How to Configure Exceptions for Netlogon Functionality

Objective

Microsoft have again made a change to the Netlogon secure channel connection which now requires the use of RPC sealing. These have a direct impact on the mounting of cifs-shares from an HNAS. This is detailed in How_to_manage_the_Netlogon_protocol_changes_related_to_CVE-2022-38023

This article provides an example of how to configure an exception to allow HNAS to continue to connect to the DC's once enforcement has been enabled.

Environment

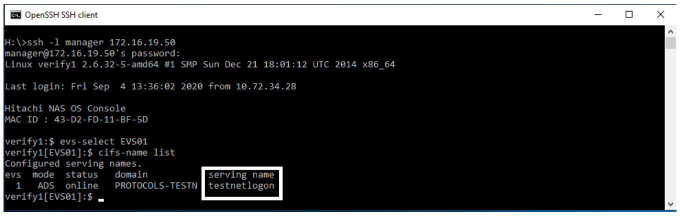
- Hitachi NAS Platform
  - Hitachi NAS Platform 4040 (HNAS 4040)
  - Hitachi NAS Platform 4060 (HNAS 4060)
  - Hitachi NAS Platform 4080 (HNAS 4080)
  - Hitachi NAS Platform 4100 (HNAS 4100)
  - Hitachi NAS Platform 3080 (HNAS 3080) End of Support Life
  - Hitachi NAS Platform 3090 (HNAS 3090) End of Support Life
  - Hitachi NAS Platform 5200 (HNAS 5200)
  - Hitachi NAS Platform 5300 (HNAS 5300)
  - Hitachi Virtual Storage Platform G/Fx00 models (VSP G/Fx00) NAS modules
  - Hitachi Virtual Storage Platform Nx00 models (VSP Nx00) NAS modules

Procedure

Configuring Exceptions

Configuring an exception that allows CIFS shares from one or more HNAS's to still be successfully mounted is an involved process.

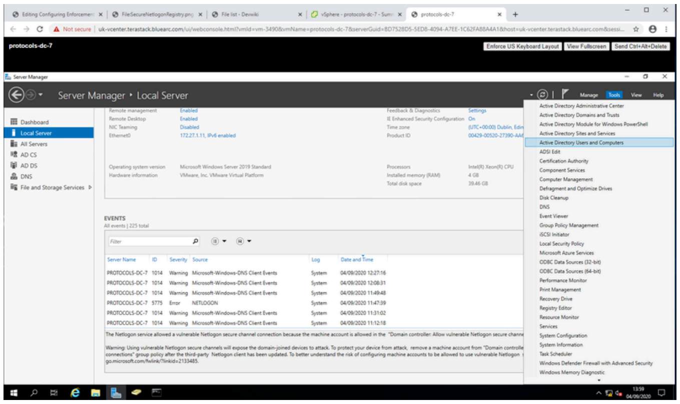
Firstly, identify the name of the machine account that the HNAS uses when trying to make a connection. This will be the serving name supplied when the cifs-name command was used to register the EVS with the domain controller. You can find the name out by using the "cifs-name list" command on the HNAS:



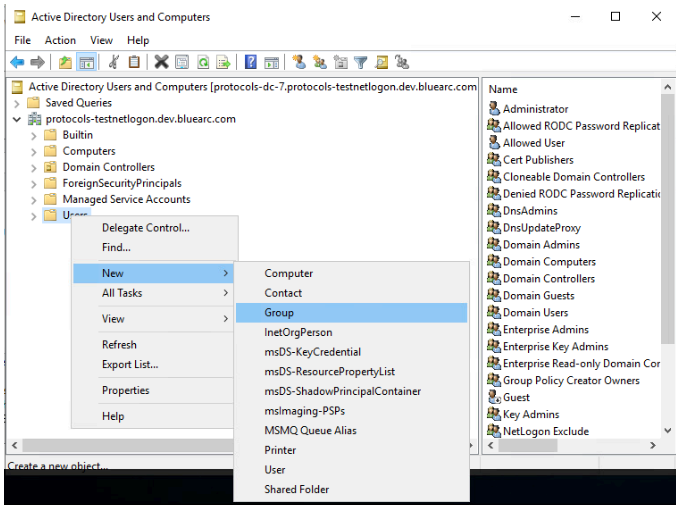
```
H:\>ssh -l manager 172.16.19.50
manager@172.16.19.50's password:
Linux verify1 2.6.32-5-amd64 #1 SMP Sun Dec 21 18:01:12 UTC 2014 x86_64

Last login: Fri Sep  4 13:36:02 2020 from 10.72.34.28

Hitachi NAS OS Console
MAC ID : 43-D2-FD-11-BF-5D

verify1:$ evs-select EVS01
verify1[EVS01]:$ cifs-name list
Configured serving names.
evs  mode  status   domain          serving name
  1   ADS  online   PROTOCOLS-TESTN  testnetlogon
verify1[EVS01]:$
```

You now need to set up the security group property object on the domain controller. This example is for Windows 2019 server, the process would be similar on other versions of Windows Server.

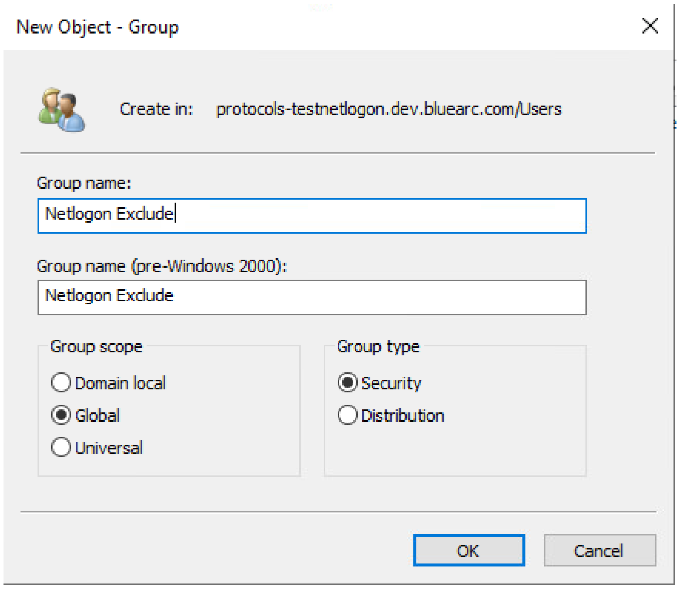
On the Server Manager on the domain controller, select "Tools" -> "Active Directory Users and Computers":


Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Server Manager • Local Server
Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Certification Authority
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Recovery Drive
Registry Editor
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Defender Firewall with Advanced Security
Windows Memory Diagnostic

In the "Active Directory Users and Computers" dialogue, right click on "Users" and select "New" -> "Group":



In the "New Object - Group" dialogue, enter a group name. In this example I have used the group name "Netlogon Exclude". Leave the group scope as the default "Global". Leave the group type as the default "Security":



New Object - Group

Create in: protocols-testnetlogon.dev.bluearc.com/Users

Group name:
Netlogon Exclude

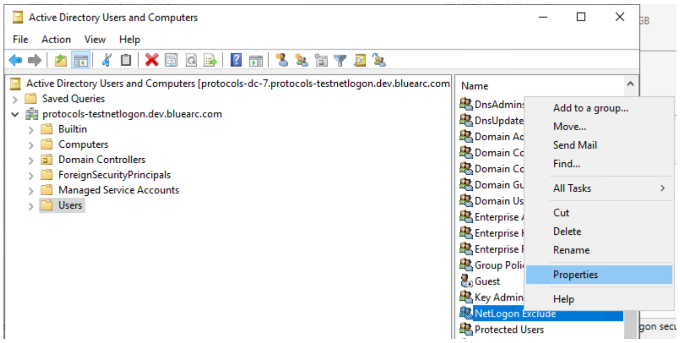
Group name (pre-Windows 2000):
Netlogon Exclude

Group scope
○ Domain local
● Global
○ Universal

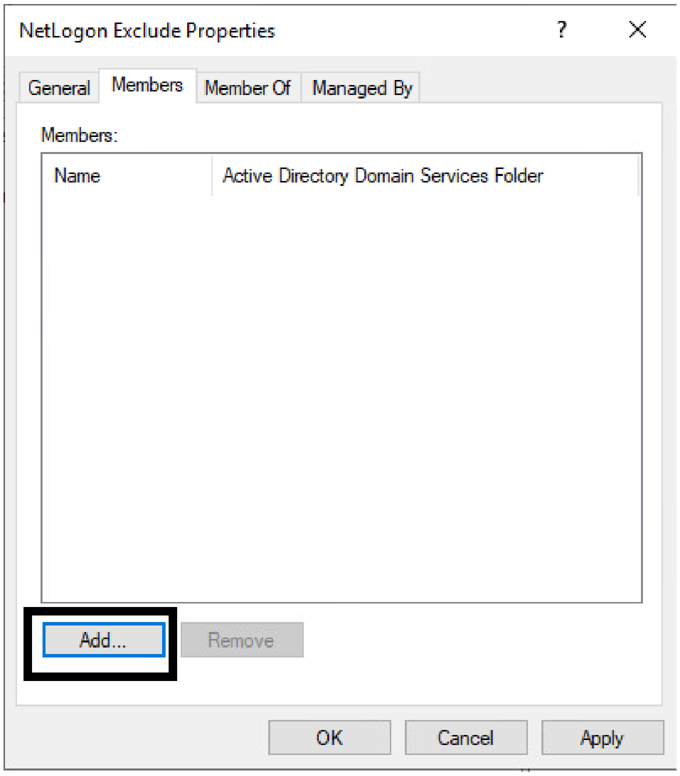
Group type
● Security
○ Distribution

Click on the OK button to create the group and close the "New Object - Group" dialogue.

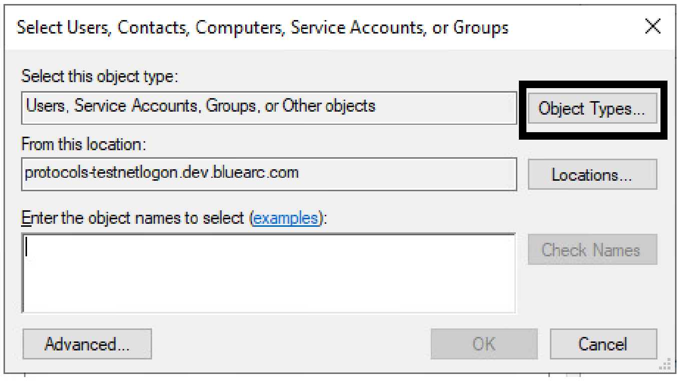
Next, in the list of Users, right click on the group that you have just added and select "Properties":



In the group property dialogue that this brings up, select the members tab. This will initially be empty. Click on the Add button:



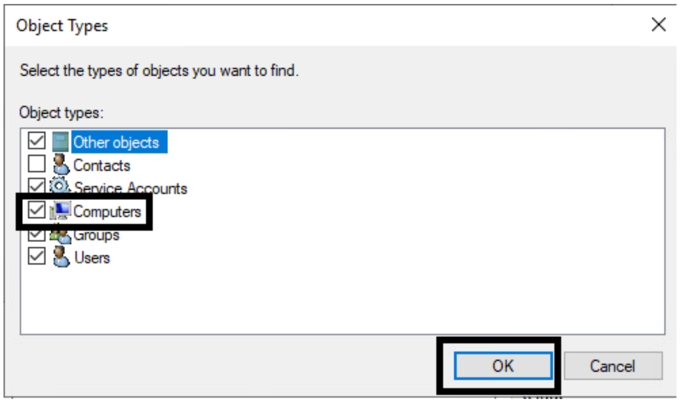
In the selection dialogue that this brings up, click on the "Object types" button:


Select Users, Contacts, Computers, Service Accounts, or Groups
X
Select this object type:
Object Types...
From this location:
Locations...
Enter the object names to select (examples):
Check Names
Advanced...
OK
Cancel

Select this object type: Users, Service Accounts, Groups, or Other objects

From this location: protocols-testnetlogon.dev.bluearc.com

In the "Object Types" dialogue, ensure that the tickbox next to "Computers" is selected and then click on OK:



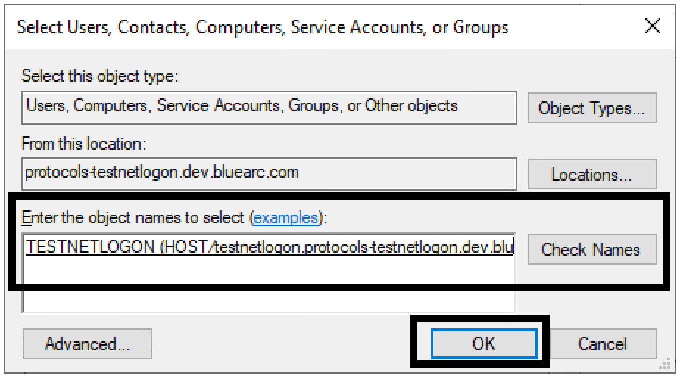
Object Types

Select the types of objects you want to find.

Object types:

☑ Other objects
□ Contacts
☑ Service Accounts
☑ Computers
☑ Groups
☑ Users

Back in the selection dialogue, enter the machine account name (that's the serving name which you found earlier) in the "Enter the object names" dialogue box, and then click on the "Check Names" button. This will cause the system to find the fully qualified version of the machine account name and display it in the "Enter the object names" field. Then click on the OK button:



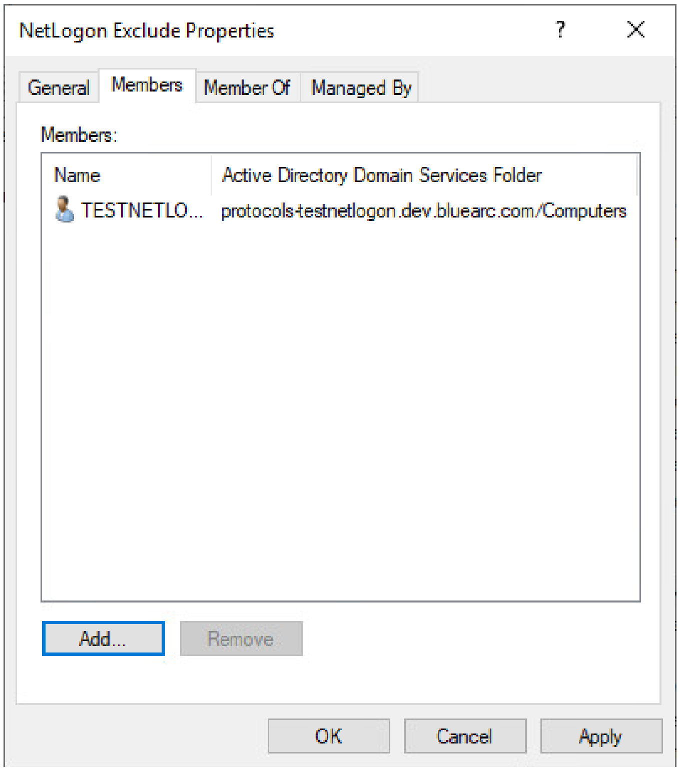
Select Users, Contacts, Computers, Service Accounts, or Groups

Select this object type:
Users, Computers, Service Accounts, Groups, or Other objects

From this location:
protocols-testnetlogon.dev.bluearc.com

Enter the object names to select (examples):
TESTNETLOGON (HOST/testnetlogon.protocols-testnetlogon.dev.blu

The members tab in the group properties now shows the machine account which you just added:



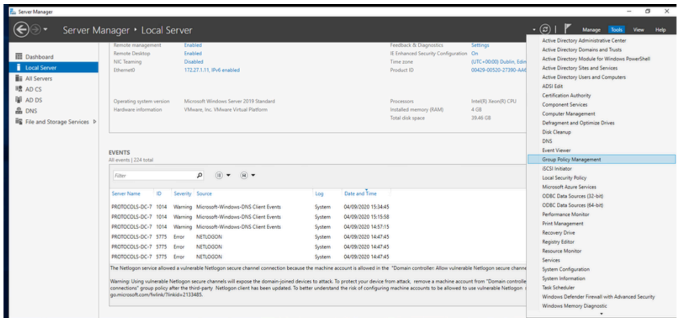
Members:

Name	Active Directory Domain Services Folder
TESTNETLO...	protocols-testnetlogon.dev.bluearc.com/Computers

This example is for one serving name on one EVS on one HNAS. However, if you wanted the exclusion to apply to multiple HNAS's and/or multiple EVS's and/or multiple serving names defined using cifs-name, then you need to repeat the above process to add each of the relevant machine accounts to this group. The remaining steps of this process then only need to be done once and will apply to all members of the group.

Once you have added the machine account or accounts, click on "Apply" then "OK" to exit this dialogue. Then click on the top right "X" to close the "Active Directory Users and Computers" window.

Now back in Server Manager again, select "Tools" -> "Group Policy Management" from the menu:



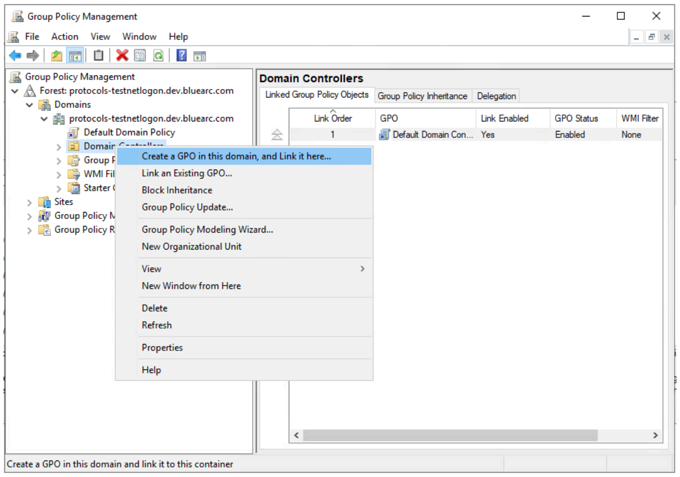
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Enabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC+00:00) Dublin, Edin
Ethernet0	172.27.1.11, IPv6 enabled	Product ID	00429-00520-27390-AA
Operating system version	Microsoft Windows Server 2019 Standard	Processors	Intel(R) Xeon(R) CPU
Hardware information	VMware, Inc. VMware Virtual Platform	Installed memory (RAM)	4 GB
		Total disk space	39.46 GB

EVENTS
All events | 224 total

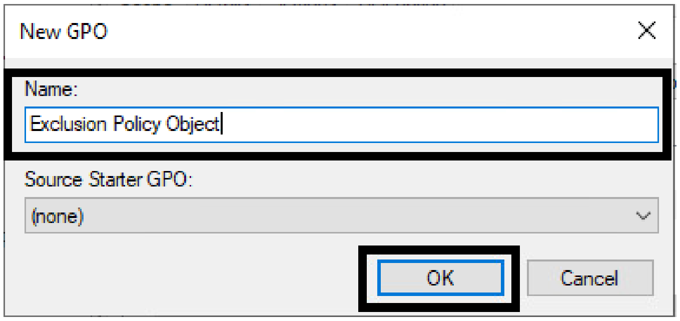
Server Name	ID	Severity	Source	Log	Date and Time
PROTOCOLS-DC-7	1014	Warning	Microsoft-Windows-DNS Client Events	System	04/09/2020 15:34:45
PROTOCOLS-DC-7	1014	Warning	Microsoft-Windows-DNS Client Events	System	04/09/2020 15:15:58
PROTOCOLS-DC-7	1014	Warning	Microsoft-Windows-DNS Client Events	System	04/09/2020 14:57:15
PROTOCOLS-DC-7	5775	Error	NETLOGON	System	04/09/2020 14:47:45
PROTOCOLS-DC-7	5775	Error	NETLOGON	System	04/09/2020 14:47:45
PROTOCOLS-DC-7	5775	Error	NETLOGON	System	04/09/2020 14:47:45

```
The Netlogon service allowed a vulnerable Netlogon secure channel connection because the machine account is allowed in the "Domain controller: Allow vulnerable Netlogon secure channe

Warning: Using vulnerable Netlogon secure channels will expose the domain-joined devices to attack. To protect your device from attack, remove a machine account from "Domain controlle
connections" group policy after the third-party Netlogon client has been updated. To better understand the risk of configuring machine accounts to be allowed to use vulnerable Netlogon
go.microsoft.com/fwlink/?linkid=2133485.
```

This opens the Group Policy management window. Right click on domain controllers and select "Create a GPO in this domain, and Link it here...":



This brings up the dialogue for creating a new group policy object. Enter a name for the group policy object (in this example it is called it "Exclusion Policy Object") and then click on OK:

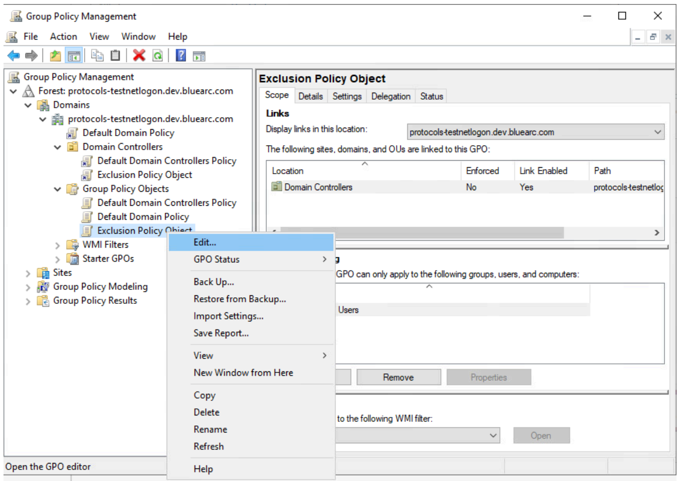


Name: Exclusion Policy Object

Source Starter GPO: (none)

If you now expand the "Domain Controllers" item in the left pane, included under it is a link (note the small arrow on its icon) to "Exclusion Policy Object".

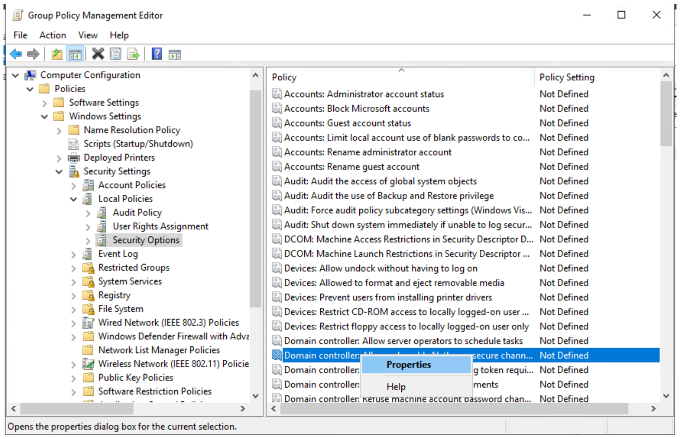
Also expand the "Group Policy Objects" item in the left pane. The includes the actual item for "Exclusion Policy Object". Right click on this and select "Edit..." from the menu:



This opens the Group Policy Management Editor.

In the left pane, expand "Computer Configuration" -> "Policies" -> "Windows Settings" -> "Security Settings" -> "Local Policies", and select "Security Options"

In the right pane, right click on "Domain Controller: Allow vulnerable Netlogon secure channel connections" and select "Properties":



Group Policy Management Editor

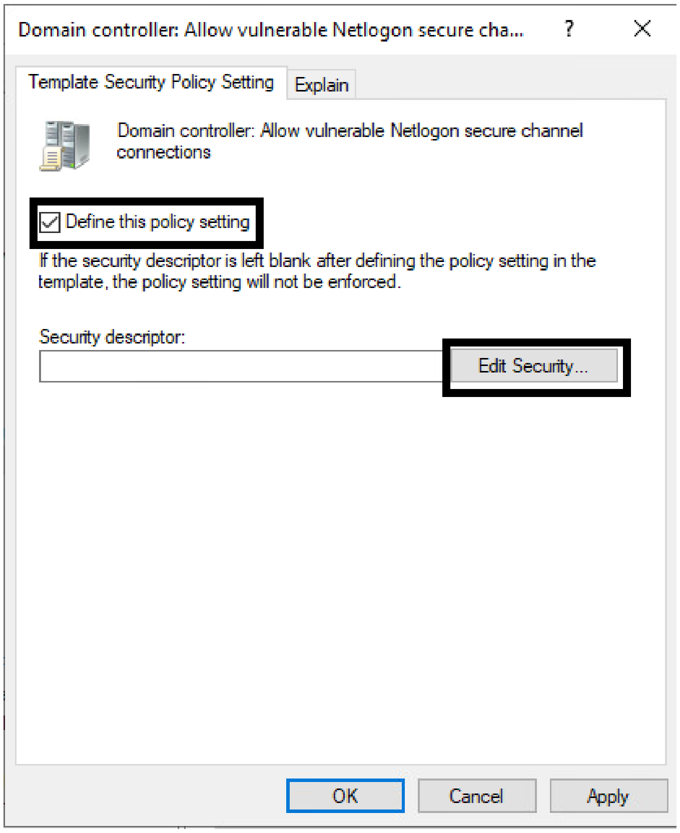
File Action View Help

- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Policies
        - Windows Defender Firewall with Adva
        - Network List Manager Policies
        - Wireless Network (IEEE 802.11) Policie
        - Public Key Policies
        - Software Restriction Policies

Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to co...	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: secure chann...	Not Defined
Domain controller: g token requi...	Not Defined
Domain controller: ments	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined

Opens the properties dialog box for the current selection.

In the "Domain Controller: Allow vulnerable Netlogon secure cha..." dialogue that is opened, select the "Define this policy setting" tickbox, and then click on the "Edit Security" button:



Domain controller: Allow vulnerable Netlogon secure cha...

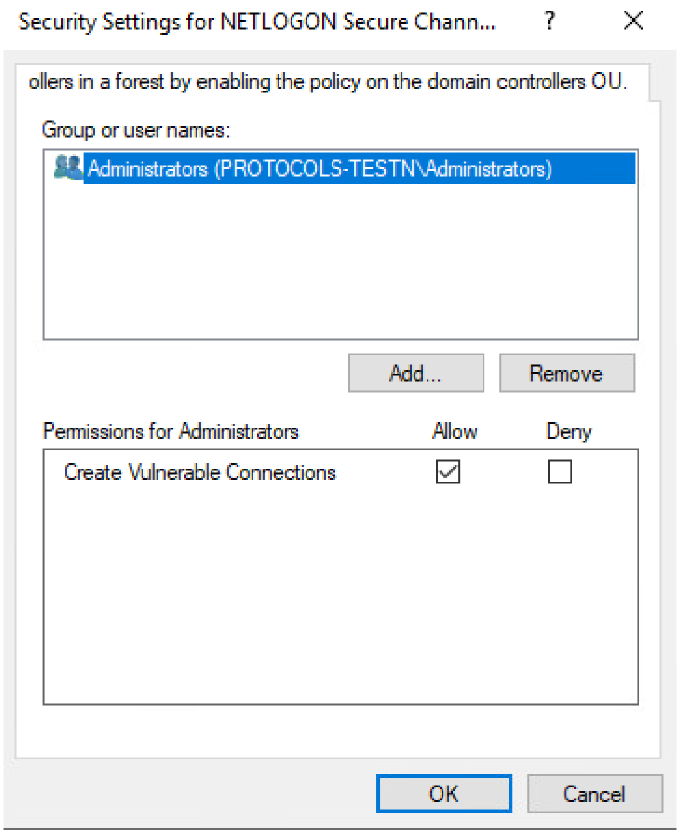
Domain controller: Allow vulnerable Netlogon secure channel connections

☑ Define this policy setting

If the security descriptor is left blank after defining the policy setting in the template, the policy setting will not be enforced.

Security descriptor:

In the "Security Settings for NETLOGON Secure Chann..." dialogue that this brings up, it initially shows the Administrators group in the top pane:



Security Settings for NETLOGON Secure Chann...

ollers in a forest by enabling the policy on the domain controllers OU.

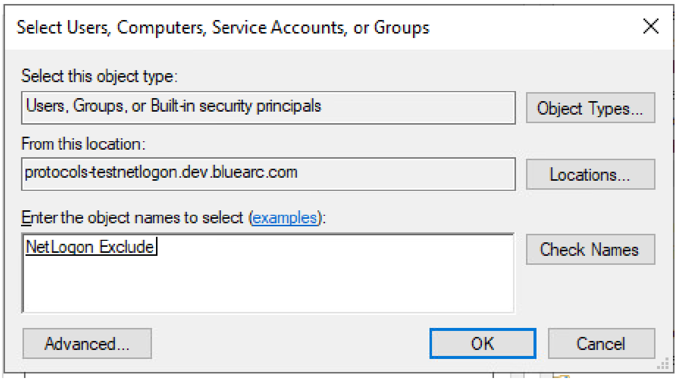
Group or user names:

Administrators (PROTOCOLS-TESTN\Administrators)

Permissions for Administrators	Allow	Deny
Create Vulnerable Connections	☑	□

Click on the "Remove" button to remove the Administrators group. Then click on the "Add" button.

In the "Select Users, Computers, Service Accounts, or Groups", under "Enter the object names to select" enter the name of the security group (so in this case "Netlogon Exclude") and then click on the "Check Names" button. This will cause the verified name of the group to appear in the box:



Select Users, Computers, Service Accounts, or Groups

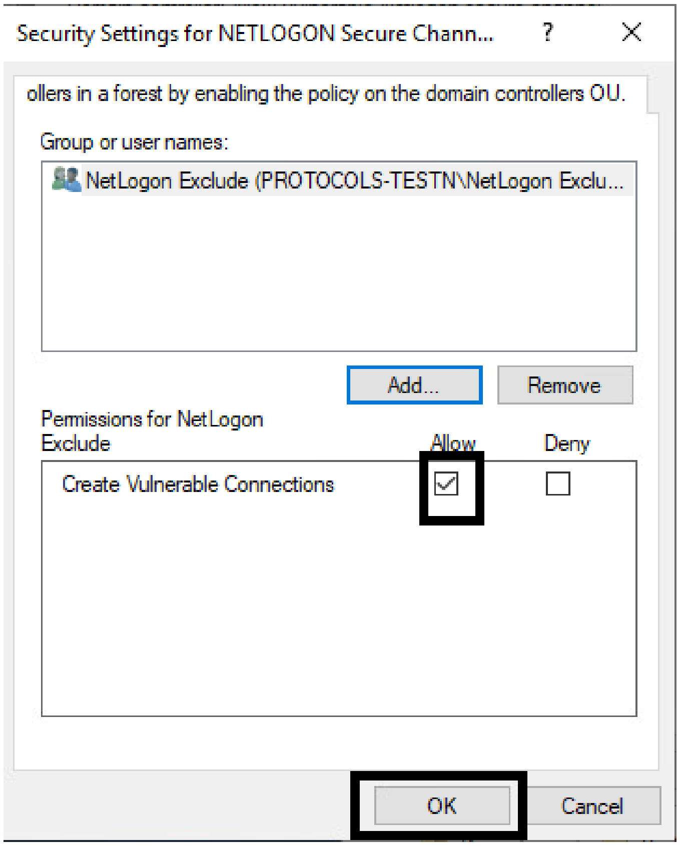
Select this object type:
Users, Groups, or Built-in security principals

From this location:
protocols-testnetlogon.dev.bluearc.com

Enter the object names to select (examples):
NetLogon Exclude

Click "OK" to close the "Select Users, Computers, Service Accounts, or Groups" dialogue.

Back in the "Security Settings for NETLOGON Secure Chann...", make sure that the "Allow" tickbox next to "Create Vulnerable Connections" is selected, and then click the "OK" button:



Security Settings for NETLOGON Secure Chann... ? ×

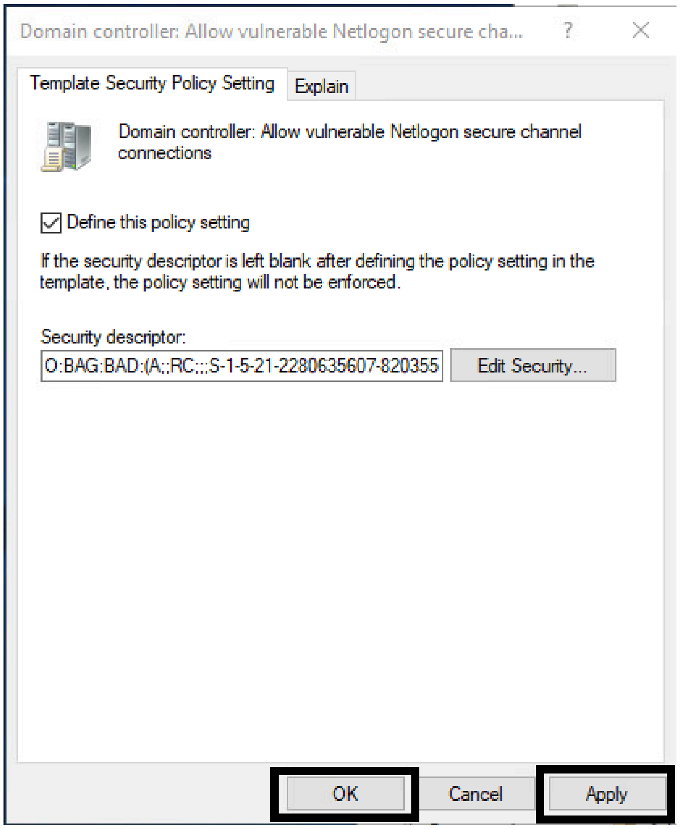
ollers in a forest by enabling the policy on the domain controllers OU.

Group or user names:

NetLogon Exclude (PROTOCOLS-TESTN\NetLogon Exclu...

Permissions for NetLogon Exclude	Allow	Deny
Create Vulnerable Connections	☑	□

You will see that a security descriptor is now filled in in the "Domain Controller: Allow vulnerable Netlogon secure cha..." dialogue. Click "Apply", then "OK":


Domain controller: Allow vulnerable Netlogon secure cha...
?
Template Security Policy Setting
Explain

Domain controller: Allow vulnerable Netlogon secure channel connections

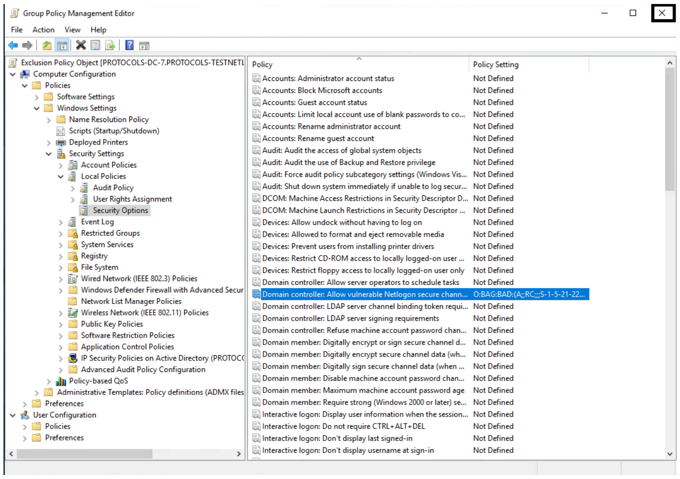
☑ Define this policy setting

If the security descriptor is left blank after defining the policy setting in the template, the policy setting will not be enforced.

Security descriptor:
O:BAG:BAD:(A;;RC;;;S-1-5-21-2280635607-820355

Edit Security...
OK
Cancel
Apply

The Group Policy Management Editor now shows a value stored against "Domain Controller: Allow vulnerable Netlogon secure channel connections". Click on the top right "X" to close the window:


Group Policy Management Editor
File
Action
View
Help
Exclusion Policy Object [PROTOCOLS-DC-7.PROTOCOLS-TESTNETL
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Secur
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (PROTOCO
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX files
Preferences
User Configuration
Policies
Preferences

Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to co...	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	O:BAG:BAD:(A;;RC;;;S-1-5-21-22...
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Not Defined
Domain member: Digitally encrypt secure channel data (wh...	Not Defined
Domain member: Digitally sign secure channel data (when ...	Not Defined
Domain member: Disable machine account password chan...	Not Defined
Domain member: Maximum machine account password age	Not Defined
Domain member: Require strong (Windows 2000 or later) se...	Not Defined
Interactive logon: Display user information when the session...	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Don't display last signed-in	Not Defined
Interactive logon: Don't display username at sign-in	Not Defined

Then click on the top right "X" to close the Group Policy Management window.

That is all of the configuration completed. All that remains is to try to ensure that your changes get propagated as quickly as possible. One key way of doing this is to:

1. Open a Command Prompt with Administrator privilege (i.e. in the Windows Start button search field, search for "Command Prompt", right click on the Command Prompt icon that it finds, and choose "Run as administrator").

2. From the Administrator Command Prompt, run the command "gpupdate /force".

Additional Notes

Internal Notes