Lab 5: Using Wazuh to Add PowerShell Script Block Logging

Author: Phanindhar Reddy Karnati

Date: 03/10/2025

System Used: Windows Server (OT-DC1) & Wazuh Agent

---

1. Introduction

In this lab, we enabled **PowerShell Script Block Logging** using **Group Policy** on Windows Server (OT-DC1) and configured **Wazuh Agent** to collect PowerShell logs. This setup enhances **security monitoring** by logging PowerShell commands executed on the system. We also verified that these logs were correctly recorded in **Event Viewer, Wazuh logs, and Kibana (if applicable).**

---

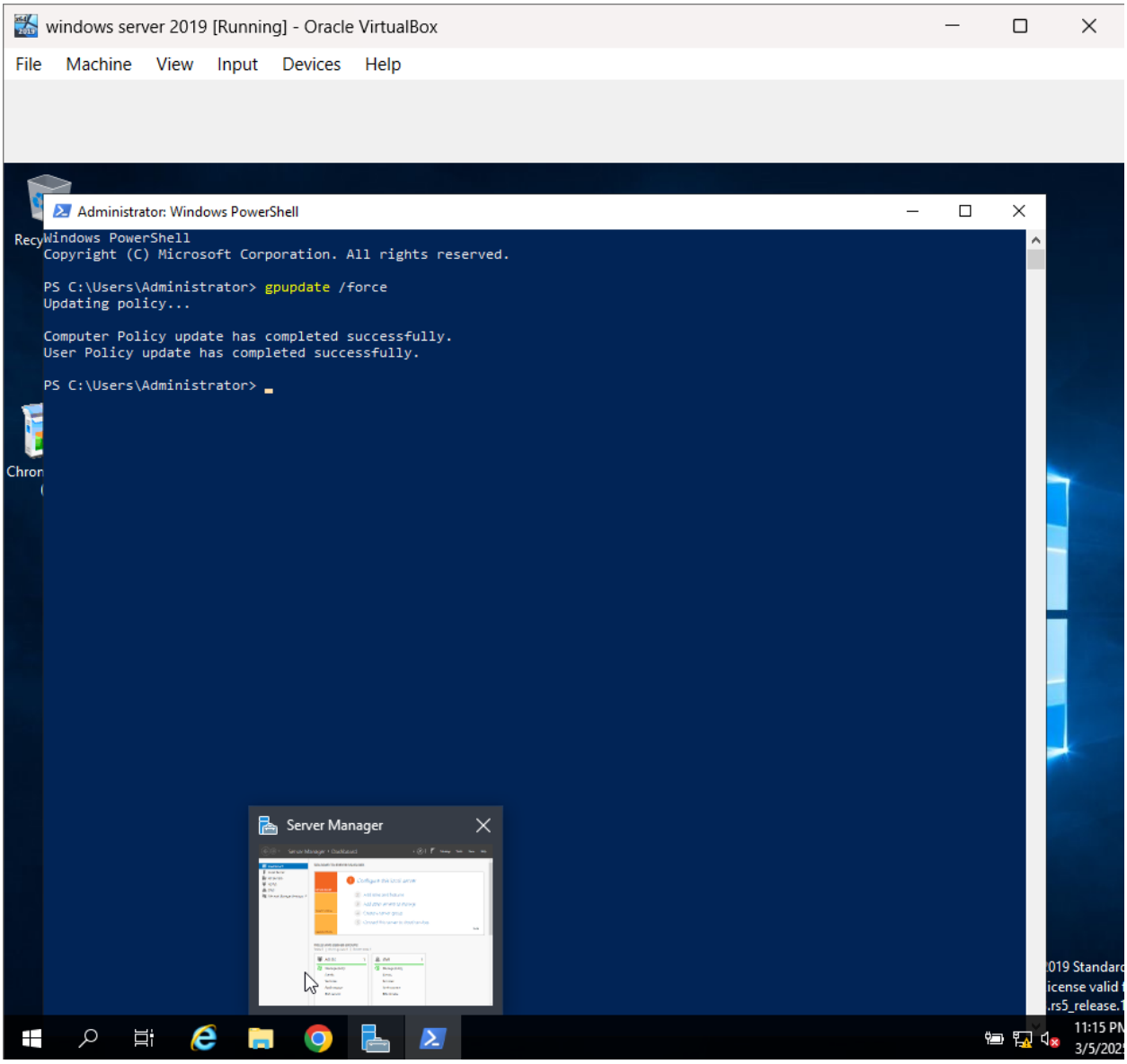
2. Steps Performed

Step 1: Apply Group Policy Changes

After enabling **PowerShell Script Block Logging**, the following steps were performed to apply the Group Policy settings:

1. **Open PowerShell as Administrator** on OT-DC1.
2. Run the command:
3. gpupdate /force

4. **Restart the Windows Client Machines** to ensure policies take effect.



Screenshot 1: Group Policy Editor showing PowerShell Script Block Logging enabled.

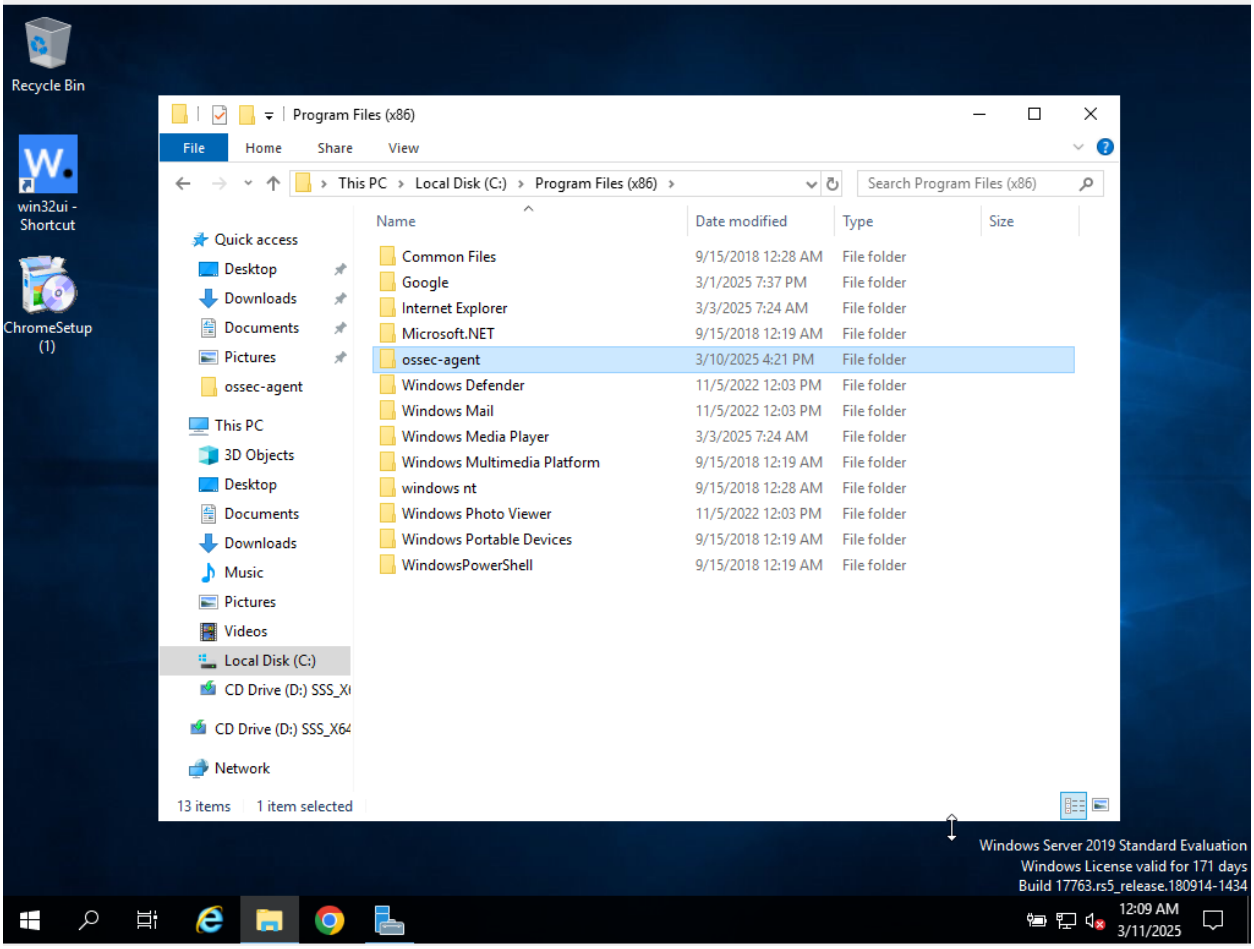
Step 2: Configure Wazuh Agent to Collect PowerShell Logs

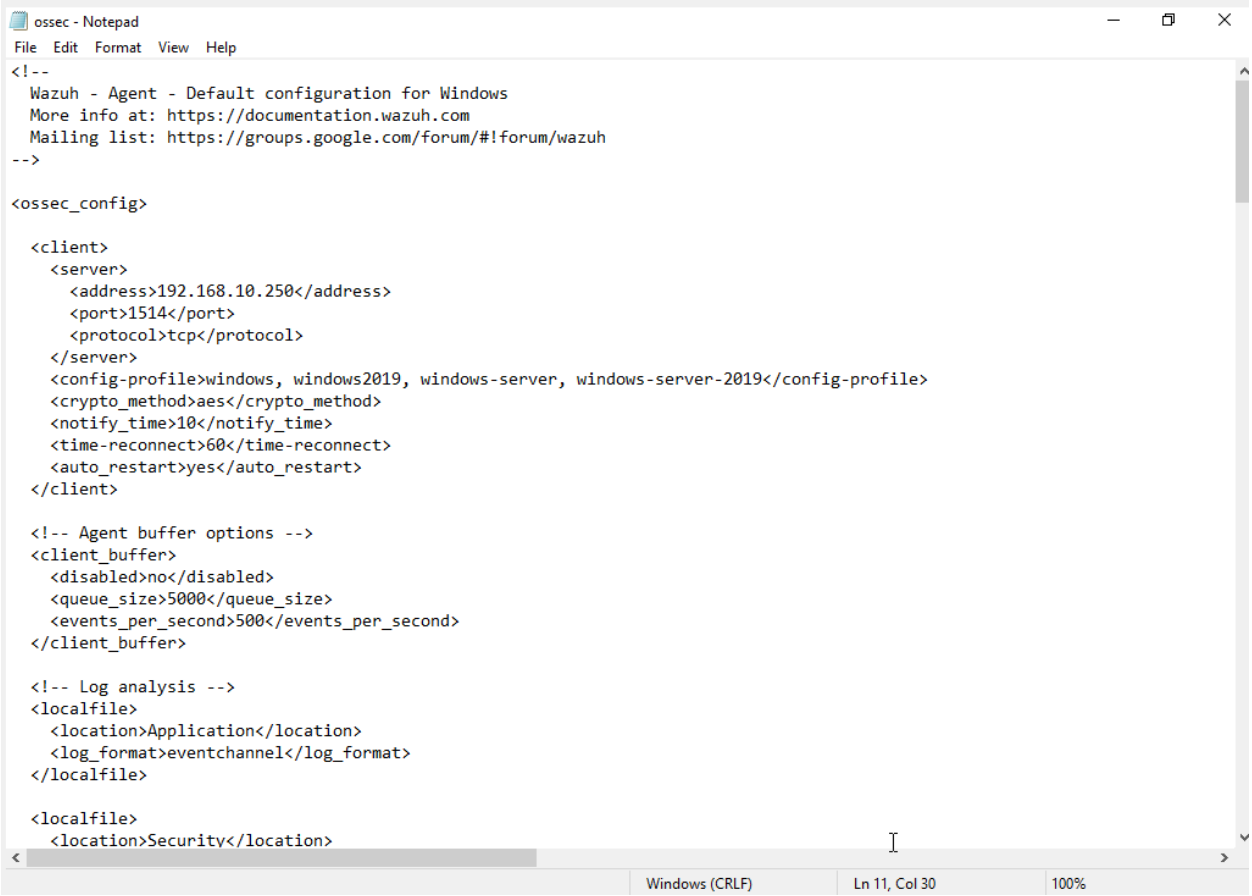
Since Wazuh Agent is installed on OT-DC1, we configured it to monitor PowerShell logs.

1. **Open File Explorer** and navigate to:
2. C:\Program Files (x86)\ossec-agent\

3. **Edit the ossec.conf file**:
    - Open ossec.conf in **Notepad (Run as Administrator)**.
    - Locate the <localfile> section and **add the following lines:**
    - <localfile>
    - <location>Microsoft-Windows-PowerShell/Operational</location>
    - <log_format>eventchannel</log_format>
    - </localfile>

4. **Save the file** and close Notepad.





ossec - Notepad

File Edit Format View Help

```
<!--
  Wazuh - Agent - Default configuration for Windows
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>

  <client>
    <server>
      <address>192.168.10.250</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>windows, windows2019, windows-server, windows-server-2019</config-profile>
    <crypto_method>aes</crypto_method>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
  </client>

  <!-- Agent buffer options -->
  <client_buffer>
    <disabled>no</disabled>
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
  </client_buffer>

  <!-- Log analysis -->
  <localfile>
    <location>Application</location>
    <log_format>eventchannel</log_format>
  </localfile>

  <localfile>
    <location>Security</location>
```

Windows (CRLF) | Ln 11, Col 30 | 100%

5. **Restart Wazuh Agent**:
   - Open **Command Prompt as Administrator**.
   - Run:
   - net stop wazuh
   - net start wazuh

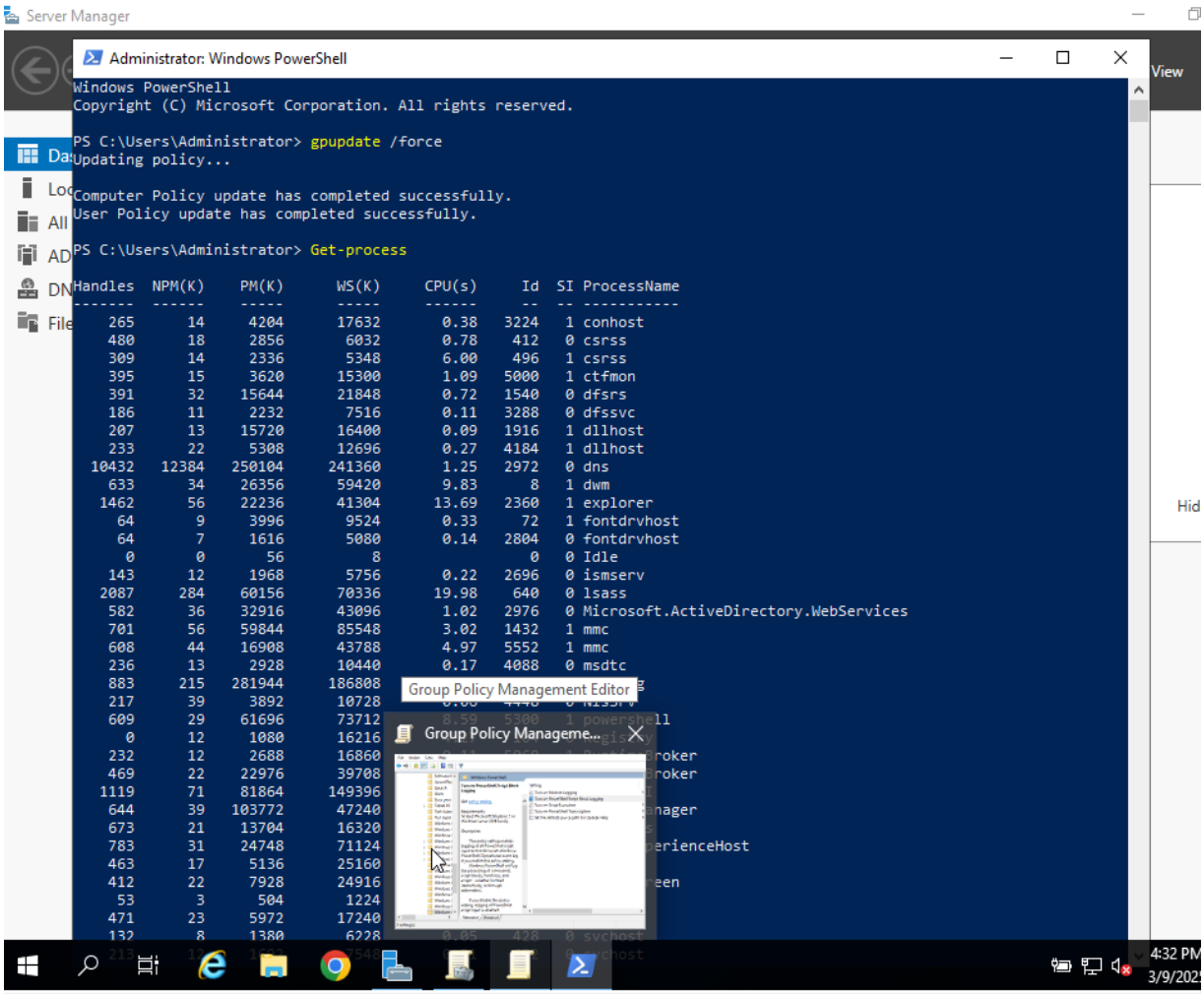
Screenshot 2: Wazuh Agent configuration file (ossec.conf) showing PowerShell logging setup.

Step 3: Generate a PowerShell Event

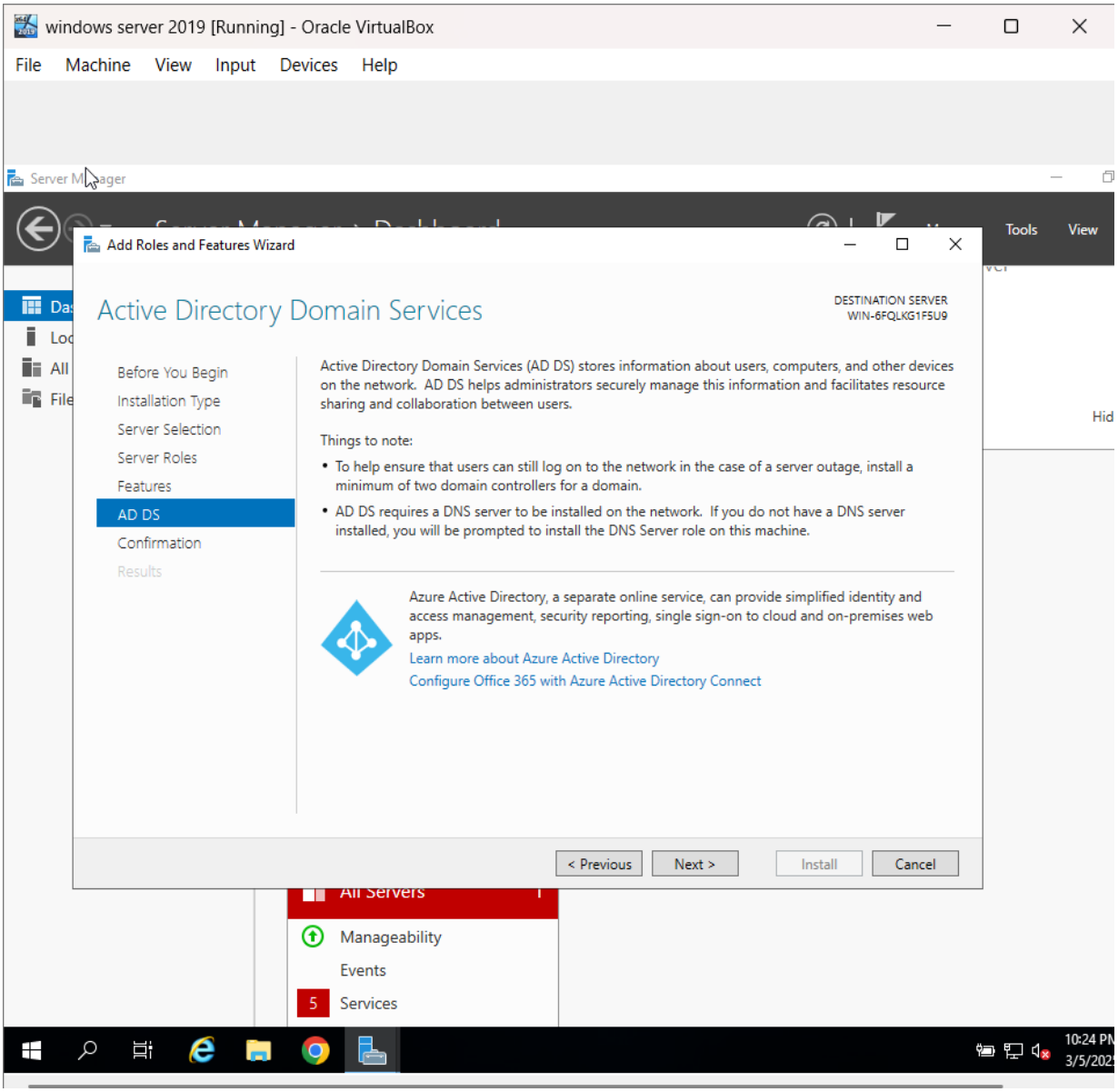
To verify that PowerShell logs are being collected, a **test PowerShell command** was executed.

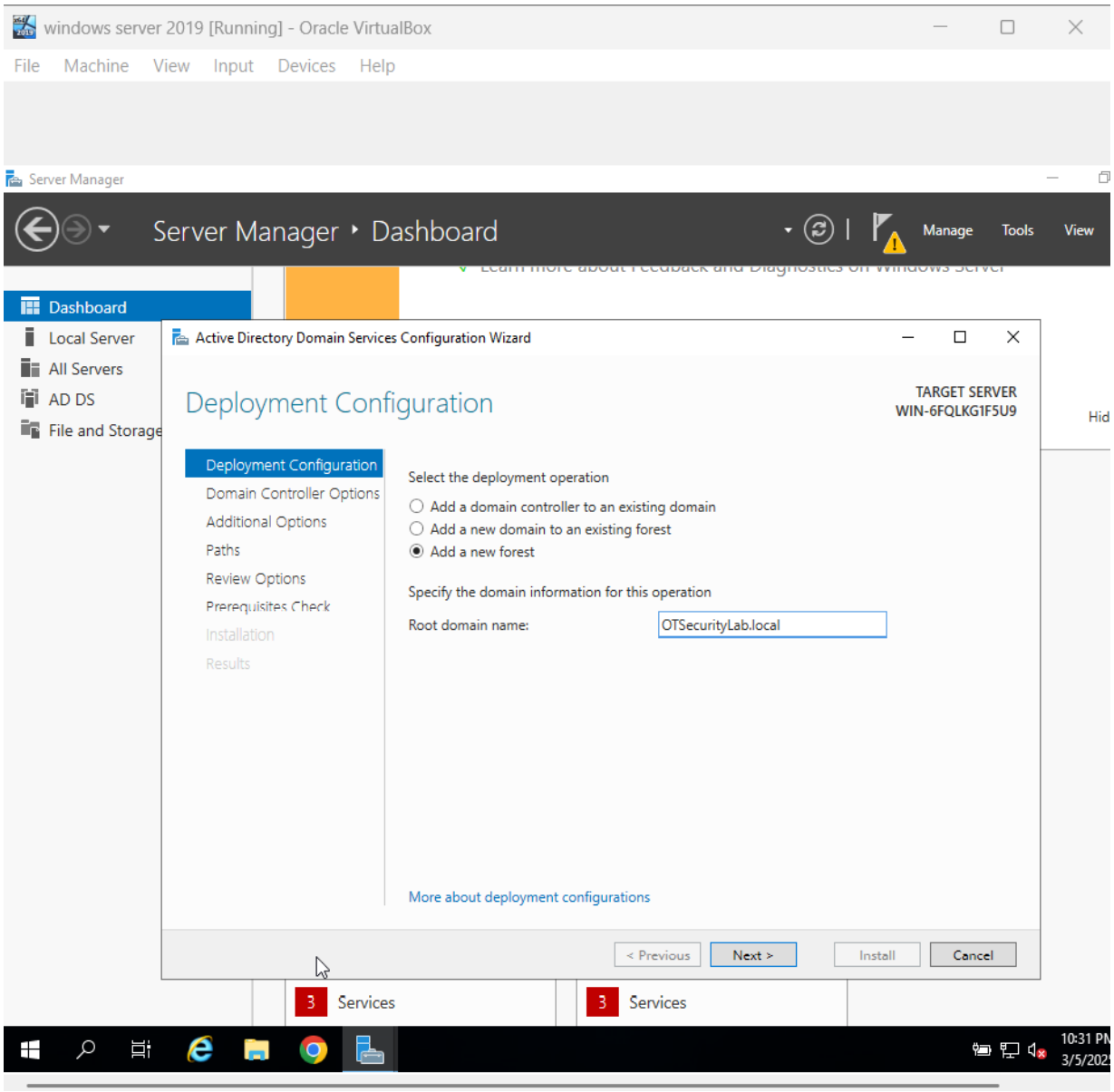
1. **Open PowerShell as Administrator**.
2. Run:

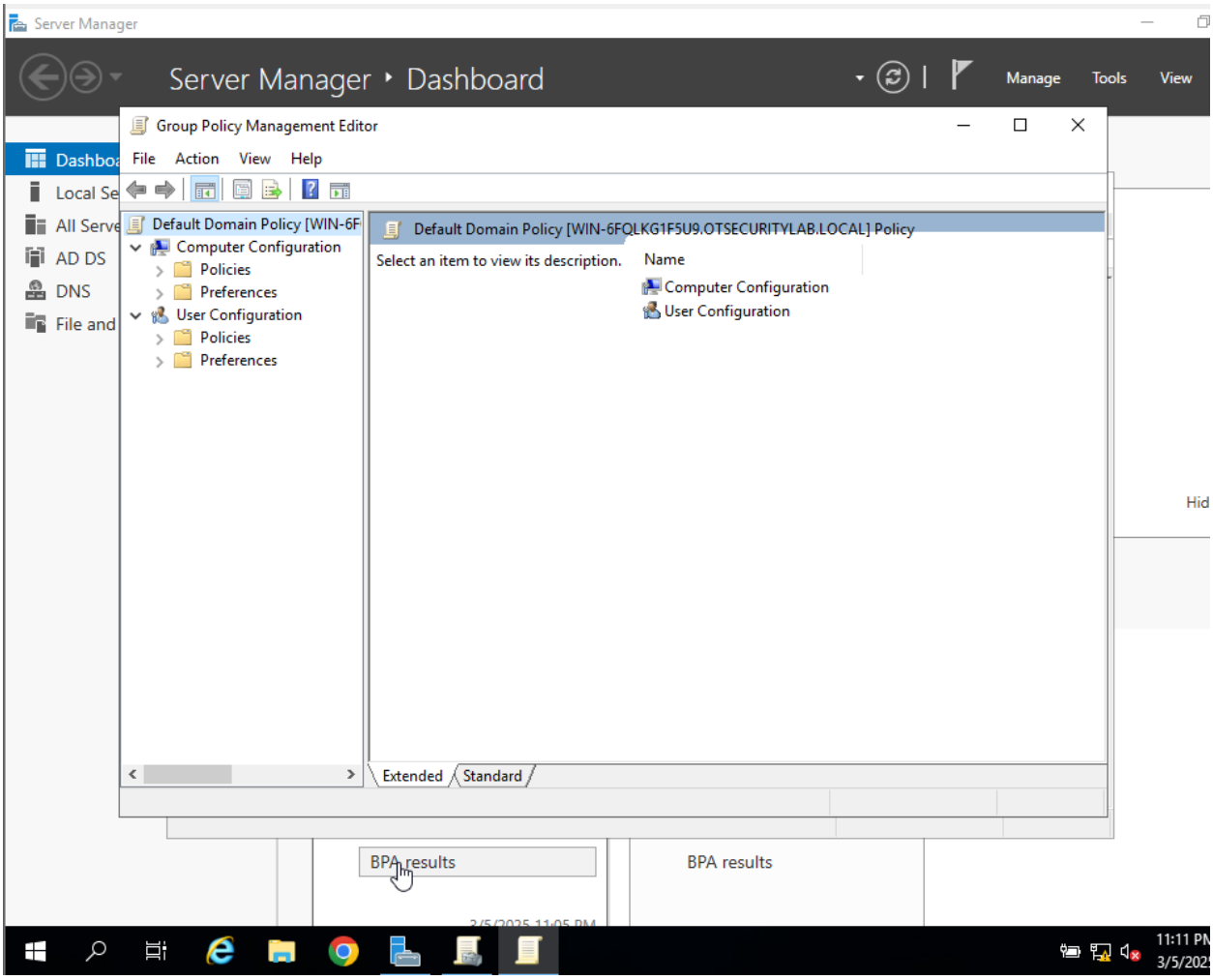
3. Get-Process
4. **Check Event Viewer for Event ID 4104**:
    - Open **Run (Win + R)**, type eventvwr.msc, and press **Enter**.
    - Navigate to:
    - Applications and Services Logs → Microsoft → Windows → PowerShell → Operational
    - Look for **Event ID 4104**.

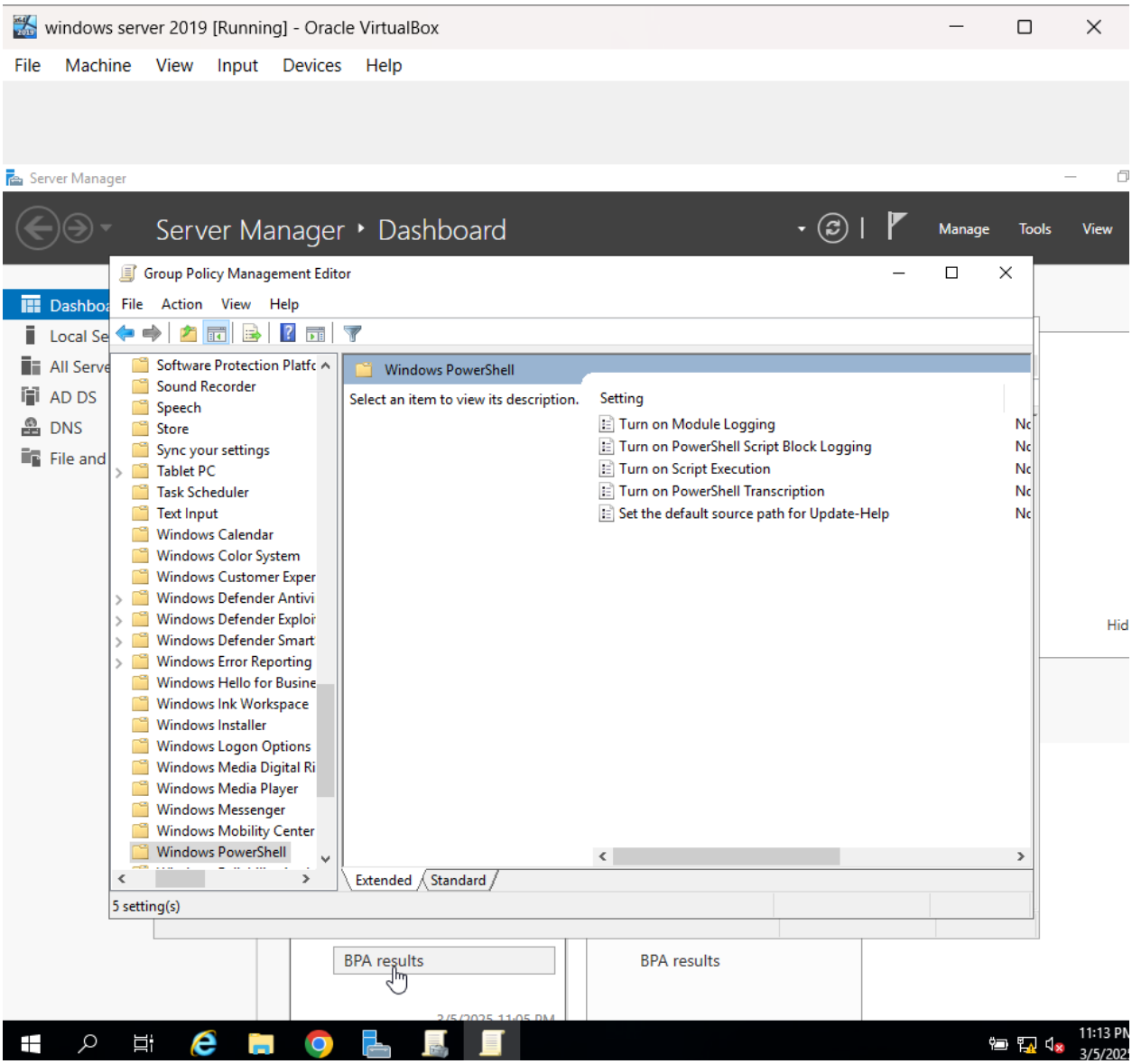


Event Viewer displaying Event ID 4104 for PowerShell script execution.


windows server 2019 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Server Manager
Tools View
Add Roles and Features Wizard
Active Directory Domain Services
DESTINATION SERVER
WIN-6FQLKG1F5U9
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.
Things to note:
• To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
• AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.
Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.
Learn more about Azure Active Directory
Configure Office 365 with Azure Active Directory Connect
< Previous
Next >
Install
Cancel
All Servers
Manageability
Events
5
Services
10:24 PM


windows server 2019 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager ‣ Dashboard
Manage Tools View
Dashboard
Local Server
All Servers
AD DS
File and Storage
Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
WIN-6FQLKG1F5U9
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
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:
OTSecurityLab.local
More about deployment configurations
< Previous
Next >
Install
Cancel
3 Services
3 Services
10:31 PM


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Group Policy Management Editor
File
Action
View
Help
Default Domain Policy [WIN-6F
Computer Configuration
Policies
Preferences
User Configuration
Policies
Preferences
Default Domain Policy [WIN-6FQLKG1F5U9.OTSECURITYLAB.LOCAL] Policy
Select an item to view its description.
Name
Computer Configuration
User Configuration
Extended
Standard
Dashboa
Local Se
All Serve
AD DS
DNS
File and
Hid
BPA results
BPA results
11:11 PM



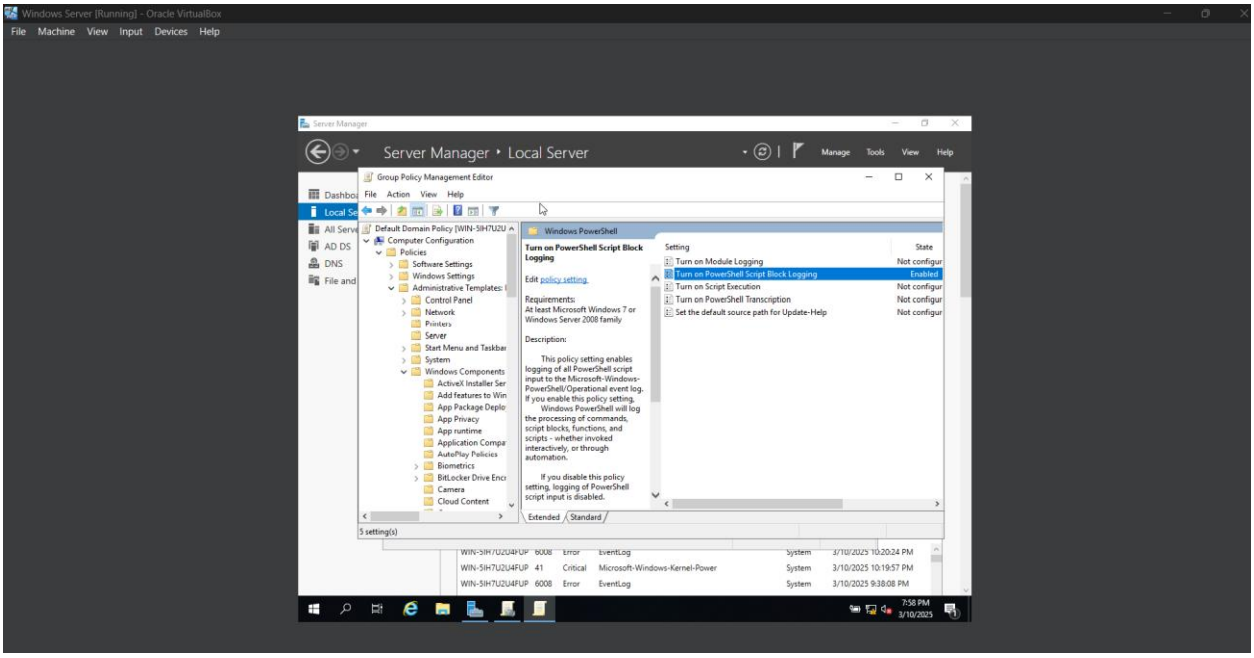
Step 4: Verify Wazuh is Collecting PowerShell Logs

Next, we verified that Wazuh Agent is successfully logging PowerShell activity.

1. **Open Command Prompt as Administrator**.
2. Run:
3. type "C:\Program Files (x86)\ossec-agent\logs\ossec.log"
4. Look for logs mentioning:

5. eventchannel: Microsoft-Windows-PowerShell/Operational
6. event.code: 4104

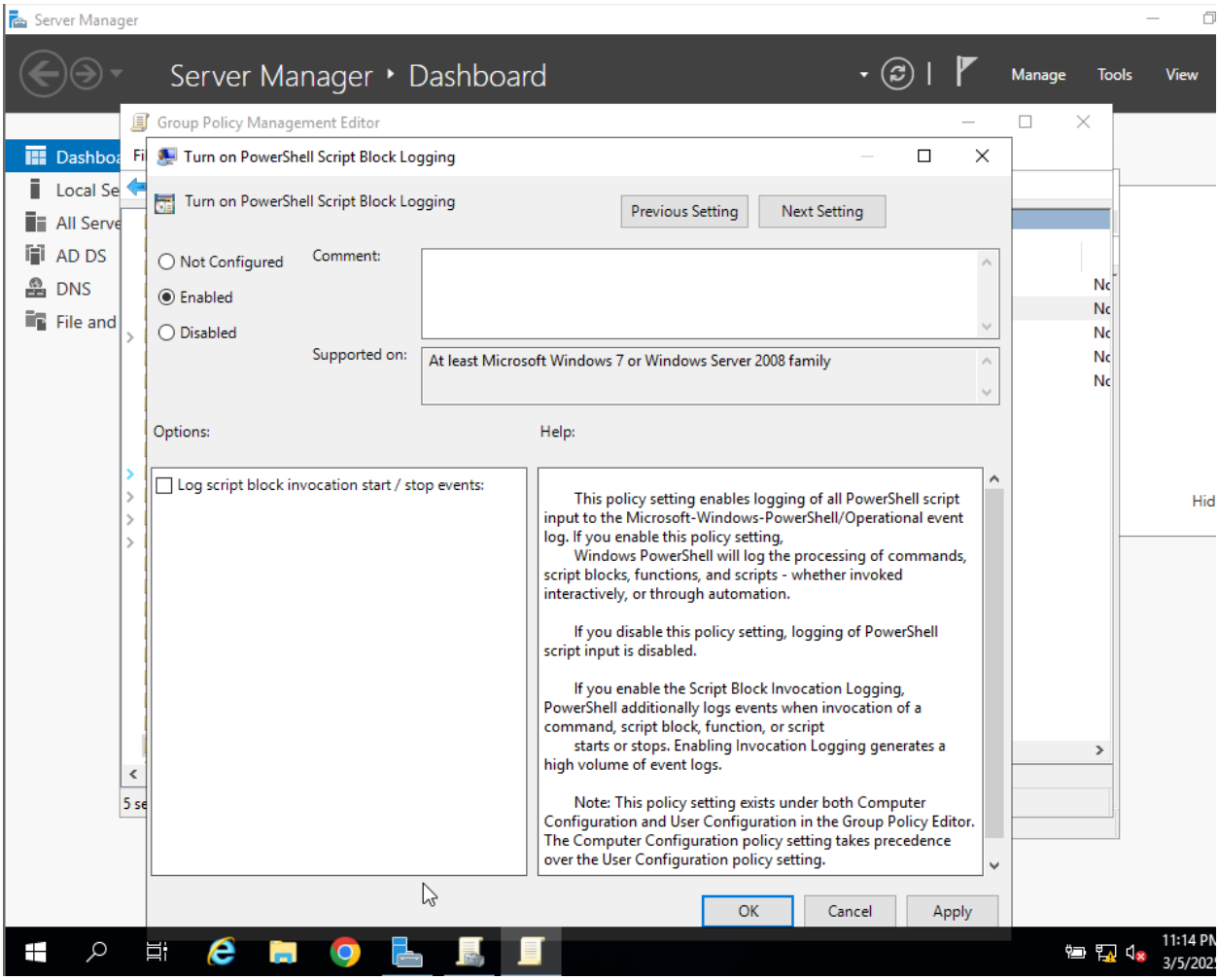
Screenshot 4: Wazuh logs (ossec.log) displaying PowerShell event data.

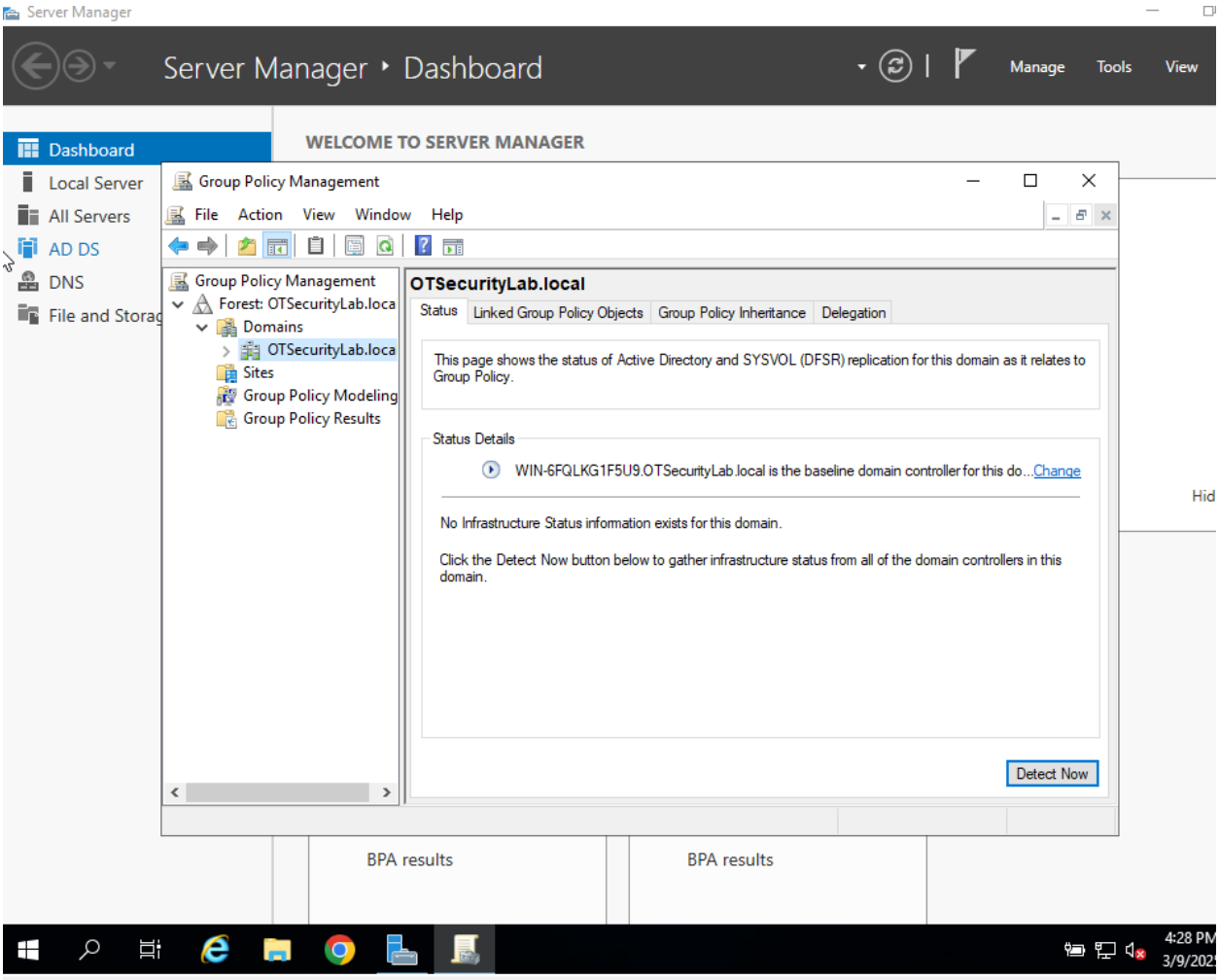


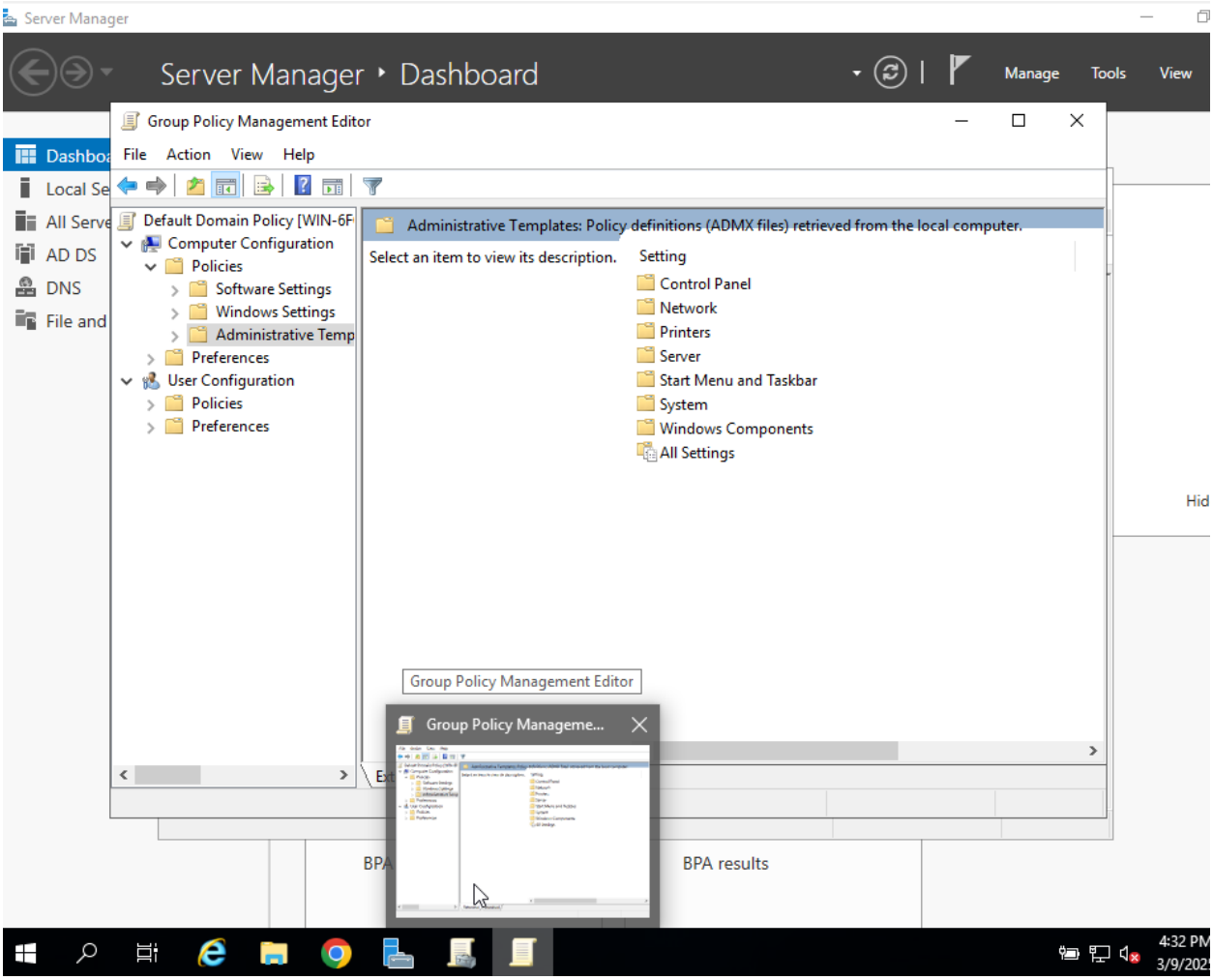
Step 5: View Logs in Kibana (Optional)

If Security Onion was used, logs were checked in **Kibana**.

1. Open a **web browser**.
2. Navigate to **Kibana's URL**:
3. http://securityonion-ip:5601
4. **Log in** using Kibana credentials.
5. Click **Discover**.
6. In the search bar, type:
7. event.code:4104
8. Press **Enter** to filter logs.


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Group Policy Management Editor
Turn on PowerShell Script Block Logging
Turn on PowerShell Script Block Logging
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Microsoft Windows 7 or Windows Server 2008 family
Options:
Help:
Log script block invocation start / stop events:
This policy setting enables logging of all PowerShell script input to the Microsoft-Windows-PowerShell/Operational event log. If you enable this policy setting,
Windows PowerShell will log the processing of commands, script blocks, functions, and scripts - whether invoked interactively, or through automation.
If you disable this policy setting, logging of PowerShell script input is disabled.
If you enable the Script Block Invocation Logging, PowerShell additionally logs events when invocation of a command, script block, function, or script
starts or stops. Enabling Invocation Logging generates a high volume of event logs.
Note: This policy setting exists under both Computer Configuration and User Configuration in the Group Policy Editor. The Computer Configuration policy setting takes precedence over the User Configuration policy setting.
OK
Cancel
Apply
Dashboa
Local Se
All Serve
AD DS
DNS
File and
11:14 PM
3/5/2025


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storag
WELCOME TO SERVER MANAGER
Group Policy Management
File
Action
View
Window
Help
Group Policy Management
Forest: OTSecurityLab.loca
Domains
OTSecurityLab.loca
Sites
Group Policy Modeling
Group Policy Results
OTSecurityLab.local
Status
Linked Group Policy Objects
Group Policy Inheritance
Delegation
This page shows the status of Active Directory and SYSVOL (DFSR) replication for this domain as it relates to Group Policy.
Status Details
WIN-6FQLKG1F5U9.OTSecurityLab.local is the baseline domain controller for this do...Change
No Infrastructure Status information exists for this domain.
Click the Detect Now button below to gather infrastructure status from all of the domain controllers in this domain.
Detect Now
BPA results
BPA results
Hid
4:28 PM
3/9/202

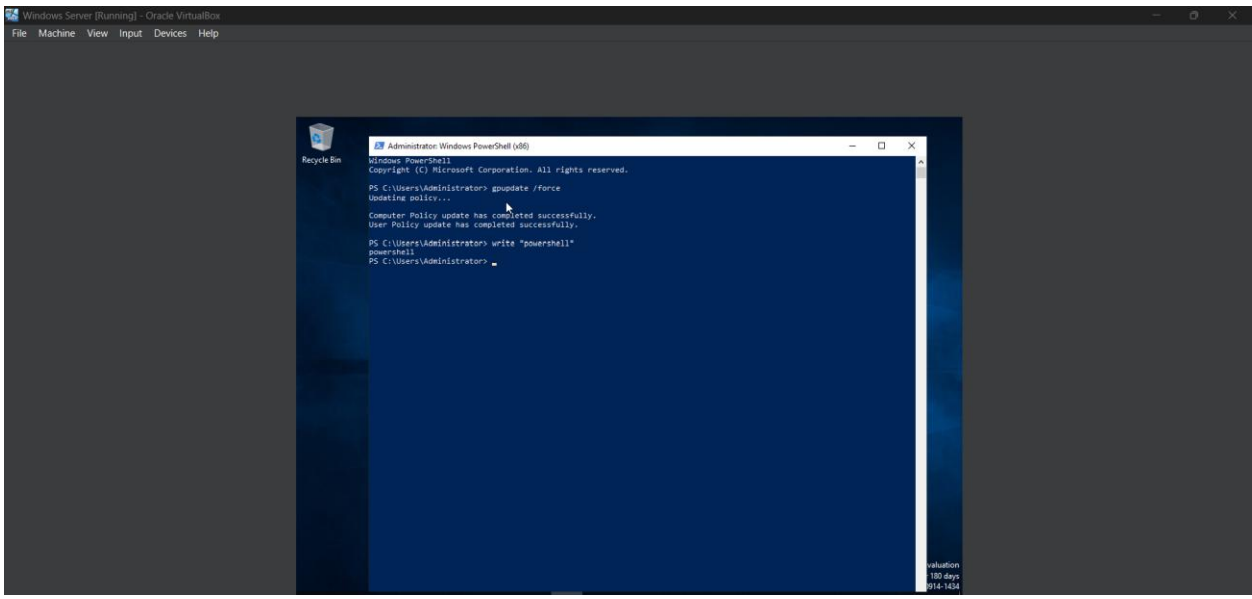


---

3. Observations & Issues Encountered

1. **Observations:**
   - Group Policy changes took effect successfully.
   - PowerShell logs were correctly recorded in **Event Viewer (Event ID 4104).**
   - Wazuh logs (ossec.log) showed successful **PowerShell log collection**.

- (Optional) **Kibana displayed PowerShell logs correctly**.



2. **Issues Encountered & Solutions:**
   - *Issue:* Wazuh Agent was not starting properly.
     - **Solution:** Restarted the Wazuh service using net stop wazuh and net start wazuh.
   - *Issue:* PowerShell logs were not appearing in Kibana.
     - **Solution:** Confirmed that logs were being forwarded to Security Onion by checking ossec.log.

ossec.conf - Notepad

File Edit Format View Help

```
<!--
  Wazuh - Agent - Default configuration for Windows
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>

  <client>
    <server>
      <address>192.168.10.100</address>
      <port>1514</port>
      <protocol>udp</protocol>
    </server>
    <crypto_method>aes</crypto_method>
    <notify_time>10</notify_time>
    <time-reconnect>120</time-reconnect>
    <auto_restart>yes</auto_restart>
  </client>

  <!-- Agent buffer options -->
  <client_buffer>
    <disabled>no</disabled>
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
  </client_buffer>

  <!-- Log analysis -->
  <localfile>
    <location>Application</location>
    <log_format>eventchannel</log_format>
  </localfile>

  <localfile>
    <location>Security</location>
```

ossec.conf - Notepad

File Edit Format View Help

```
<!--
  Wazuh - Agent - Default configuration for Windows
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>

  <client>
    <server>
      <address>192.168.10.100</address>
      <port>1514</port>
      <protocol>udp</protocol>
    </server>
    <crypto_method>aes</crypto_method>
    <notify_time>10</notify_time>
    <time-reconnect>120</time-reconnect>
    <auto_restart>yes</auto_restart>
  </client>

  <!-- Agent buffer options -->
  <client_buffer>
    <disabled>no</disabled>
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
  </client_buffer>

  <!-- Log analysis -->
  <localfile>
    <location>Application</location>
    <log_format>eventchannel</log_format>
  </localfile>

  <localfile>
    <location>Security</location>
```

ossec.conf - Notepad

File Edit Format View Help

```
<!--
  Wazuh - Agent - Default configuration for Windows
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>

  <client>
    <server>
      <address>192.168.10.100</address>
      <port>1514</port>
      <protocol>udp</protocol>
    </server>
    <crypto_method>aes</crypto_method>
    <notify_time>10</notify_time>
    <time-reconnect>120</time-reconnect>
    <auto_restart>yes</auto_restart>
  </client>

  <!-- Agent buffer options -->
  <client_buffer>
    <disabled>no</disabled>
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
  </client_buffer>

  <!-- Log analysis -->
  <localfile>
    <location>Application</location>
    <log_format>eventchannel</log_format>
  </localfile>

  <localfile>
    <location>Security</location>
```

---

4. Conclusion

This lab successfully demonstrated the ability to **enable PowerShell Script Block Logging**, configure **Wazuh Agent** to collect logs, and verify log entries in **Event Viewer, Wazuh logs, and Kibana**. This setup is critical for **security monitoring**, as it helps in detecting malicious PowerShell activity.

Key Learnings:

- **Group Policy can enforce PowerShell logging across the domain**.
- **Wazuh Agent can collect PowerShell logs and forward them to Wazuh Manager**.
- **Kibana provides a centralized way to analyze PowerShell logs in real-time**.

Lab Successfully Completed!