Dealership IT Support Simulation

"What's up guys Christian Leep here, back at it again for the first time with one of my IT projects. Today I will be simulating a Dealership's infrastructure and be working as an IT Support specialist in-order-to resolve technical problems that arise around the Dealership."

"In-order-to get started I want to first build the environment I will be working in, and to do that I'll be using VirtualBox with Windows Server 2022 and Windows 11 ISOs. I'll start inside VirtualBox by creating a Domain Controller using my Windows Server 2022. If you'd like to follow along, all the links and instructions will be in the description. So without further ado, Let's get right into it."

* VirtualBox
* Windows Server 2022 ISO
* Windows 11 ISO
* Instructions
* Discord Server

"In VirtualBox, click new and add the following, and hit finish"

* VM Name: Dealership-DC
* ISO: Windows Server 2022
* OS Edition: Standard Evaluation
* Username: Dealership-DC
* Password: ThisIsaStrongPa$$
* Hostname: Dealership-DC
* RAM: 4GB
* CPUs: 2
* Disk: 50GB

"Now the server will be installed. Once it comes up, I want to power it down to change some settings in VirtualBox. Click on the Server and hit settings. Then click Network. Here I want to change Adapter 1 to be attached to Internal Network. Then go to adapter 2 and enable the network adapter and attach it to NAT so we can access the internet if needed."

"Now we need to login to the Default Administrator account by typing in 12 to switch users then sign in using the password: ThisIsaStrongPa$$"

"Now go in and change the network settings by hitting 8, then select the 1st network adapter. From here I'll add my values."

* Static IP address: 192.168.1.10
* Subnet mask: 255.255.255.0
* Default gateway: 192.168.1.1
* DNS: 192.168.1.10

"Now that I have my network settings set up, I'm going to head into PowerShell by typing 15 to install Active Directory, DNS, DHCP, and Group Policy."

*# Install Active Directory Domain Services*

Install-WindowsFeature AD-Domain-Services -IncludeManagementTools

#Verify

Get-WindowsFeature AD-Domain-Services

*# Install DHCP*

Install-WindowsFeature DHCP -IncludeManagementTools

*#Verify*

Get-WindowsFeature DHCP

*# Install DNS*

Install-WindowsFeature DNS -IncludeManagementTools

#Verify

Get-WindowsFeature DNS

*#Install Group Policy Management Console*

Install-WindowsFeature -Name GPMC -IncludeManagementTools

#Verify

Get-WindowsFeature GPMC

*# Create Domain Controller/Active Directory Root Forest*

Install-ADDSForest -DomainName "dealership.local" -DomainNetbiosName "DEALERSHIP" -InstallDNS

"This will force a restart"

"After Restart hit ESC to switch users then use the Uername: DEALERSHIP\Administrator and the Password: ThisIsaStrongPa$$ to log in and then go back into powershell by hitting 15."

"Now that DNS is installed, I'm going to lock down the zone so only secure, authenticated updates are allowed so that it prevents rogue devices from registering bogus DNS entries."

*#Ensure PowerShell loads cmdlets for DNS*

Import-Module DnsServer

*#Create Forward Zone*

Set-DnsServerPrimaryZone -Name "dealership.local" -DynamicUpdate Secure

*#Verify*

Get-DnsServerZone -Name "dealership.local"| Select-Object ZoneName, DynamicUpdate

*# Create an AD-integrated reverse zone for 192.168.1.0/24*

Add-DnsServerPrimaryZone -NetworkId 192.168.1.0/24 -ReplicationScope Domain

*# Secure dynamic updates on the reverse zone*

Set-DnsServerPrimaryZone -Name '1.168.192.in-addr.arpa' -DynamicUpdate Secure

*# Verify,*

Get-DnsServerZone -Name '1.168.192.in-addr.arpa' | Select ZoneName,DynamicUpdate

"Next Let's add a DNS forwarder to resolve any web traffic,"

*#Add DNS Forwarder*

Add-DnsServerForwarder -IPAddress 1.1.1.1,8.8.8.8 -PassThru

*# Make it where only the internal NIC should register in AD DNS*

Get-NetAdapter | % { Set-DnsClient -InterfaceAlias $\_.Name -RegisterThisConnectionsAddress $false }

Set-DnsClient -InterfaceAlias 'Ethernet' -RegisterThisConnectionsAddress $true

"Let's add in some DNS Scavenging/aging in order to prevent DNS from filling with stale entries as machines come and go. This ensures that only active devices resolve correctly, which avoids name conflicts and makes the dealership network easier to manage."

# Enable DNS scavenging/aging

Set-DnsServerScavenging -ScavengingState $true -NoRefreshInterval 7.00:00:00 -RefreshInterval 7.00:00:00

Set-DnsServerZoneAging -Name 'dealership.local' -Aging $true -NoRefreshInterval 7.00:00:00 -RefreshInterval 7.00:00:00

Set-DnsServerZoneAging -Name '1.168.192.in-addr.arpa' -Aging $true -NoRefreshInterval 7.00:00:00 -RefreshInterval 7.00:00:00

"Now that DNS is set up I now need to set up DHCP by typing,"

#Ensure PowerShell loads cmdlets for DHCP

Import-Module DhcpServer

# Create AD security groups

Add-DhcpServerSecurityGroup

*# Authorize DHCP server in Active Directory*

Add-DhcpServerInDC -DnsName "DEALERSHIP-DC.dealership.local" -IpAddress 192.168.1.10

*#Verify*

Get-DhcpServerInDC

"Then I need to set the scope, default gateway, and DNS"

*#Set scope*

Add-DhcpServerv4Scope -Name "DealershipScope" -StartRange 192.168.1.100 -EndRange 192.168.1.200 -SubnetMask 255.255.255.0 -State Active

*# Exclude servers/network devices*

Add-DhcpServerv4ExclusionRange -ScopeId 192.168.1.0 -StartRange 192.168.1.1 -EndRange 192.168.1.20

*#Verify*

Get-DhcpServerv4Scope

*# Set default gateway*

Set-DhcpServerv4OptionValue -ScopeId 192.168.1.0 -Router 192.168.1.1

*# Set DNS (point to your DC/DNS server)*

Set-DhcpServerv4OptionValue -ScopeId 192.168.1.0 -DnsServer 192.168.1.10 -DnsDomain dealership.local

* Scope Name: DealershipScope
* Subnet: 192.168.1.0
* Range: 192.168.1.100 → 192.168.1.200
* Subnet Mask: 255.255.255.0
* Default Gateway: 192.168.1.1

*#Verify*

Get-DhcpServerv4OptionValue -ScopeId 192.168.1.0

“Next I'm going to configure DHCP to always update DNS records for clients, to clean up records when leases expire, and to create both forward and reverse entries. This keeps DNS accurate, prevents stale entries, and ensures that both name → IP and IP → name lookups work properly across the dealership network.”

*#Add DHCP Parameters*

Set-DhcpServerv4DnsSetting -DynamicUpdates Always -DeleteDnsRROnLeaseExpiry $true -DisableDnsPtrRRUpdate $false

*#Verify*

Get-DhcpServerv4DnsSetting | fl \*

"Now the scope is set let's check that DHCP is accessible and starts automatically, This should already be set by default but if it wasn't this is what you'd do,"

# Ensure DHCP is accessible + starts automatically

Get-NetFirewallRule -DisplayGroup "DHCP Server" | Set-NetFirewallRule -Enabled True

Get-Service DhcpServer | Set-Service -StartupType Automatic

"Now, that the basic setup is complete, it's time to create Organizational Units within Active Directory so that I can organize users, groups, and computers more efficiently,"

#Create OU's

New-ADOrganizationalUnit -Name 'Dealership' -ProtectedFromAccidentalDeletion $true

New-ADOrganizationalUnit -Name 'Servers' -Path 'OU=Dealership,DC=dealership,DC=local'

New-ADOrganizationalUnit -Name 'Workstations'-Path 'OU=Dealership,DC=dealership,DC=local'

New-ADOrganizationalUnit -Name 'Users' -Path 'OU=Dealership,DC=dealership,DC=local'

New-ADOrganizationalUnit -Name 'Groups' -Path 'OU=Dealership,DC=dealership,DC=local'

*#Verify*

Get-ADOrganizationalUnit -Filter \* | Select Name,DistinguishedName

"Now let's make sure to redirect any new computers and workstations,"

# New computers → Workstations OU

redircmp "OU=Workstations,OU=Dealership,DC=dealership,DC=local"

# New users → Users OU

redirusr "OU=Users,OU=Dealership,DC=dealership,DC=local"

#Prestage MGMT-SRV

New-ADComputer -Name "MGMT-SRV" -Path "OU=Servers,OU=Dealership,DC=dealership,DC=local"

"With the OU's Created, I can now create the Groups,"

*# Create the groups*

New-ADGroup -Name "SalesDept" -SamAccountName SalesDept -GroupScope Global -GroupCategory Security -Path 'OU=Groups,OU=Dealership,DC=dealership,DC=local'

New-ADGroup -Name "ServiceDept" -SamAccountName ServiceDept -GroupScope Global -GroupCategory Security -Path 'OU=Groups,OU=Dealership,DC=dealership,DC=local'

New-ADGroup -Name "ITAdmins" -SamAccountName ITAdmins -GroupScope Global -GroupCategory Security -Path 'OU=Groups,OU=Dealership,DC=dealership,DC=local'

"Now, that the group setup is complete, it's time to create the Domain Accounts,"

*# Create a new Sales Rep account*

New-ADUser -Name "Sales Rep 01" `

-SamAccountName SalesRep01 `

-AccountPassword (ConvertTo-SecureString "SalesP@ss1" -AsPlainText -Force) `

-Enabled $true `

-Path 'OU=Users,OU=Dealership,DC=dealership,DC=local'

"Let's also create a service rep account,"

*# Create a new Service Rep account*

New-ADUser -Name "Service Rep 01" `

-SamAccountName ServiceRep01 `

-AccountPassword (ConvertTo-SecureString "ServiceP@ss1" -AsPlainText -Force) `

-Enabled $true `

-Path 'OU=Users,OU=Dealership,DC=dealership,DC=local'

"Let's also create an IT Admin account,"

*# Create a new IT Admin account*

New-ADUser -Name "ITAdmin 01" `

-SamAccountName ITAdmin01 `

-AccountPassword (ConvertTo-SecureString "ITAdminP@ss1" -AsPlainText -Force) `

-Enabled $true `

-Path 'OU=Users,OU=Dealership,DC=dealership,DC=local'

"Now that the accounts are created, let's add them to their respected groups,"

*# Add Users to Groups*

Add-ADGroupMember -Identity "SalesDept" -Members "SalesRep01"

Add-ADGroupMember -Identity "ServiceDept" -Members "ServiceRep01"

Add-ADGroupMember -Identity "ITAdmins" -Members "ITAdmin01"

"To verify that both were created and to see some additional information,"

*#See all Domain Accounts*

Get-ADUser -Filter \* -Properties \* | Select-Object Name, Enabled, PasswordLastSet, WhenCreated, MemberOf

"Before we move on to setting up the next server, Let's add in a time Sync,"

*# Configure DC as authoritative time source*

w32tm /config /manualpeerlist:"time.windows.com,0x9" /syncfromflags:manual /reliable:yes /update

net stop w32time

net start w32time

w32tm /resync

"Now that I have set up the permissions for the domain accounts split into groups now, I need to setup a Group Policy Management. To do this I need to create a Windows Server 2022 Desktop Experience that will act like a management workstation."

"In VirtualBox, click new and add the following, and hit finish"

* VM Name: Management-Server
* ISO: Windows Server 2022
* OS Edition: Desktop Experience
* Username: MGMT-SRV
* Password: ThisIsaStrongPa$$
* RAM: 4GB
* CPUs: 2
* Disk: 50GB

"Once the Management Server has fully come up, I want to power it down and do the same thing to the network settings as I did to the Domain Controller."

"Now that the Management server is on the correct network, I can continue setting it up. First Hit Win+r then type ncpa.cpl. Right click Ethernet 2 adapter, click properties and enter the admin username and password. Then click IPv4 and properties. Then click advanced. Click DNS tab and uncheck Register this connection's addresses in DNS then hit ok ok and close.

Next, Right click dealership.local Ethernet adapter, click properties and enter the admin username and password. Then click IPv4 and properties and set the Preferred DNS to 192.168.1.10

* Username DEALERSHIP\Administrator
* Password: ThisIsaStrongPa$$

Then use Win+r > sysdm.cpl and then Change. Then click member of domain and type in dealership.local and a username and password entry will come up and from there put in the domain admin username and password. From here, Restart the Management Server for the changes to take effect."

* Username DEALERSHIP\Administrator
* Password: ThisIsaStrongPa$$

"After the restart you should see other user popup on and after clicking on it you can see that it is connected to the DEALERSHIP domain. Now login to the admin account. Now I want to confirm the DNS is set correctly. Hit Win+r then type ncpa.cpl. Right click dealership.local Ethernet adapter, click properties. Then click IPv4 and properties and verify the Preferred DNS to 192.168.1.10

"Now let's turn on remote desktop,"

#Turn on Remote Desktop

Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server' -Name 'fDenyTSConnections' -Value 0

#Require Network Level Authentication

Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -Name 'UserAuthentication' -Value 1

#Allow Firewall Rule

Enable-NetFirewallRule -DisplayGroup "Remote Desktop"

#Grant the domain group RDP sign-in rights locally

net localgroup "Remote Desktop Users" "DEALERSHIP\ITAdmins" /add

"Now, let's add some folders,"

# Create the folders

New-Item -Path "C:\Shares\Sales" -ItemType Directory -Force

New-Item -Path "C:\Shares\Service" -ItemType Directory -Force

"We can verify by going into file explorer>ThisPC>Local Disk C:>Shares, and here you'll see the folders we just made,"

"Now the folders are created, Let's share them on the network."

# Share the folders on the network

New-SmbShare -Name "Sales" -Path "C:\Shares\Sales" -FullAccess "DEALERSHIP\SalesDept"

New-SmbShare -Name "Service" -Path "C:\Shares\Service" -FullAccess "DEALERSHIP\ServiceDept"

"Perfect, the folders are on the network, but I need to set up NTFS permissions so only members of the corresponding team has access to the folders."

# Remove inherited permissions

icacls "C:\Shares\Sales" /inheritance:r

icacls "C:\Shares\Service" /inheritance:r

# Grant SalesDept full control over Sales folder

icacls "C:\Shares\Sales" /grant "DEALERSHIP\SalesDept:(OI)(CI)F"

# Grant ServiceDept full control over Service folder

icacls "C:\Shares\Service" /grant "DEALERSHIP\ServiceDept:(OI)(CI)F"

"Now the Management Server is connected, run powershell as an administrator and finish setting up Group Policies"

*#Install Active directory users and GPM*

Install-WindowsFeature RSAT-ADDS, GPMC -IncludeManagementTools

"Now launch Group Policy by typing gpmc.msc. From here expand the forest and domains to get to dealership.local and right click it then create a GPO in this domain, and Link it here.. I'm going to name it Department Drive Mapping."

"From there Right click Department Drive Mapping and under

User Configuration > Preferences > Windows Settings click drive maps. Then right click in white area and hit new > mapped drive.

* General
  + Action: Create
  + Location: [\\MGMT-SRV\Sales](file:///\\MGMT-SRV\Sales)
  + Label as: SalesDept
  + Drive Letter: S
* Common
  + Item-level targeting
    - Targeting
    - New Item
    - Security Group
      * Group: …SalesDept then hit apply

"Now let's do the same thing for the ServiceDept"

* General
  + Action: Create
  + Location: \\MGMT-SRV\Service
  + Label as: ServiceDept
  + Drive Letter: T
* Common
  + Item-level targeting
    - Targeting
    - New Item
    - Security Group
      * Group: …ServiceDept then hit apply

"Now that I have the group policy set to use department specific drives I now want to set some basic security hardening like a Password Policy, and an account lockout policy.

Under Default Domain Policy right click and edit.

Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy."

* Enforce password history: 5 passwords remembered
* Maximum password age: 30 days
* Minimum password length: 10 characters
* Password must meet complexity requirements: Enabled

"Now for the Account Lockout Policy. Click Account Lockout Policy."

* Account lockout threshold: 5 Invalid attempts
* Account lockout duration: 15 Minutes
* Reset account lockout counter after 15 minutes

"Next I'm going to add and configure an Audit Policy. Go back to Forest:

dealership.local → Domains → dealership.local → Domain Controllers. Right click default domain controllers policy and click edit. From here

Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies → Logon/Logoff

* Audit Account Lockout: Success, Failure
* Audit Logoff: Success
* Audit Logon: Success, Failure
* Audit Other Logon/Logoff Events: Success, Failure
* Audit Special Logon: Succes

"Then go to Account Logon and change,"

* Audit Credential Validation: Success, Failure
* Audit Kerberos Authentication Service: Success, Failure

"With these things changed I'm going to go back to the Domain Controller and gpupdate /force."

"Now I'm going to open event viewer as administrator and set up a filter for my logs. On the right hand side "Actions" click create custom view then set logged time to any time and then event level to

Warning, Error, and Information.

By Log – Security then use the following event ID's and name it Logon and Lockout Events

* 4624 → Successful logon
* 4625 → Failed logon
* 4634 → Logoff
* 4647 → User initiated logoff
* 4672 → Special privileges assigned (e.g., admin login)
* 4740 → Account locked out

"You can now see the new custom view on the left and see all the events that happen"

"We've set a few things up already and now I want to get into setting up a virtual printer shared my domain. To do this I'm going to use my Management Server. In the control panel go to devices and printers. From here click Add Printer then The printer that I want isn't listed. Next choose add a local printer or network printer with manual settings. Then Select Use an existing port (LPT1: Printer Port) and name the printer SalesPrinter with the location of [\\mgmt-srv\SalesPrinter](file:///\\mgmt-srv\SalesPrinter) and do the same for the Service printer just switch to LPT2"

"Now to add the printers to Group Policy. Win+r > gpmc.msc then under domains right click dealership.local and click Create a GPO in this domain, and Link it here…. Then name it Sales Printer Policy. Then right click and edit. From there

User Configuration → Preferences → Control Panel Settings → Printers. Right click the right pane hit new and shared printer. Create with a shared path of [\\MGMT-SRV\SalesPrinter](file:///\\MGMT-SRV\SalesPrinter) and check set this printer as default printer then in the common tab check item-level targeting and add security group SalesDept"

"Now do the same for the Service Dept"

"Let's jump back to add in an RDP GPO,"

Create your RDP GPOs from MGMT-SRV (gpmc.msc)

Right-click Group Policy Objects → New →

Name: Workstations - RDP (Admins Only)

Name: MGMT-SRV - RDP (Admins Only)

Under Dealership → You should see "Groups, Servers, Users, and Workstations"

Then right-click and “Link an Existing GPO” to their respective OUs:

Workstations - RDP (Admins Only) → Linked to OU=Workstations

MGMT-SRV - RDP (Admins Only) → Linked to OU=Servers

Configure Restricted Groups & RDP Settings:

From MGMT-SRV – RDP (Admins Only) & Workstations – RDP (Admins Only) right click and edit

Computer Configuration → Policies → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Host → Connections

Allow Users to connect remotely using Remote Desktop Services = Enabled

→ Security

Require user authentication for remote connections by using NLA = Enabled

Computer Configuration → Policies → Windows Settings → Security Settings → Windows Defender Firewall with Advanced Security → Inbound Rules

Right click → new rule → Predefined → Remote Desktop → Check all 3 boxes, Remote Desktop – User Mode (UDP-In and TCP-IN) Shadow (TCP-In) → Next → Allow the Connection → Finish

Apply the new inbound rule to only effect domain users

Double click Remote Desktop – User Mode (TCP-In) → Advanced → only check Domain → apply

Then do the same for the other two inbound rules

Next we are going to Limit RDP Access to the ITAdmins Group (Restricted Groups)

Computer Configuration → Policies → Windows Settings → Security Settings → Restricted Groups

Right-click → Add Group → Type "Remote Desktop Users"

In the "Members of this Group" section: Click add and type DEALERSHIP\ITAdmins → Apply

Do the same thing for Workstations - RDP (Admins Only)

"From here let's just go ahead and gpupdate on our servers"

"Now that we have most everything on our servers set up let's go set up our client computers."

"On VirtualBox click New.

* VM Name: Sales-PC
* ISO: Windows 11
* OS Edition: Pro
* Username: Sales-PC
* Password: ThisIsaStrongPa$$
* Hostname: Sales-PC
* RAM: 4GB
* CPUs: 2
* Disk: 80GB
* Windows Key: VK7JG-NPHTM-C97JM-9MPGT-3V66T

"I've ran into some issues with administrator accounts so I'm going to go through a quick work around to get the system set up and later we will disable the local administrator account. Once the system comes up power it off and change the network settings like we did on the management server. Then once you're in it again reboot system into safe mode (restart while holding Shift)

When it comes back up hit Troubleshoot, then advanced, then startup settings and click restart

Once restarted

Boot to safe mode click start then switch user then loginto administrator with the password you created in virtualbox

From there you need to make the accounts Admin accounts by going into the control panel and accessing the users and create a user.

Once in then open the network settings. First Hit Win+r then type ncpa.cpl and join the domain (dealership.local)

Then use Win+r > sysdm.cpl and then Change. Then click member of domain and type in dealership.local and a username and password entry will come up and from there put in the domain admin username and password.

From here you can know test the whole environment.