite Automaton  : DFA
| Alphabet Size     : 256 Chars
| Sizeof State      : Variable (1,2,4 bytes)
| Instances         : 225
|     1 byte states : 212
|     2 byte states : 11
|     4 byte states : 2
| Characters        : 226099
| States            : 179269
| Transitions       : 31396069
| State Density     : 68.4%
| Patterns          : 10652
| Match States      : 10948
| Memory (MB)       : 160.31
|   Patterns        : 1.24
|   Match Lists     : 2.82
|   DFA
|     1 byte states : 1.24
|     2 byte states : 18.60
|     4 byte states : 136.03
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 618 ]

MaxRss at the end of detection rules:615907472
```



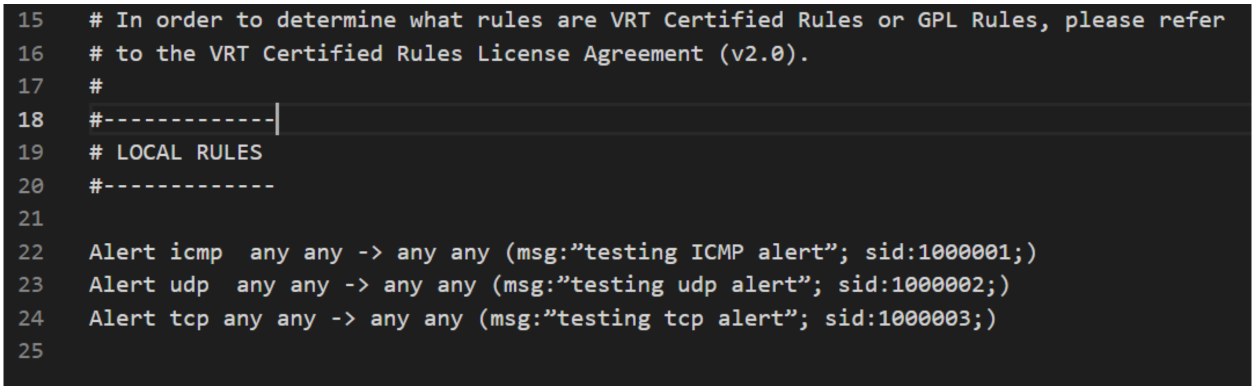
```
MaxRss at the end of detection rules:615907472
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{778925A0-89F7-4A3F-BE35-617BC2671673}".

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>

Total snort Fixed Memory Cost - MaxRss:1744646816
Snort successfully validated the configuration!
```

4. Checking white.list and black.list are exit



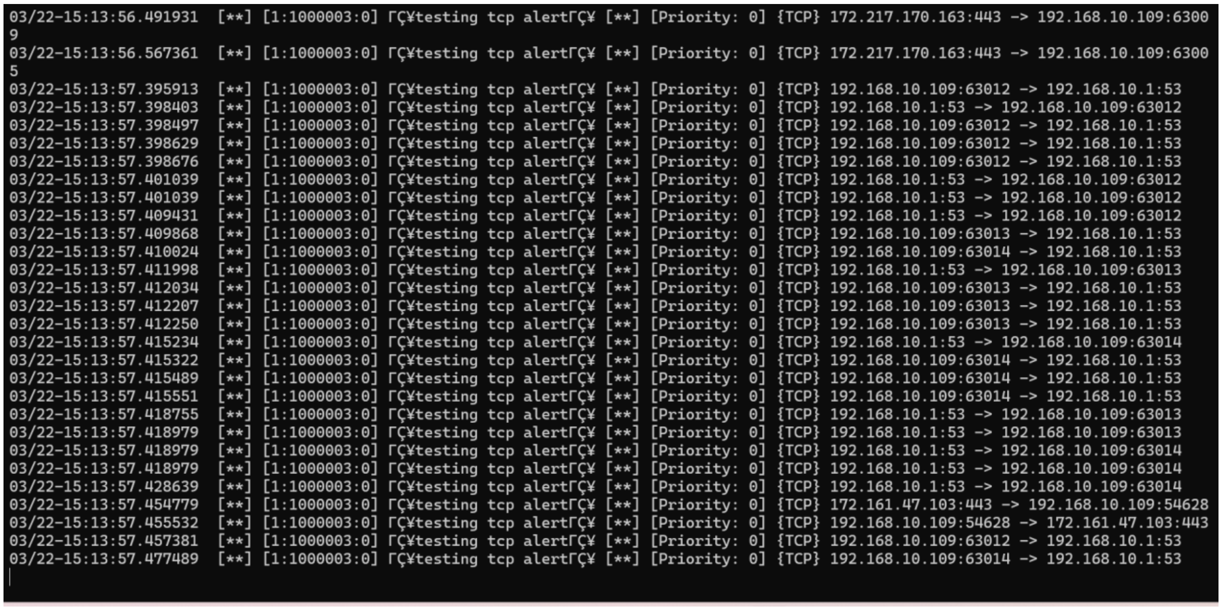
backdoor.rules	4/16/2024 1
bad-traffic.rules	4/16/2024 1
black.list	3/17/2025 1
blacklist.rules	3/17/2025 1

5. Create Local.rules file for protection



```
# In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
# to the VRT Certified Rules License Agreement (v2.0).
#
#-------------
# LOCAL RULES
#-------------

Alert icmp  any any -> any any (msg:”testing ICMP alert”; sid:1000001;)
Alert udp  any any -> any any (msg:”testing udp alert”; sid:1000002;)
Alert tcp any any -> any any (msg:”testing tcp alert”; sid:1000003;)

```

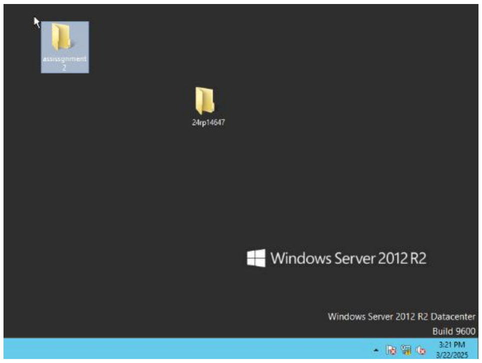
6. Snort -i 5 -c c:\snort\etc\snort.conf -A   console for checking service

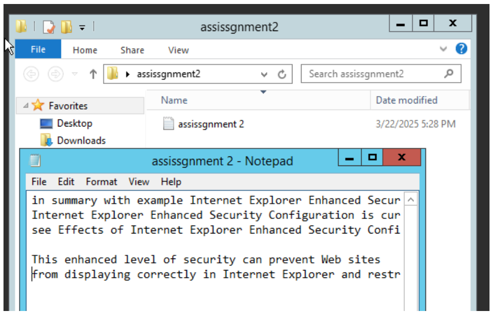


```
03/22-15:13:56.491931  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 172.217.170.163:443 -> 192.168.10.109:6300
9
03/22-15:13:56.567361  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 172.217.170.163:443 -> 192.168.10.109:6300
5
03/22-15:13:57.395913  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63012 -> 192.168.10.1:53
03/22-15:13:57.398403  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63012
03/22-15:13:57.398497  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63012 -> 192.168.10.1:53
03/22-15:13:57.398629  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63012 -> 192.168.10.1:53
03/22-15:13:57.398676  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63012 -> 192.168.10.1:53
03/22-15:13:57.401039  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63012
03/22-15:13:57.401039  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63012
03/22-15:13:57.409431  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63012
03/22-15:13:57.409868  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63013 -> 192.168.10.1:53
03/22-15:13:57.410024  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63014 -> 192.168.10.1:53
03/22-15:13:57.411998  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63013
03/22-15:13:57.412034  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63013 -> 192.168.10.1:53
03/22-15:13:57.412207  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63013 -> 192.168.10.1:53
03/22-15:13:57.412250  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63013 -> 192.168.10.1:53
03/22-15:13:57.415234  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63014
03/22-15:13:57.415322  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63014 -> 192.168.10.1:53
03/22-15:13:57.415489  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63014 -> 192.168.10.1:53
03/22-15:13:57.415551  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63014 -> 192.168.10.1:53
03/22-15:13:57.418755  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63013
03/22-15:13:57.418979  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63013
03/22-15:13:57.418979  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63014
03/22-15:13:57.418979  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63014
03/22-15:13:57.428639  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63014
03/22-15:13:57.454779  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 172.161.47.103:443 -> 192.168.10.109:54628
03/22-15:13:57.455532  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:54628 -> 172.161.47.103:443
03/22-15:13:57.457381  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63012 -> 192.168.10.1:53
03/22-15:13:57.477489  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63014 -> 192.168.10.1:53
```

I. RBAC/window server, describe the best practices measures to implement for protection of information.

1. Create a folder and create file use to protect

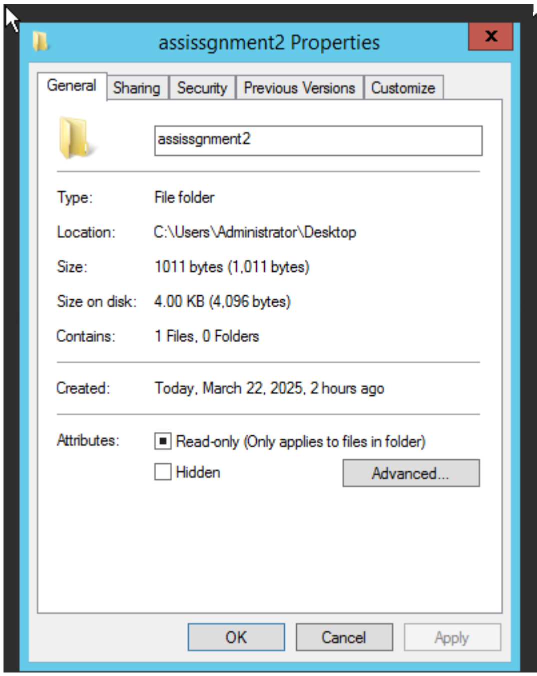




assissgnment 2 — 3/22/2025 5:28 PM

```
in summary with example Internet Explorer Enhanced Secur
Internet Explorer Enhanced Security Configuration is cur
see Effects of Internet Explorer Enhanced Security Confi

This enhanced level of security can prevent Web sites
from displaying correctly in Internet Explorer and restr
```

2. Selection on folder for security and permission to the users


assissgnment2 Properties

assissgnment2

Type: File folder

Location: C:\Users\Administrator\Desktop

Size: 1011 bytes (1,011 bytes)

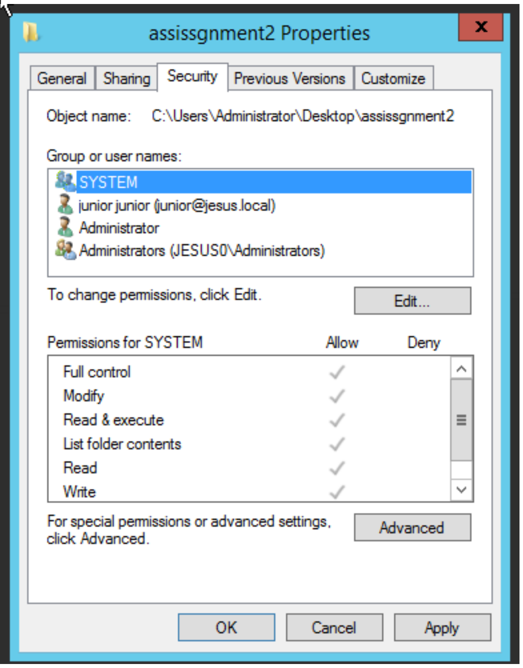
Size on disk: 4.00 KB (4,096 bytes)

Contains: 1 Files, 0 Folders

Created: Today, March 22, 2025, 2 hours ago

Attributes: ■ Read-only (Only applies to files in folder)

□ Hidden


assissgnment2 Properties

Object name: C:\Users\Administrator\Desktop\assissgnment2

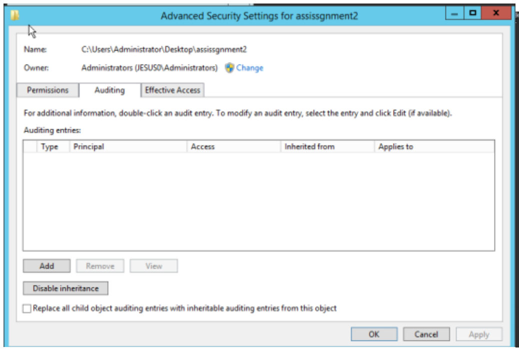
Group or user names:

- SYSTEM
- junior junior (junior@jesus.local)
- Administrator
- Administrators (JESUS0\Administrators)

To change permissions, click Edit.

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.


Advanced Security Settings for assissgnment2

Name: C:\Users\Administrator\Desktop\assissgnment2

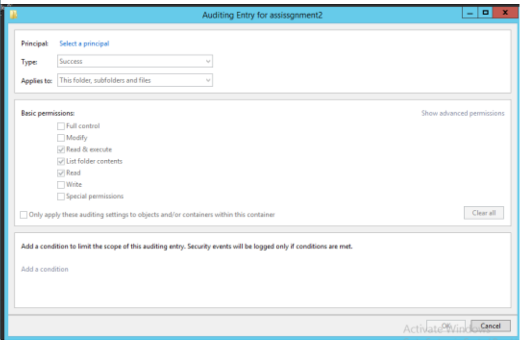
Owner: Administrators (JESUS0\Administrators) Change

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to

□ Replace all child object auditing entries with inheritable auditing entries from this object


Auditing Entry for assissgnment2

Principal: Select a principal

Type: Success

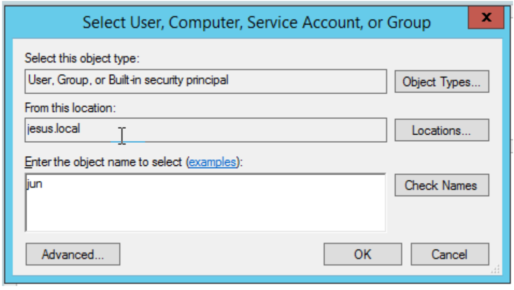
Applies to: This folder, subfolders and files

Basic permissions:

- □ Full control
- □ Modify
- ☑ Read & execute
- ☑ List folder contents
- ☑ Read
- □ Write
- □ Special permissions

□ Only apply these auditing settings to objects and/or containers within this container

Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.


Select User, Computer, Service Account, or Group

Select this object type:

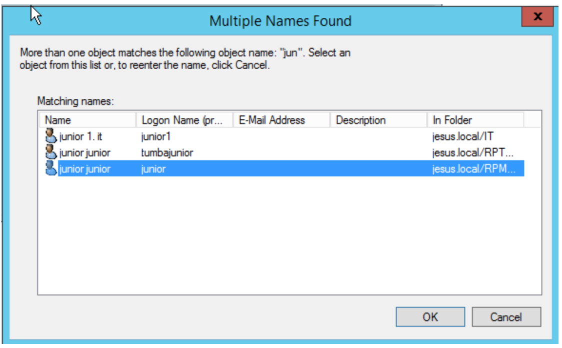
User, Group, or Built-in security principal

From this location:

jesus.local

Enter the object name to select (examples):

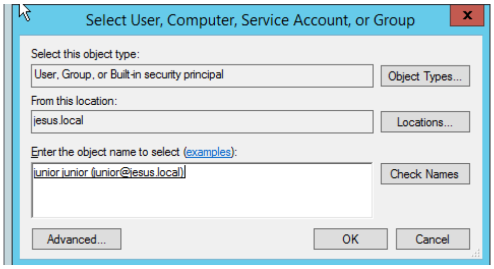
jun


Multiple Names Found

More than one object matches the following object name: "jun". Select an object from this list or, to reenter the name, click Cancel.

Matching names:

Name	Logon Name (pr...	E-Mail Address	Description	In Folder
junior 1. it	junior1			jesus.local/IT
junior junior	tumbajunior			jesus.local/RPT...
junior junior	junior			jesus.local/RPM...


Select User, Computer, Service Account, or Group

Select this object type:

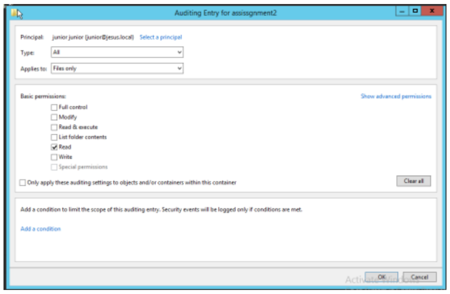
User, Group, or Built-in security principal

From this location:

jesus.local

Enter the object name to select (examples):

junior junior (junior@jesus.local)


Auditing Entry for assissgnment2

Principal: junior junior (junior@jesus.local) Select a principal

Type: All

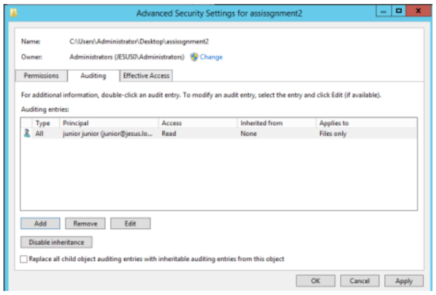
Applies to: Files only

Basic permissions:

- □ Full control
- □ Modify
- □ Read & execute
- □ List folder contents
- ☑ Read
- □ Write
- □ Special permissions

□ Only apply these auditing settings to objects and/or containers within this container

Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.



Advanced Security Settings for assissgnment2

Name: C:\Users\Administrator\Desktop\assissgnment2

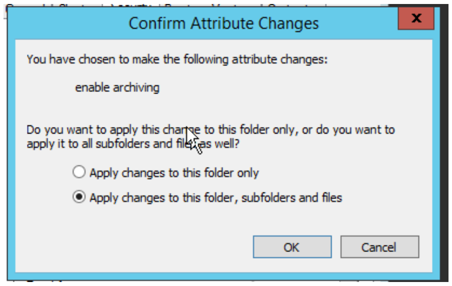
Owner: Administrators (JESUS0\Administrators) Change

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to
All	junior junior (junior@jesus.lo...	Read	None	Files only

□ Replace all child object auditing entries with inheritable auditing entries from this object



Confirm Attribute Changes

You have chosen to make the following attribute changes:

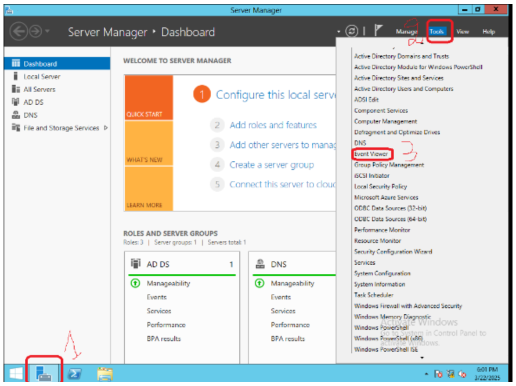
enable archiving

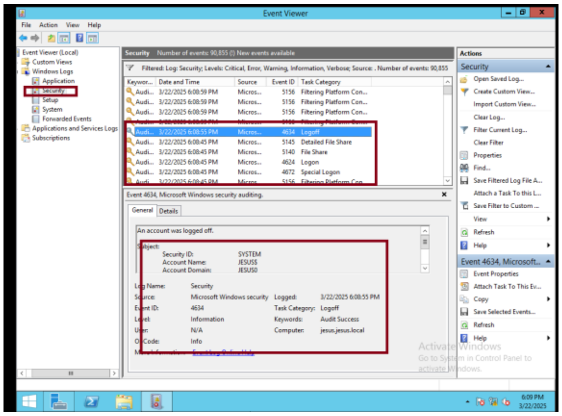
Do you want to apply this change to this folder only, or do you want to apply it to all subfolders and files as well?

○ Apply changes to this folder only

● Apply changes to this folder, subfolders and files

3. Review event





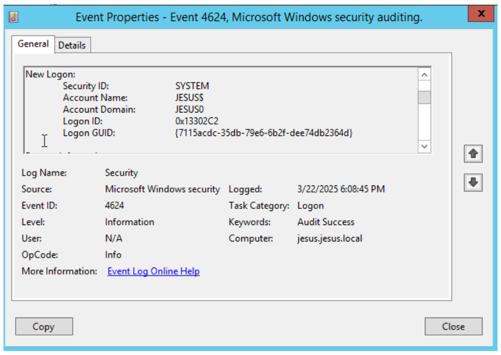
Security Number of events: 90,855 (!) New events available

Filtered: Log: Security; Levels: Critical, Error, Warning, Information, Verbose; Source: . Number of events: 90,855

Keywor...	Date and Time	Source	Event ID	Task Category
Audi...	3/22/2025 6:08:59 PM	Micros...	5156	Filtering Platform Con...
Audi...	3/22/2025 6:08:59 PM	Micros...	5156	Filtering Platform Con...
Audi...	3/22/2025 6:08:59 PM	Micros...	5156	Filtering Platform Con...
Audi...	3/22/2025 6:08:55 PM	Micros...	4634	Logoff
Audi...	3/22/2025 6:08:45 PM	Micros...	5145	Detailed File Share
Audi...	3/22/2025 6:08:45 PM	Micros...	5140	File Share
Audi...	3/22/2025 6:08:45 PM	Micros...	4624	Logon
Audi...	3/22/2025 6:08:45 PM	Micros...	4672	Special Logon
Audi...	3/22/2025 6:08:45 PM	Micros...	5156	Filtering Platform Con...

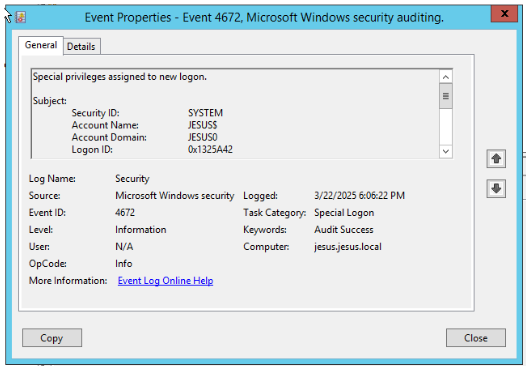
Event 4634, Microsoft Windows security auditing.

```
An account was logged off.

Subject:
        Security ID:        SYSTEM
        Account Name:       JESUS$
        Account Domain:     JESUS0

Log Name:      Security
Source:        Microsoft Windows security   Logged:         3/22/2025 6:08:55 PM
Event ID:      4634                         Task Category:  Logoff
Level:         Information                  Keywords:       Audit Success
User:          N/A                          Computer:       jesus.jesus.local
OpCode:        Info
More Information:  Event Log Online Help
```



Event Properties - Event 4624, Microsoft Windows security auditing.

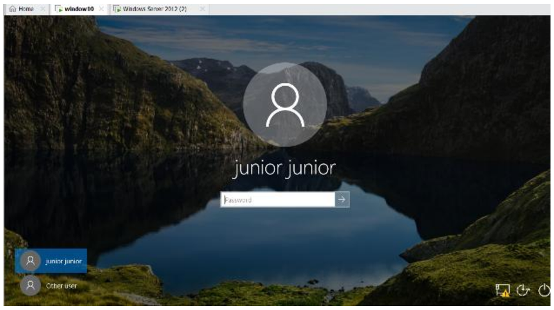
```
New Logon:
        Security ID:        SYSTEM
        Account Name:       JESUS$
        Account Domain:     JESUS0
        Logon ID:           0x13302C2
        Logon GUID:         {7115acdc-35db-79e6-6b2f-dee74db2364d}

Log Name:      Security
Source:        Microsoft Windows security   Logged:         3/22/2025 6:08:45 PM
Event ID:      4624                         Task Category:  Logon
Level:         Information                  Keywords:       Audit Success
User:          N/A                          Computer:       jesus.jesus.local
OpCode:        Info
More Information:  Event Log Online Help
```

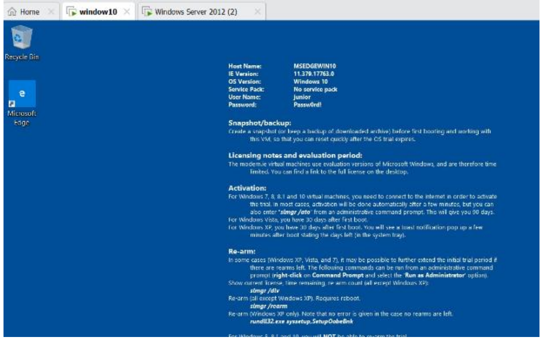


Event Properties - Event 4672, Microsoft Windows security auditing.

```
Special privileges assigned to new logon.

Subject:
        Security ID:        SYSTEM
        Account Name:       JESUS$
        Account Domain:     JESUS0
        Logon ID:           0x1325A42

Log Name:      Security
Source:        Microsoft Windows security   Logged:         3/22/2025 6:06:22 PM
Event ID:      4672                         Task Category:  Special Logon
Level:         Information                  Keywords:       Audit Success
User:          N/A                          Computer:       jesus.jesus.local
OpCode:        Info
More Information:  Event Log Online Help
```

4. Login with window 10





Host Name:	MSEDGEWIN10
IE Version:	11.379.17763.0
OS Version:	Windows 10
Service Pack:	No service pack
User Name:	Junior
Password:	Passw0rd!

Snapshot/backup:
Create a snapshot (or keep a backup of downloaded archive) before first booting and working with this VM, so that you can reset quickly after the OS trial expires.

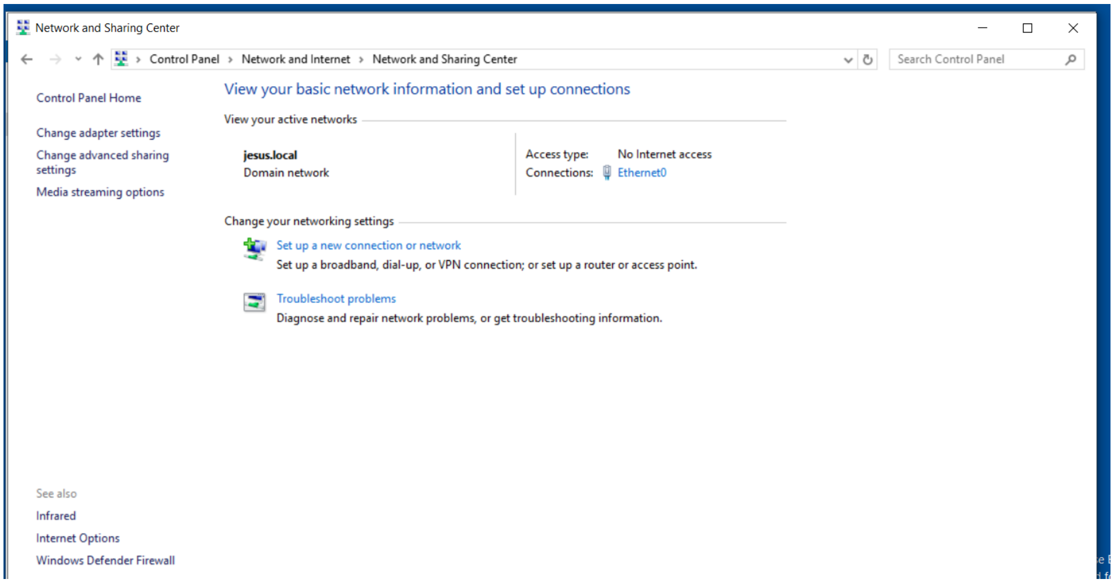
Licensing notes and evaluation period:
The modern.ie virtual machines use evaluation versions of Microsoft Windows, and are therefore time limited. You can find a link to the full license on the desktop.

Activation:
For Windows 7, 8, 8.1 and 10 virtual machines, you need to connect to the internet in order to activate the trial. In most cases, activation will be done automatically after a few minutes, but you can also enter "***slmgr /ato***" from an administrative command prompt. This will give you 90 days.
For Windows Vista, you have 30 days after first boot.
For Windows XP, you have 30 days after first boot. You will see a toast notification pop up a few minutes after boot stating the days left (in the system tray).

Re-arm:
In some cases (Windows XP, Vista, and 7), it may be possible to further extend the initial trial period if there are rearms left. The following commands can be run from an administrative command prompt (**right-click** on **Command Prompt** and select the '**Run as Administrator**' option).
Show current license, time remaining, re-arm count (all except Windows XP):
slmgr /dlv
Re-arm (all except Windows XP). Requires reboot.
slmgr /rearm
Re-arm (Windows XP only). Note that no error is given in the case no rearms are left.
rundll32.exe syssetup,SetupOobeBnk

For Windows 8, 8.1 and 10 you will **NOT** be able to re-arm the trial.

5. Checking when window 10 connected to server


Network and Sharing Center
Control Panel › Network and Internet › Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
Media streaming options
See also
Infrared
Internet Options
Windows Defender Firewall

View your basic network information and set up connections

View your active networks

jesus.local
Domain network

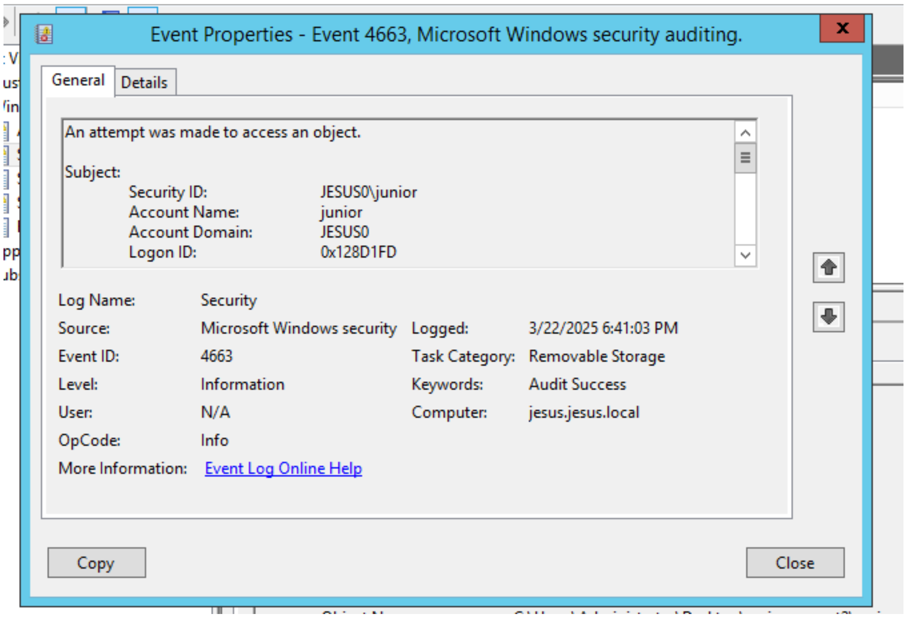
Access type: No Internet access
Connections: Ethernet0

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

6. After connected to domain check permission



Event Properties - Event 4663, Microsoft Windows security auditing.

```
An attempt was made to access an object.

Subject:
        Security ID:          JESUS0\junior
        Account Name:         junior
        Account Domain:       JESUS0
        Logon ID:             0x128D1FD
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          3/22/2025 6:41:03 PM
Event ID:          4663                          Task Category:   Removable Storage
Level:             Information                   Keywords:        Audit Success
User:              N/A                           Computer:        jesus.jesus.local
OpCode:            Info
More Information:  Event Log Online Help
```