

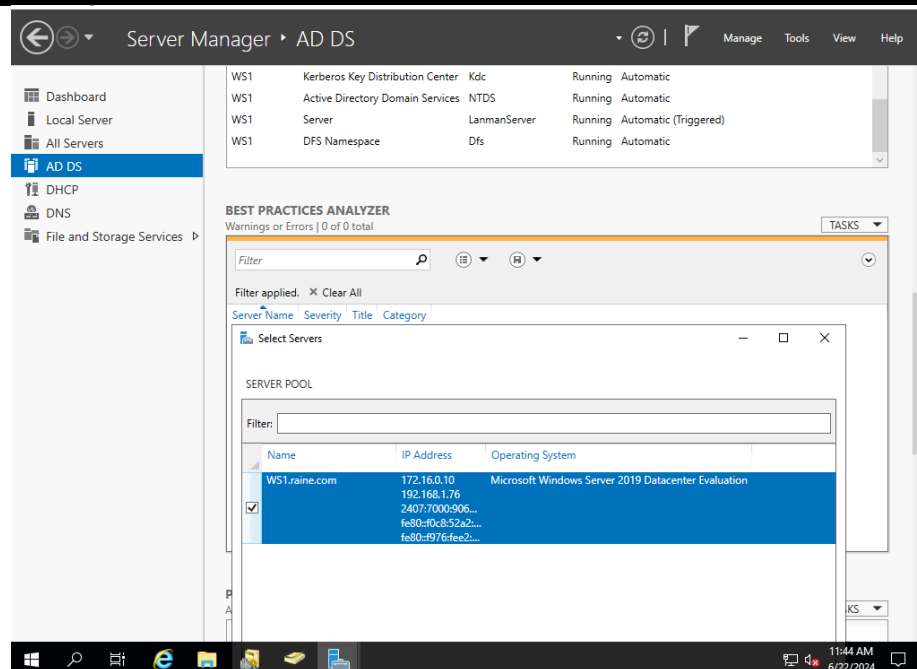
## Lab Number: 3. Active Directory

Student name: Raine

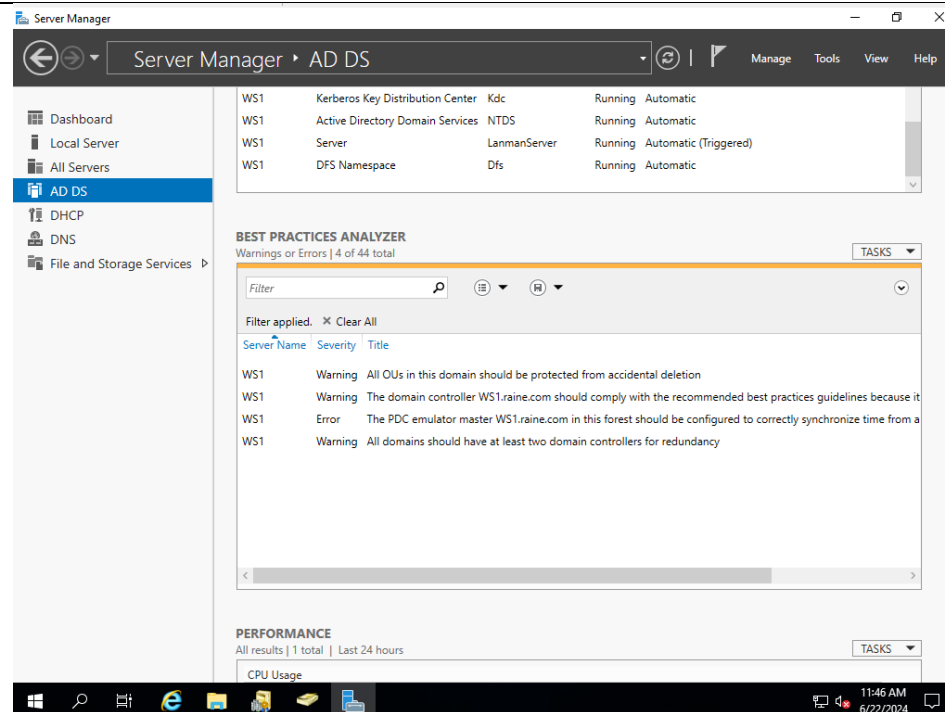
<b>Section Summary</b>	<p><b>Section 3: Active Directory</b></p> <p>All group members work together for this section</p> <p><b>Goals</b></p> <ul style="list-style-type: none"><li>• Use Windows Admin Center to manager a domain controller</li><li>• Remove child domain and have two DCs on a single domain</li><li>• AD replication between domain controllers<ul style="list-style-type: none"><li>○ Specify AD replication interval and schedule</li></ul></li><li>• Make WS1 the Global catalog server</li><li>• Configure AD OU, groups and users according to a defined company structure on WS1</li><li>• Restrict user access to weekdays only</li><li>• Use Best Practices Analyser (BPA) scan to ensure services from the previous section is working properly</li><li>• Create a checkpoint of server VMs</li></ul> <p><b>Implementation steps</b></p> <ol style="list-style-type: none"><li>1. Use BPA scan on WS1 - start BPA scan<ul style="list-style-type: none"><li>○ What information is received?</li></ul></li><li>2. Delete child domain from WS2</li><li>3. Use Windows Admin Centre (WAC) on WS2<ul style="list-style-type: none"><li>○ Google search for WAC and download the latest version and install it<ul style="list-style-type: none"><li>▪ Generate a self-sign certificate</li><li>▪ Use default port number 443</li><li>▪ What is the URL provided to access WAC for your server?</li></ul></li><li>○ Note this cannot be added to a domain controller</li><li>○ Access it from a client web-browser<ul style="list-style-type: none"><li>▪ Add the server name WS1</li><li>▪ Create a new folder in WS1 and download it WS2</li><li>▪ Restart the DHCP service on WS1 via WAC</li><li>▪ What information cab be changed at the menu items: firewall, network, roles, updates, files, devices, services, and local users &amp; Groups?</li></ul></li></ul></li><li>4. Remove WAC role once confirmed that is working correctly from WS2 as we want to make a domain controller now</li><li>5. Make WS2 a second domain controller in the dileep1 domain</li><li>6. Ensure AD replication between the domain controllers (Every 180 minutes)</li><li>7. Remove the WS2 global catalog ability from WS2 but leave it on WS1</li><li>8. Check the current domain and forest functional levels to Windows server 2016 user Server manager using the Active directory domains and trusts tool</li></ol>
------------------------	--

9. User AD sites and services to remove global catalog from WS2 (it should be enabled for WS1 only)
10. Use Active directory users and computers to:
  - a. Verify that the client computers have been added to the domain
  - b. Verify that WS1 and WS2 are domain controllers for the same domain
  - c. Configure AD OU, groups and users (one user per group) on WS2
    - OU Staff
      - Universal user that can log in to both domains
      - OU: DevelopersOU
      - Group: Developers
    - OU: ManagersOU
      - Group: Managers
    - OU: AccountsOU
      - Group: Accounts
11. Restrict Developer user access to weekdays only
12. Test that users can log correctly from the client node
13. Use VMware to create a checkpoint of WS1 and WS2. May need to revert back to this if any issues happen in project 4

1



Starting BPA on AD DS Server

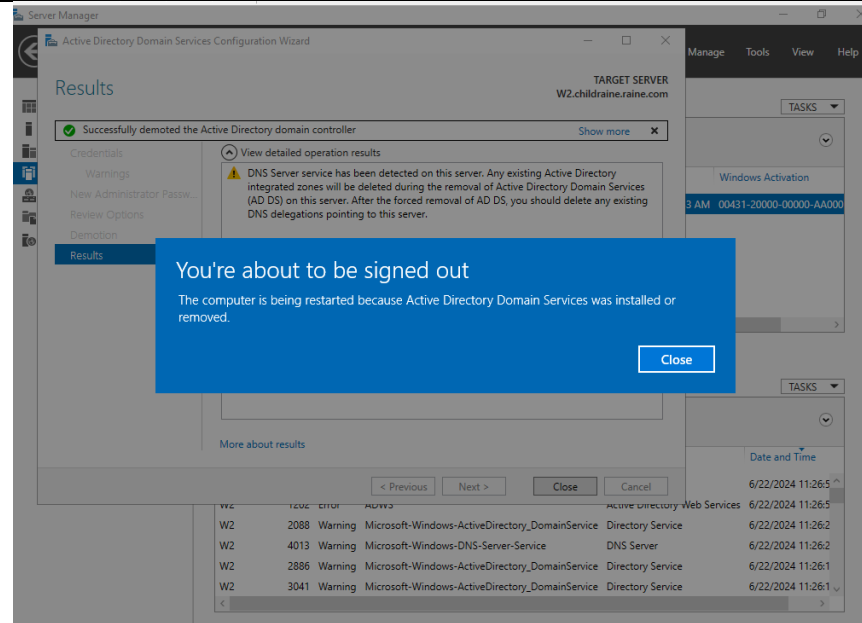


Results of the BPA scan on the AD DS server on WS1

### Types of Information Received from a BPA Scan:

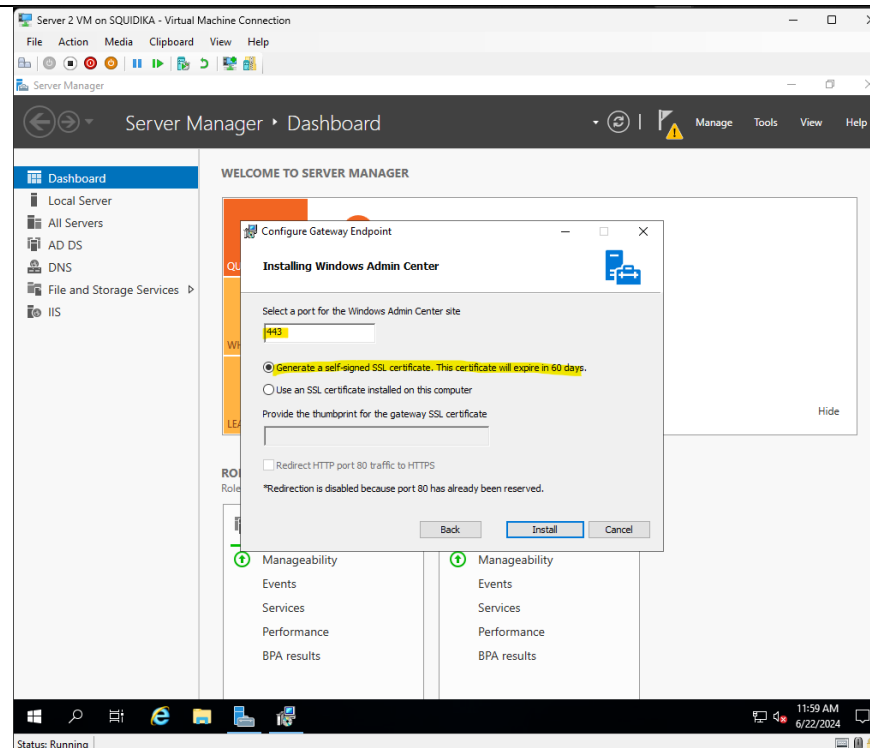
- **Compliance Issues:** Lists any non-compliant configurations according to best practices.
- **Recommendations:** Provides specific suggestions to correct the compliance issues.
- **Warnings and Errors:** Details about potential problems with the server configuration.
- **Performance Suggestions:** Tips to improve server performance and efficiency.
- **Security Issues:** Highlights any security risks or vulnerabilities.

2



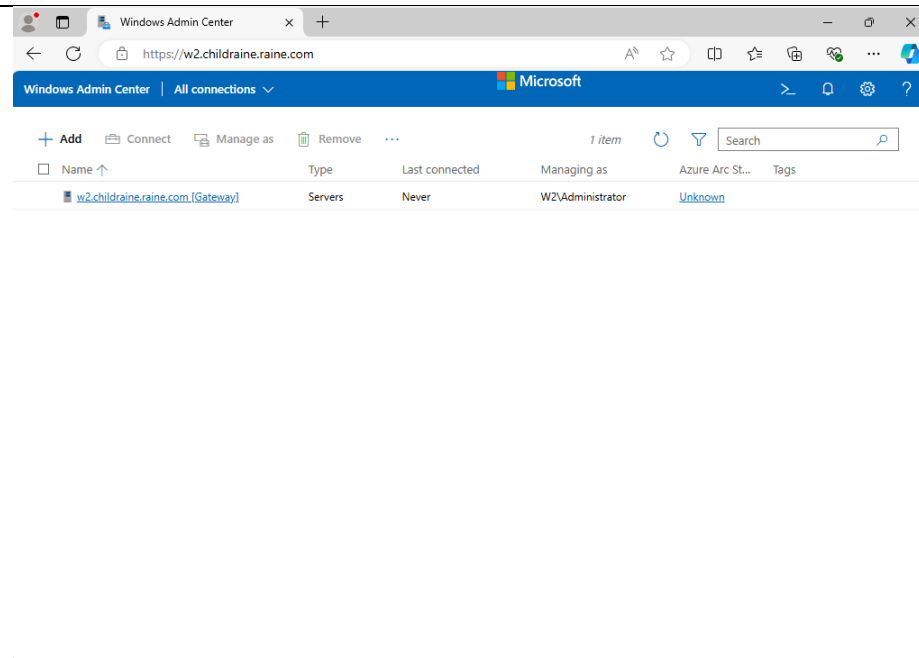
Forcefully demoting the domain controller to remove it as a child and remove child.raine.com

3

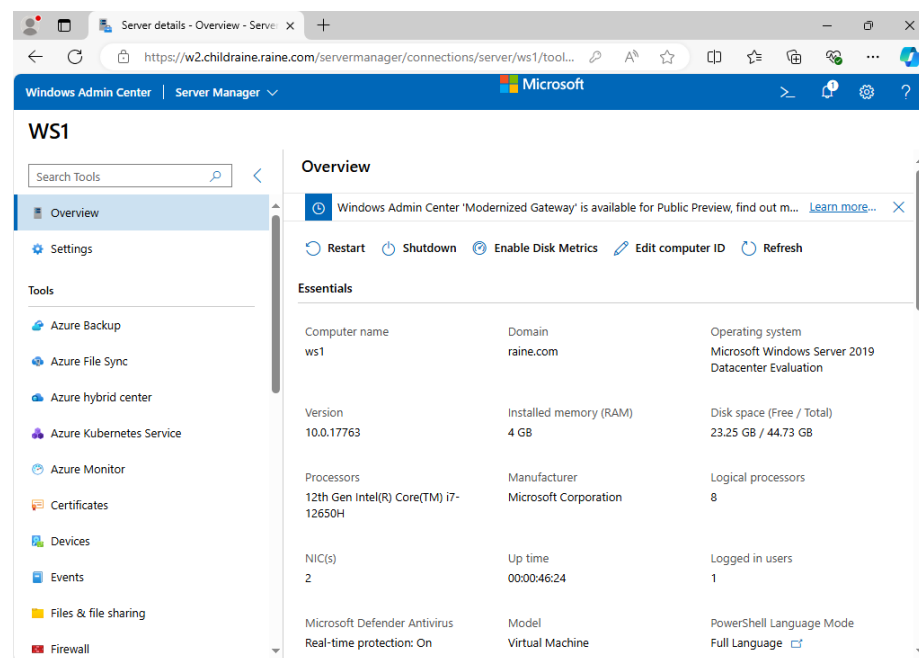


Download and install WAC on WS2

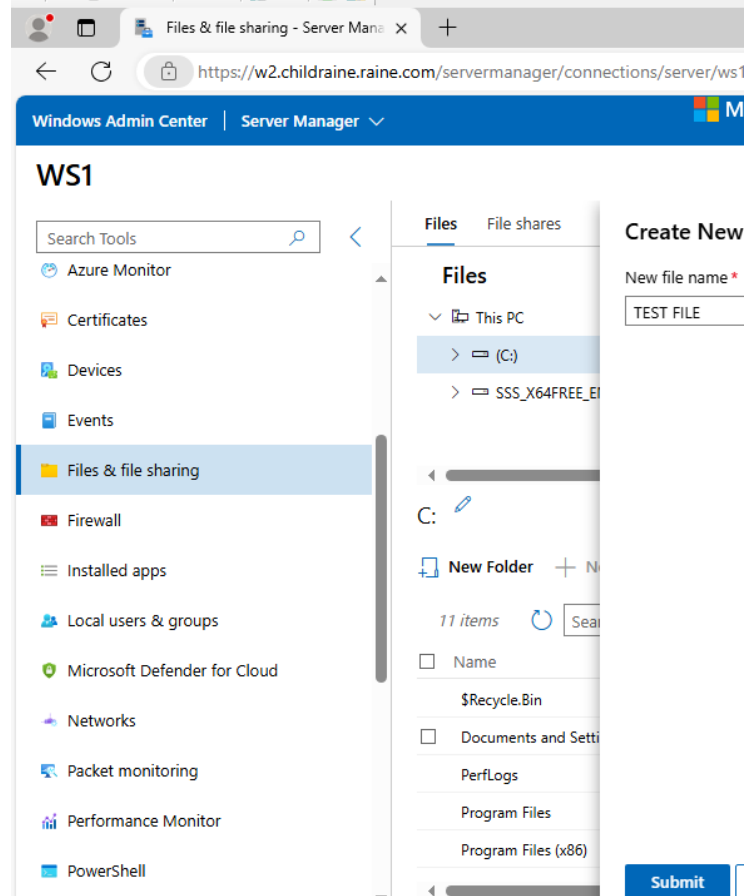
- Generate self-sign certificate option checked
- Use port number 443
- url to access WAC <https://w2.childrairie.raine.com>



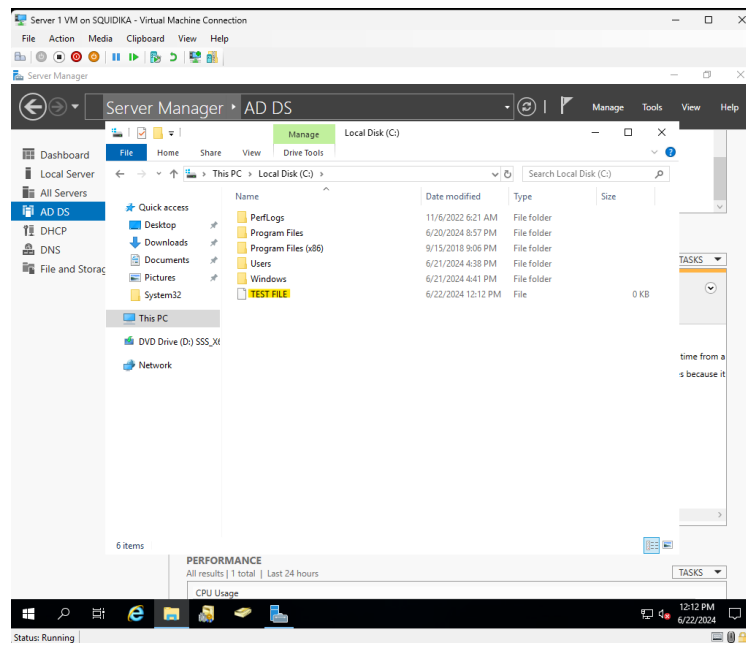
## Access WAC on the host device



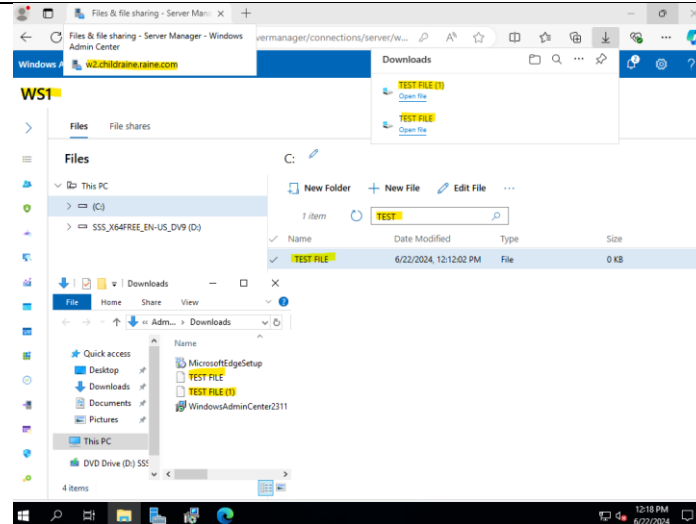
## Add WS1 server to WAC



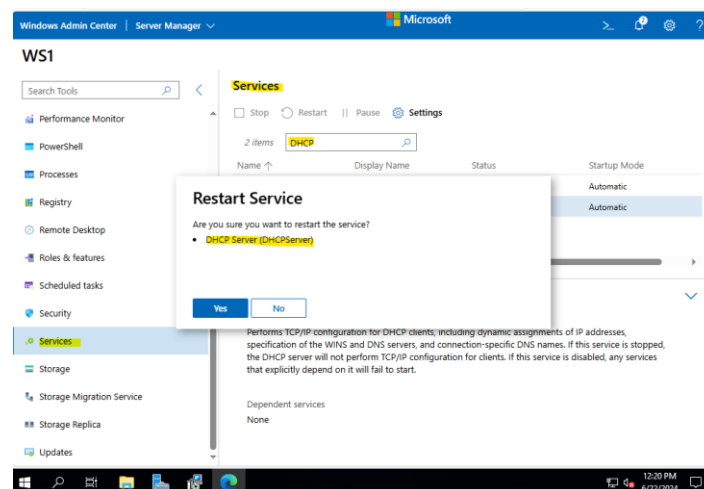
Create a test file in WS1 using WAC on host device



The file is created in the location in WS1



Use WAC to download the file created by the host device on WS1 to the device of WS2



Restart the HDCP Server on WS1 via WAC on host device

### Information that Can Be Changed in Menu Items

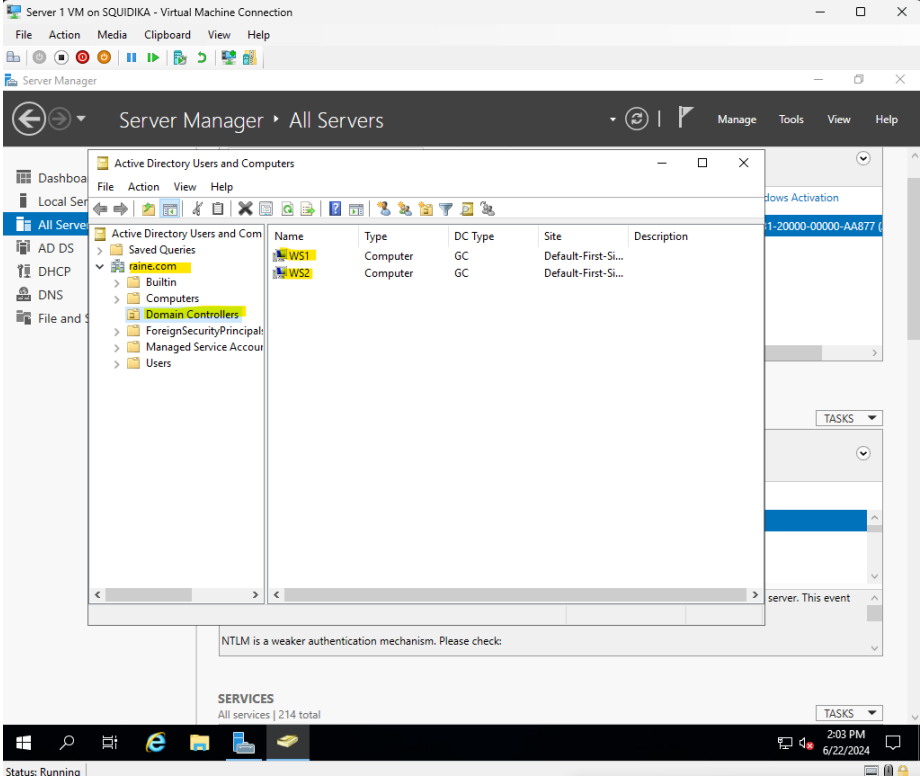
- **Firewall:** Configure and manage Windows Firewall rules.
- **Network:** View and configure network adapters, IP settings, DNS, and gateways.
- **Roles:** Add or remove server roles and features.
- **Updates:** Check for, install, and manage Windows updates.
- **Files:** Manage files and folders, create new files/folders, delete, move, and download files.
- **Devices:** Manage hardware devices and device drivers.
- **Services:** Start, stop, and configure services running on the server.

- **Local Users & Groups:** Manage local user accounts and groups, add or remove users/groups, and configure user properties.

4

WAC Role removed from WS2

5

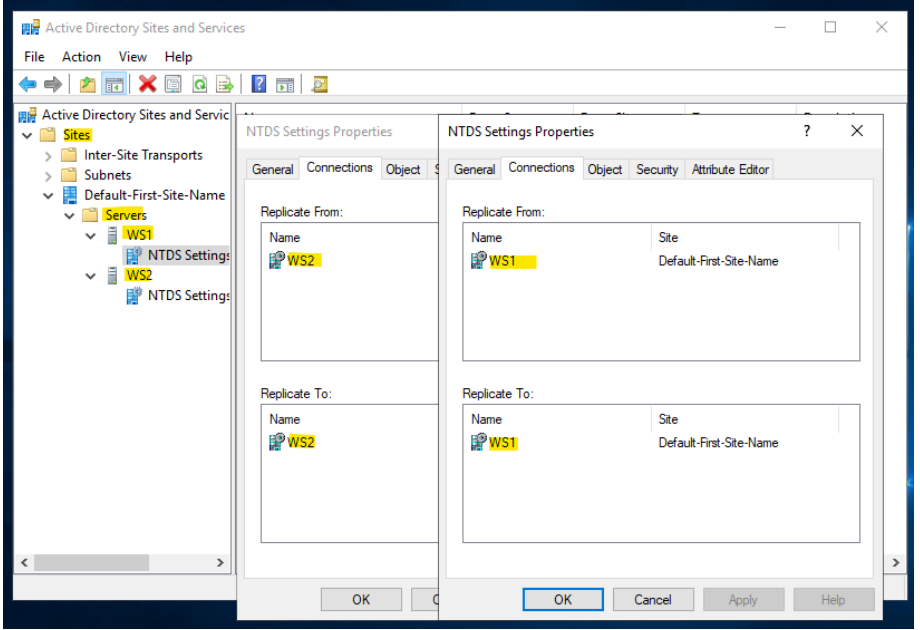


NTLM is a weaker authentication mechanism. Please check:

SERVICES  
All services | 214 total

Created a second domain controller computer WS2 in the raine.com domain

6



NTDS Settings Properties

Replicate From:

Name	Site
WS2	Default-First-Site-Name

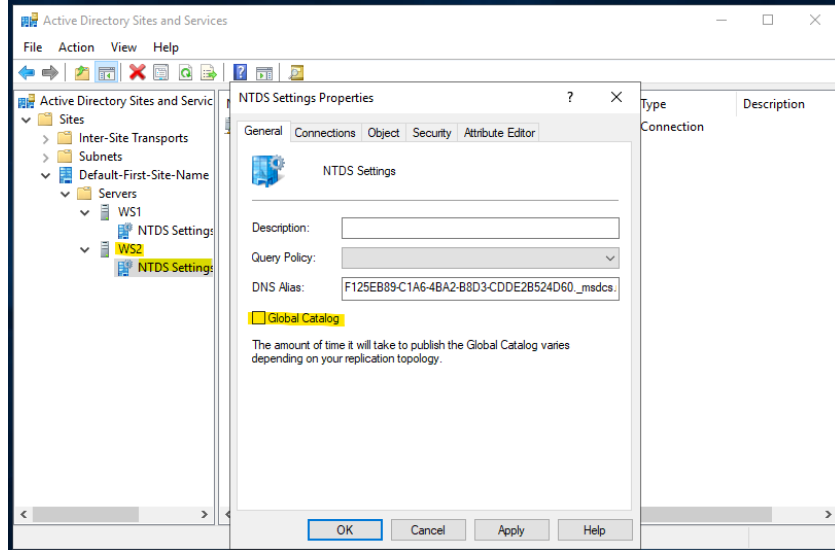
Replicate To:

Name	Site
WS1	Default-First-Site-Name

Created connections between both servers to replicate AD between each other

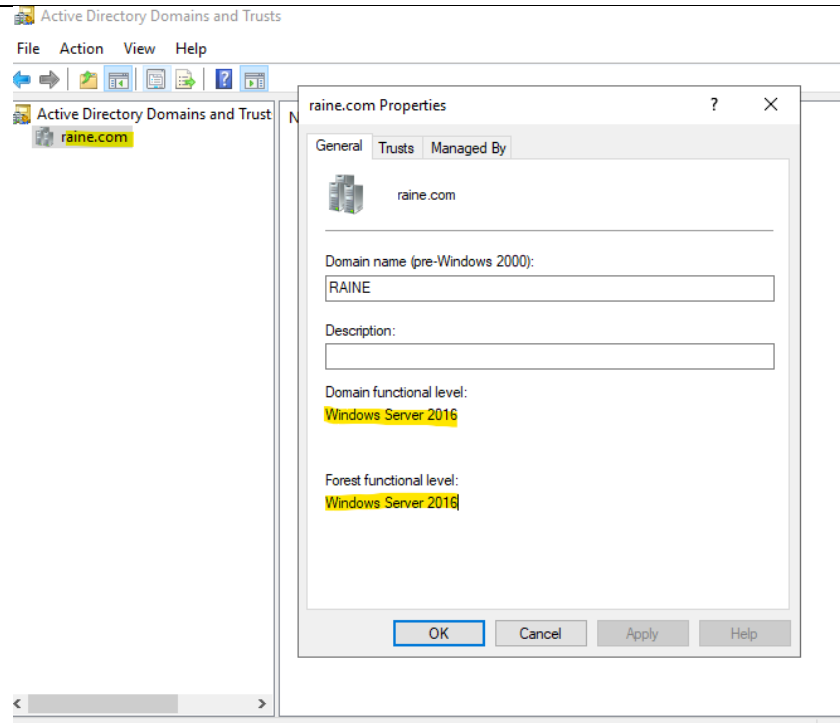


7



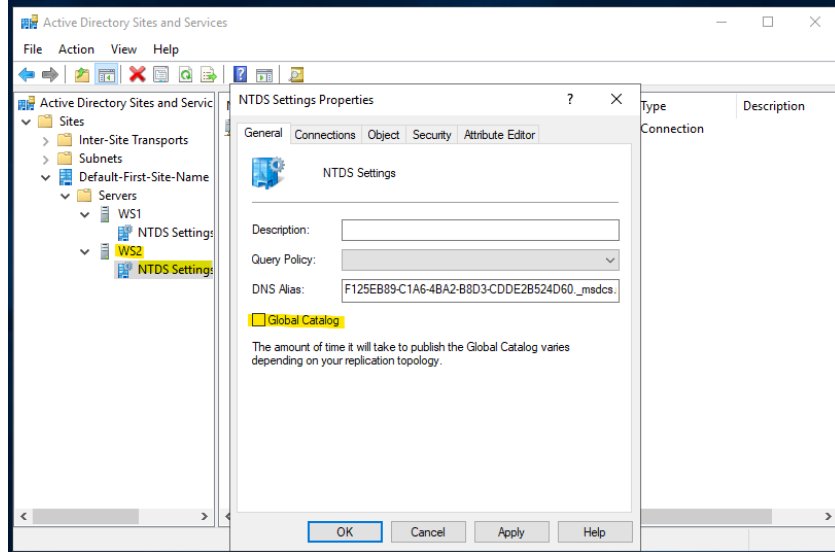
Remove WS2 global catalog ability from WS2

8



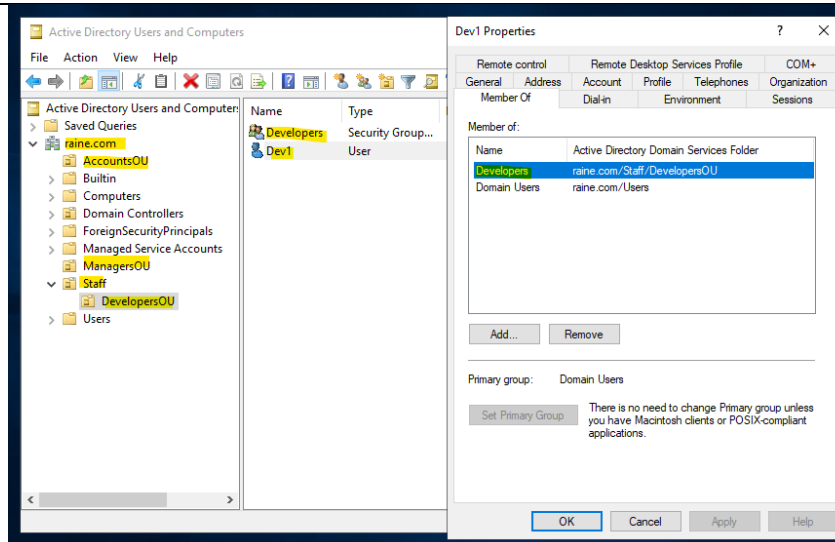
Both domain and forest functional level set to windows server 2016

9



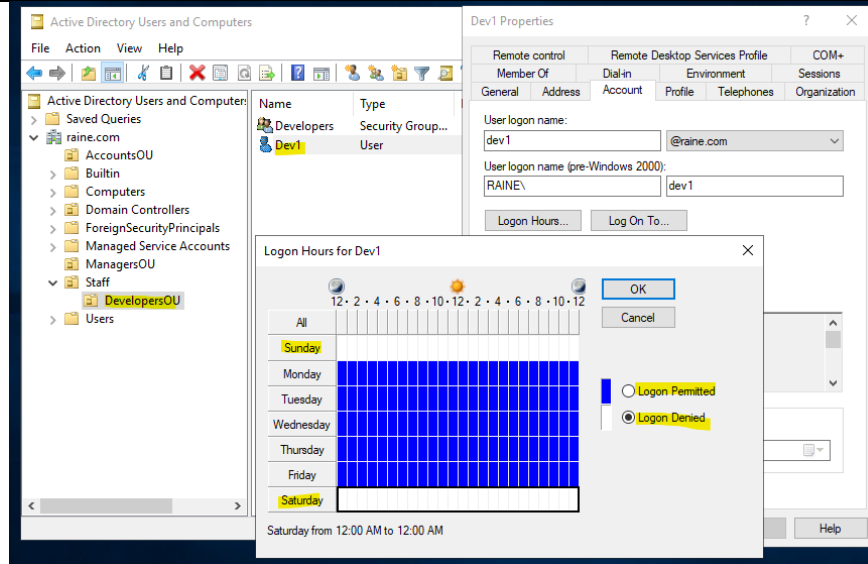
Previously configured in step 7

10



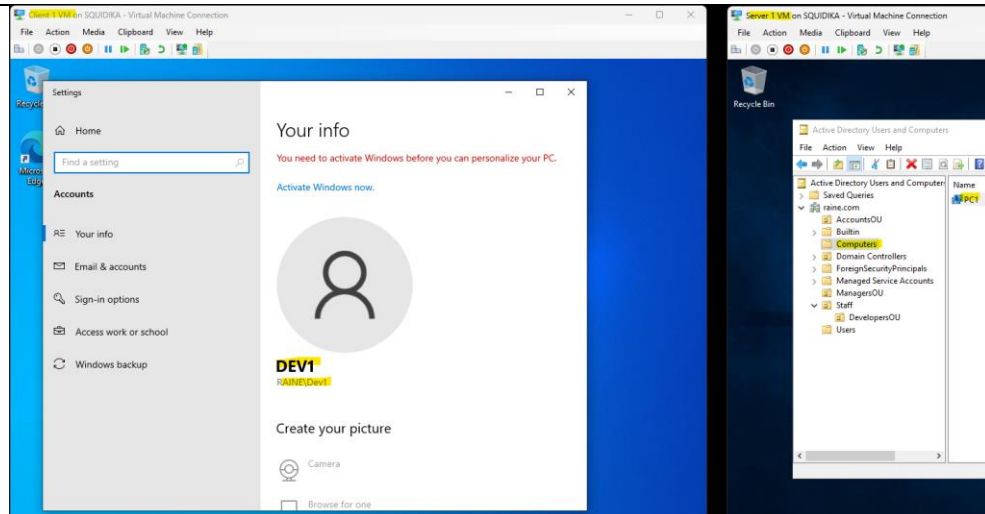
Groups and OU's configured correctly, users created and groups assigned to users

11

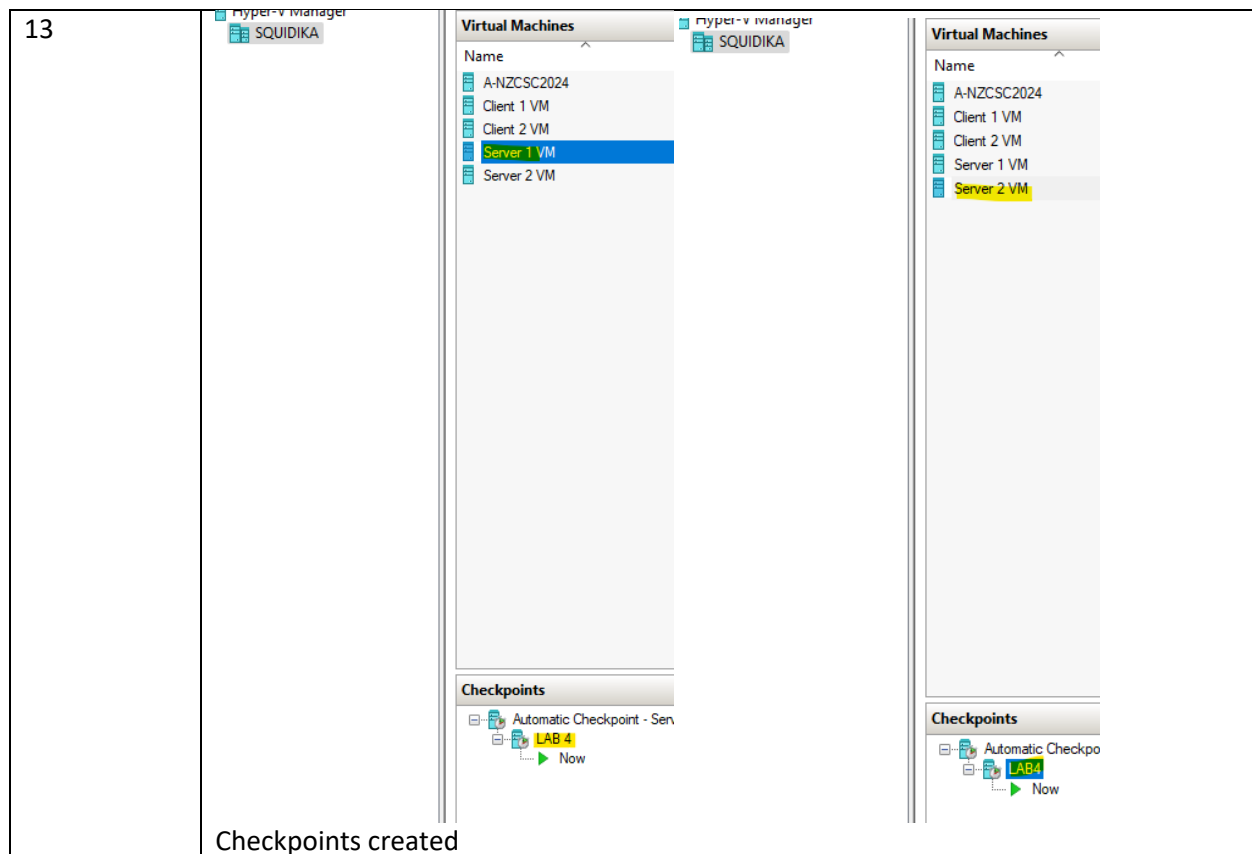


Logon for user Dev1 restricted to weekdays only

12



Test that the user DEV1 can login on the client machine on the domain, with evidence of the PC being located in the domain.

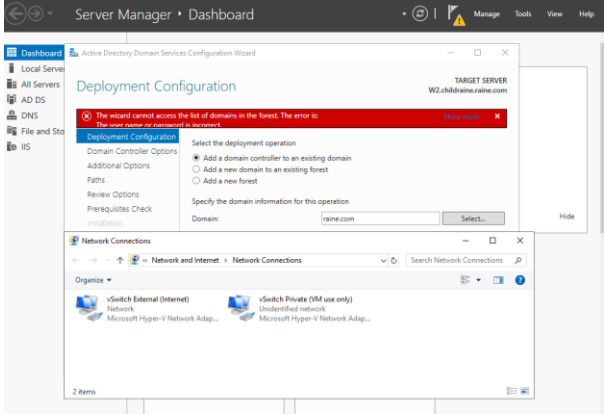


List At the three most useful Internet resources that you used (provided by the tutor)

<ul style="list-style-type: none"> <li>○ BPA scan</li> <li>○ <a href="https://docs.microsoft.com/en-us/windows-server/administration/server-manager/run-best-practices-analyzer-scans-and-manage-scan-results">https://docs.microsoft.com/en-us/windows-server/administration/server-manager/run-best-practices-analyzer-scans-and-manage-scan-results</a></li> </ul>
<ul style="list-style-type: none"> <li>● Add DC to exisiting domain and AD replication</li> <li>● <a href="https://www.youtube.com/watch?v=-R7Ryy7-4e0">https://www.youtube.com/watch?v=-R7Ryy7-4e0</a></li> </ul>
<ul style="list-style-type: none"> <li>● Set Functional levels</li> <li>● <a href="https://www.youtube.com/watch?v=-R7Ryy7-4e0">https://www.youtube.com/watch?v=-R7Ryy7-4e0</a></li> </ul>

List all (at least three) Internet resources that you found and used that were not provided by the tutor)

<ul style="list-style-type: none"> <li>● <a href="https://www.rebeladmin.com/2015/07/how-to-enable-universal-group-membership-caching-ugmc/">https://www.rebeladmin.com/2015/07/how-to-enable-universal-group-membership-caching-ugmc/</a></li> </ul>
<ul style="list-style-type: none"> <li>● <a href="https://www.youtube.com/watch?v=cETbT22TWEE">https://www.youtube.com/watch?v=cETbT22TWEE</a></li> </ul>
<ul style="list-style-type: none"> <li>● <a href="https://www.youtube.com/watch?v=E39_MzvCFXA">https://www.youtube.com/watch?v=E39_MzvCFXA</a></li> </ul>

Problem	Solution
<p>WAC cannot be accessed via Windows Server default internet browser Internet Explorer.</p>	<p>Download and install a compatible internet browser, for this lab I have downloaded Microsoft Edge as the most compatible with the service.</p>
<div data-bbox="203 472 803 882">  </div> <p>Wizard cannot access domains in the forest the username or password is incorrect despite being correct.</p>	<p>Solution is to disable the connection to vSwitch Private and renable the connection, this should re-establish the connection to WS1/raine.com</p>