CQURE Guide

NTLM Phase-out Guide in Active Directory Environments

Warsaw New York Dubai Zug

info@cqure.pl

www.cqure.pl
www.cqureacademy.com

Table of Contents

1 Disclaimer

The following instruction has been prepared for a laboratory environment and is intended solely for illustrative purposes. Its aim is to demonstrate example steps that may be taken to monitor the use of the NTLM protocol and to potentially disable it.

This instruction does not constitute a universal guide or a ready-to-use procedure and should not be applied directly in production environments. Each domain environment has its own specific configuration and dependencies, which may render the steps described here insufficient or inappropriate.

Before applying any of the guidance described herein, you must:

1. perform a detailed analysis of dependencies within your environment,
2. validate the impact of the changes in a controlled test/lab environment,
3. adjust the configuration to match the specifics of your infrastructure.

The authors of this instruction accept no liability for any consequences resulting from its direct use in production systems.

2 Introduction

Microsoft officially deprecated the NTLM (NT LAN Manager) protocol in June 2024, ending active development of this technology after more than 30 years of use. NTLMv1 has already been removed from Windows 11 24H2 and Windows Server 2025, and the complete retirement of all NTLM versions is planned for the end of 2027.

2.1 Why Must NTLM Be Retired?

2.1.1 Main Security Issues with NTLM

2.1.1.1 Cryptographic weaknesses:

1. Uses outdated hashing algorithms (MD4/MD5)
2. Vulnerable to pass-the-hash attacks
3. No mutual authentication (only client authenticates to the server)

2.1.1.2 Vulnerabilities exploited by attackers:

1. NTLM relay attacks
2. Brute-force attacks on password hashes
3. Hash extraction from LSASS memory
4. Hash replication in attacks

2.1.1.3 Functional limitations:

1. Poor performance (requires more network round-trips)
2. No support for Single Sign-On (SSO)
3. No support for authentication delegation

2.2 NTLM Phase-out Timeline

1. June 2024: Official deprecation of all NTLM versions
2. December 2024: Removal of NTLMv1 from Windows 11 24H2 and Server 2025
3. Early 2025: Start of gradual phase-out process
4. Mid-2026: NTLM unavailable in new Microsoft system installations
5. End of 2027: Complete phase-out, including legacy support removal

2.3 Phase 1: Conducting an NTLM Audit

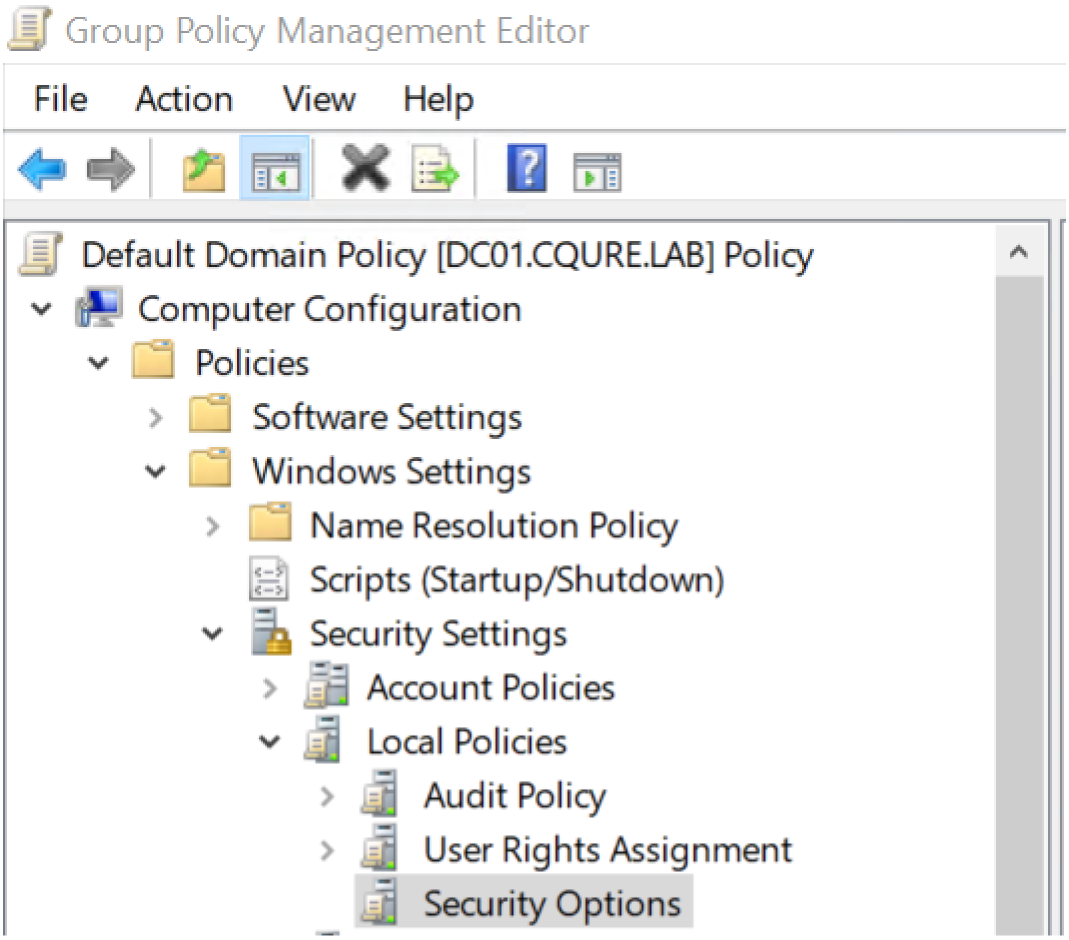
2.3.1 Enabling NTLM Audit in Domain

2.3.1.1 GPO Configuration for Default Domain Policy:

1. Open Group Policy Management Console

2. Edit *Default Domain Policy*

3. Navigate to:
   `Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options`

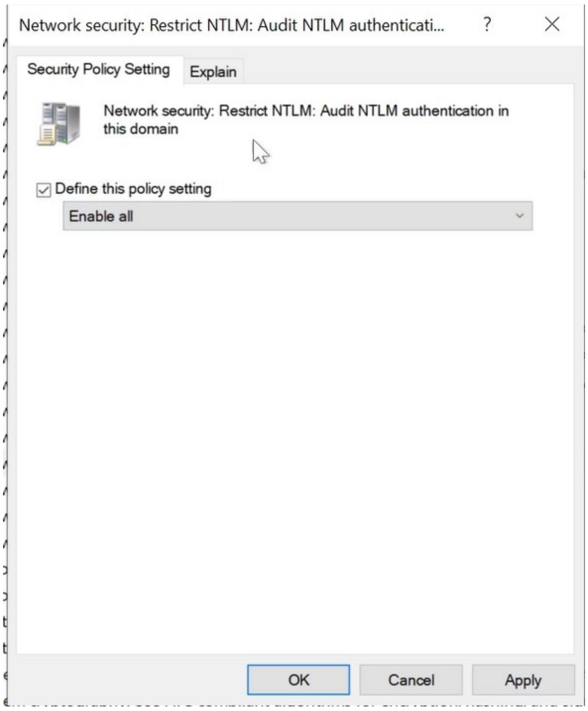


Group Policy Management Editor

Default Domain Policy [DC01.CQURE.LAB] Policy
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options

4. Configure:

   Network security: Restrict NTLM: Audit NTLM authentication in this domain = Enable all



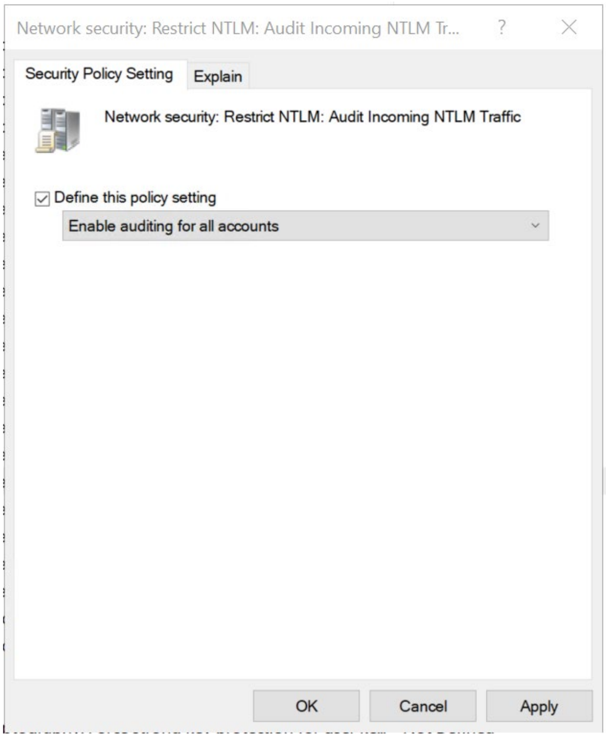
Network security: Restrict NTLM: Audit NTLM authenticati...

Network security: Restrict NTLM: Audit NTLM authentication in this domain

☑ Define this policy setting

Enable all

Network security: Restrict NTLM: Audit Incoming NTLM Traffic = Enable auditing for all accounts.



Network security: Restrict NTLM: Audit Incoming NTLM Tr...

Network security: Restrict NTLM: Audit Incoming NTLM Traffic

☑ Define this policy setting

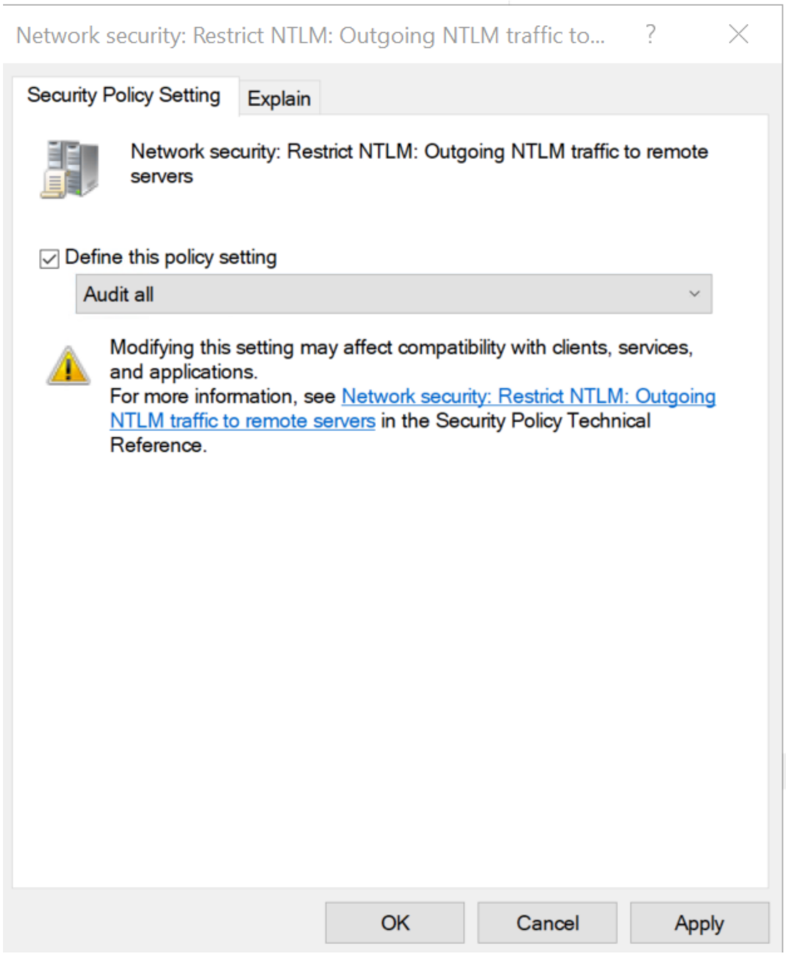
Enable auditing for all accounts

2.3.1.2 GPO Configuration for Default Domain Policy:

1. Edit *Default Domain Policy*

2. Configure:

   Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers = Audit all



Network security: Restrict NTLM: Outgoing NTLM traffic to...
?
Security Policy Setting
Explain
OK
Cancel
Apply

Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers

☑ Define this policy setting

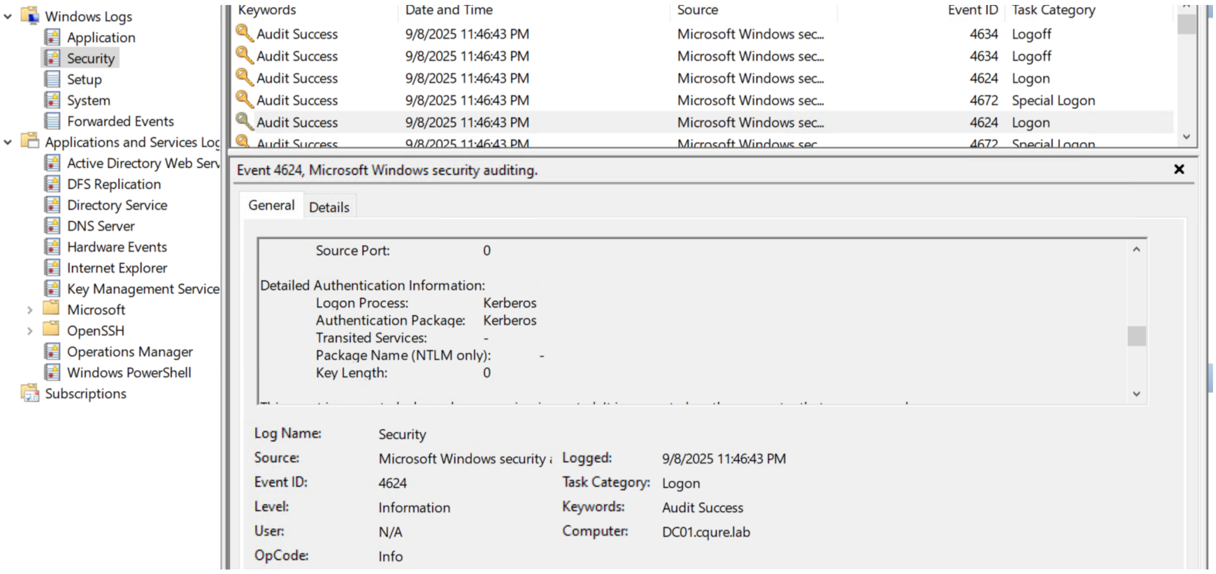
Audit all

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers in the Security Policy Technical Reference.

2.3.2 Event Viewer Log Analysis

2.3.2.1 Key Event IDs to monitor

Event ID 4624: Logon with authentication package details



Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	9/8/2025 11:46:43 PM	Microsoft Windows sec...	4634	Logoff
Audit Success	9/8/2025 11:46:43 PM	Microsoft Windows sec...	4634	Logoff
Audit Success	9/8/2025 11:46:43 PM	Microsoft Windows sec...	4624	Logon
Audit Success	9/8/2025 11:46:43 PM	Microsoft Windows sec...	4672	Special Logon
Audit Success	9/8/2025 11:46:43 PM	Microsoft Windows sec...	4624	Logon
Audit Success	9/8/2025 11:46:43 PM	Microsoft Windows sec	4672	Special Logon

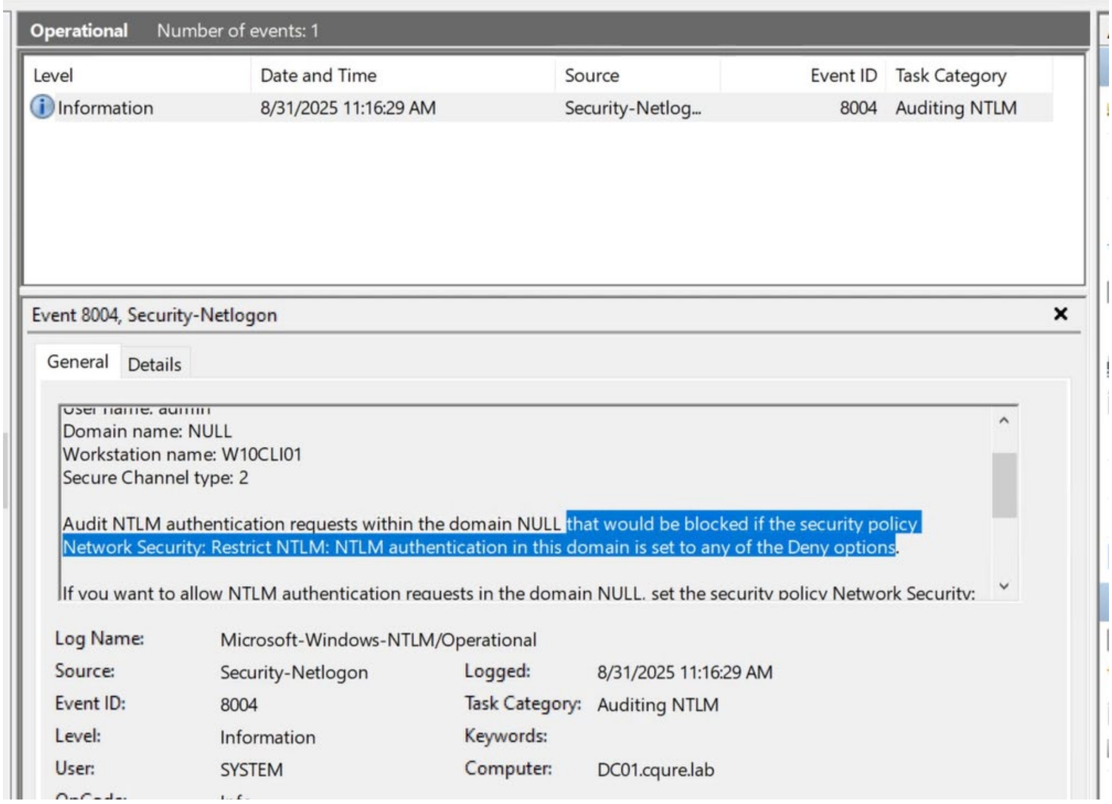
Event 4624, Microsoft Windows security auditing.

```
        Source Port:            0

Detailed Authentication Information:
        Logon Process:          Kerberos
        Authentication Package: Kerberos
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0
```

Log Name:	Security		
Source:	Microsoft Windows security a	Logged:	9/8/2025 11:46:43 PM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DC01.cqure.lab
OpCode:	Info		

Event ID 8004: NTLM usage details (requires prior configuration) (Applications and ServicesLogs -> Microsoft -> Windows -> NTLM -> Operational)



Level	Date and Time	Source	Event ID	Task Category
Information	8/31/2025 11:16:29 AM	Security-Netlog...	8004	Auditing NTLM

Event 8004, Security-Netlogon

```
User name: admin
Domain name: NULL
Workstation name: W10CLI01
Secure Channel type: 2

Audit NTLM authentication requests within the domain NULL that would be blocked if the security policy
Network Security: Restrict NTLM: NTLM authentication in this domain is set to any of the Deny options.

If you want to allow NTLM authentication requests in the domain NULL, set the security policy Network Security:
```

Log Name:	Microsoft-Windows-NTLM/Operational		
Source:	Security-Netlogon	Logged:	8/31/2025 11:16:29 AM
Event ID:	8004	Task Category:	Auditing NTLM
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	DC01.cqure.lab
OpCode:	Info		

2.3.3 Identifying Applications Using NTLM

2.3.3.1 Identification methods

1. Log analysis:
   a. Check processes active during Event ID 4624
   b. Correlate application logs with authentication logs
2. Network monitoring:
   a. Use Wireshark to filter NTLMSSP traffic
   b. Use tcpdump with NTLM filters
3. Microsoft tools:
   a. Microsoft Defender for Identity
   b. Azure AD Connect Health

2.4 Phase 2: Preparing Migration to Kerberos

2.4.1 Infrastructure Readiness Check

2.4.1.1 Kerberos requirements:

1. Time synchronization across all systems (NTP)
2. Correct DNS configuration
3. Proper Service Principal Names (SPNs) for services

2.4.1.2 Infrastructure checklist:

1. All domain controllers synchronized within ±5 minutes
2. DNS forward and reverse lookup working correctly
3. All servers joined to AD domain
4. Firewall allows Kerberos traffic (port 88)
5. NTP servers properly configured

2.4.2 Configuring Service Principal Names (SPN)

Check existing SPNs:

```
setspn -L server_name
```

Register SPNs for applications:

```
setspn -S HTTP/webapp.domain.com service_account

setspn -S HOST/server.domain.com computer_account
```

2.4.3 Moving to Protocol Negotiate

2.4.3.1 Why negotiate?

The Negotiate protocol tries Kerberos authentication first, and if unavailable, falls back to NTLM.

Implementation in application code:

```
// Instead of

credentialsHandle = AcquireCredentialsHandle("NTLM");


// Use

credentialsHandle = AcquireCredentialsHandle("Negotiate");
```

2.5 Phase 3: Testing and Deployment

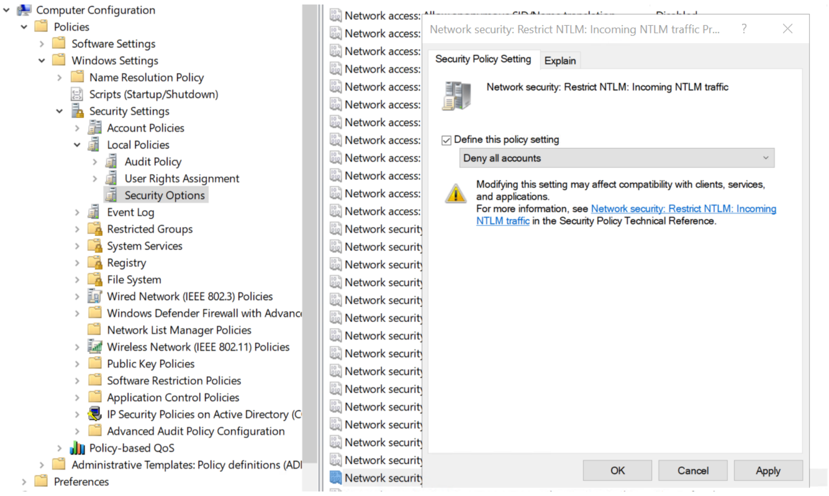
2.5.1 Test Environment

2.5.1.1 Test group setup:

1. Create a security group NTLM_Test_Disable
2. Add selected test computers
3. Create dedicated test GPO

2.5.1.2 Test GPO (disable NTLM):

Network security: Restrict NTLM: Incoming NTLM traffic = Deny all accounts


Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
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 Advanc
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 (C
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADI
Preferences
Network access:
Network securit
Network security: Restrict NTLM: Incoming NTLM traffic Pr...
Security Policy Setting
Explain
OK
Cancel
Apply

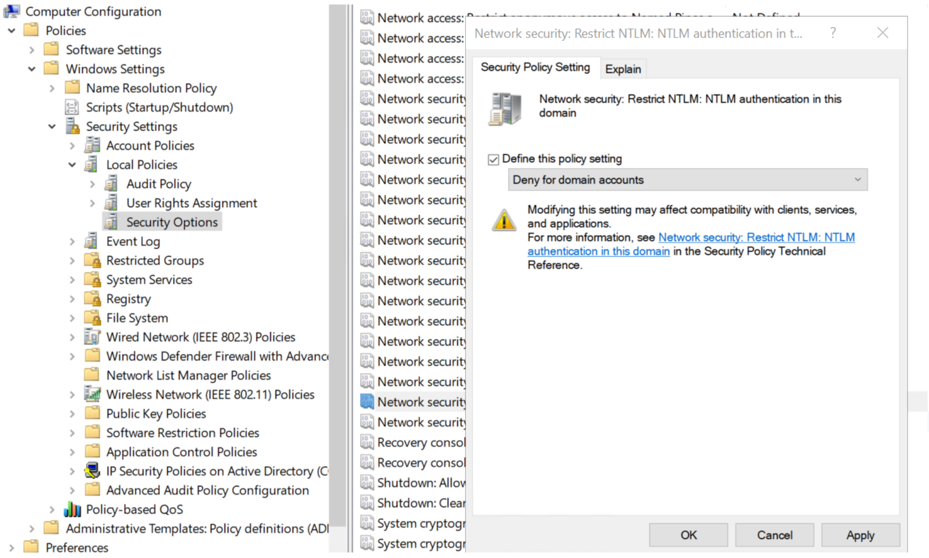
Network security: Restrict NTLM: Incoming NTLM traffic

☑ Define this policy setting

Deny all accounts

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network security: Restrict NTLM: Incoming NTLM traffic in the Security Policy Technical Reference.

Network security: Restrict NTLM: NTLM authentication in this domain = Deny for domain accounts



Network security: Restrict NTLM: NTLM authentication in this domain

☑ Define this policy setting

Deny for domain accounts

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network security: Restrict NTLM: NTLM authentication in this domain in the Security Policy Technical Reference.

2.5.2 Test Procedure

2.5.2.1 Step 1: Basic functionality

1. User login
2. Access to network resources
3. Business applications

2.5.2.2 Step 2: Critical applications

1. ERP/CRM systems
2. Database servers
3. File and print servers

2.5.2.3 Step 3: Monitoring and analysis

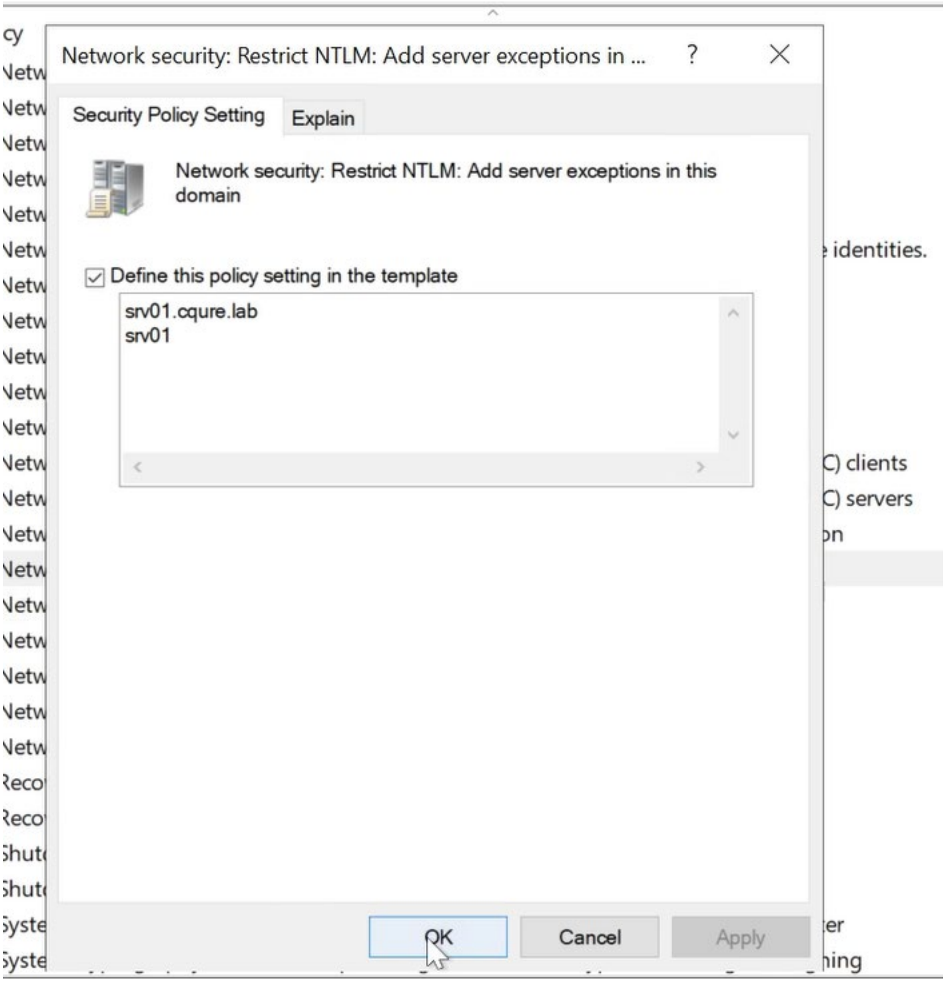
1. Track Event ID 4771 (Kerberos pre-authentication failed)
2. Monitor application performance
3. Collect user feedback

2.5.3 NTLM Exceptions List

For applications unable to use Kerberos:

1. Configure GPO Policy (NTLM_Disable_Policy) : *Network security: Restrict NTLM: Add server exceptions in this domain*
2. On domain controller navigate to:
   `Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > Network security: Restrict NTLM: Add server exceptions in this domain`

3. Add FQDN and NetBIOS of the server



Network security: Restrict NTLM: Add server exceptions in ...

Network security: Restrict NTLM: Add server exceptions in this domain

☑ Define this policy setting in the template

srv01.cqure.lab
srv01

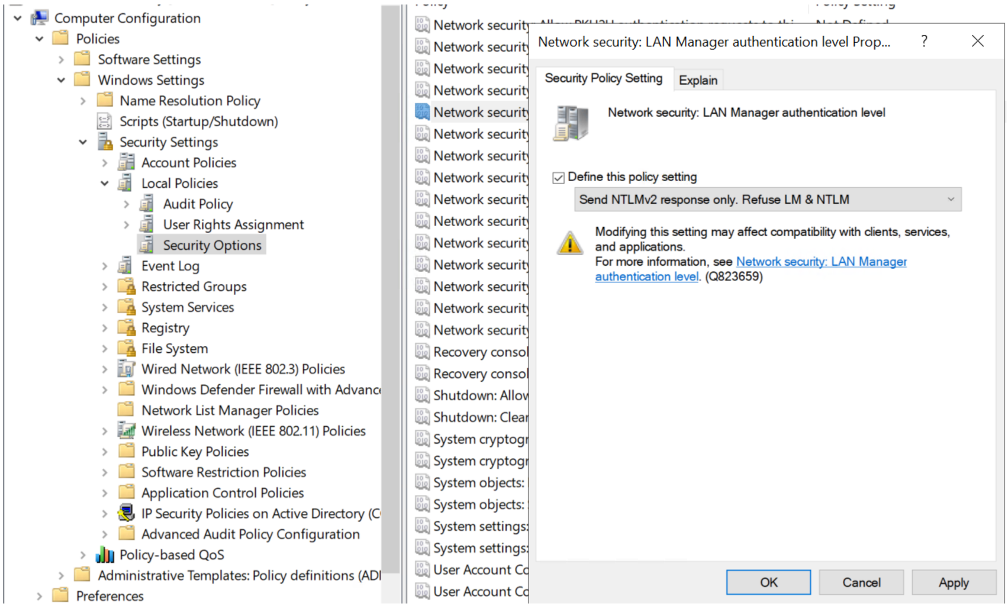
4. Run command prompt as domain admin and run command *gpupdate /force*

2.6 Phase 4: Production Deployment

2.6.1 Gradual Rollout Plan

2.6.1.1 Step 1: Disable NTLMv1

Network security: LAN Manager authentication level = Send NTLMv2 response only. Refuse LM & NTLM



Network security: LAN Manager authentication level Prop... ? ×

Network security: LAN Manager authentication level

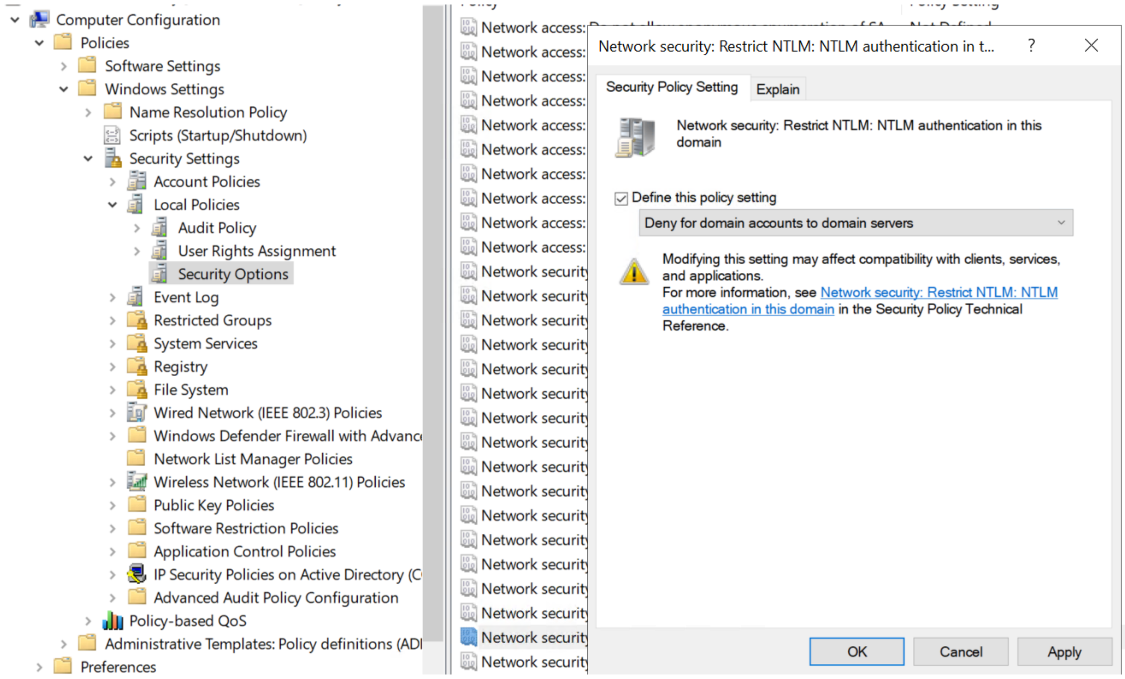
☑ Define this policy setting

Send NTLMv2 response only. Refuse LM & NTLM

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network security: LAN Manager authentication level. (Q823659)

2.6.1.2 Step 2: Restrict NTLM for domain accounts

Network security: Restrict NTLM: NTLM authentication in this domain = Deny for domain accounts to domain servers



Network security: Restrict NTLM: NTLM authentication in t... ? ×

Network security: Restrict NTLM: NTLM authentication in this domain

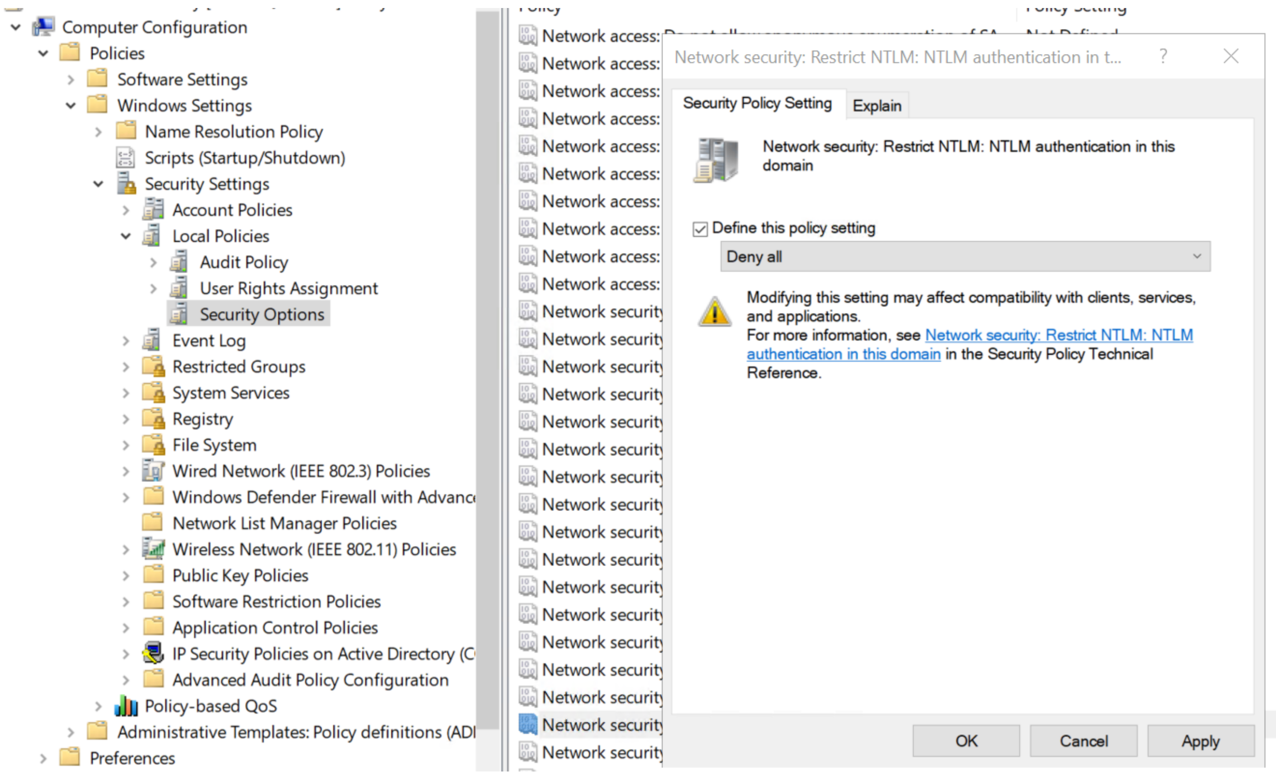
☑ Define this policy setting

Deny for domain accounts to domain servers

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network security: Restrict NTLM: NTLM authentication in this domain in the Security Policy Technical Reference.

2.6.1.3 Step 3: Full NTLM disablement

Network security: Restrict NTLM: NTLM authentication in this domain = Deny all



Network security: Restrict NTLM: NTLM authentication in this domain

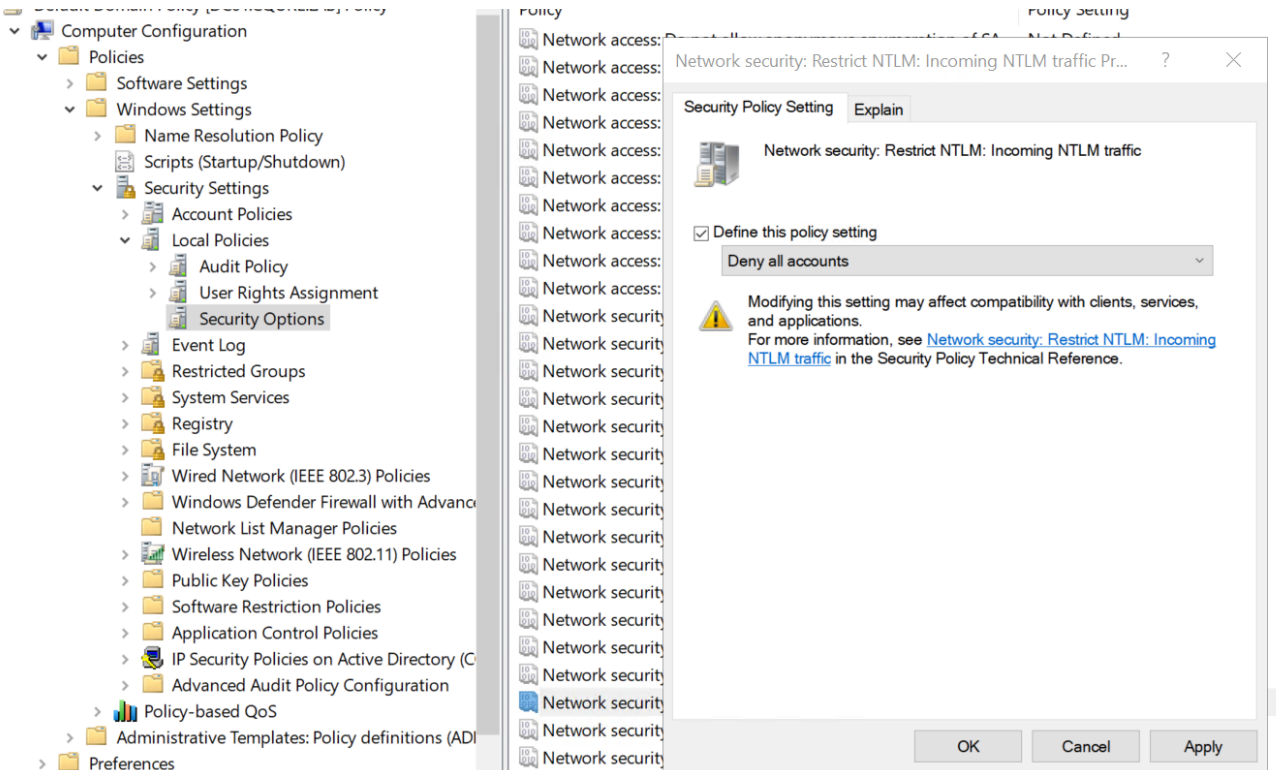
☑ Define this policy setting

Deny all

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network security: Restrict NTLM: NTLM authentication in this domain in the Security Policy Technical Reference.

Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
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 Advanc
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 (C
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADI
Preferences
Network access:
Network securit
Network security: Restrict NTLM: NTLM authentication in t...
Security Policy Setting
Explain
OK
Cancel
Apply

Network security: Restrict NTLM: Incoming NTLM traffic = Deny all accounts



Network security: Restrict NTLM: Incoming NTLM traffic

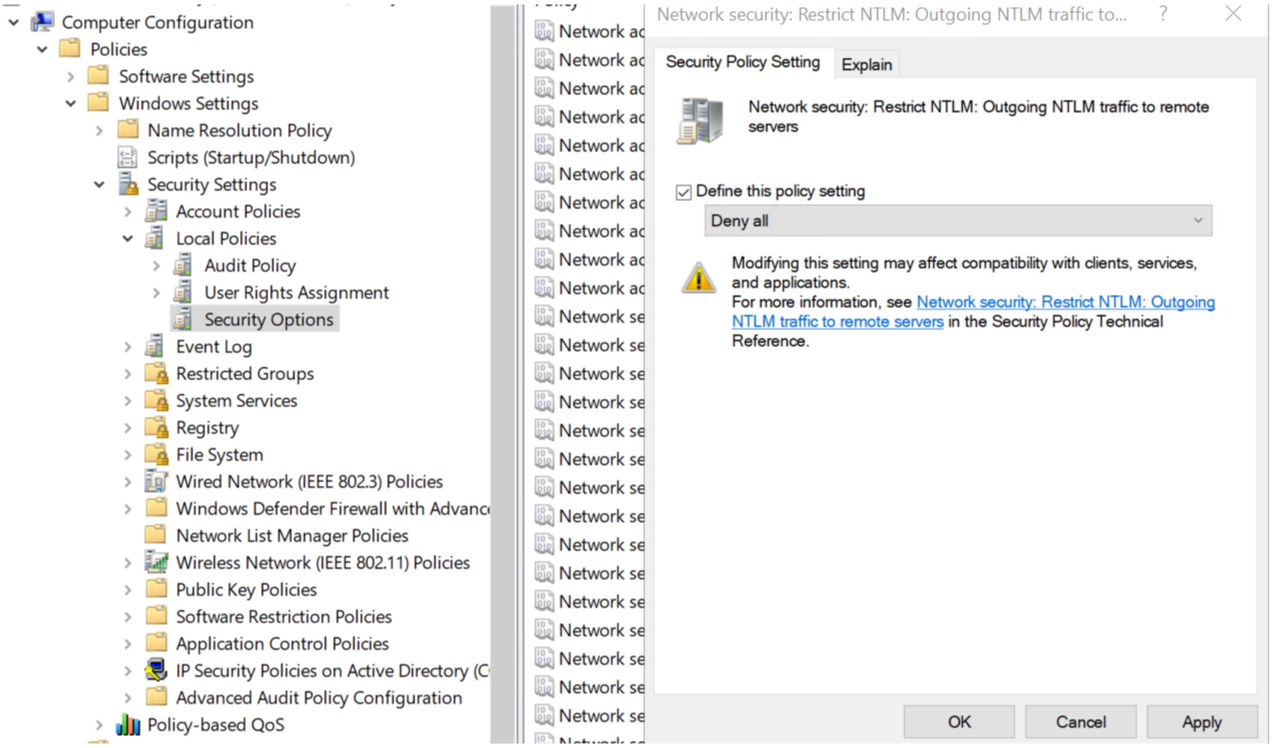
☑ Define this policy setting

Deny all accounts

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network security: Restrict NTLM: Incoming NTLM traffic in the Security Policy Technical Reference.

Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
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 Advanc
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 (C
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADI
Preferences
Network access:
Network securit
Network security: Restrict NTLM: Incoming NTLM traffic Pr...
Security Policy Setting
Explain
OK
Cancel
Apply

Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers = Deny all



Network security: Restrict NTLM: Outgoing NTLM traffic to...

Security Policy Setting | Explain

Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers

☑ Define this policy setting

Deny all

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers in the Security Policy Technical Reference.

2.6.2 Stakeholder Communication

2.6.2.1 Pre-deployment message template:

Subject: [ACTION REQUIRED] Authentication Protocol Migration – NTLM Phase-out

Dear All,

As part of enhancing our IT security, Microsoft is officially retiring the outdated NTLM protocol. On [DATE], we will begin migrating to the more secure Kerberos protocol.

Impact on users:

1. Logging into systems will remain unchanged
2. Some applications may require re-login
3. For issues, please contact IT Support

Timeline:

1. [DATE] – NTLMv1 deactivation (test phase)
2. [DATE] – Full deployment for pilot groups
3. [DATE] – Organization-wide rollout

IT Team

2.7 Phase 5: Monitoring and Optimization

2.7.1 Post-deployment Monitoring

2.7.1.1 KPIs to track

1. Number of failed Kerberos authentications

Description: Monitoring failed Kerberos logons helps identify configuration issues (e.g., incorrect SPNs, time synchronization problems) as well as potential attack attempts (e.g., brute-force password guessing).

Data sources:

1. Event Viewer on Domain Controllers
   a. Event ID 4771 (Kerberos pre-authentication failed)
   b. Event ID 4769 (Kerberos service ticket request – errors)
2. SIEM platforms (e.g., Microsoft Sentinel, Splunk, QRadar) – correlation rules for repeated authentication failures

PowerShell example:

```
Get-WinEvent -FilterHashtable @{
    LogName='Security';
    ID=4771;
    StartTime=(Get-Date).AddDays(-1)
} | Group-Object -Property @{Expression={$_.Properties[0].Value}} |
Select-Object Name, Count
```

Reports the number of users with failed Kerberos logons in the last 24 hours.

2. Helpdesk tickets related to authentication

Description: Tracking authentication-related helpdesk incidents provides visibility into the real user impact of NTLM deprecation. This KPI reflects the business perspective.

Data sources:

1. Ticketing systems (e.g., ServiceNow, Jira, OTRS, Freshdesk)
2. Categorization of tickets under Authentication / Logon Issues

Best practices:

1. Introduce dedicated categories for authentication issues
2. Automate ticket tagging for keywords such as *"login failed"*, *"account locked"*, *"Kerberos"*
3. Produce monthly reports: number of tickets, average resolution time, and trend analysis compared to the pre-NTLM phase-out period
4. Correlate ticket data with Event Viewer logs and SIEM reports

2.8 Summary

The retirement of NTLM is an unavoidable necessity in the face of growing cybersecurity threats. With a systematic approach, thorough planning, and phased implementation, organizations can safely transition to the Kerberos protocol, significantly improving security without disrupting business operations.

2.9 Keys to success:

1. Comprehensive audit of current NTLM usage
2. Phased rollout with proper testing
3. Continuous monitoring and quick incident response readiness
4. Effective communication with all stakeholders

Remember: this is not just a technical matter it is a strategic investment in the organization’s security for the years to come.

CQURE

Warsaw New York Dubai Zug

info@cqure.pl

www.cqure.pl www.cqureacademy.com