NETWORK OPERATING SYSTEM

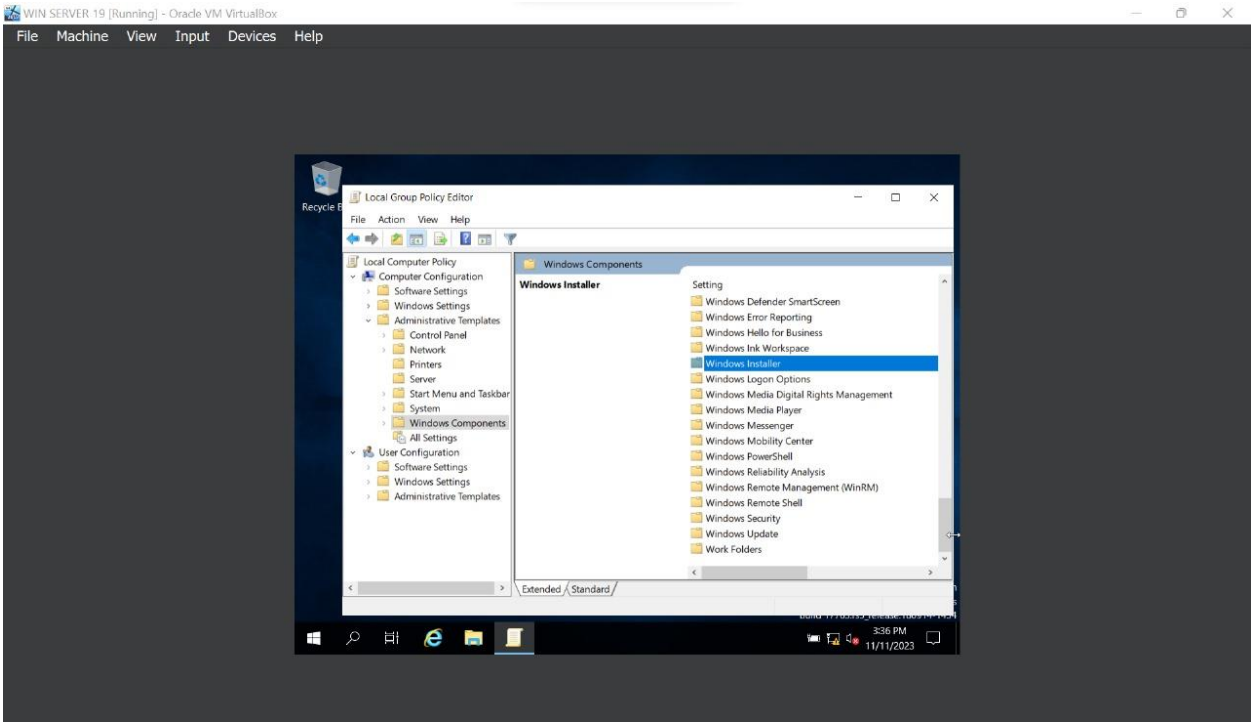
Task 8

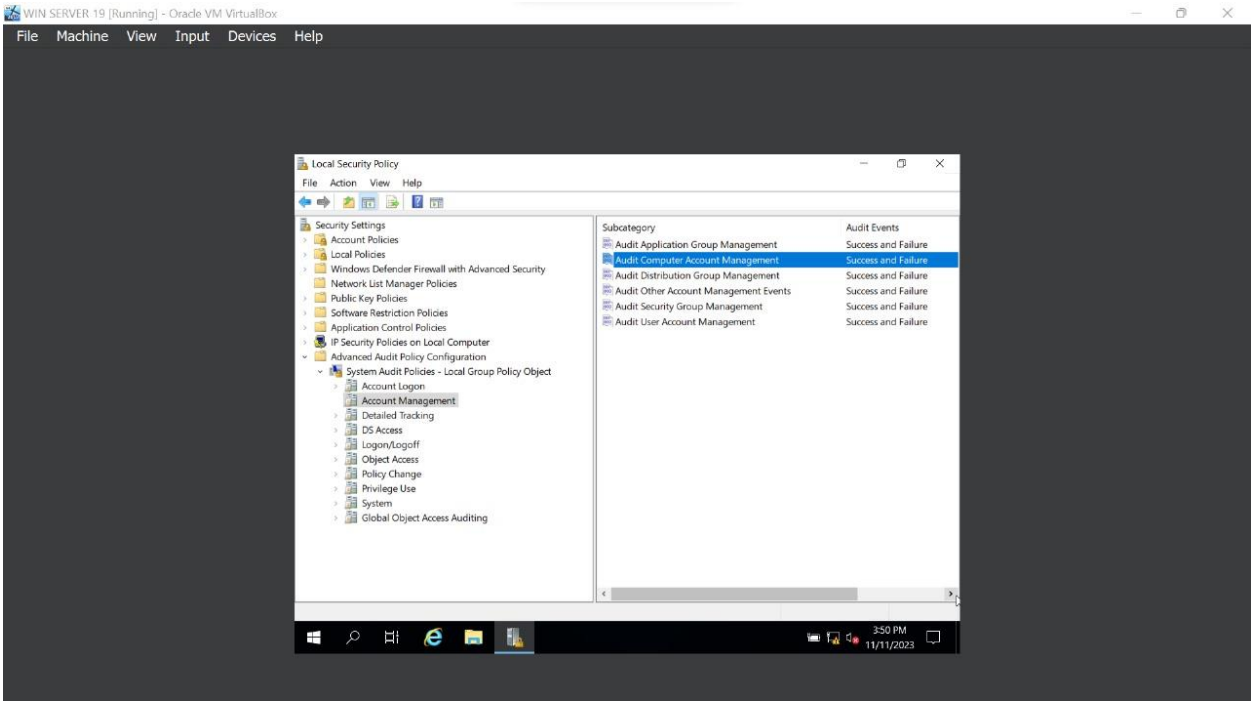
Planning an Audit Policy

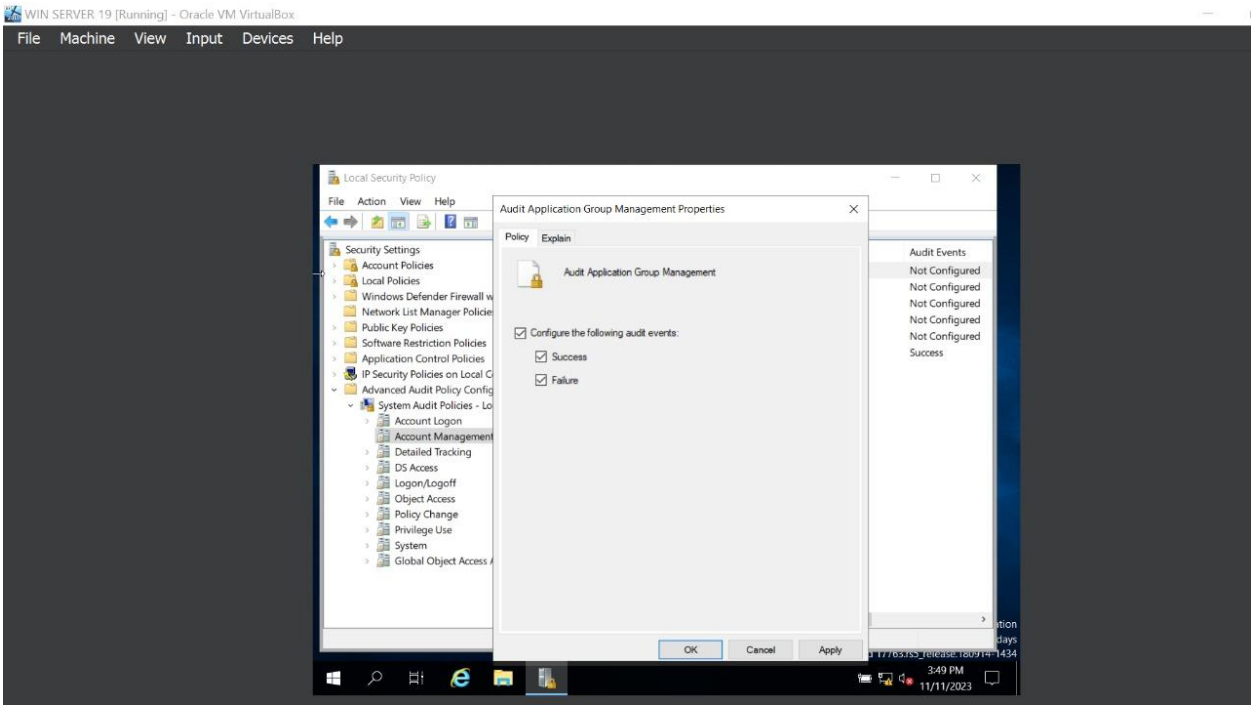
By

DEWTON KIPROP

- Open Local Security Policy
  Press Windows Key + R to open the Run dialog, type **secpol.msc,** and press Enter. This will open the Local Security Policy console.
- Configure Audit Policy Settings
  In the Local Security Policy console, navigate to Security Settings -> Local Policies -> Audit Policy.
  Double-click on each audit policy setting related to Account Management to configure it.
  Select "Success" and/or "Failure" checkboxes as needed to audit the corresponding events.
- Review Audit Log Settings
  Optionally, review the settings under Security Settings -> Event Log, such as log size limits and retention policies.
- Apply Settings
  Close the Local Security Policy console after configuring the audit policy settings.
  The settings will be applied immediately to the local server.

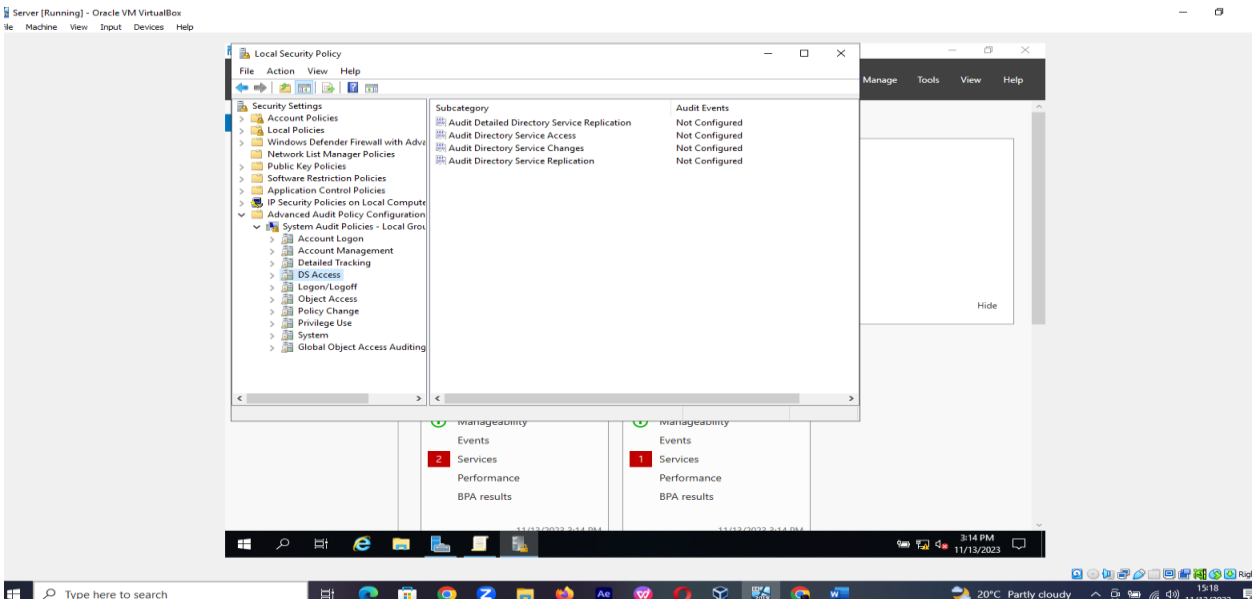




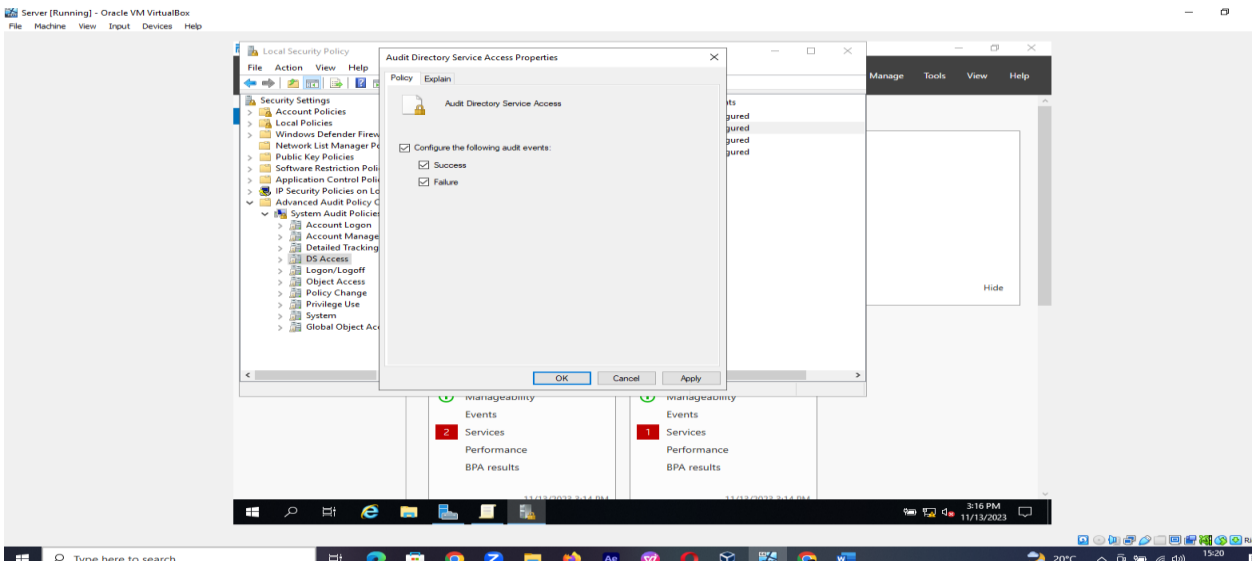


Directory Service Access

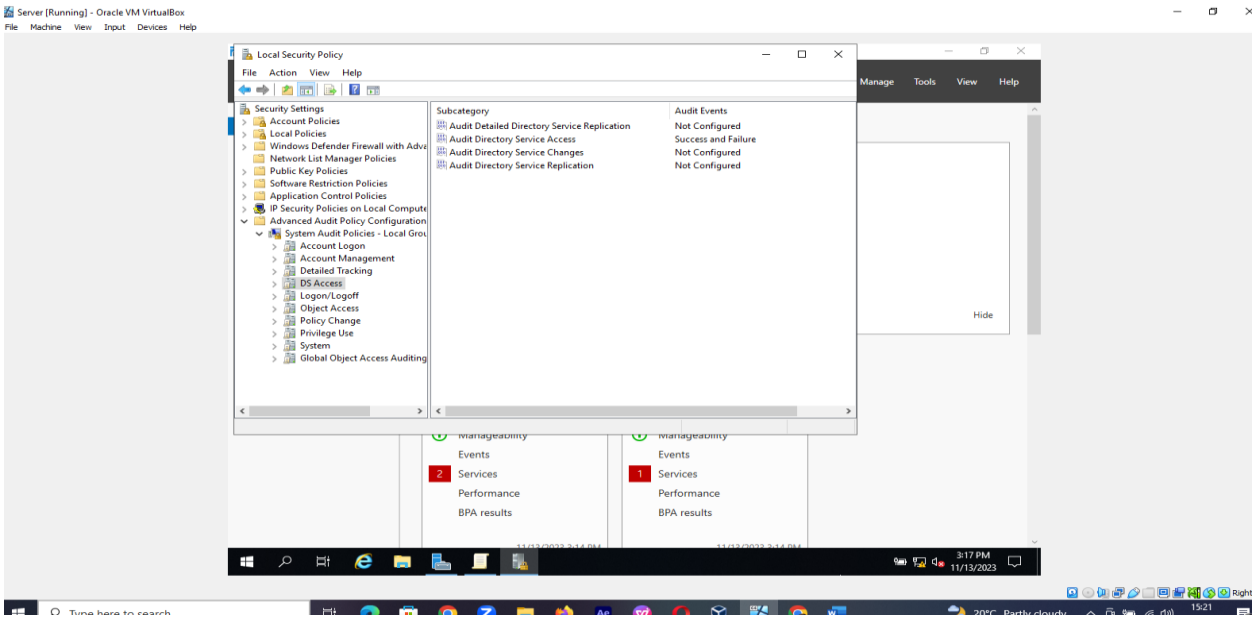
Navigating to DS Access



Configuring

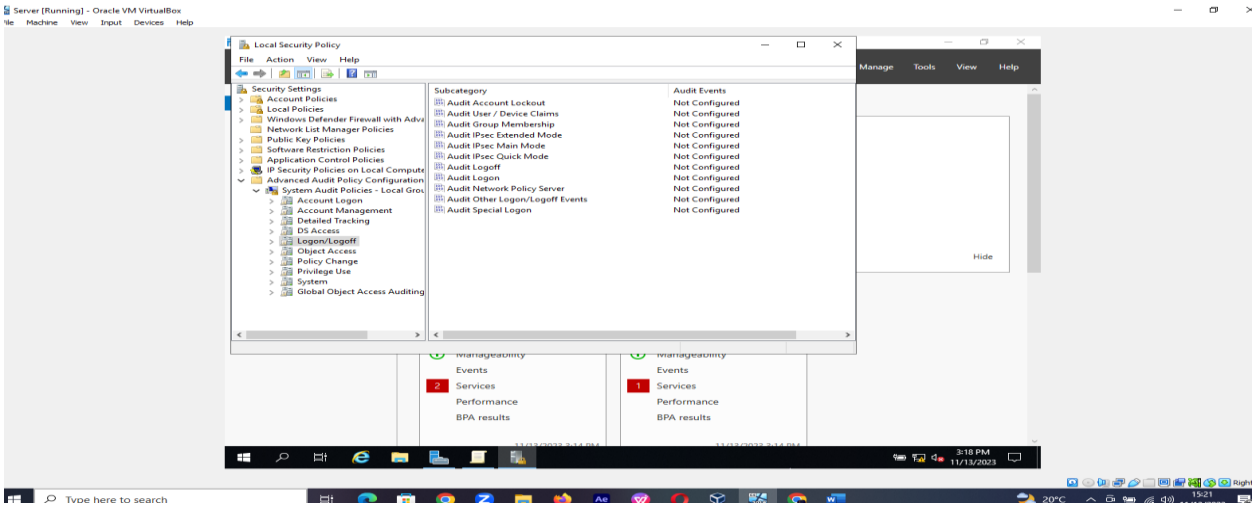


Results

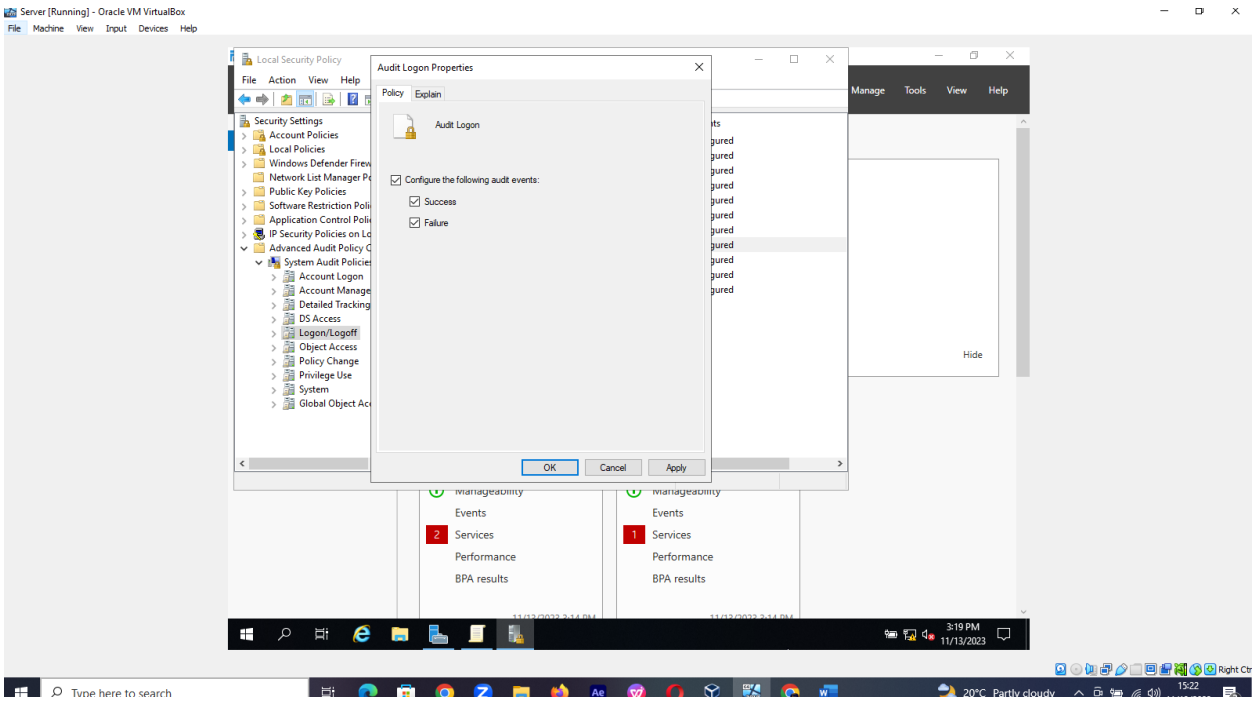


Logon Events

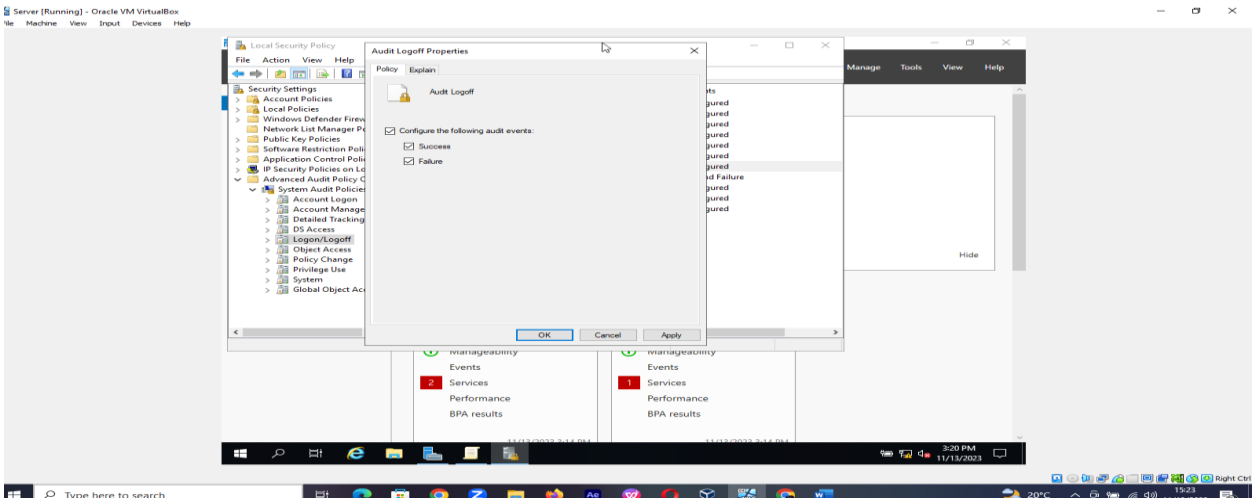
Navigating to log on events



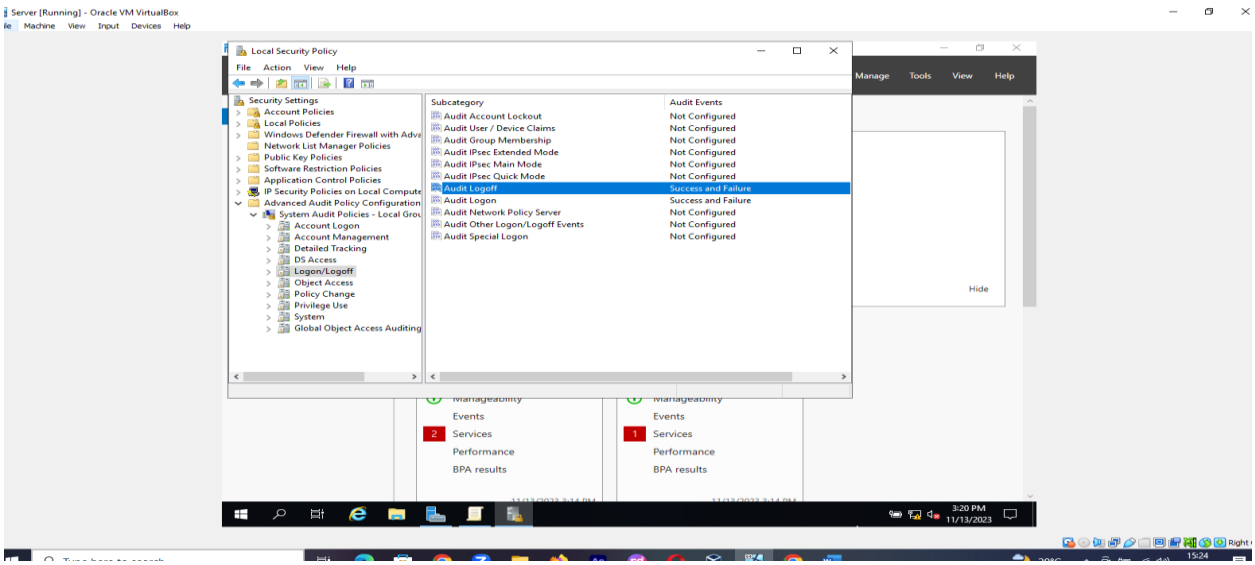
Configuring logon



Configuring logoff

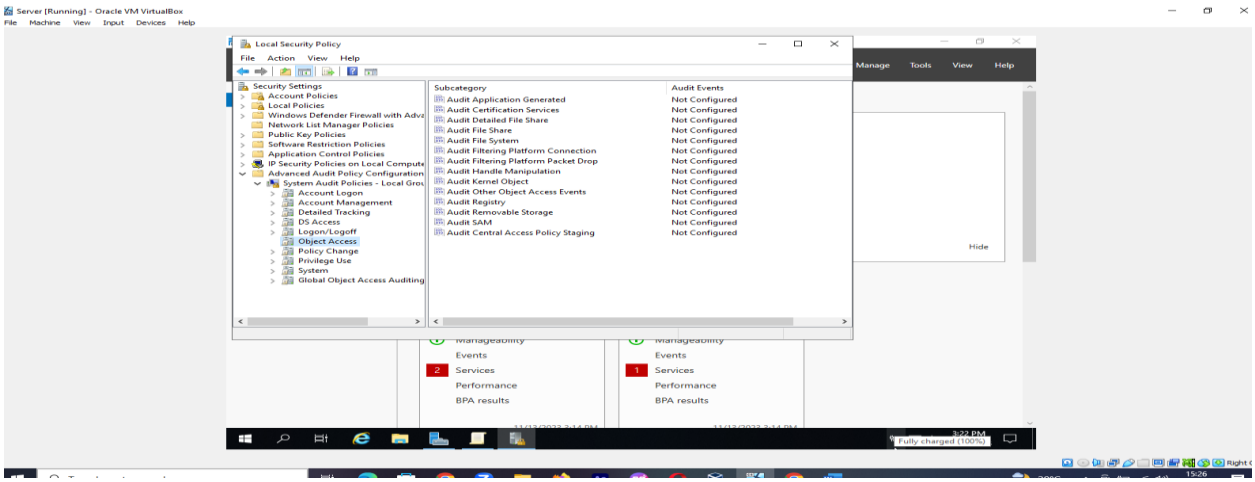


Results

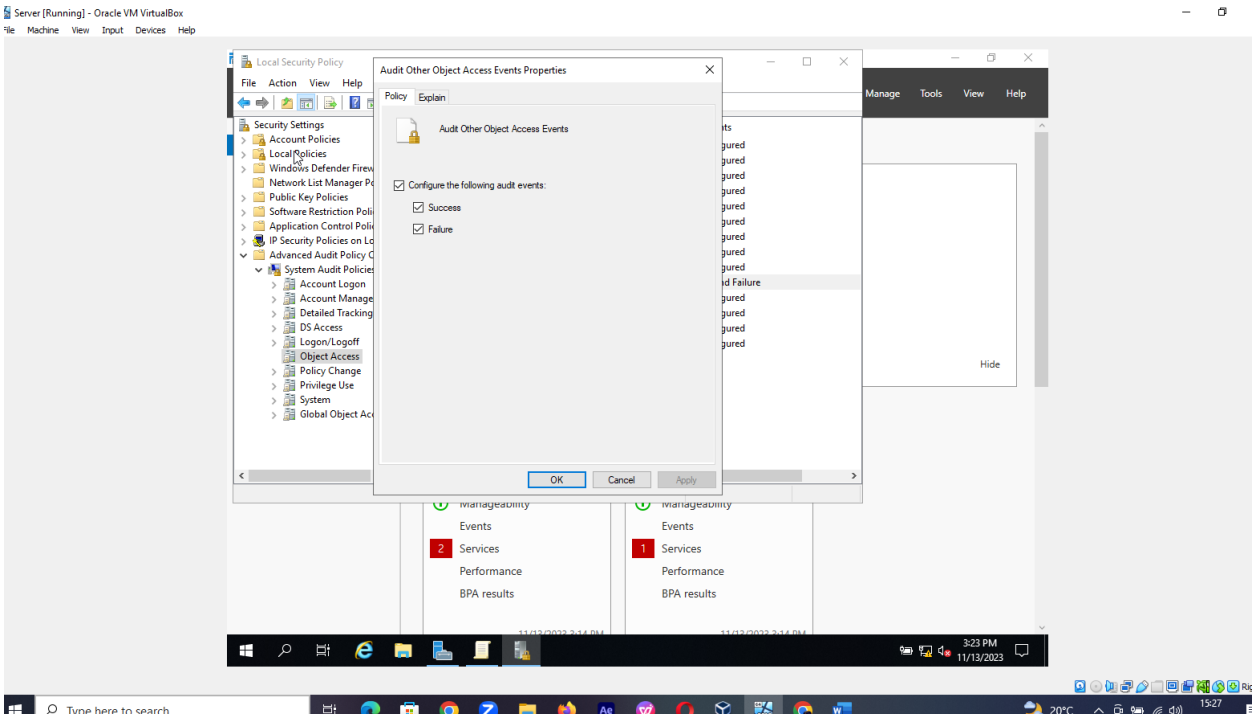


Object Access

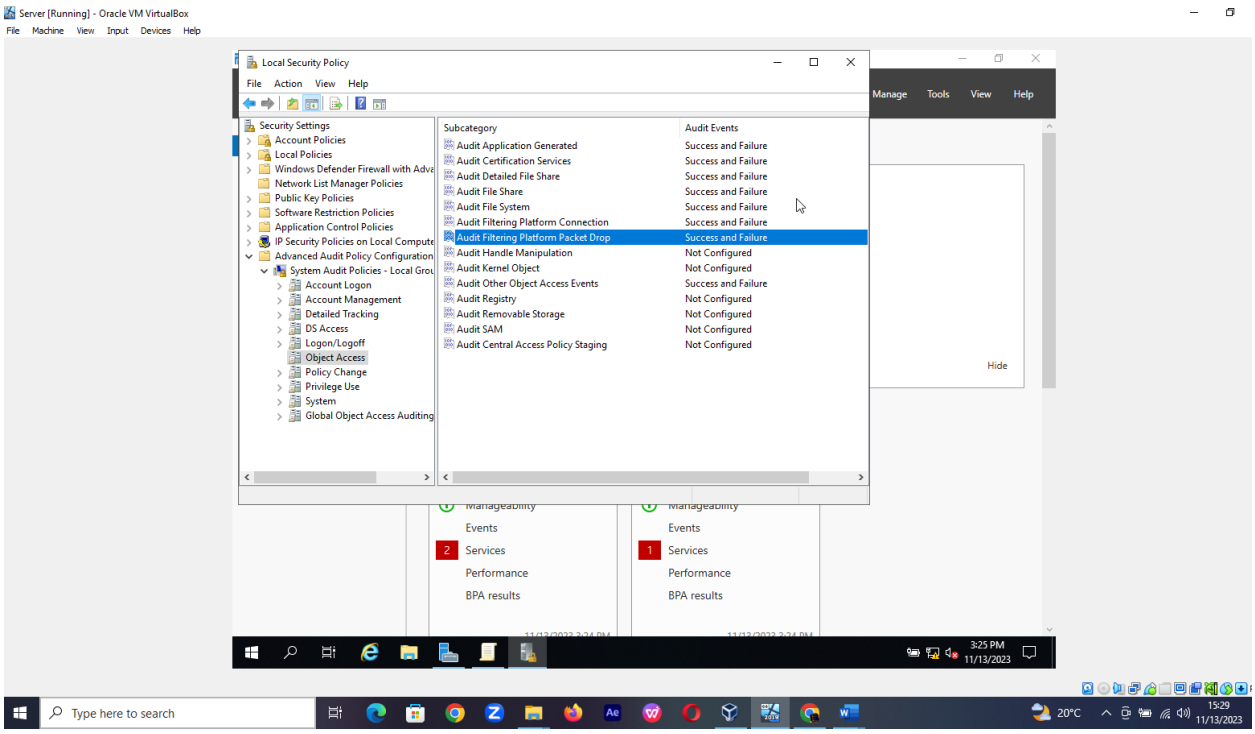
Navigating to object access



Configuration

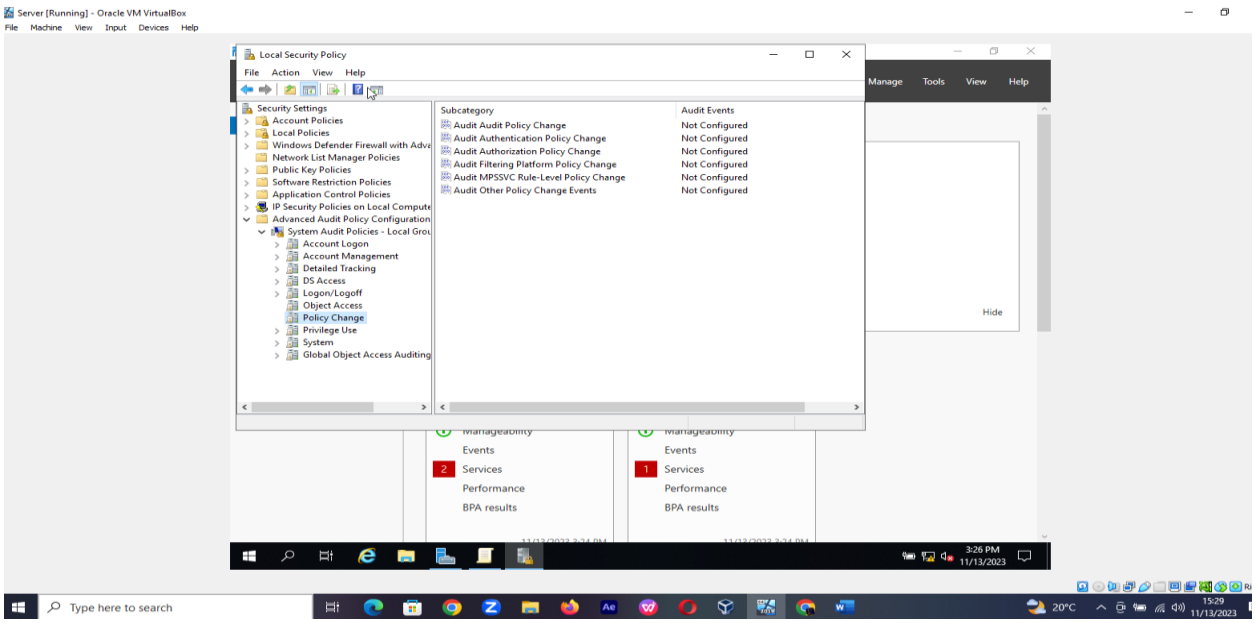


Results

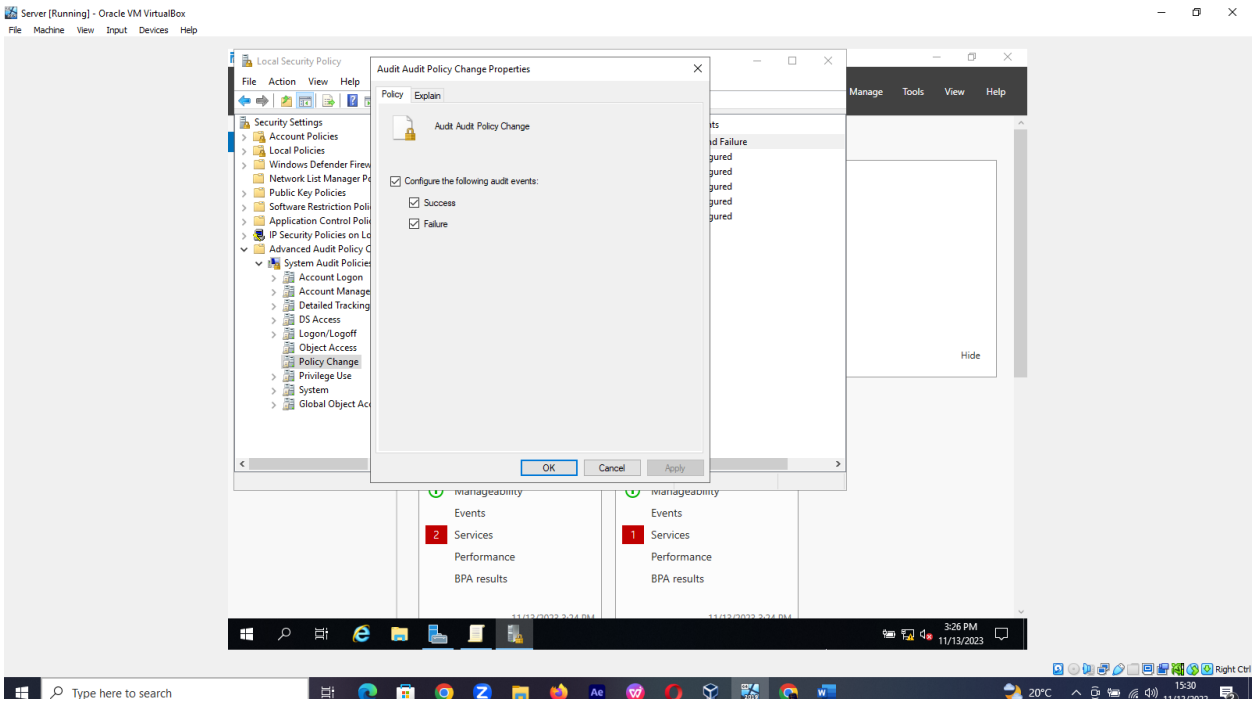


Policy Change

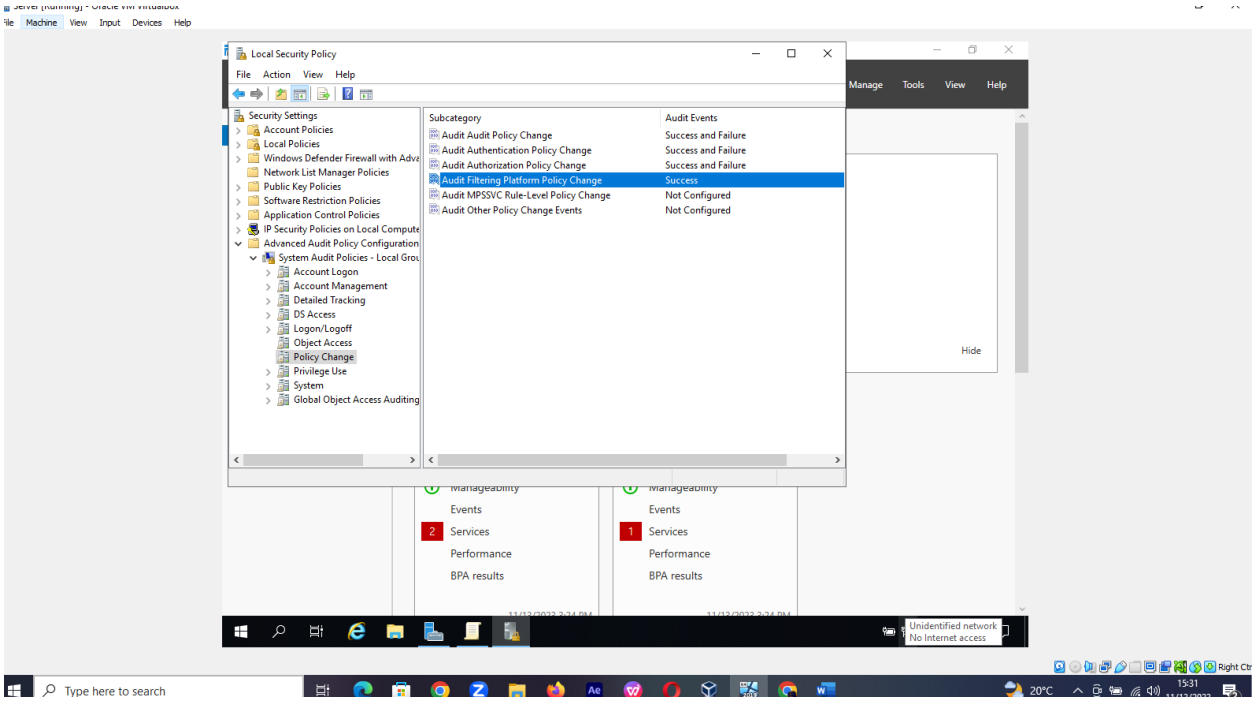
Navigating to policy change

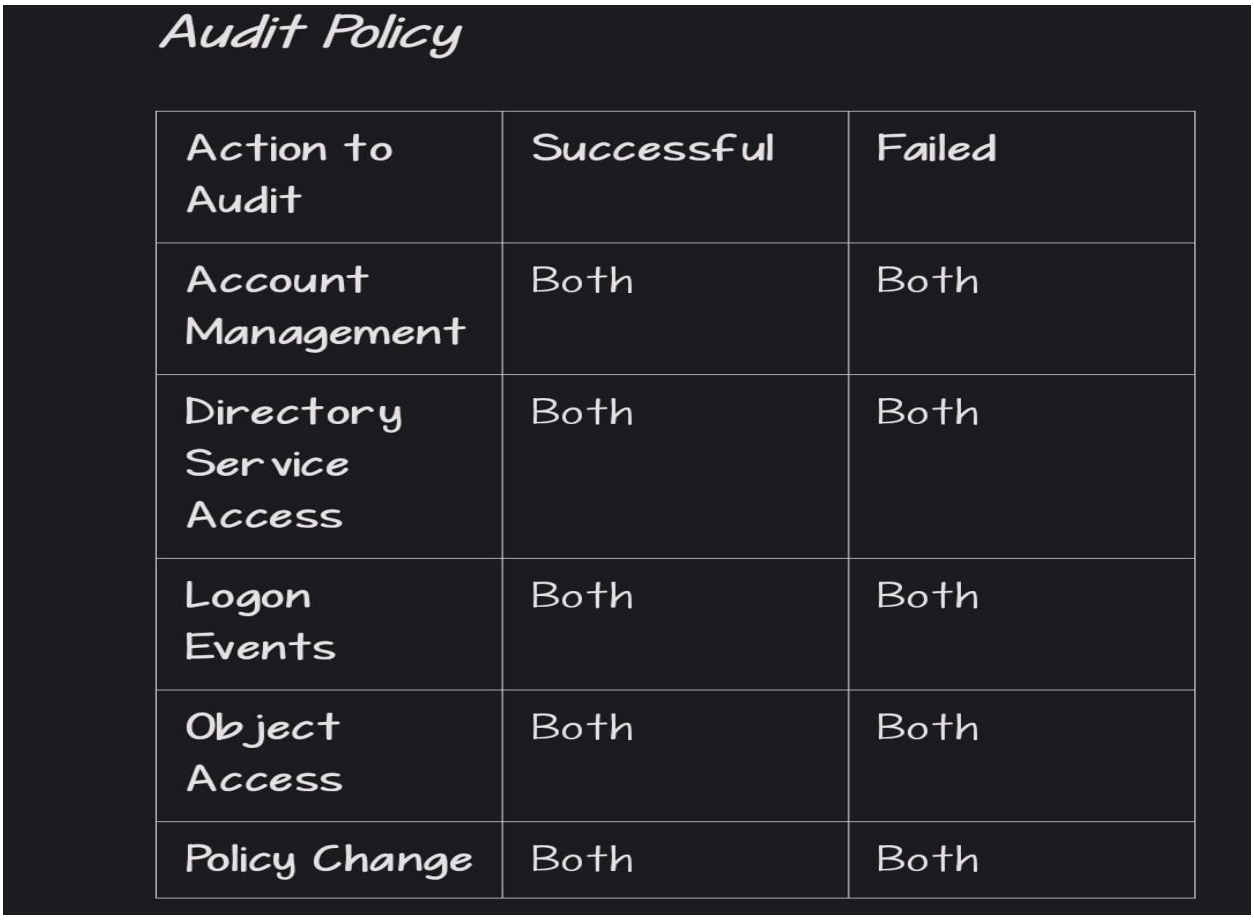


Configuration



Results


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
System Audit Policies - Local Grou
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing
Subcategory
Audit Events
Audit Audit Policy Change
Success and Failure
Audit Authentication Policy Change
Success and Failure
Audit Authorization Policy Change
Success and Failure
Audit Filtering Platform Policy Change
Success
Audit MPSSVC Rule-Level Policy Change
Not Configured
Audit Other Policy Change Events
Not Configured
Manage Tools View Help
Hide
Events
Services
Performance
BPA results
Unidentified network
No Internet access
Type here to search
20°C



Action to Audit	**Successful**	**Failed**
Account Management	✓	✓
Directory Service Access	✓	✓
Logon Events	✓	✓
Object Access	✓	✓
Policy Change	✓	✓