Business College HELSINKI

View Windows Event Viewer

Target

- View Windows Event Viewer in order to find out about various events on the server and on the web.

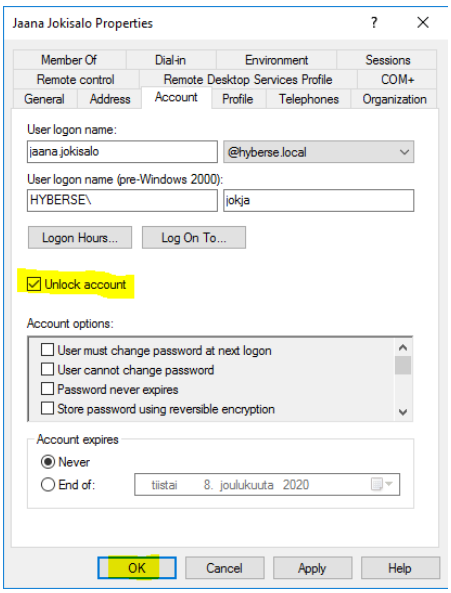
Tasks

Launching virtual machines creation

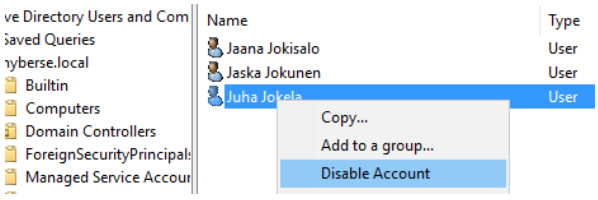
1. If necessary, start the VirtualBox virtualization software.
2. Launch the Apollo virtual machine.
3. Log in to the Apollo server with your CYBERSE\Administrator username and password to the Passw0rd§ server.
4. Start the Win10 virtual machine

Create events.

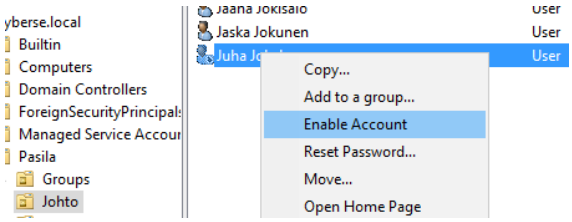
5. Try logging in to the Win10 virtual machine with two different usernames (eg. Pasi Paasi, Kalle Kaarna) using twice the wrong password.
6. Try logging in to the Win10 virtual machine with a third username (eg. Jaana Jokisalo) using the wrong password so many times that the user account is locked. (on the fourth attempt, a notification should appear that the account is locked)
    - Based on the previously defined Group Policy, the lock would be lifted after 30 minutes.
7. On the Apollo server, open the Active Directory Users and Computers console.
8. In the Active Directory Users and Computers console, delete the previously locked user account (eg. Jaana Jokisalo) locking.



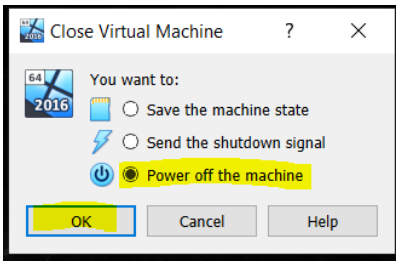
9. The Apollo server's Active Directory Users and Computers console disabloises a user account. (eg. Juha Jokela)



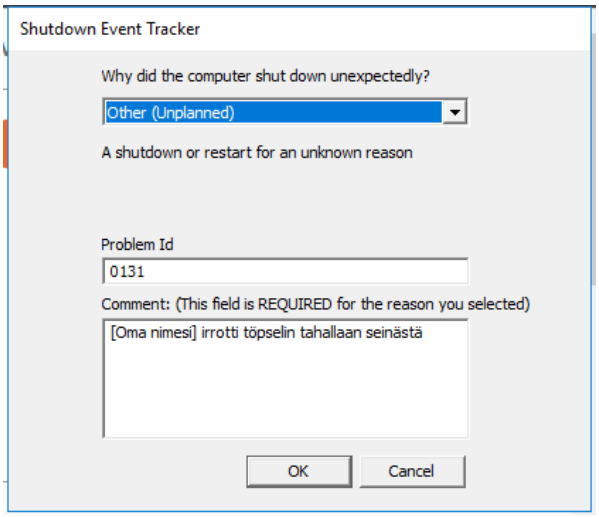
10. The Apollo server in the Active Directory Users and Computers console enable the previously disabled user account. (eg. Juha Jokela)



11. Turn off the Apollo server "on the fly" by clicking the tick in the upper right corner of the virtual machine window, and in the Close Virtual Machine box, select the Power off the machine check box and click OK.



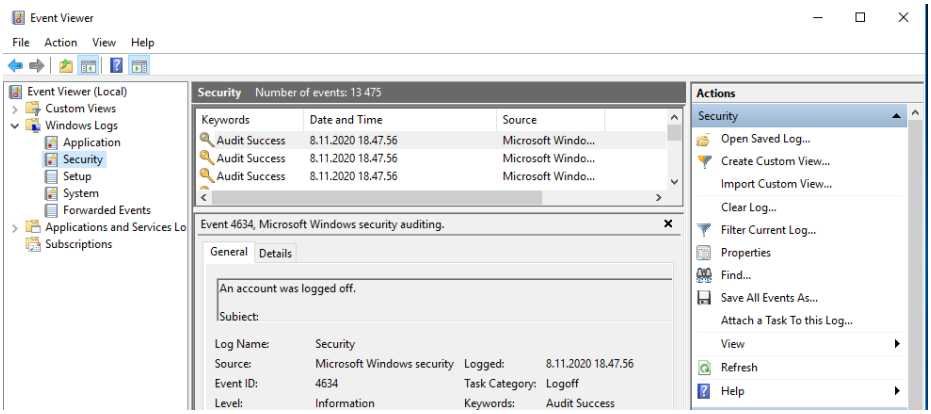
12. Restart the Apollo virtual machine and log in to the server with the CYBERSE\Administrator username and password to the Passw0rd§ server.
13. On the Apollo server, enter Problem Id: 0131 in the Shutdown Event Tracker and in the Comment field: [My name] removed the plug from the wall quite deliberately.



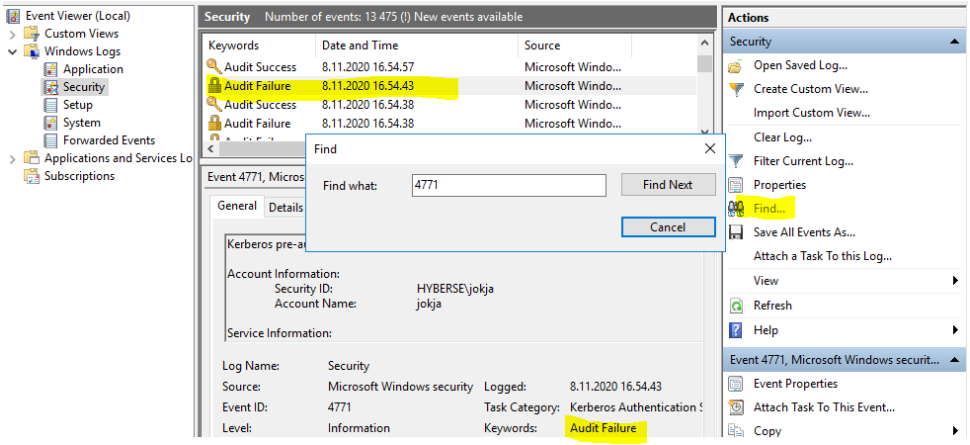
View logs

14. To open the Apollo server,open the Event Viewer by typing event in the search box and selecting Event Viewer from the menu that appears, or by selecting Start > Windows Administrative Tools > Event Viewer.

15. In the Event Viewer window, expand Windows Logs and select Security.

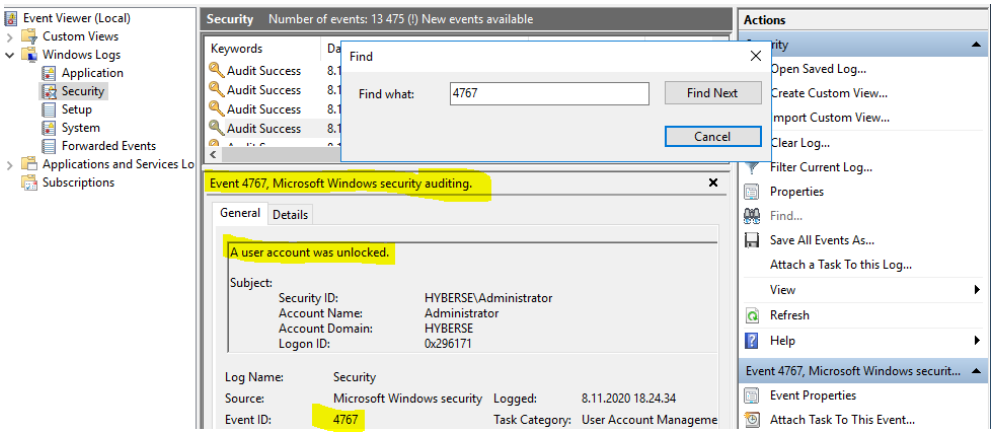


16. In the Event Viewer window, click the Find... link and search for Audit Failure EventID: 4771 in the Find what: field and click Find Next.

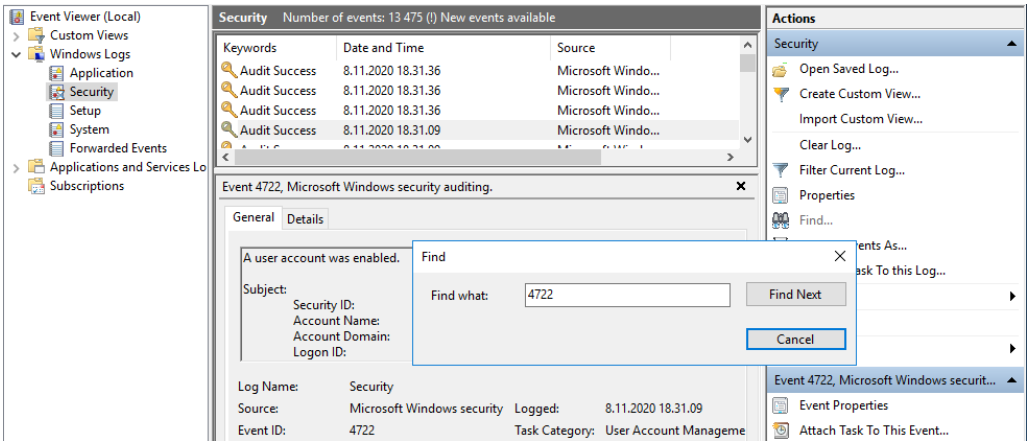


- See what information can be found about the event.
- Also select the Details tab and see what information can be found if you select Friendly View or XML View
- By clicking Find Next again or scrolling through events on the scroll bar, you can search for more failed login attempts and see what information can be found about them.

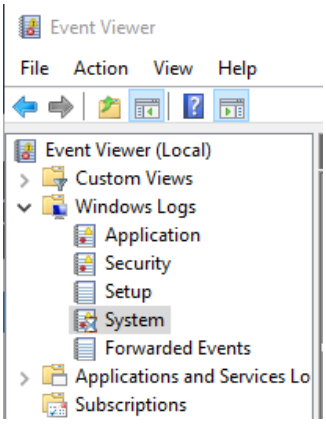
17. Next, find information about how to unlock a locked account by typing EventID: number 4767 in the search box and clicking Find Next.
    - Note! The first search may not yet reveal the information you have applied for. If necessary, click Find Next again.



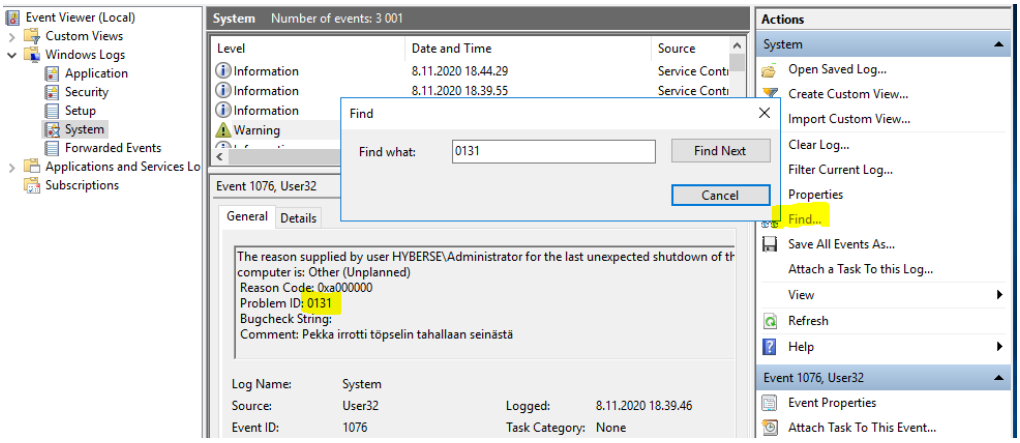
18. Next, search for "enable" by entering EventID:-number 4722 in the search box and clicking Find Next.



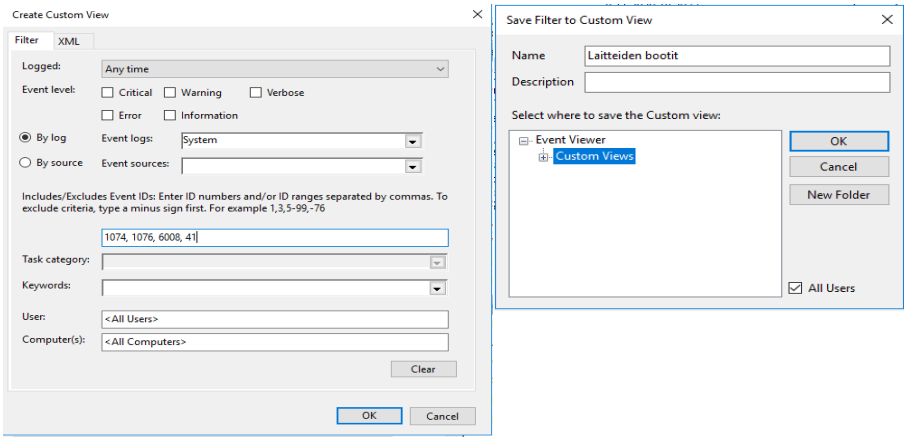
19. In the Event Viewer window, expand Windows Logs and select System.



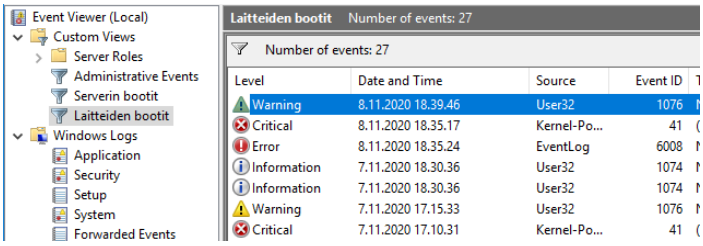
20. In the Event Viewer window, search for data logged in the Shutdown Event Tracker after an unexpected restart of the server by clicking Find... and typing 0131 in Find what:



21. In the Event Viewer window, click Create Custom View to search for different types of server restarts in a single search. and in the Create Custom View window, in the <All Event IDs> field, type 1074, 1076, 6008, 41 and click OK. In the Save Filter to Custom View window, enter "Device boots" in the Name field and click OK.



- Browse events found with search and see why notifications have come in



- Searches made in this way are saved under Custom Views , from where the corresponding search can be done again later.

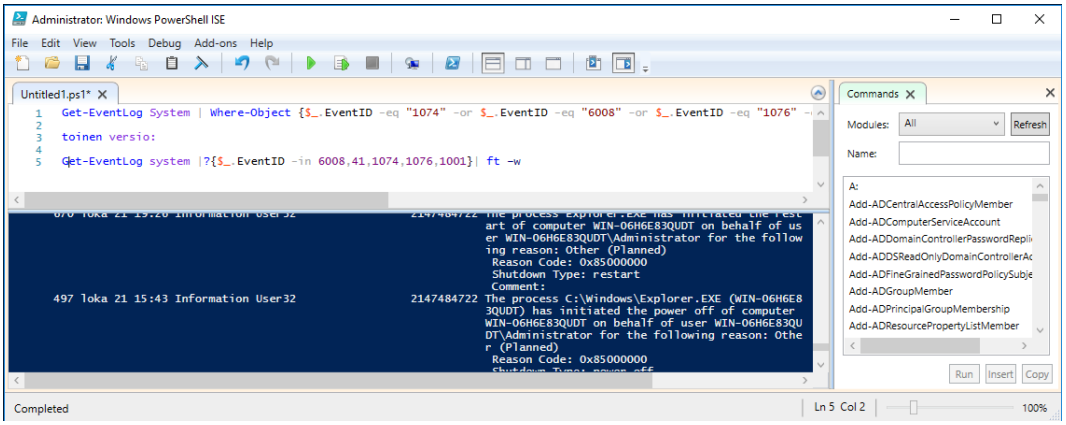
View logs with a PowerShell script

22. Open PowerShell ISE
23. Try the following scripts to find out the reasons for device reboots

    in the Get-EventLog System | Where-Object {$_. EventID -eq "1074" -or $_. EventID -eq "6008" -or $_. EventID -eq "1076" -or $_. EventID -eq "41"} | ft Machinename, TimeWritten, UserName, EventID, Message -AutoSize –Wrap

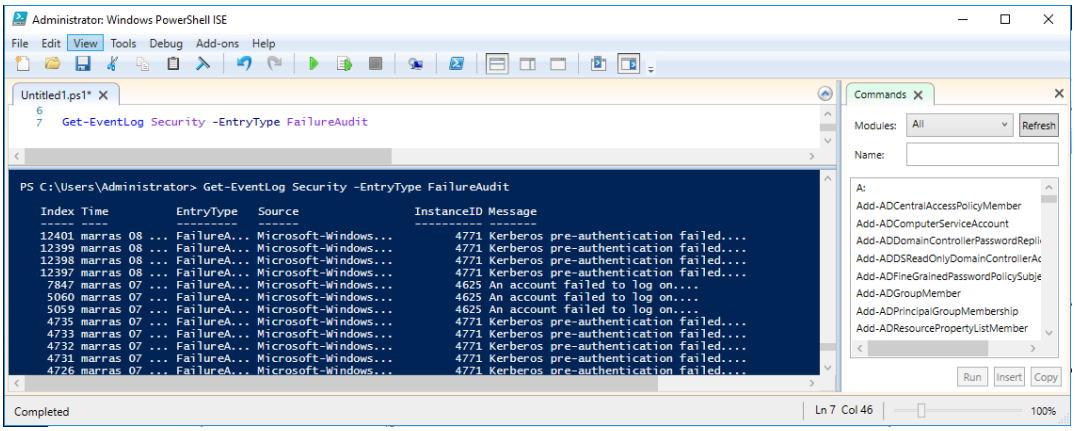
    second version:

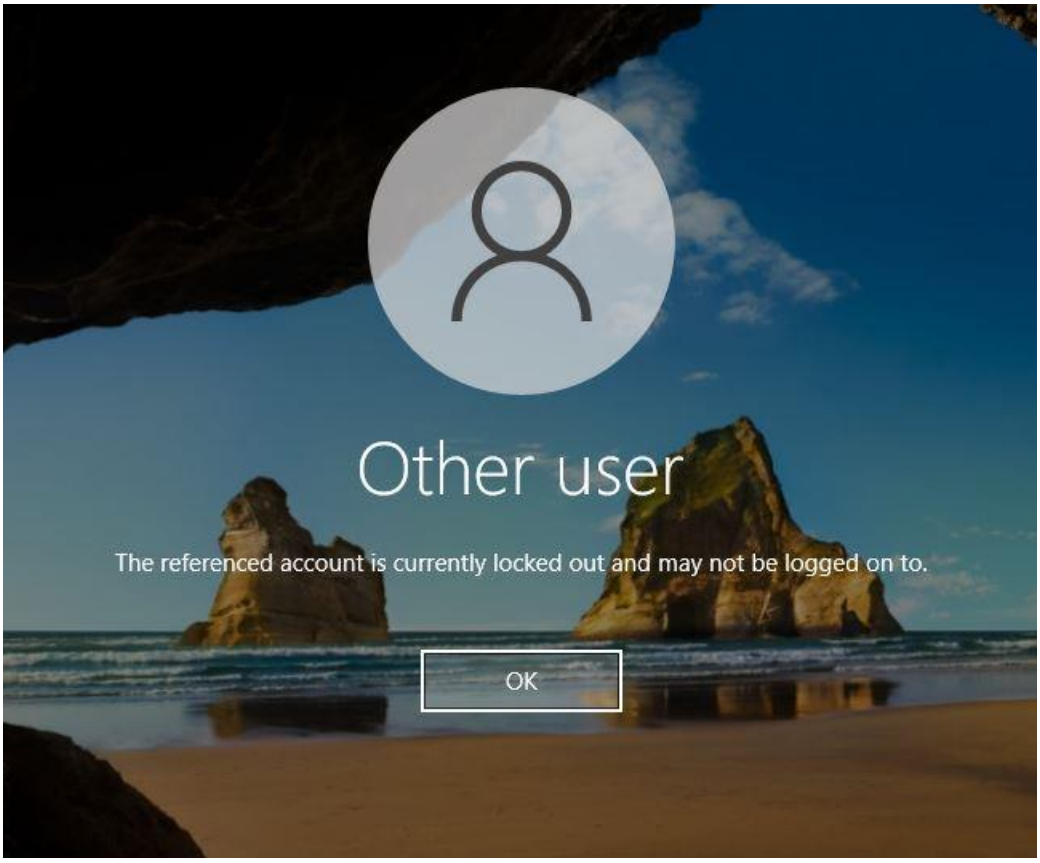
    Get-EventLog system |? {$_. EventID -in 6008,41,1074,1076,1001}| FT –W

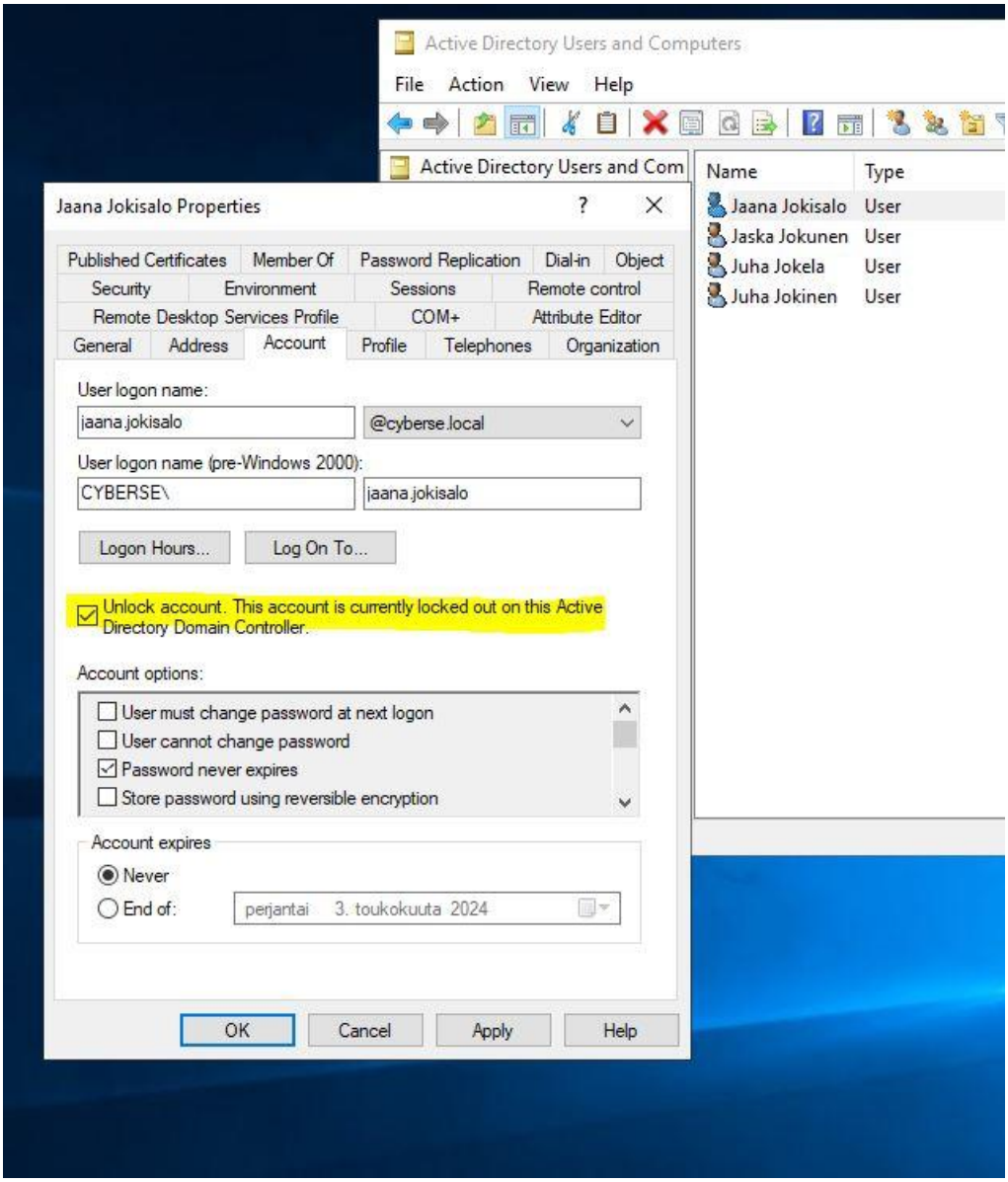


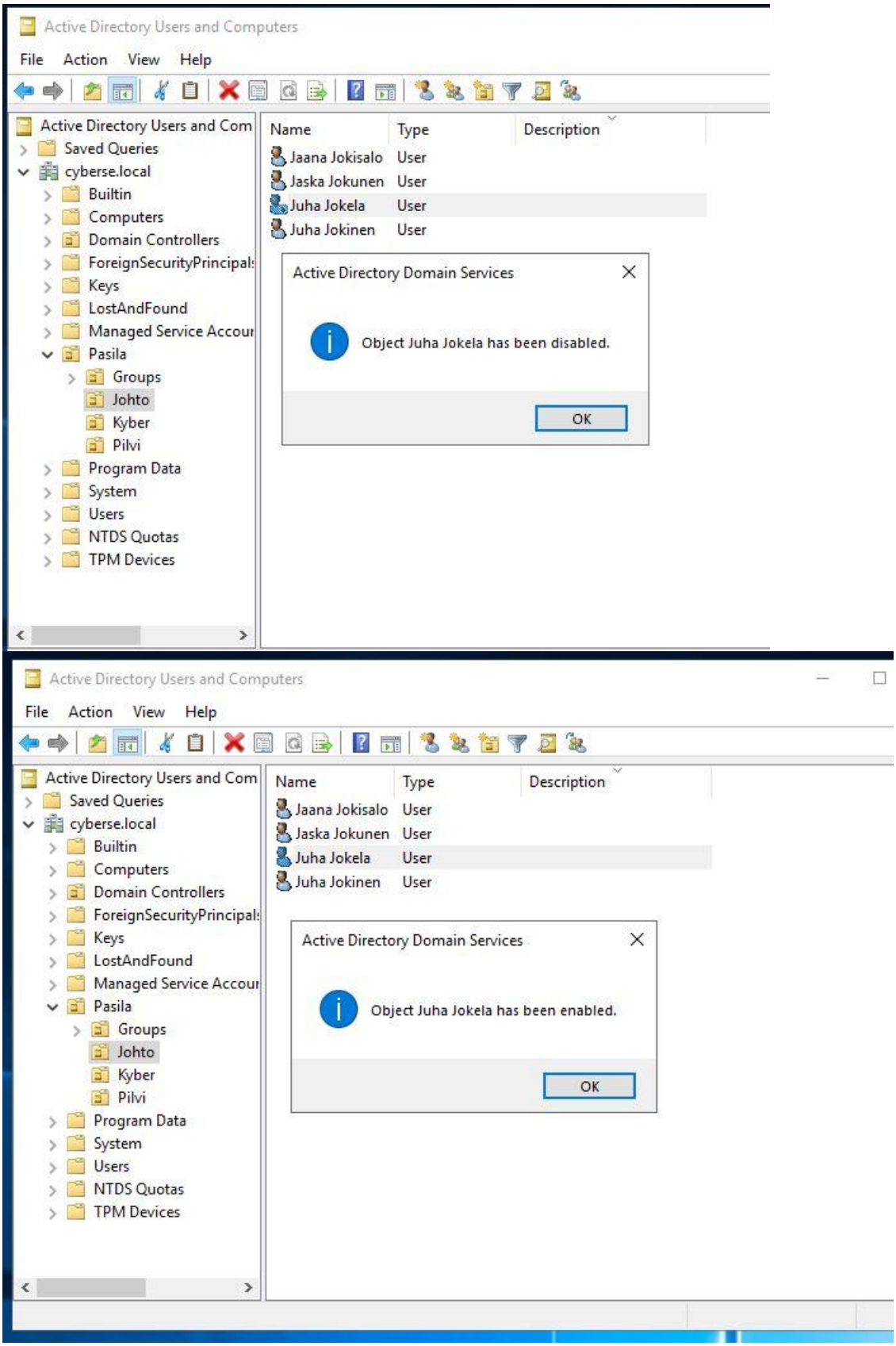
24. Try the following script to search for failed logins

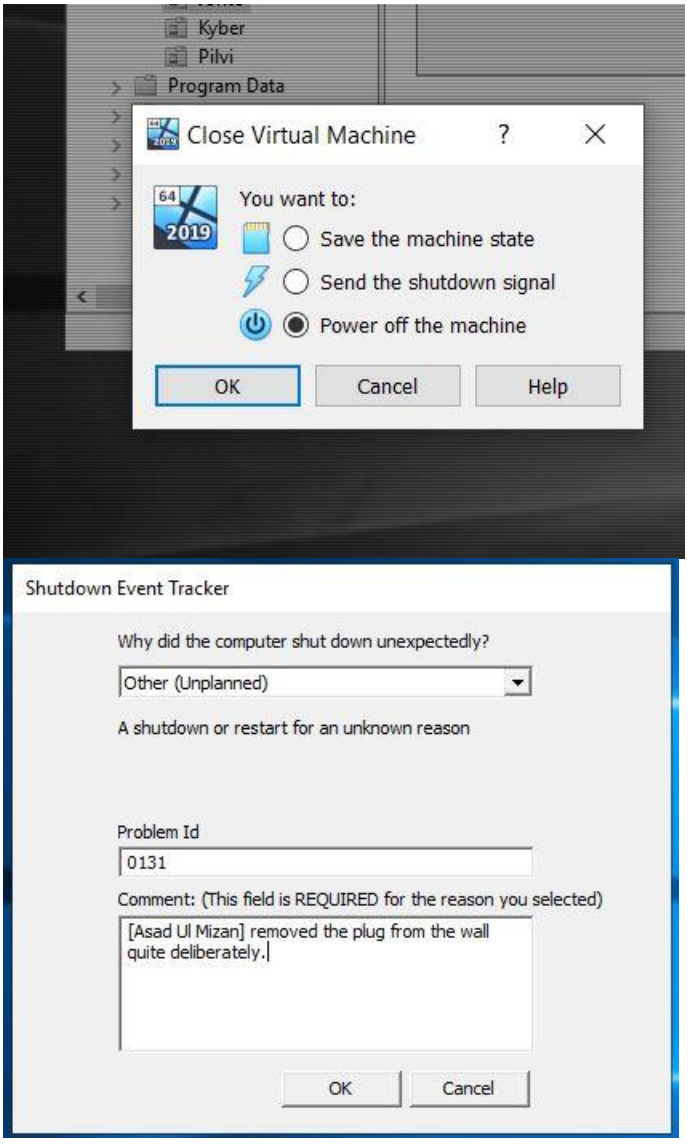
    Get-EventLog Security -EntryType FailureAudit

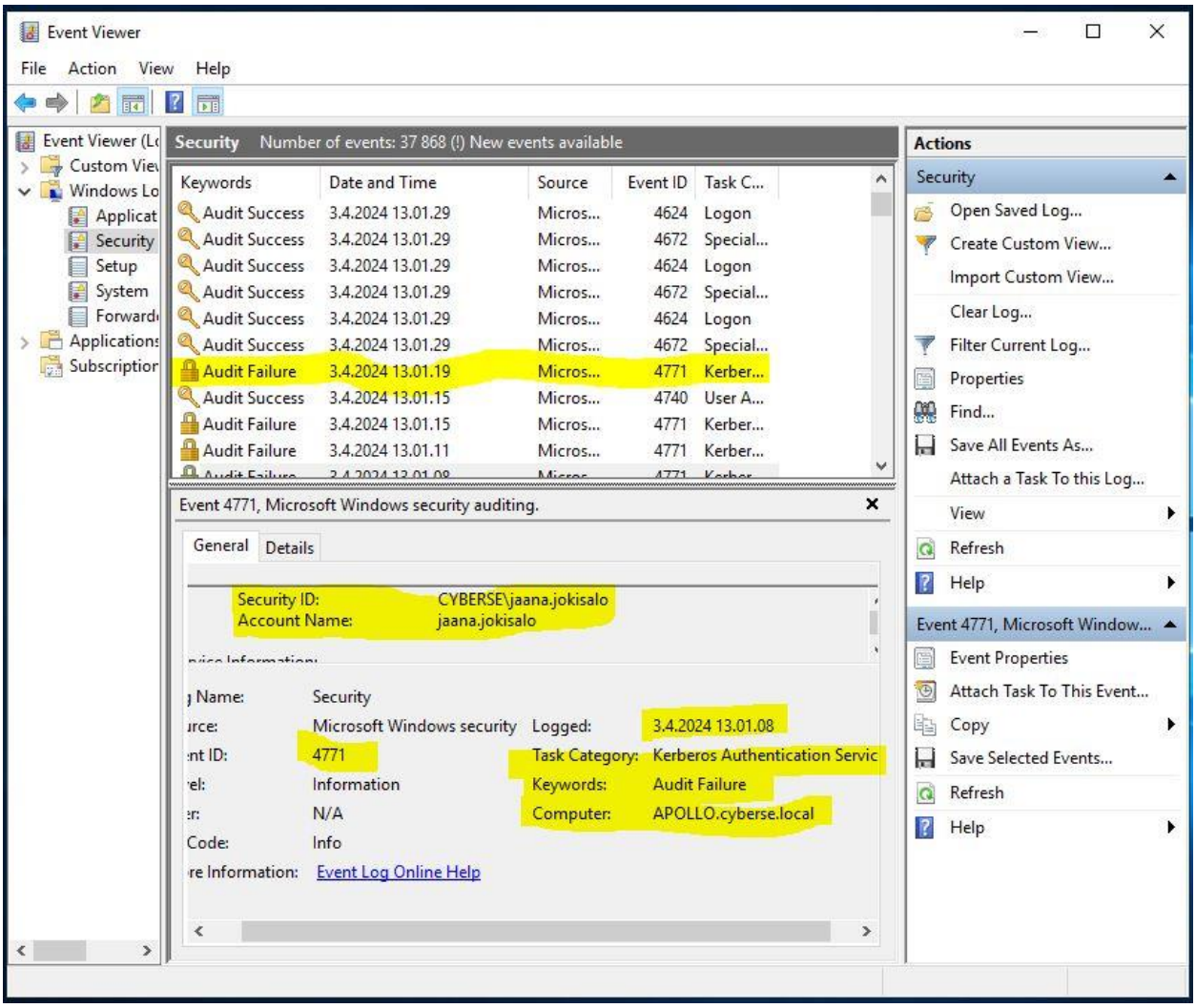


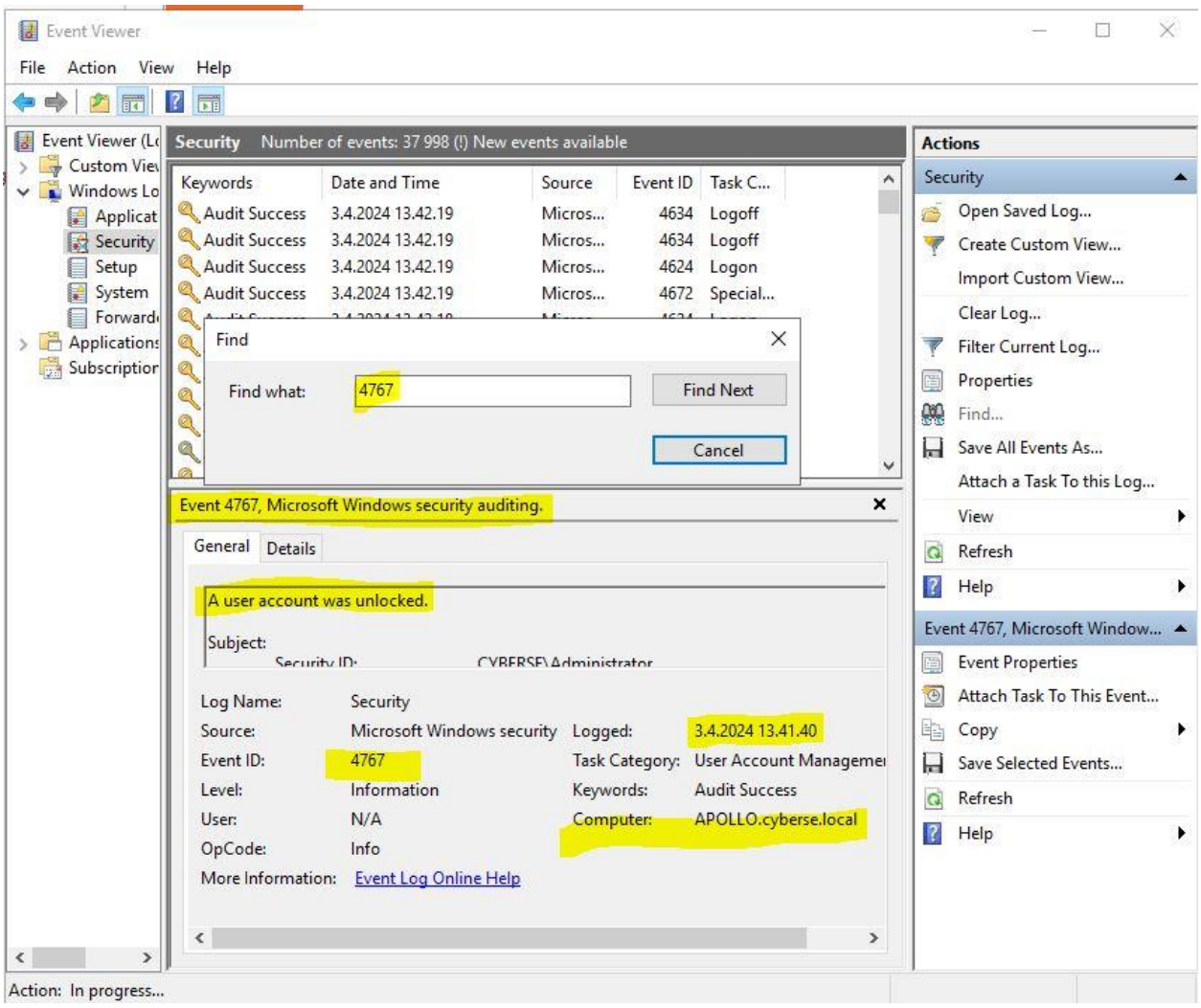

Other user
The referenced account is currently locked out and may not be logged on to.
OK

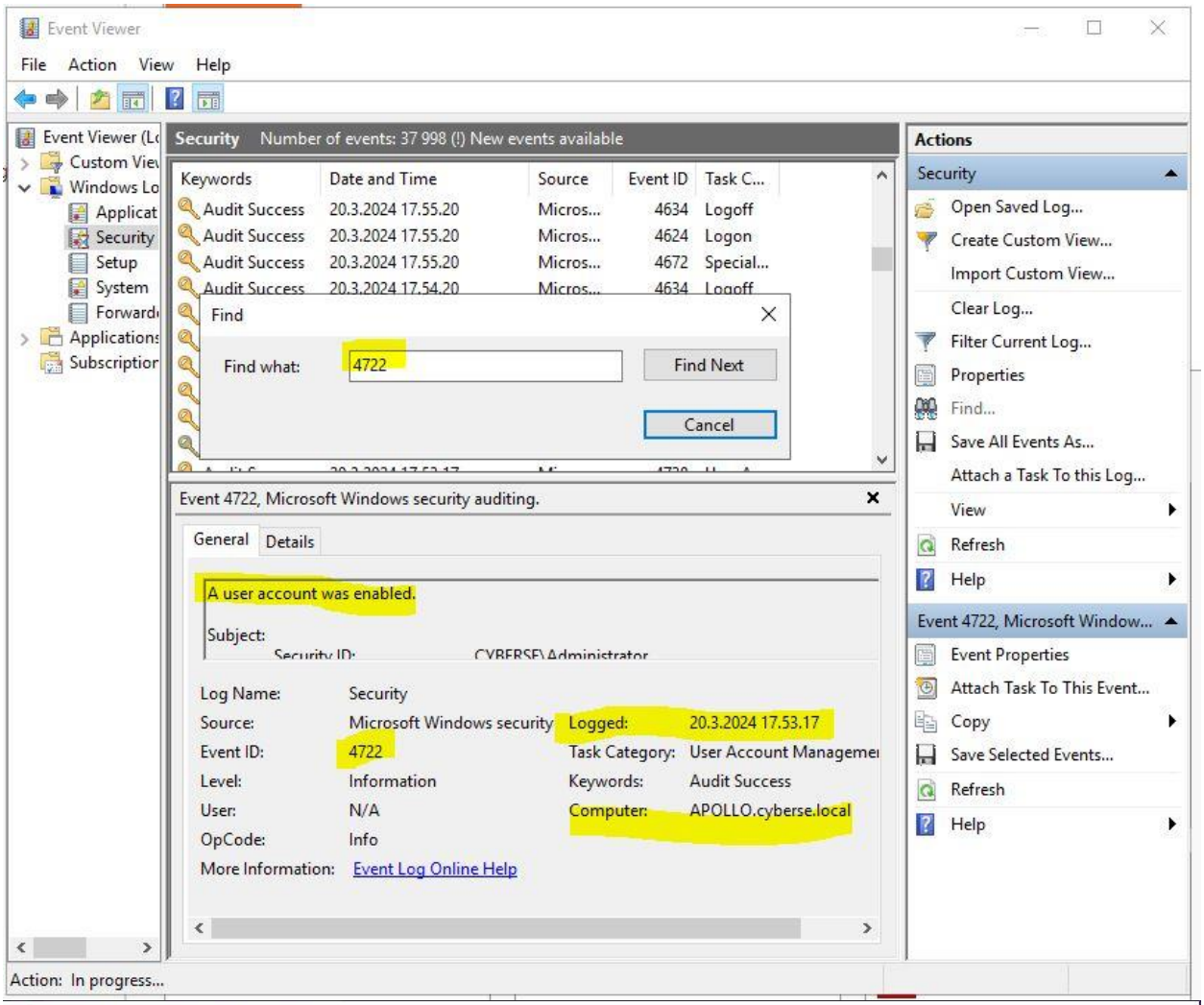

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Name Type
Jaana Jokisalo User
Jaska Jokunen User
Juha Jokela User
Juha Jokinen User
Jaana Jokisalo Properties
Published Certificates Member Of Password Replication Dial-in Object
Security Environment Sessions Remote control
Remote Desktop Services Profile COM+ Attribute Editor
General Address Account Profile Telephones Organization
User logon name:
jaana.jokisalo
@cyberse.local
User logon name (pre-Windows 2000):
CYBERSE\
jaana.jokisalo
Logon Hours...
Log On To...
Unlock account. This account is currently locked out on this Active Directory Domain Controller.
Account options:
User must change password at next logon
User cannot change password
Password never expires
Store password using reversible encryption
Account expires
Never
End of:
perjantai 3. toukokuuta 2024
OK
Cancel
Apply
Help

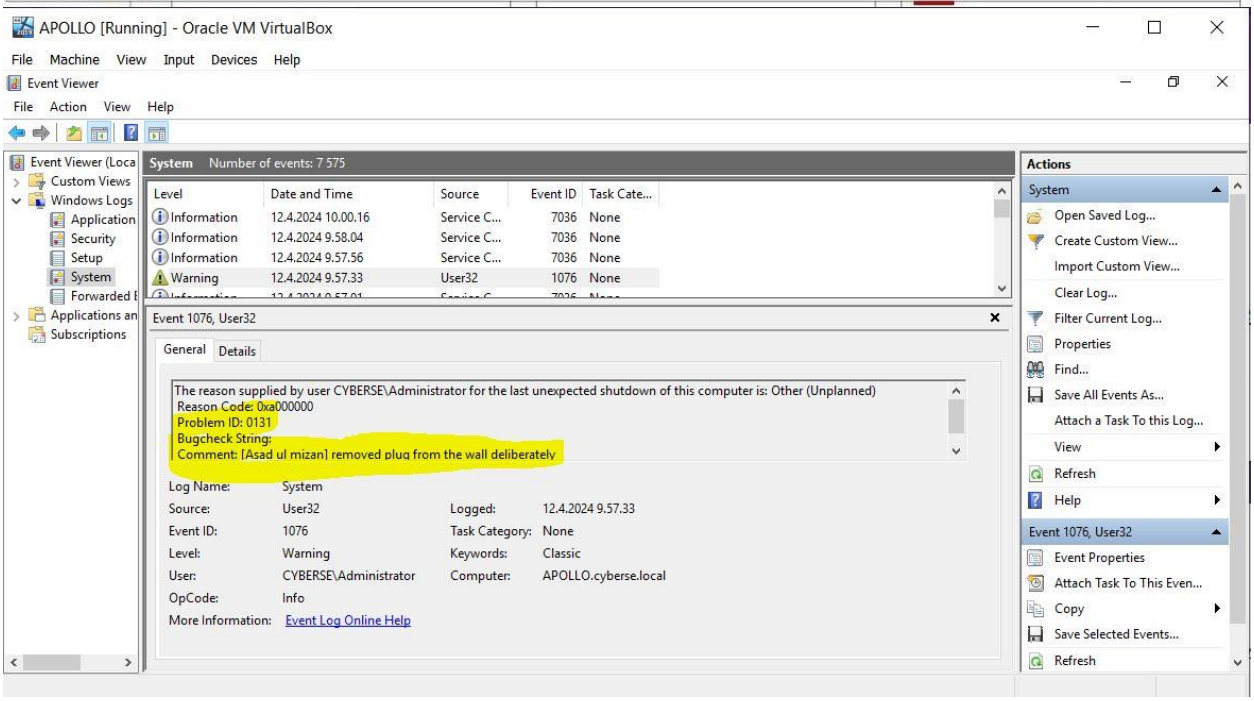

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
cyberse.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Keys
LostAndFound
Managed Service Accou
Pasila
Groups
Johto
Kyber
Pilvi
Program Data
System
Users
NTDS Quotas
TPM Devices
Name Type Description
Jaana Jokisalo User
Jaska Jokunen User
Juha Jokela User
Juha Jokinen User
Active Directory Domain Services
Object Juha Jokela has been disabled.
OK
Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
cyberse.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Keys
LostAndFound
Managed Service Accou
Pasila
Groups
Johto
Kyber
Pilvi
Program Data
System
Users
NTDS Quotas
TPM Devices
Name Type Description
Jaana Jokisalo User
Jaska Jokunen User
Juha Jokela User
Juha Jokinen User
Active Directory Domain Services
Object Juha Jokela has been enabled.
OK

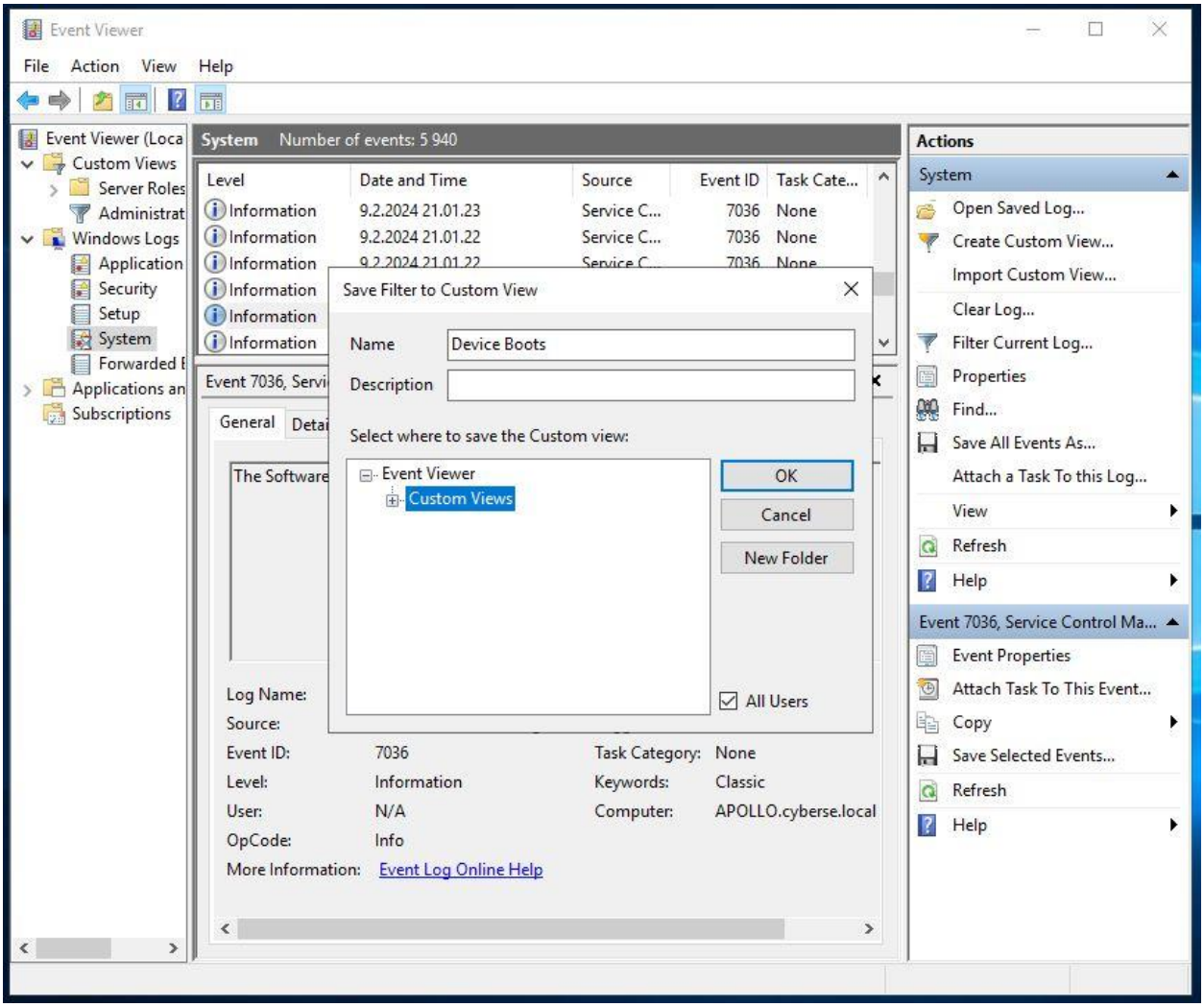

Kyber
Pilvi
Program Data
Close Virtual Machine
You want to:
Save the machine state
Send the shutdown signal
Power off the machine
OK
Cancel
Help
Shutdown Event Tracker
Why did the computer shut down unexpectedly?
Other (Unplanned)
A shutdown or restart for an unknown reason
Problem Id
0131
Comment: (This field is REQUIRED for the reason you selected)
[Asad Ul Mizan] removed the plug from the wall quite deliberately.
OK
Cancel

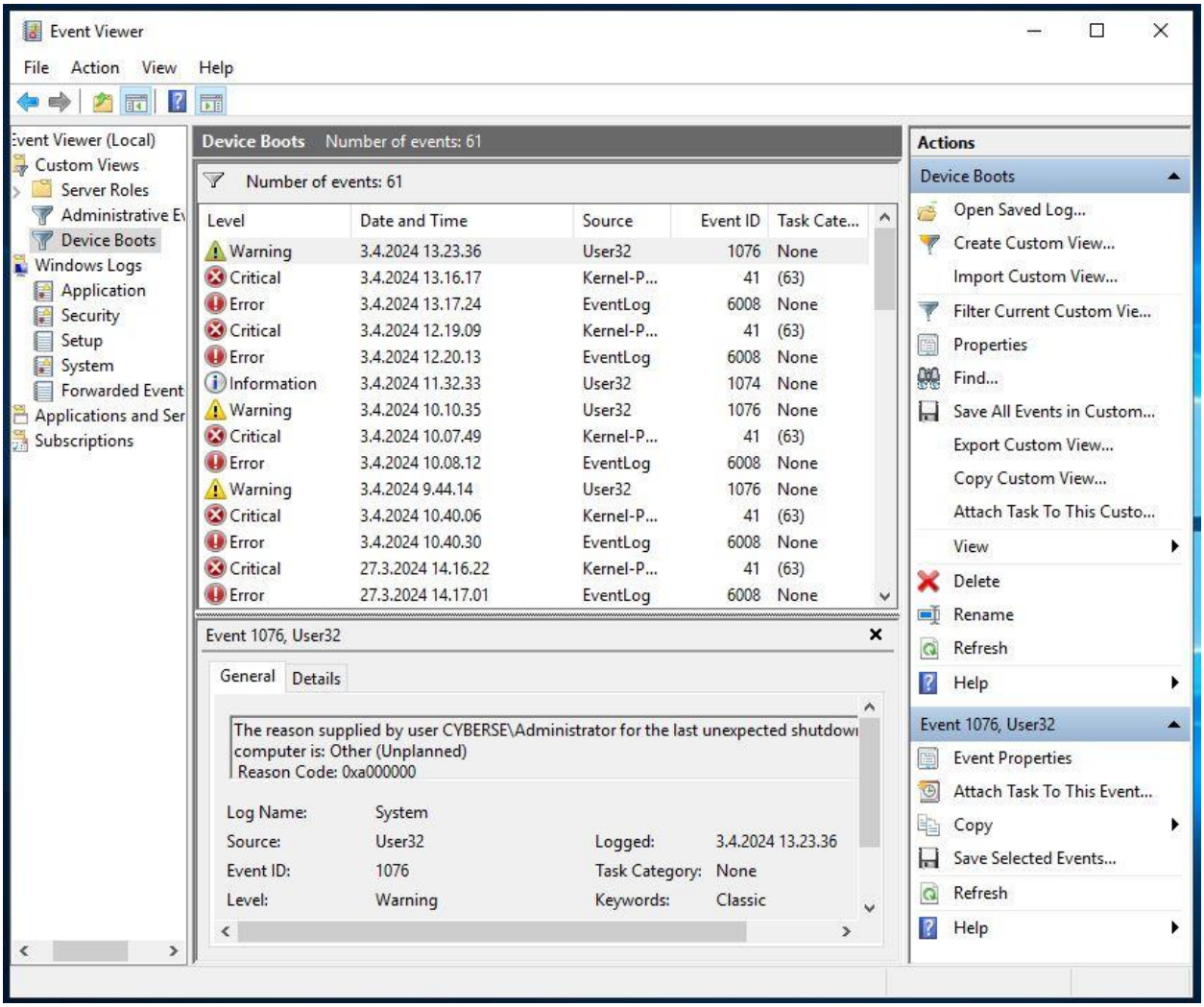

Event Viewer
File Action View Help
Event Viewer (Lo
Custom Vie
Windows Lo
Applicat
Security
Setup
System
Forwarde
Applications
Subscriptior
Security Number of events: 37 868 (!) New events available
Keywords Date and Time Source Event ID Task C...
Audit Success 3.4.2024 13.01.29 Micros... 4624 Logon
Audit Success 3.4.2024 13.01.29 Micros... 4672 Special...
Audit Success 3.4.2024 13.01.29 Micros... 4624 Logon
Audit Success 3.4.2024 13.01.29 Micros... 4672 Special...
Audit Success 3.4.2024 13.01.29 Micros... 4624 Logon
Audit Success 3.4.2024 13.01.29 Micros... 4672 Special...
Audit Failure 3.4.2024 13.01.19 Micros... 4771 Kerber...
Audit Success 3.4.2024 13.01.15 Micros... 4740 User A...
Audit Failure 3.4.2024 13.01.15 Micros... 4771 Kerber...
Audit Failure 3.4.2024 13.01.11 Micros... 4771 Kerber...
Event 4771, Microsoft Windows security auditing.
General Details
Security ID: CYBERSE\jaana.jokisalo
Account Name: jaana.jokisalo
Name: Security
urce: Microsoft Windows security
nt ID: 4771
el: Information
r: N/A
Code: Info
re Information: Event Log Online Help
Logged: 3.4.2024 13.01.08
Task Category: Kerberos Authentication Servic
Keywords: Audit Failure
Computer: APOLLO.cyberse.local
Actions
Security
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 4771, Microsoft Window...
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help

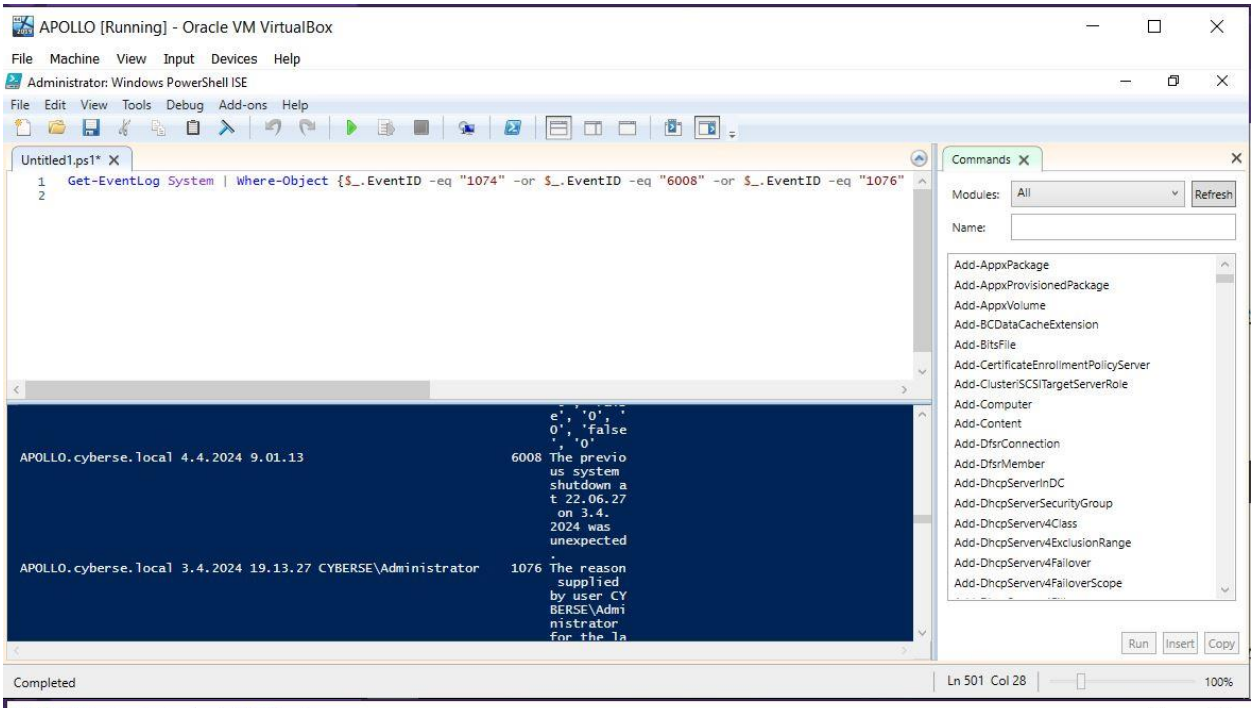

Event Viewer
File Action View Help
Event Viewer (Lo
Custom View
Windows Lo
Applicat
Security
Setup
System
Forwarde
Applications
Subscriptior
Security Number of events: 37 998 (!) New events available
Keywords Date and Time Source Event ID Task C...
Audit Success 3.4.2024 13.42.19 Micros... 4634 Logoff
Audit Success 3.4.2024 13.42.19 Micros... 4634 Logoff
Audit Success 3.4.2024 13.42.19 Micros... 4624 Logon
Audit Success 3.4.2024 13.42.19 Micros... 4672 Special...
Find
Find what: 4767
Find Next
Cancel
Event 4767, Microsoft Windows security auditing.
General Details
A user account was unlocked.
Subject:
Security ID: CYBERSE\Administrator
Log Name: Security
Source: Microsoft Windows security
Logged: 3.4.2024 13.41.40
Event ID: 4767
Task Category: User Account Manageme
Level: Information
Keywords: Audit Success
User: N/A
Computer: APOLLO.cyberse.local
OpCode: Info
More Information: Event Log Online Help
Actions
Security
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 4767, Microsoft Window...
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help
Action: In progress...

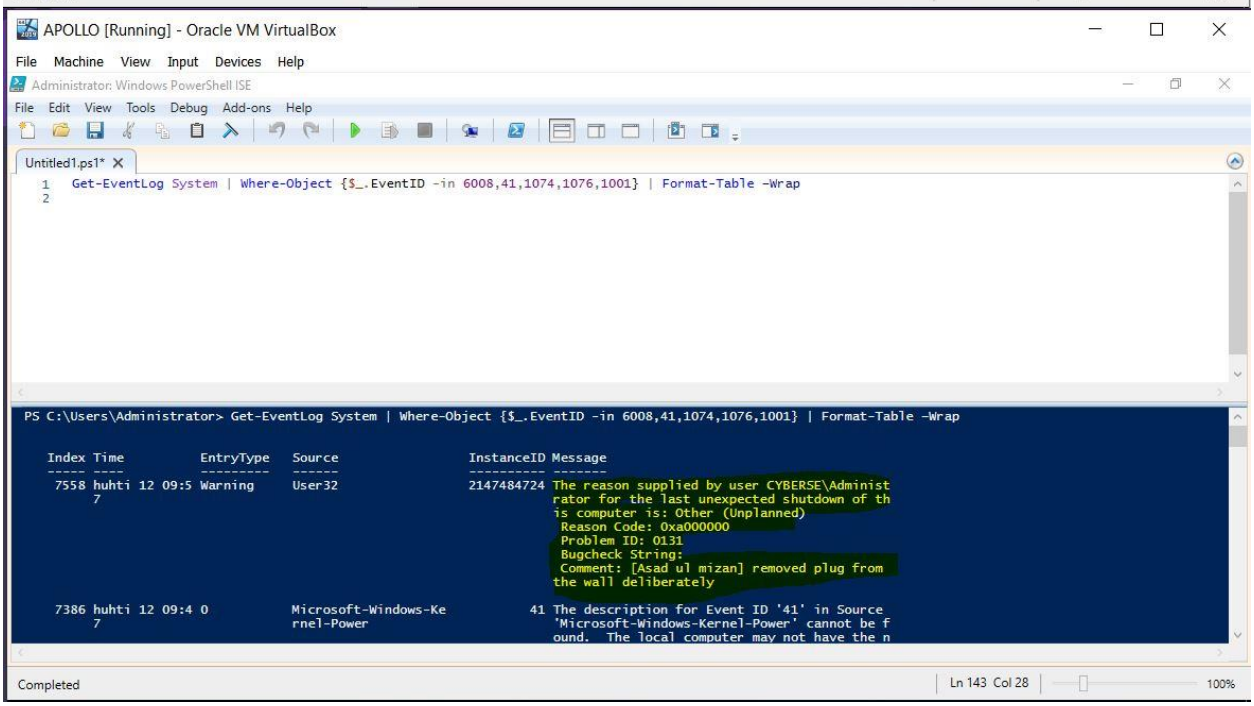

Event Viewer
File Action View Help
Security Number of events: 37 998 (!) New events available
Keywords Date and Time Source Event ID Task C...
Audit Success 20.3.2024 17.55.20 Micros... 4634 Logoff
Audit Success 20.3.2024 17.55.20 Micros... 4624 Logon
Audit Success 20.3.2024 17.55.20 Micros... 4672 Special...
Audit Success 20.3.2024 17.54.20 Micros... 4634 Logoff
Find
Find what: 4722
Find Next
Cancel
Event 4722, Microsoft Windows security auditing.
General Details
A user account was enabled.
Subject:
Log Name: Security
Source: Microsoft Windows security
Logged: 20.3.2024 17.53.17
Event ID: 4722
Task Category: User Account Manageme
Level: Information
Keywords: Audit Success
User: N/A
Computer: APOLLO.cyberse.local
OpCode: Info
More Information: Event Log Online Help
Actions
Security
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 4722, Microsoft Window...
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help
Action: In progress...

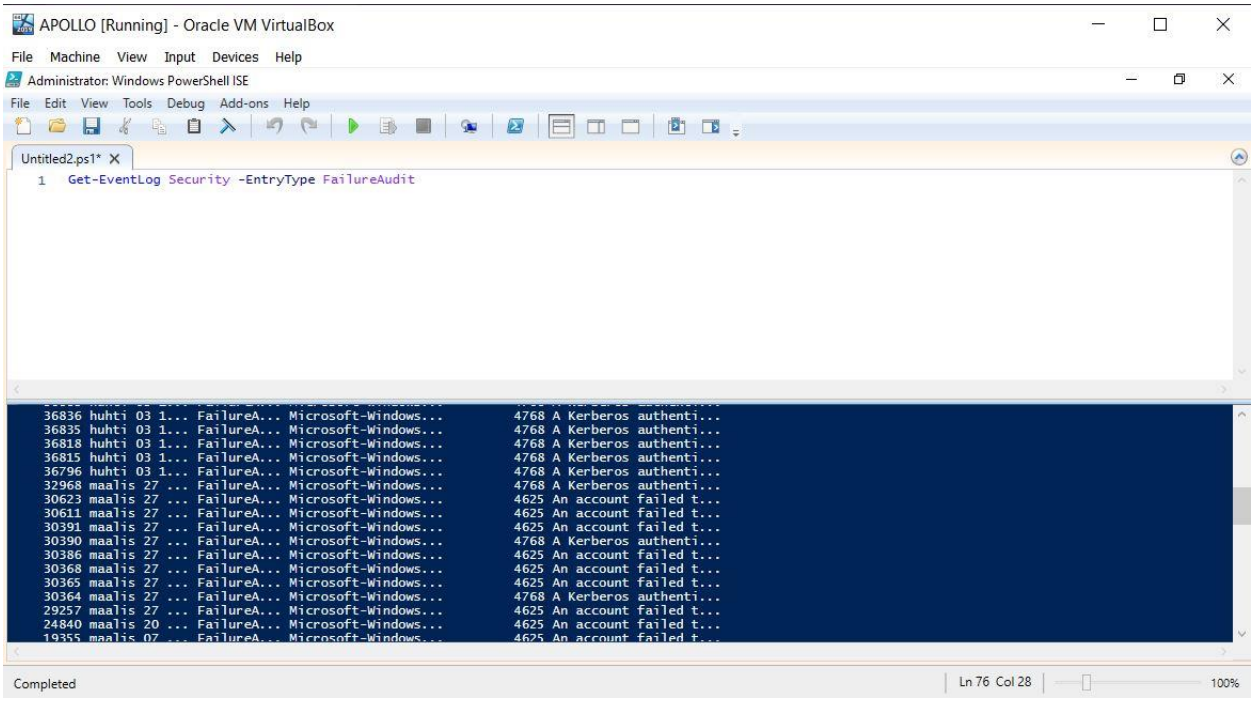

APOLLO [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Event Viewer
File Action View Help
System Number of events: 7 575
Level Date and Time Source Event ID Task Cate...
Information 12.4.2024 10.00.16 Service C... 7036 None
Information 12.4.2024 9.58.04 Service C... 7036 None
Information 12.4.2024 9.57.56 Service C... 7036 None
Warning 12.4.2024 9.57.33 User32 1076 None
Event 1076, User32
General Details
The reason supplied by user CYBERSE\Administrator for the last unexpected shutdown of this computer is: Other (Unplanned)
Reason Code: 0xa000000
Problem ID: 0131
Bugcheck String:
Comment: [Asad ul mizan] removed plug from the wall deliberately
Log Name: System
Source: User32
Logged: 12.4.2024 9.57.33
Event ID: 1076
Task Category: None
Level: Warning
Keywords: Classic
User: CYBERSE\Administrator
Computer: APOLLO.cyberse.local
OpCode: Info
More Information: Event Log Online Help
Actions
System
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 1076, User32
Event Properties
Attach Task To This Even...
Copy
Save Selected Events...
Refresh


Event Viewer
File Action View Help
Event Viewer (Loca
Custom Views
Server Roles
Administrat
Windows Logs
Application
Security
Setup
System
Forwarded E
Applications an
Subscriptions
System Number of events: 5 940
Level Date and Time Source Event ID Task Cate...
Information 9.2.2024 21.01.23 Service C... 7036 None
Information 9.2.2024 21.01.22 Service C... 7036 None
Information 9.2.2024 21.01.22 Service C... 7036 None
Information
Information
Information
Save Filter to Custom View
Name Device Boots
Description
Select where to save the Custom view:
Event Viewer
Custom Views
OK
Cancel
New Folder
All Users
Event 7036, Servi
General Detai
The Software
Log Name:
Source:
Event ID: 7036
Task Category: None
Level: Information
Keywords: Classic
User: N/A
Computer: APOLLO.cyberse.local
OpCode: Info
More Information: Event Log Online Help
Actions
System
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 7036, Service Control Ma...
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Server Roles
Administrative Ev
Device Boots
Windows Logs
Application
Security
Setup
System
Forwarded Event
Applications and Ser
Subscriptions
Device Boots Number of events: 61
Number of events: 61
Level Date and Time Source Event ID Task Cate...
Warning 3.4.2024 13.23.36 User32 1076 None
Critical 3.4.2024 13.16.17 Kernel-P... 41 (63)
Error 3.4.2024 13.17.24 EventLog 6008 None
Critical 3.4.2024 12.19.09 Kernel-P... 41 (63)
Error 3.4.2024 12.20.13 EventLog 6008 None
Information 3.4.2024 11.32.33 User32 1074 None
Warning 3.4.2024 10.10.35 User32 1076 None
Critical 3.4.2024 10.07.49 Kernel-P... 41 (63)
Error 3.4.2024 10.08.12 EventLog 6008 None
Warning 3.4.2024 9.44.14 User32 1076 None
Critical 3.4.2024 10.40.06 Kernel-P... 41 (63)
Error 3.4.2024 10.40.30 EventLog 6008 None
Critical 27.3.2024 14.16.22 Kernel-P... 41 (63)
Error 27.3.2024 14.17.01 EventLog 6008 None
Event 1076, User32
General Details
The reason supplied by user CYBERSE\Administrator for the last unexpected shutdow
computer is: Other (Unplanned)
Reason Code: 0xa000000
Log Name: System
Source: User32 Logged: 3.4.2024 13.23.36
Event ID: 1076 Task Category: None
Level: Warning Keywords: Classic
Actions
Device Boots
Open Saved Log...
Create Custom View...
Import Custom View...
Filter Current Custom Vie...
Properties
Find...
Save All Events in Custom...
Export Custom View...
Copy Custom View...
Attach Task To This Custo...
View
Delete
Rename
Refresh
Help
Event 1076, User32
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help


APOLLO [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1*
1 Get-EventLog System | Where-Object {$_.EventID -eq "1074" -or $_.EventID -eq "6008" -or $_.EventID -eq "1076"
2
Commands
Modules: All
Refresh
Name:
Add-AppxPackage
Add-AppxProvisionedPackage
Add-AppxVolume
Add-BCDataCacheExtension
Add-BitsFile
Add-CertificateEnrollmentPolicyServer
Add-ClusteriSCSITargetServerRole
Add-Computer
Add-Content
Add-DfsrConnection
Add-DfsrMember
Add-DhcpServerInDC
Add-DhcpServerSecurityGroup
Add-DhcpServerv4Class
Add-DhcpServerv4ExclusionRange
Add-DhcpServerv4Failover
Add-DhcpServerv4FailoverScope
APOLLO.cyberse.local 4.4.2024 9.01.13 6008 The previous system shutdown at 22.06.27 on 3.4.2024 was unexpected.
APOLLO.cyberse.local 3.4.2024 19.13.27 CYBERSE\Administrator 1076 The reason supplied by user CYBERSE\Administrator for the la
Run Insert Copy
Completed
Ln 501 Col 28
100%


APOLLO [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1*
1 Get-EventLog System | Where-Object {$_.EventID -in 6008,41,1074,1076,1001} | Format-Table -Wrap
2
PS C:\Users\Administrator> Get-EventLog System | Where-Object {$_.EventID -in 6008,41,1074,1076,1001} | Format-Table -Wrap
Index Time EntryType Source InstanceID Message
7558 huhti 12 09:57 Warning User32 2147484724 The reason supplied by user CYBERSE\Administrator for the last unexpected shutdown of this computer is: Other (Unplanned)
Reason Code: 0xa000000
Problem ID: 0131
Bugcheck String:
Comment: [Asad ul mizan] removed plug from the wall deliberately
7386 huhti 12 09:40 Microsoft-Windows-Kernel-Power 41 The description for Event ID '41' in Source 'Microsoft-Windows-Kernel-Power' cannot be found. The local computer may not have the n
Completed
Ln 143 Col 28
100%


APOLLO [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled2.ps1*
1 Get-EventLog Security -EntryType FailureAudit
36836 huhti 03 1... FailureA... Microsoft-Windows... 4768 A Kerberos authenti...
36835 huhti 03 1... FailureA... Microsoft-Windows... 4768 A Kerberos authenti...
36818 huhti 03 1... FailureA... Microsoft-Windows... 4768 A Kerberos authenti...
36815 huhti 03 1... FailureA... Microsoft-Windows... 4768 A Kerberos authenti...
36796 huhti 03 1... FailureA... Microsoft-Windows... 4768 A Kerberos authenti...
32968 maalis 27 ... FailureA... Microsoft-Windows... 4768 A Kerberos authenti...
30623 maalis 27 ... FailureA... Microsoft-Windows... 4625 An account failed t...
30611 maalis 27 ... FailureA... Microsoft-Windows... 4625 An account failed t...
30391 maalis 27 ... FailureA... Microsoft-Windows... 4625 An account failed t...
30390 maalis 27 ... FailureA... Microsoft-Windows... 4768 A Kerberos authenti...
30386 maalis 27 ... FailureA... Microsoft-Windows... 4625 An account failed t...
30368 maalis 27 ... FailureA... Microsoft-Windows... 4625 An account failed t...
30365 maalis 27 ... FailureA... Microsoft-Windows... 4625 An account failed t...
30364 maalis 27 ... FailureA... Microsoft-Windows... 4768 A Kerberos authenti...
29257 maalis 27 ... FailureA... Microsoft-Windows... 4625 An account failed t...
24840 maalis 20 ... FailureA... Microsoft-Windows... 4625 An account failed t...
Completed
Ln 76 Col 28
100%