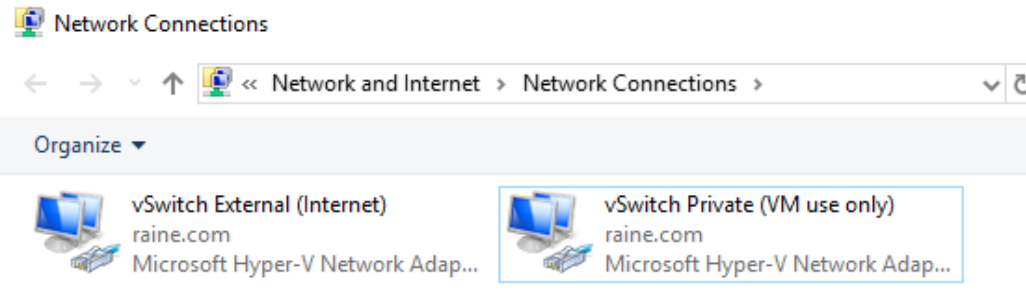
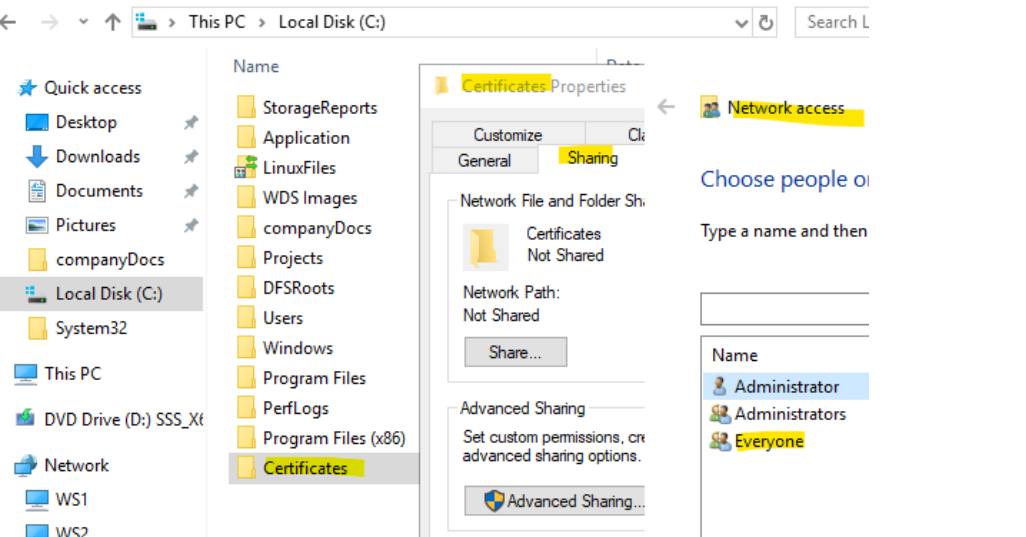


Lab Number: 5 RDP and Monitoring

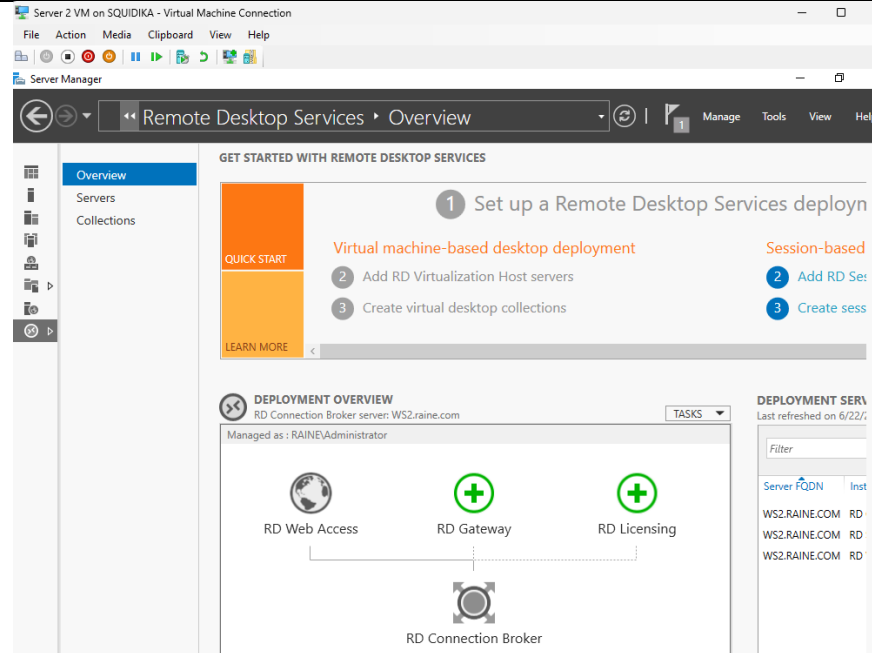
Student name: Raine

Section Summary	<p data-bbox="394 384 967 415">Section 5: Remote access and monitoring</p> <p data-bbox="394 432 467 464">Goals</p> <ul data-bbox="443 474 1409 968" style="list-style-type: none">• Configure and use Remote Desktop (RD) Session-based desktop deployment on WS2• Configure and use RD web access on WS2• Configure and use RD connection broker for WS2• Restrict RD access to specific AD groups• Make WS1 and RD gateway to R2 and connect from Rexnet/Wintec computer• Use the following built-in server monitoring tools:<ul data-bbox="540 747 1000 968" style="list-style-type: none">○ Performance monitor○ Task Manager○ Resource Manager○ Event viewer○ Reliability monitor○ Set local server performance alerts <p data-bbox="394 1020 675 1052">Implementation steps</p> <ol data-bbox="443 1062 1409 1808" style="list-style-type: none">1. Ensure WS1 has two network adapters. One connected to the Rexnet network and one connected to your internal network. It should also be a domain controller and IIS webserver.2. Create a shared folder called certificates on WS1 that can be accessed by all users from the domain.<ul data-bbox="540 1251 902 1283" style="list-style-type: none">○ Can be accessed from WS23. Add the remote desktop service on WS2<ul data-bbox="540 1325 1101 1545" style="list-style-type: none">○ Note this is the service not the role○ Standard deployment○ Enable the following services:<ul data-bbox="638 1440 1101 1545" style="list-style-type: none">▪ RD web access▪ session-based desktop deployment▪ connection broker4. Add servers: WS1 to WS2 and vice versa5. Add RD gateway role to WS1.<ul data-bbox="540 1629 1409 1808" style="list-style-type: none">○ Specify WS1 to be the RD gateway○ Specify the SSL certificate name (you will create this later): WS1_hostname.your_domain○ It takes time to install but once it is done you will see this role appear on WS1
------------------------	---

6. Create a self-signed certificate with the name from the previous step and save it in the shared folder. Name it the same as the FQDN of WS1
7. Create CAP and WAP policy that restricts access - so only Manager and accounts users can use RD to access WS2
8. Use the remote desktop application on a random Rexnet/wireless client to RDP into WS2 through the RD Gateway.
 - Hints: use FQDN of WS1 for the RD gateway settings, which should be the same as the certificate you created
 - You may need to add an entry on the rexnet client's local machine linking the FQDN of WS1 and its external IP address
 - Save the SSL certificate to the trusted root certification authorities folder on the rexnet client when prompted
9. Access WS2 from an internal client using RD web
 - Add RDApp programs that are accessible via the internet e.g. calculator and Server Manager
 - Add SSL certificate to the RD web and client PC
10. Use the following server monitoring tools on both servers and take screenshots at that point in time
 - Task Manager and resource manager
 - What application is using the most CPU and memory?
 - Which user is using the most CPU and memory?
 - Disk usage statistics
 - Network TCP connections
 - Performance monitor
 - Add three features to monitor and explain why you chose them
 - Collect system diagnostic data
 - Create a new user-defined data collection set
 - collect data
 - Set performance counter alert-> processor time and log entries in the application event log
 - Event viewer
 - See errors for the data collection set defined above
 - Reliability monitor
 - What is the average rating value (between one and ten) for your server over the last week?
 - Were there any major fluctuations?
 - Set local server performance alerts
 - Set two alerts and explain why you chose them

1	 <p>Verification of both network adaptors, one for Internet access and one for Private access for communications between VMs / for domain network.</p>
2	 <p>Shared certificates folder accessible by everyone with read/write permissions</p>

3

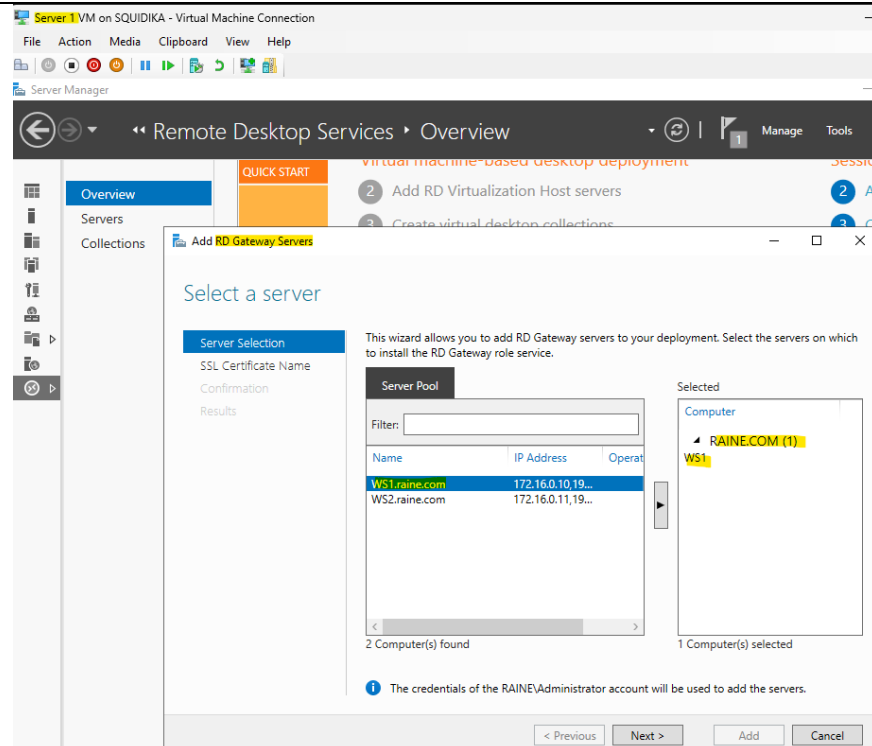


Remote Desktop Services configured on WS2 with standard deployment

4

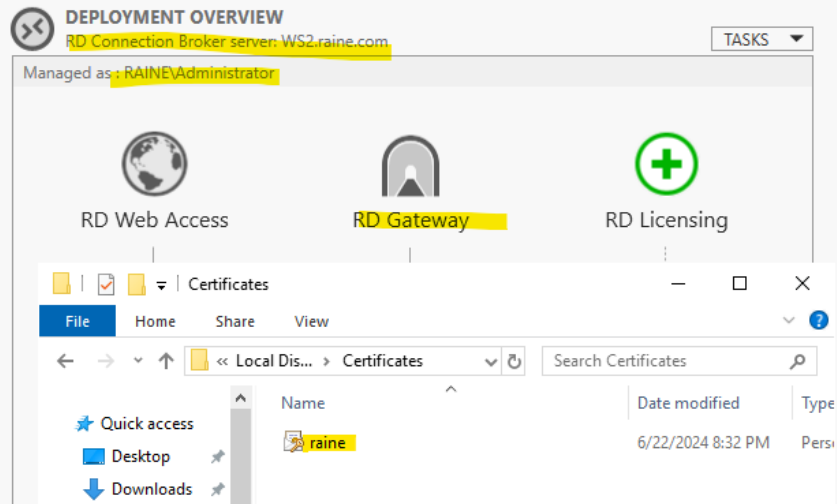
Added both servers to each other, WS2 added to WS1 and WS1 added to WS2

5



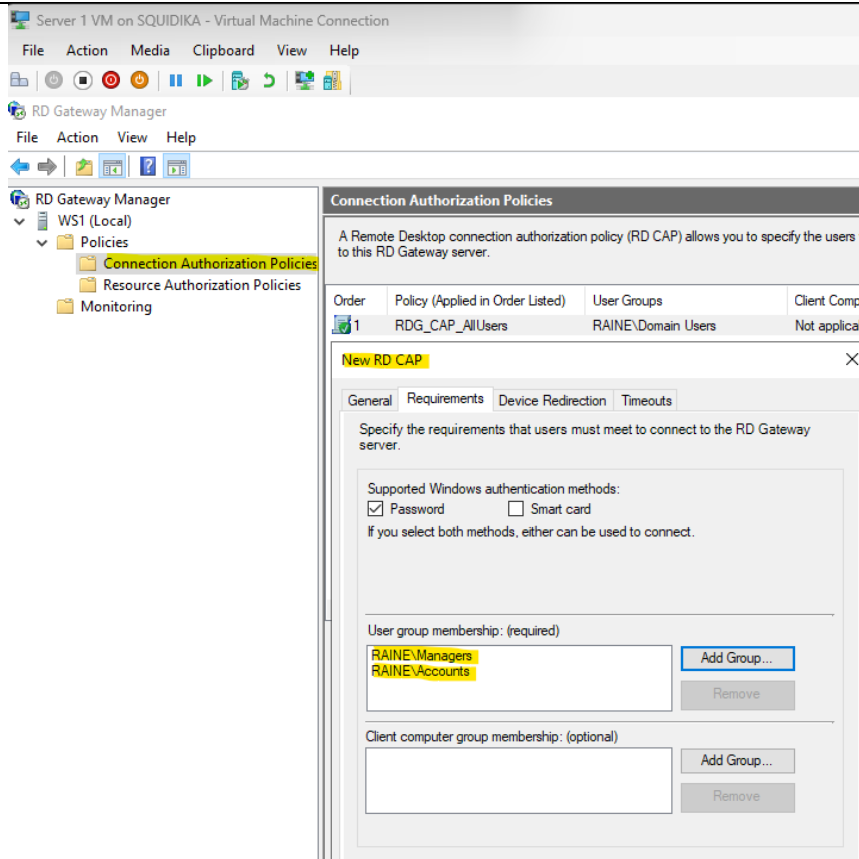
Added WS1 as the RD Gateway

6



SSL certificate created and located in certificates shared folder.

7

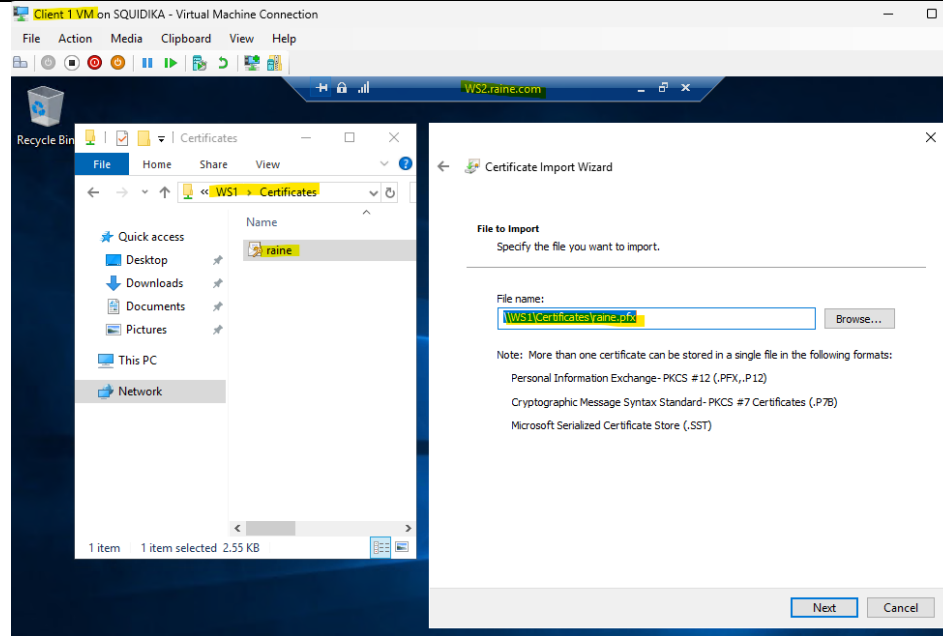


New CAP called ManagersAndAccountsCAP to apply conditional access to users in the Managers and Accounts groups only when using RDP

8

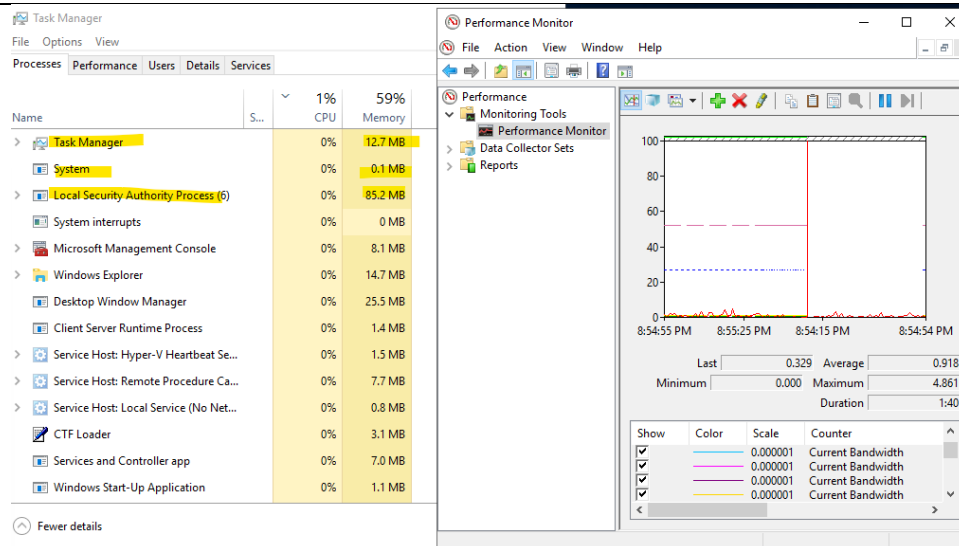
As I am completing this lab remotely using my own laptop setup at home, I am unable to use another, separate device to RDP into WS2.

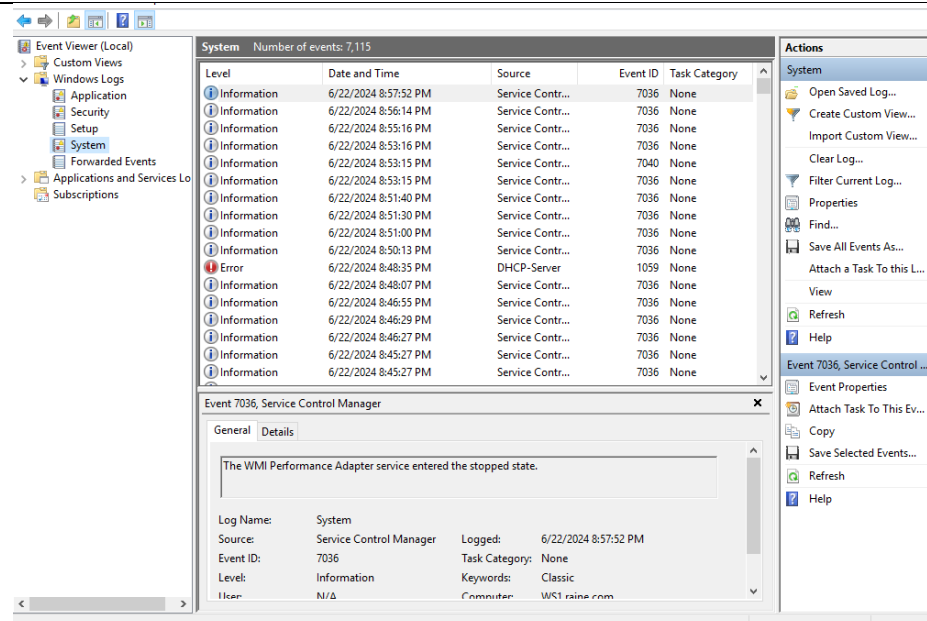
9



Logged into Remote Desktop on the client machine as the user Man1 part of the Managers Group. Remoted into WS2.raime.com, accessing the shared folder hosted on WS1 Certificates. Installing the certificate on the WS2 server using RDP from Client VM.

10





Task Manager, Resource Manager and Event Viewer on WS1:
System and Local Security Authority using the most CPU/RAM.

Using Task Manager and Resource Monitor
Open Task Manager:

On WS1 and WS2, press Ctrl + Shift + Esc to open Task Manager.
Click on the Performance tab to view CPU, Memory, Disk, and Network usage.
Open Resource Monitor:

In Task Manager, go to the Performance tab and click Open Resource Monitor at the bottom.

The Resource Monitor will provide detailed insights into CPU, Memory, Disk, and Network usage.

Information to Capture:

Application using the most CPU and Memory:

Example: SQLServer.exe is using the most CPU and Memory.

User using the most CPU and Memory:

Example: DOMAIN\Administrator is using the most CPU and Memory.

Disk Usage Statistics:

Example: The C: drive has a disk usage of 70% with high read/write activity on SQLServer.log.

Network TCP Connections:

Example: Multiple TCP connections from 192.168.1.5 to port 3389 (RDP).

Using Performance Monitor

Open Performance Monitor:

Click on the Start menu.

Type Performance Monitor and press Enter.

Add Counters to Monitor:

Click the + icon to add counters.

Add the following three counters:

Processor(_Total)% Processor Time: To monitor overall CPU usage.

Memory\Available MBytes: To monitor the available memory.

LogicalDisk(_Total)% Disk Time: To monitor disk activity.

Collect System Diagnostic Data:

In Performance Monitor, right-click on Data Collector Sets and choose System.

Select System Diagnostics and start the data collection.

Create a New User-Defined Data Collection Set:

Right-click on User Defined under Data Collector Sets.

Choose New > Data Collector Set.

Name it CustomDataCollectionSet and choose Create manually.

Add Performance Counter Alert for Processor(_Total)% Processor Time.

Set the threshold to trigger at 80% and log entries in the application event log.

Using Event Viewer

Open Event Viewer:

Click on the Start menu.

Type Event Viewer and press Enter.

View Errors for the Data Collection Set:

Navigate to Windows Logs > Application.

Look for events related to CustomDataCollectionSet.

Using Reliability Monitor

Open Reliability Monitor:

Click on the Start menu.

Type Reliability Monitor and press Enter.

Alternatively, you can access it via the Control Panel under System and Security >

Security and Maintenance > Reliability Monitor.

Check Average Rating and Fluctuations:

Example: The average rating value over the last week is 8.5.

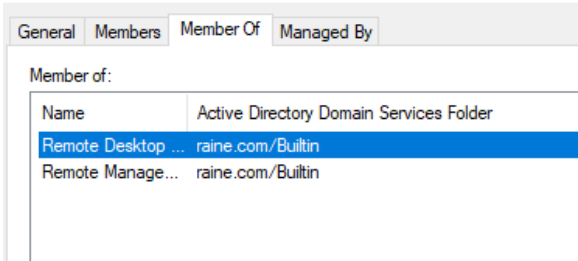
There were major fluctuations on Tuesday due to a system crash and on Thursday due to application errors.

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

<ul style="list-style-type: none"> • Remote desktop • https://www.youtube.com/watch?v=olos0TbZfjY
<ul style="list-style-type: none"> • RD gateway • https://www.youtube.com/watch?v=WD2jUQy32DI&t=921s • https://www.youtube.com/watch?v=h080znhuj8o
<ul style="list-style-type: none"> • RD Web Access • https://www.youtube.com/watch?v=2PTQIm9jmD4

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

https://www.youtube.com/watch?v=w_3E5w7qzHY
https://www.youtube.com/watch?v=7rIAv5nqi2w
https://www.youtube.com/watch?v=olos0TbZfjY

Problem	Solution
Deployed Remote Desktop Service Virtual machine-based desktop deployment instead of session-based.	Remove the role from the server as we are using session based desktops instead of creating new virtual machine based sessions per login.
Users in Managers and Accounts cannot remote into servers, despite being added to the Conditional Access Policy	<p>Managers Properties</p>  <p>Managers and Accounts groups were added to the Remote Desktop groups in AD to allow members in each group to remote.</p>