Disable SMBv1 and enable SMBv1 auditing

https://4sysops.com/archives/disable-smbv1-and-enable-smbv1-auditing/

Windows still includes some legacy protocols that pose significant security risks. This applies to SMBv1/CIFS, which Microsoft is gradually phasing out. While it is still present in new Windows versions, it is disabled by default. The audit feature can detect SMBv1 requests and assess whether the protocol is still required.

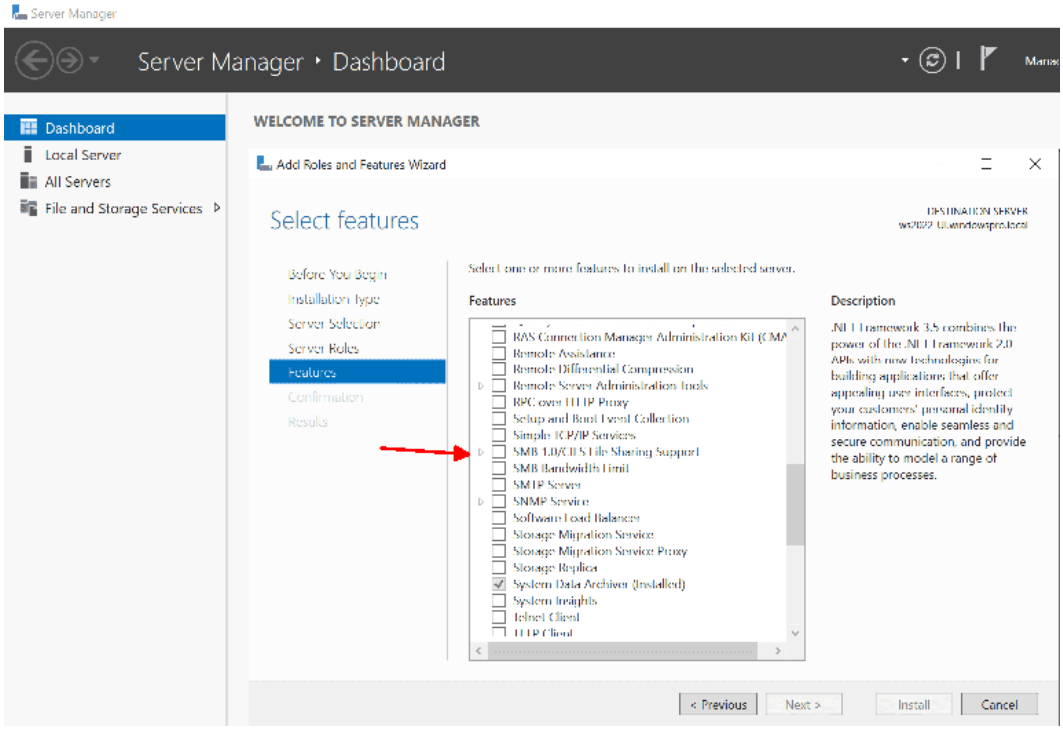
Similar to NTLM, older versions of SMB cannot easily be disabled. Especially in larger and heterogeneous environments, devices or applications often still rely on these outdated protocols.

If a server rejects an SMB request because it no longer supports the requested protocol version, it not only hinders access to a file share or printer. This also impacts domain controllers that use SMB to share SYSVOL with clients so they can retrieve Group Policy Objects (GPOs).

Hence, when auditing SMBv1 usage, it is essential to include not only file and print servers but also domain controllers.

Potential candidates for SMBv1 usage

In Windows 10/11 and Windows Server from 2019 onward, SMBv1 is disabled by default, but in Server 2016, it is still enabled.



In more recent versions of Windows Server, SMBv1 is disabled by default.

However, companies might have enabled SMBv1 on newer server versions to be compatible with older devices. But this may no longer be necessary, so keeping an eye on SMB traffic is essential.

Windows machines are unlikely candidates for SMBv1 usage, mainly since Vista already supported SMB2, and older OS versions are becoming increasingly rare. Dependencies on SMBv1 are more likely to be found in old print servers, firewalls, aging storage systems, or backup programs.

Enable SMBv1 auditing

SMBv1 is an optional feature for Windows 11/10 and a feature on Windows Server. You can easily determine if it is installed using PowerShell:

```
Get-WindowsOptionalFeature -Online -FeatureName smb1protocol
```

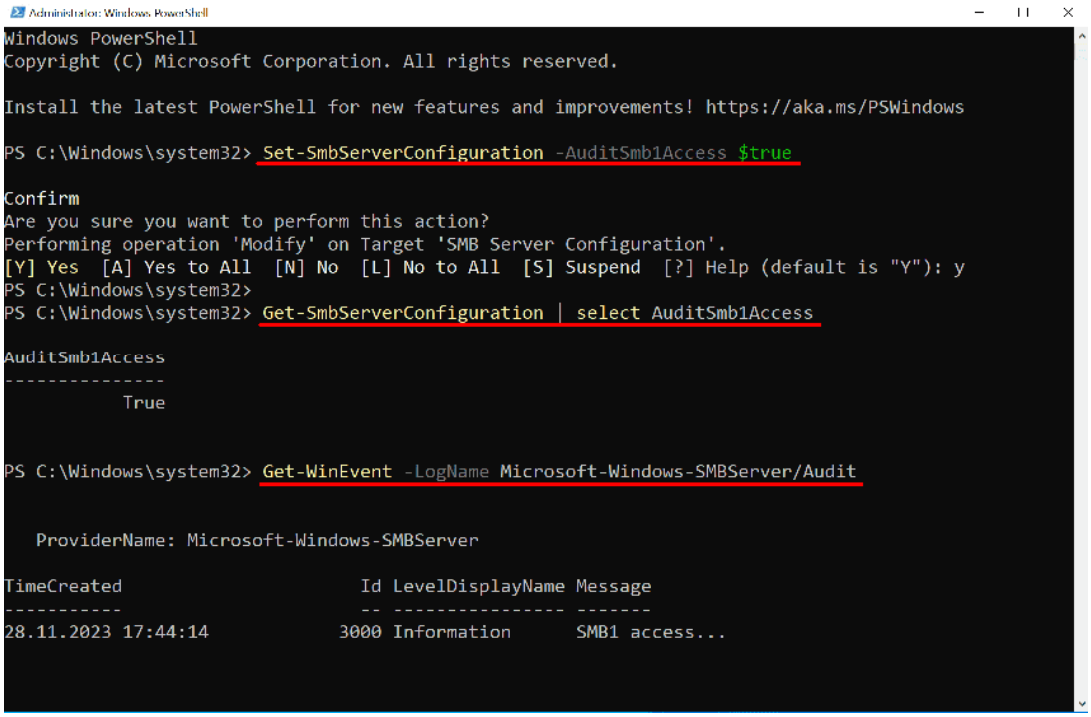
This command works on both workstations and servers. However, since SMBv1 requests can come from various devices, it's not sufficient to check only Windows PCs using this method.

Instead, you can enable SMBv1 auditing on each relevant server using the following command:

```
Set-SmbServerConfiguration -AuditSmb1Access $true
```

Afterwards, you can verify whether SMBv1 monitoring is active using:

```
Get-SmbServerConfiguration | select AuditSmb1Access
```

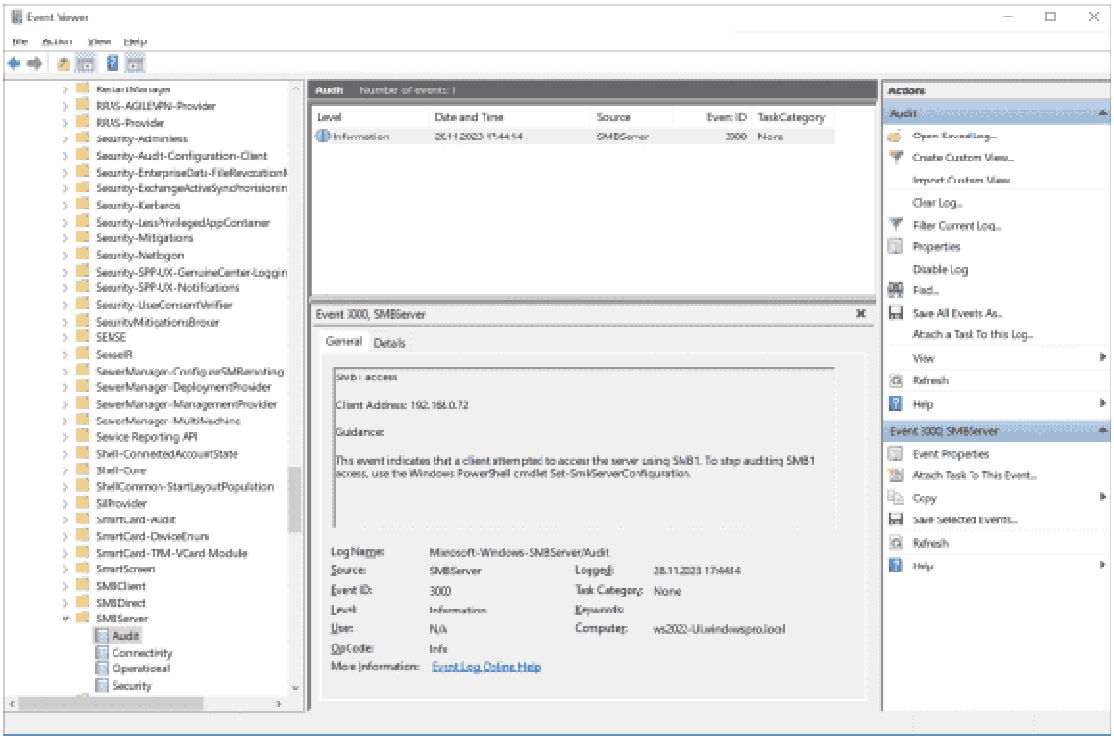


Enabling the audit function for SMBv1 with PowerShell and reading events from the log file.

Whenever a client attempts to establish a connection using SMBv1, the server writes an event with ID 3000 to the log, regardless of whether the request was accepted or rejected. These events can be retrieved using PowerShell:

```
Get-WinEvent -LogName Microsoft-Windows-SMBServer/Audit
```

Alternatively, you can also find these entries in the Event Viewer.



Event for an SMBv1 request in the event viewer

For testing purposes, you can use the SMB client on Linux to force a log entry:

```
smbclient '\\server\share' -m nt1
```

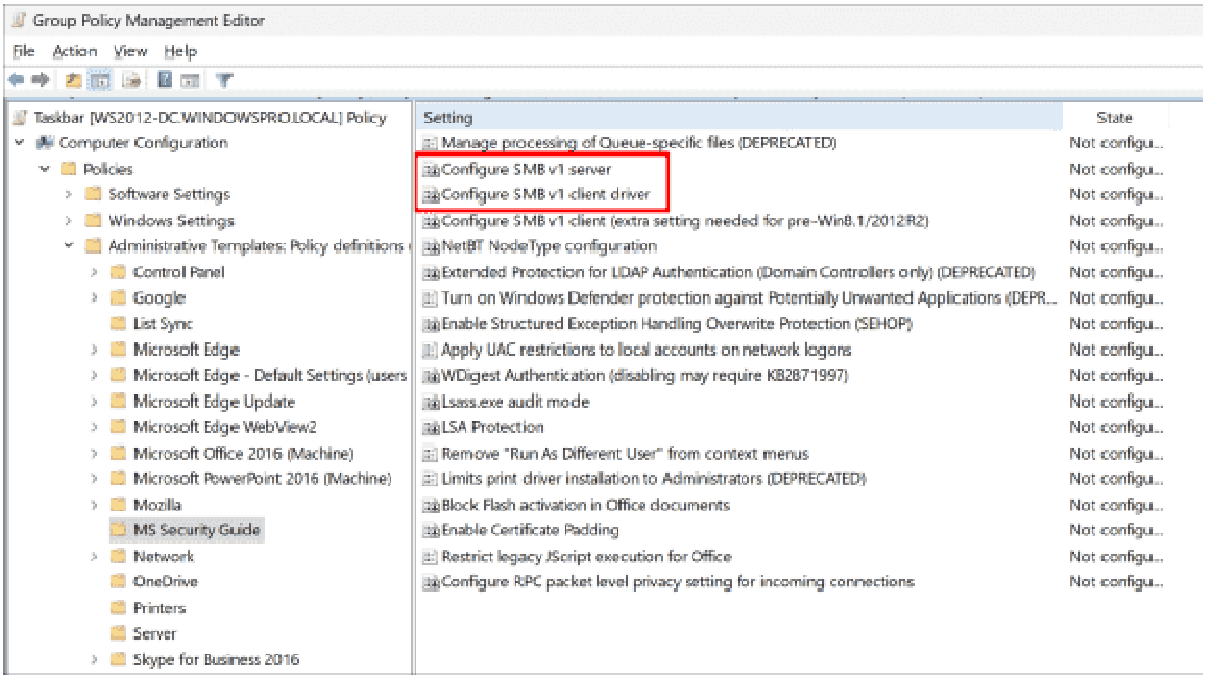
Disable SMBv1

If SMBv1 was explicitly enabled on newer versions of Windows, you can disable it through various methods. Once again, PowerShell provides a convenient approach:

Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol

Alternatively, you can use Desired State Configuration (PowerShell DSC) or Ansible, among others.

If you prefer Group Policy, the templates included in Windows do not have a setting for SMBv1. However, you can add such a setting using the *SecGuide.admx* from the Security Baseline.



The Security Baseline provides group policies for deactivating SMBv1

This allows SMBv1 to be disabled separately for clients and servers.

Summary

The outdated SMBv1 protocol poses significant security and performance deficiencies, making its retirement advisable in all environments. By default, it is already disabled on newer versions of Windows.

However, getting rid of SMBv1 is often more complex as older devices or applications may still need it. To identify these dependencies, it's recommended to enable auditing for SMBv1.