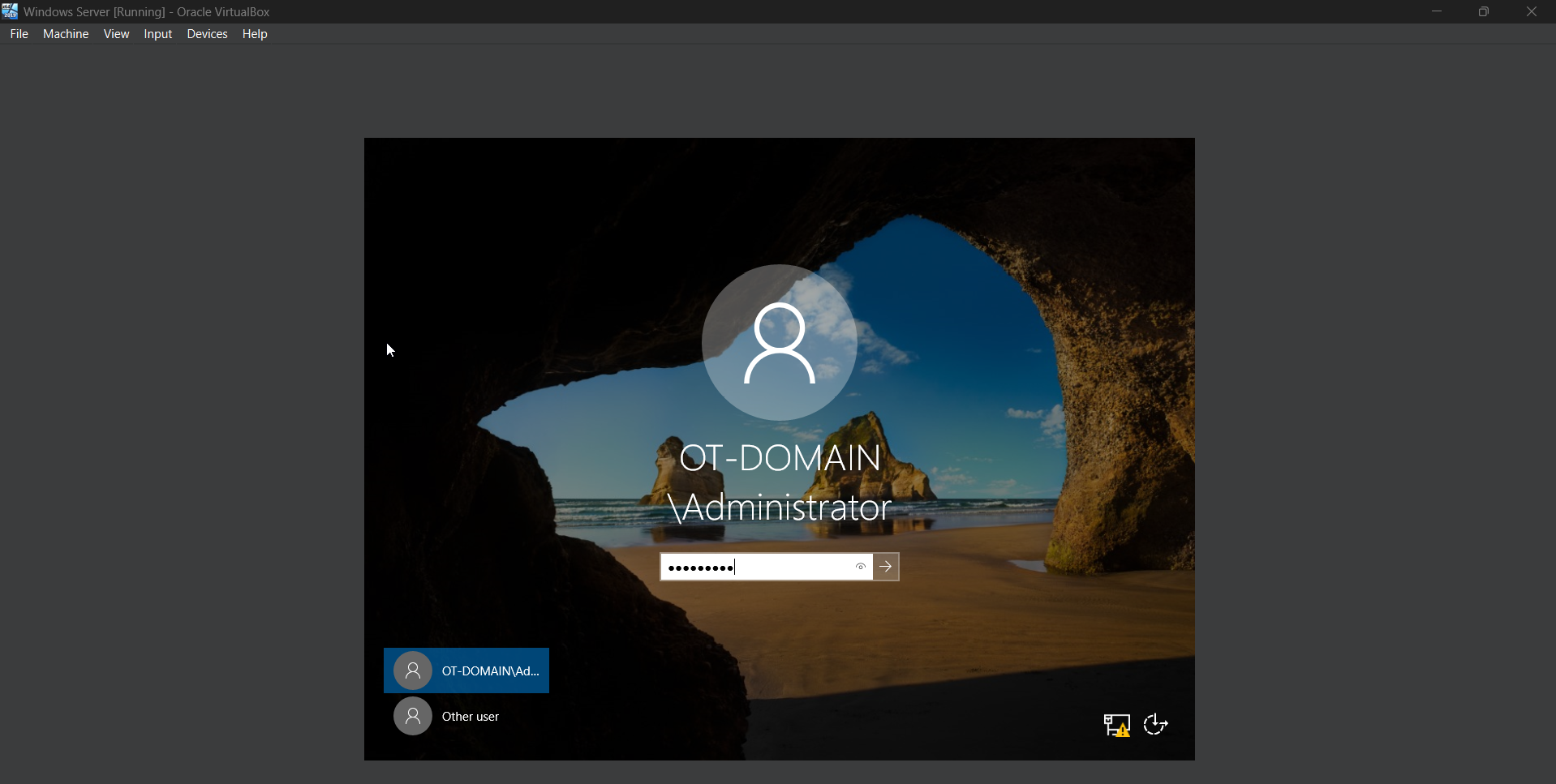
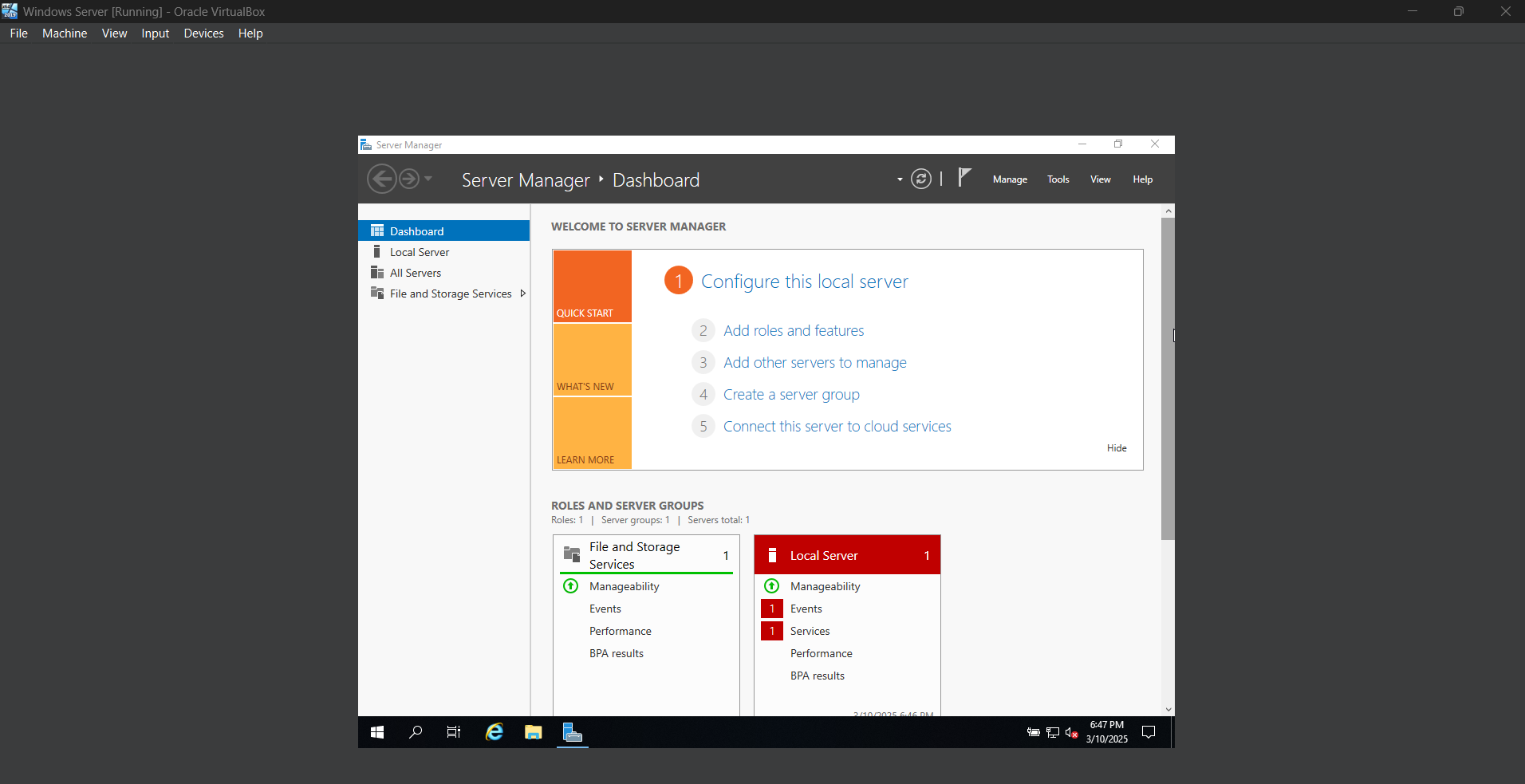
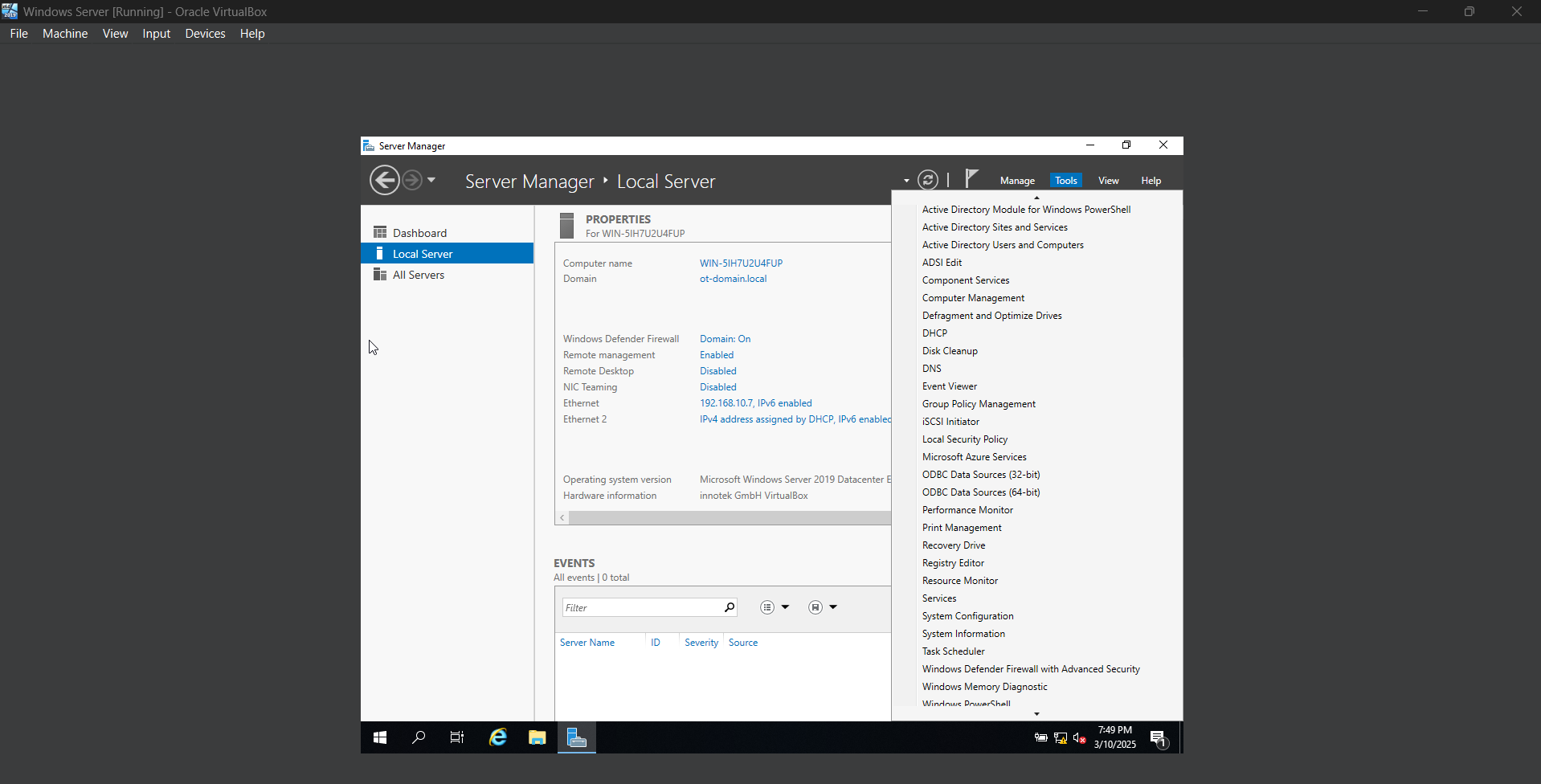
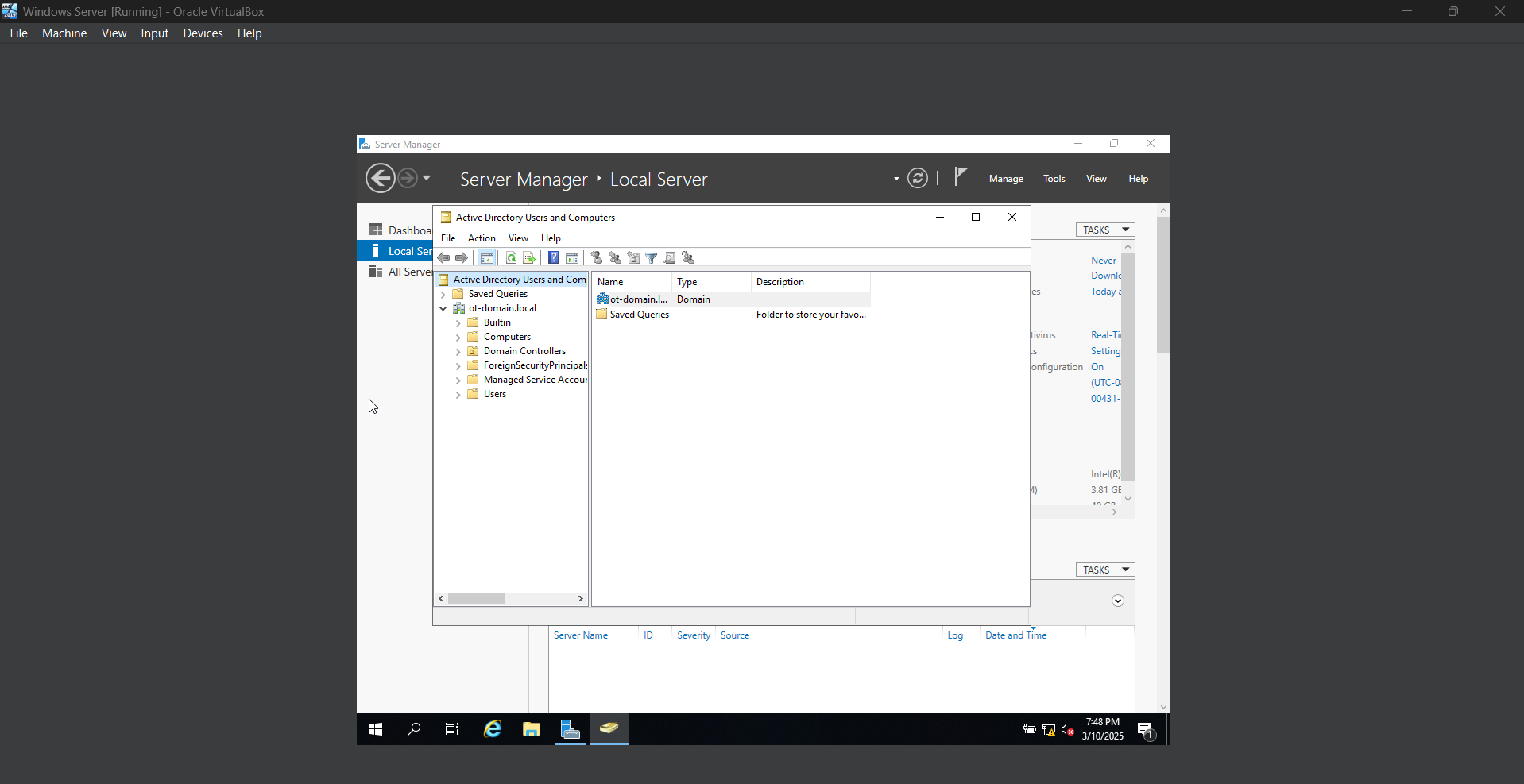
Lab 5 : Using Wazuh to add PowerShell script block logging

* Logged on to the Windows with a domain controller account

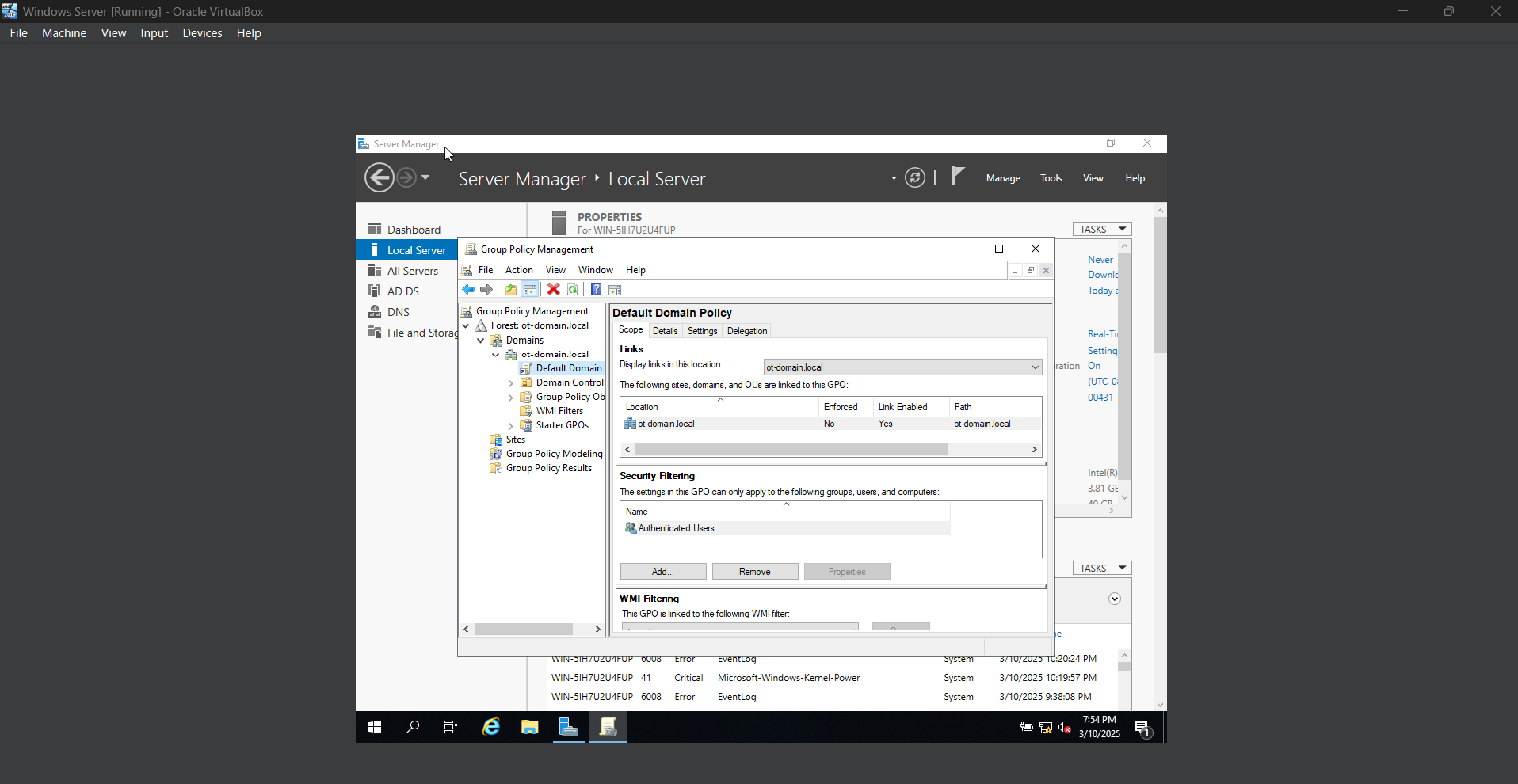


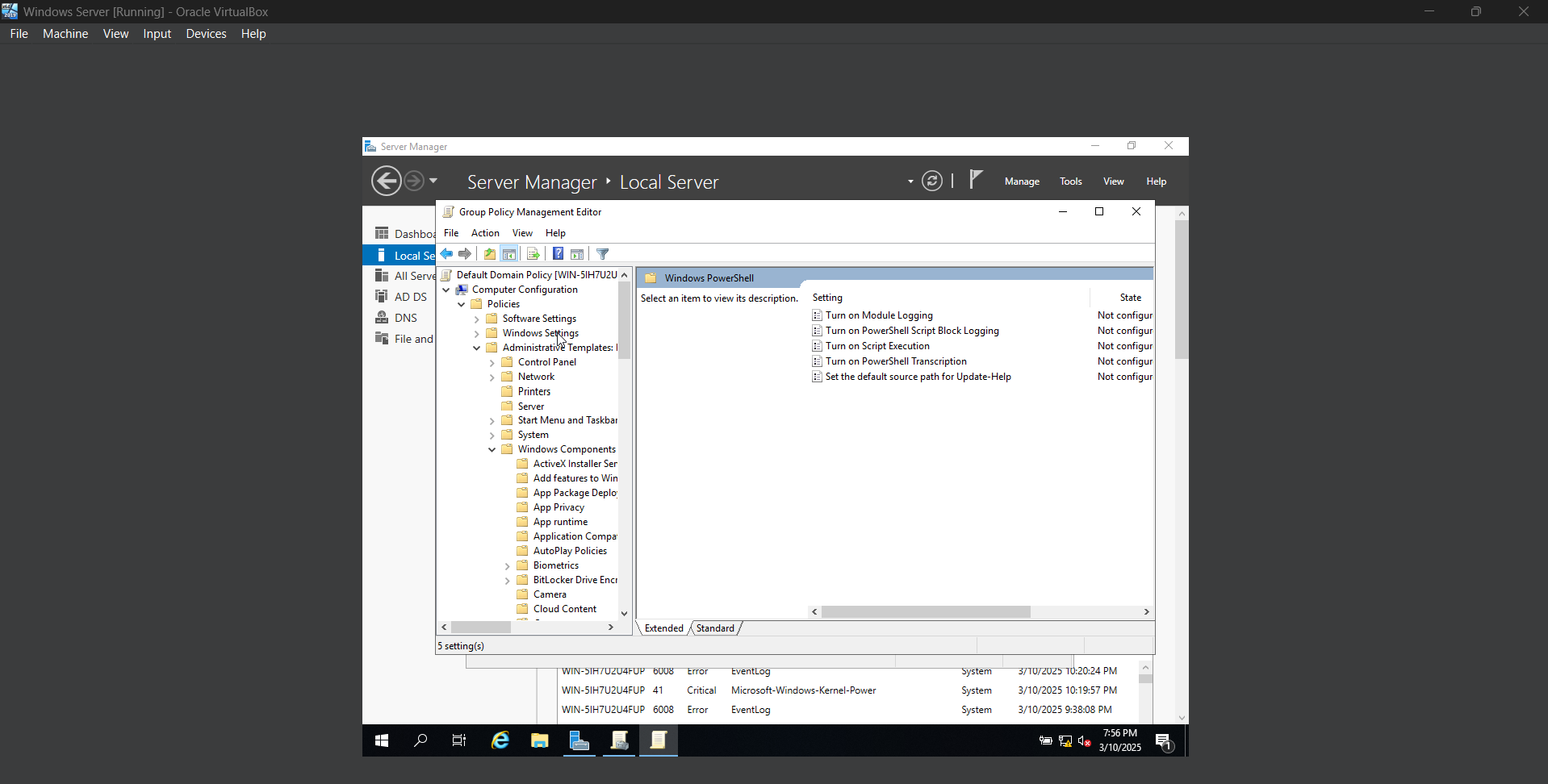


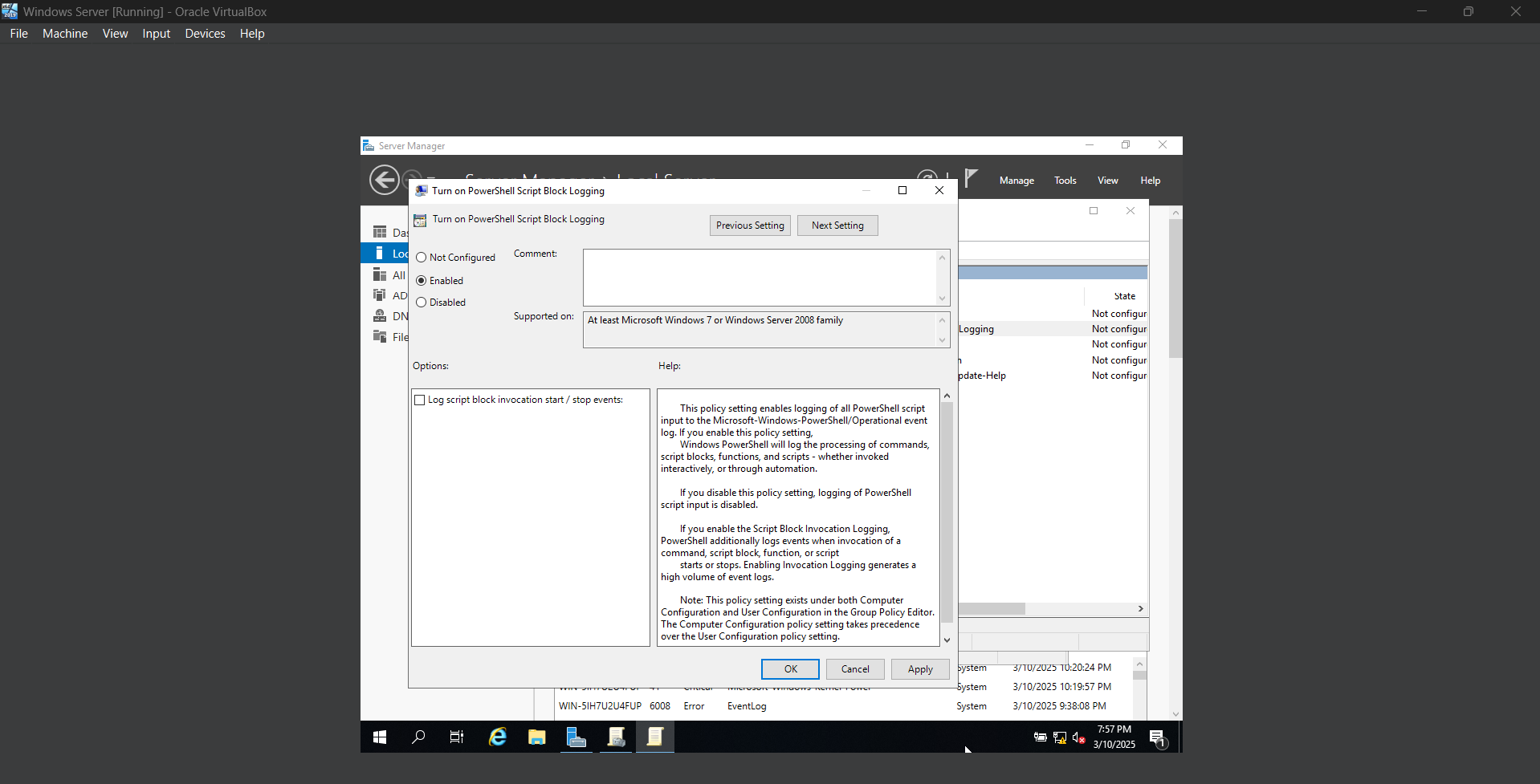


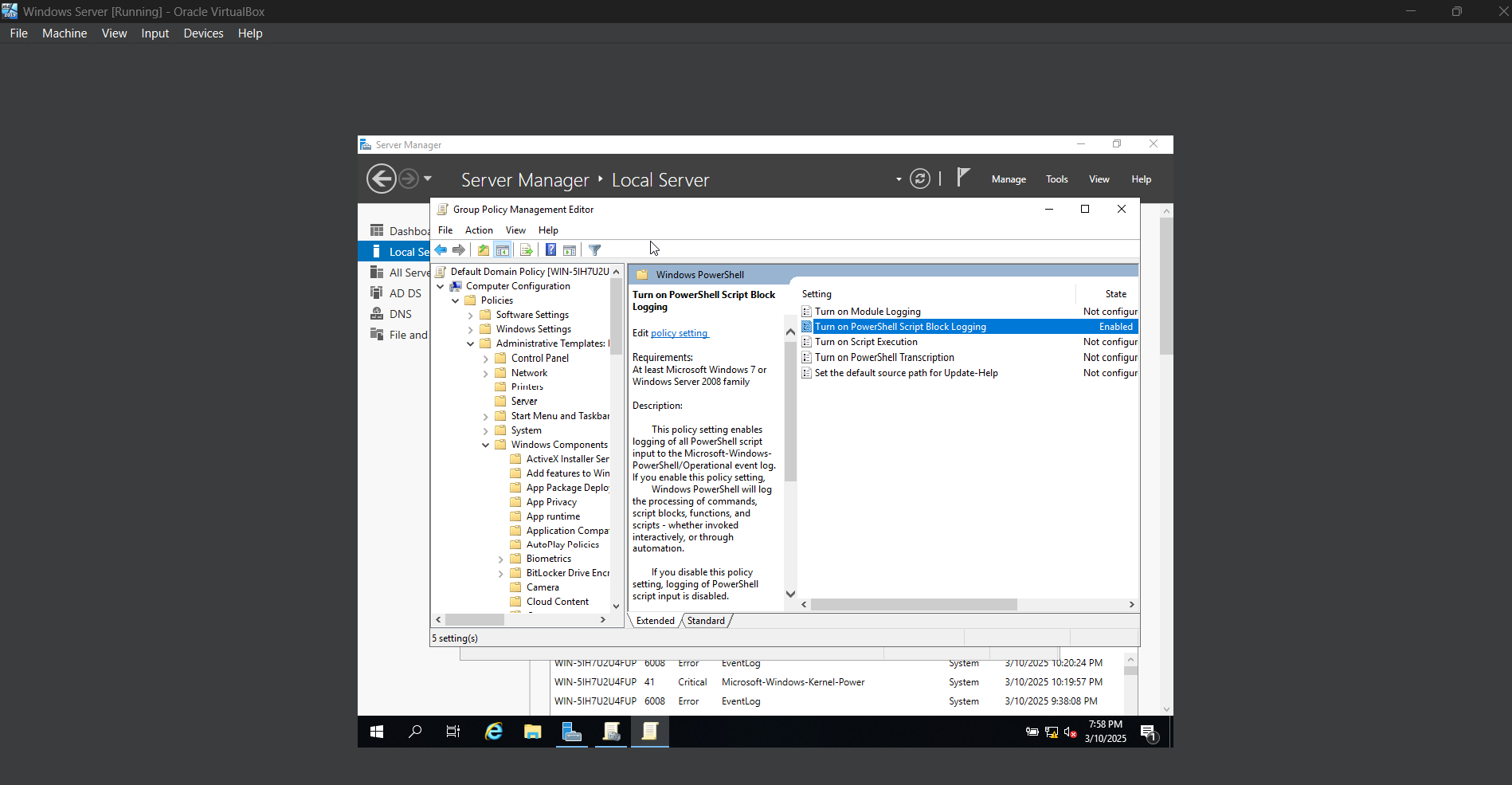


Now, in **Windows Server 2019**, enabled **PowerShell Script Block Logging** by modifying **Group Policy settings** under **Administrative Templates → Windows Components → Windows PowerShell**. Opened **Group Policy Management** from **Server Manager**, right-clicked on the **Default Domain Policy GPO**, and selected **Edit**. Navigated to **Computer Configuration → Policies → Administrative Templates → Windows Components → Windows PowerShell**, then double-clicked on **Turn on PowerShell Script Block Logging**, selected **Enabled**, and clicked **OK** to apply the changes.

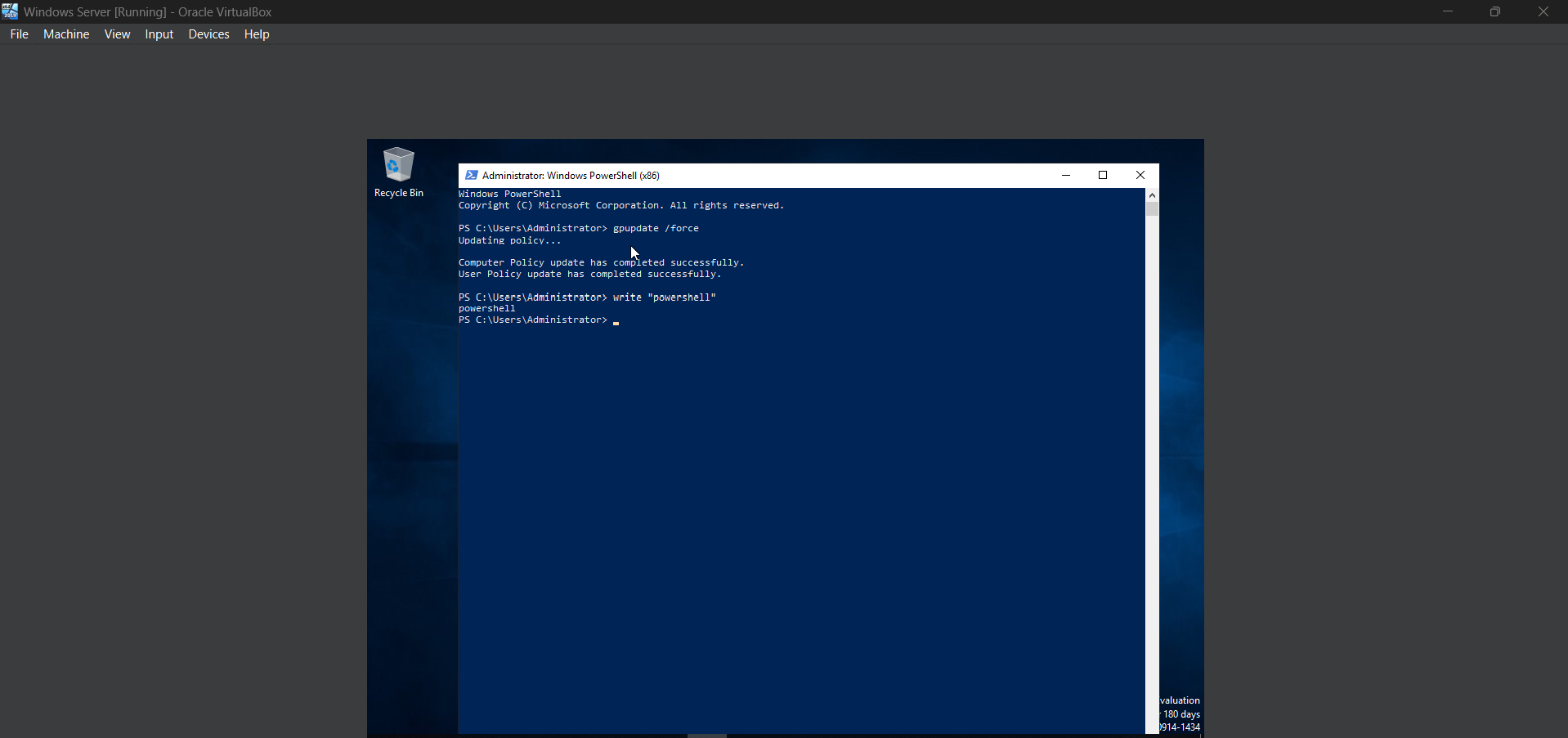








Applied **Group Policy changes** using gpupdate /force in **PowerShell** on **Windows Server 2019** to ensure immediate enforcement across all domain-joined systems.



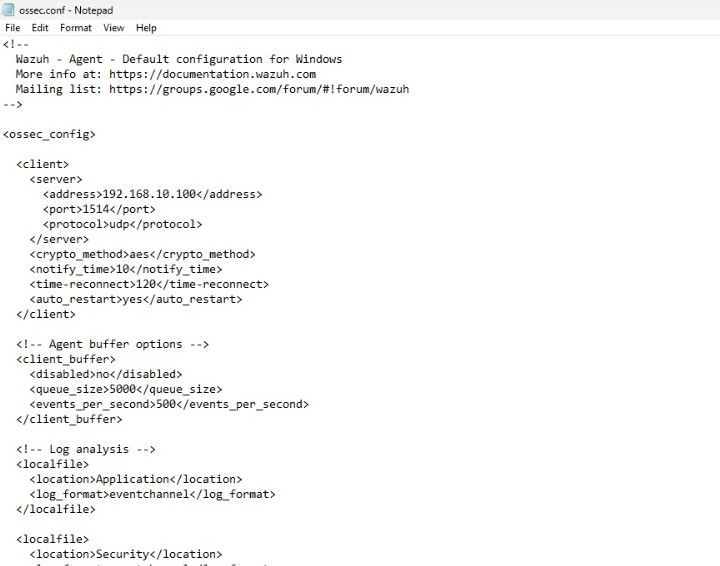
On **Security Onion**, verified that Wazuh was configured to collect PowerShell logs by ensuring the **Wazuh agent** on Windows was forwarding logs to Security Onion. Checked the **ossec.conf** configuration file located at /var/ossec/etc/ossec.conf on Security Onion and confirmed that the following log collection entry was present:

<localfile>

<location>Microsoft-Windows-PowerShell/Operational</location>

<log\_format>eventchannel</log\_format>

</localfile>



Restarted the **Wazuh manager** on Security Onion using:

sudo systemctl restart wazuh-manager

This ensured that the updated configuration took effect and logs from the **Windows Server 2019 machine** were being collected properly.

On **Windows Server 2019**, opened **PowerShell as Administrator**, executed test commands such as:

Get-Process

Then checked **Event Viewer** on Windows Server 2019 by navigating to:

Applications and Services Logs → Microsoft → Windows → PowerShell → Operational

Confirmed that **event ID 4104** was generated, indicating that PowerShell script block logging was working.

On **Security Onion**, accessed **Kibana** and searched for:

event.code:4104

Observed log entries showing PowerShell script executions, confirming that the **Windows Server 2019 logs** were successfully being collected and forwarded to Security Onion for monitoring and analysis.

With this setup, established continuous **PowerShell activity monitoring** across the domain, enhancing **security visibility** and enabling **threat detection** against suspicious PowerShell execution.