



## LDAP Signing auf Domänencontrollern erzwingen

Zum Schutz der Anmeldedaten sollte das LDAP Signing (Erzwingen einer LDAP Signatur) erzwungen werden. Damit stellen wir sicher, dass Systeme und Applikationen keine Klartext-Kennwörter mehr übermitteln. Weiterhin wird mit dieser Einstellung verhindert, das künftige unsichere LDAP Bind Implementierungen nicht mehr durchgeführt werden können.

Nach dieser Konfiguration sind Simple Bind Anforderungen über LDAP nicht mehr möglich!

Über das (Secure) LDAP/s Protokoll funktionieren Simple Binds weiterhin.

Was bringt eine komplexe Passwortrichtlinie, wenn die Daten unsicher übertragen werden können?! Im schlimmsten Fall sind es Daten von privilegierten Konten.

### Das Problem:

Gefiltert in Verzeichnisdienst (Directory Services) > Aufgabenkategorie LDAP-Schnittstelle > Events 2886, 2887, 2888, 2889

Ereigniseigenschaften - Ereignis 2887, ActiveDirectory\_DomainService

Allgemein Details

Während der vergangenen 24 Stunden haben einige Clients versucht, eine der folgenden LDAP-Bindungen vorzunehmen:  
(1) Eine SASL-LDAP-Bindung (Verhandlung, Kerberos, NTLM oder Digest), die keine Signatur (Integritätsüberprüfung) anforderte, oder  
(2) eine einfache LDAP-Bindung über eine Klartextverbindung (ohne SSL-/TLS-Verschlüsselung).

Der Verzeichnisserver ist derzeit nicht zum Zurückweisen derartiger Bindungen konfiguriert. Sie können die Sicherheit dieses Verzeichnisseservers deutlich verbessern, indem Sie den Server zum Zurückweisen derartiger Bindungen konfigurieren. Weitere Details und Informationen zum Vornehmen dieser Konfigurationsänderung auf dem Server finden Sie unter "<http://go.microsoft.com/fwlink/?LinkId=87923>".

Eine Zusammenfassung der Anzahl derartiger Bindungen, die in den vergangenen 24 Stunden eingegangen sind, finden Sie unten.

Sie können die Protokollierung erweitern und bei jeder derartigen Bindung durch einen Client ein Ereignis protokollieren. Hierzu gehören Informationen dazu, welcher Client die Bindung vornahm. Erhöhen Sie hierzu die Einstellung für die Ereignisprotokollierungskategorie "LDAP-Schnittstelleneignisse" auf Stufe 2 oder höher.

Anzahl der einfachen Bindungen, die ohne SSL/TLS erfolgten: 12  
Anzahl der Verhandlungs-/Kerberos-/NTLM-/Digestbindungen, die ohne Signatur erfolgten: 432

Protokollname: Verzeichnisdienst  
Quelle: ActiveDirectory\_DomainServ Protokolliert: 24.11.2018 16:04:56  
Ereignis-ID: 2887 Aufgabenkategorie: LDAP-Schnittstelle  
Ebene: Warnung Schlüsselwörter: Klassisch  
Benutzer: ANONYMOUS-ANMELDUNG Computer:  
OpCode: Info  
Weitere Informationen: [Onlinehilfe](#)

Kopieren Schließen



## LDAP Signing auf Domänencontrollern erzwingen

**Ereignisanzeige**  
Datei Aktion Ansicht ?

**Ereignisanzeige (Lokal)**  
Benutzerdefinierte Ansichten  
Serverrollen  
Administrative Ereignisse  
Windows-Protokolle  
Anwendungs- und Dienstprotokolle  
Abonnements

**LDAP ohne Signierung** Anzahl von Ereignissen: 92

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Warnung	07.10.2018 18:29:24	ActiveDirectory_DomainService	2886	LDAP-Schnittstelle
Warnung	07.10.2018 18:24:43	ActiveDirectory_DomainService	2886	LDAP-Schnittstelle
Warnung	03.10.2018 19:55:15	ActiveDirectory_DomainService	2886	LDAP-Schnittstelle
Warnung	28.09.2018 22:21:01	ActiveDirectory_DomainService	2886	LDAP-Schnittstelle
Warnung	21.09.2018 10:27:58	ActiveDirectory_DomainService	2886	LDAP-Schnittstelle
Warnung	19.09.2018 17:52:04	ActiveDirectory_DomainService	2886	LDAP-Schnittstelle
Warnung	17.09.2018 18:56:55	ActiveDirectory_DomainService	2886	LDAP-Schnittstelle
Warnung	16.09.2018 11:02:38	ActiveDirectory_DomainService	2886	LDAP-Schnittstelle
Warnung	14.09.2018 17:09:37	ActiveDirectory_DomainService	2886	LDAP-Schnittstelle
Warnung	14.09.2018 12:24:27	ActiveDirectory_DomainService	2886	LDAP-Schnittstelle

**Ereignis 2886, ActiveDirectory\_DomainService**

Allgemein Details

Sie können die Sicherheit dieses Verzeichnisseservers deutlich verbessern, indem Sie den Server so konfigurieren, dass SASL-Bindungen (Verhandlung, Kerberos, NTLM oder Digest), LDAP-Bindungen ohne Anforderung einer Signatur (Integritätsüberprüfung) und einfache LDAP-Bindungen über eine Klartextverbindung (ohne SSL-/TLS-Verschlüsselung) zurückgewiesen werden. Selbst wenn keine Clients derartige Bindungen nutzen, erhöht sich die Sicherheit des Servers durch diese Konfiguration beträchtlich.

Einige Clients benötigen möglicherweise unsignierte SASL-Bindungen oder einfache LDAP-Bindungen über eine Verbindung ohne SSL-/TLS-Verschlüsselung. Diese funktionieren nach der Konfigurationsänderung nicht mehr. Zur besseren Identifizierung dieser Clients protokolliert dieser Verzeichnisseserver alle 24 Stunden ein Zusammenfassungsereignis mit Informationen über die Anzahl derartigen Bindungen. Es wird empfohlen, die betroffene Clients für einen anderen Bindungstyp zu konfigurieren. Beobachten Sie zunächst über einen längeren Zeitraum diese Ereignisse, und konfigurieren Sie dann den Server so, dass derartige Bindungen zurückgewiesen werden.

Weitere Einzelheiten und Informationen dazu, wie Sie diese Konfigurationsänderung auf dem Server vornehmen, finden Sie unter "<http://go.microsoft.com/fwlink/?LinkID=87923>".

Sie können die Protokollierung erweitern und bei jeder derartigen Bindung durch einen Client ein Ereignis protokollieren. Hierzu gehören Informationen dazu, welcher Client die Bindung vornahm. Erhöhen Sie hierzu die Einstellung für die Ereignisprotokollierungskategorie "LDAP-Schnittstelleneignisse" auf Stufe 2 oder höher.

Protokollname: Directory Service  
Quelle: ActiveDirectory\_DomainServ Protokolliert: 07.10.2018 18:24:43  
Ereignis-ID: 2886 Aufgabenkategorie: LDAP-Schnittstelle  
Ebene: Warnung Schlüsselwörter: Klassisch  
Benutzer: ANONYMOUS-ANMELDUNG Computer: DC01.ndsdev.de  
Vorgangscode: Info  
Weitere Informationen: [Onlinehilfe](#)

Sie können die Sicherheit dieses Verzeichnisseservers deutlich verbessern, indem Sie den Server so konfigurieren, dass SASL-Bindungen (Verhandlung, Kerberos, NTLM oder Digest), LDAP-Bindungen ohne Anforderung einer Signatur (Integritätsüberprüfung) und einfache LDAP-Bindungen über eine Klartextverbindung (ohne SSL-/TLS-Verschlüsselung) zurückgewiesen werden. Selbst wenn keine Clients derartige Bindungen nutzen, erhöht sich die Sicherheit des Servers durch diese Konfiguration beträchtlich.

Einige Clients benötigen möglicherweise unsignierte SASL-Bindungen oder einfache LDAP-Bindungen über eine Verbindung ohne SSL-/TLS-Verschlüsselung. Diese funktionieren nach der Konfigurationsänderung nicht mehr. Zur besseren Identifizierung dieser Clients protokolliert dieser Verzeichnisseserver alle 24 Stunden ein Zusammenfassungsereignis mit Informationen über die Anzahl derartigen Bindungen. Es wird empfohlen, die betroffene Clients für einen anderen Bindungstyp zu konfigurieren. Beobachten Sie zunächst über einen längeren Zeitraum diese Ereignisse, und konfigurieren Sie dann den Server so, dass derartige Bindungen zurückgewiesen werden.

Weitere Einzelheiten und Informationen dazu, wie Sie diese Konfigurationsänderung auf dem Server vornehmen, finden Sie unter "<http://go.microsoft.com/fwlink/?LinkID=87923>".

Sie können die Protokollierung erweitern und bei jeder derartigen Bindung durch einen Client ein Ereignis protokollieren. Hierzu gehören Informationen dazu, welcher Client die Bindung vornahm. Erhöhen Sie hierzu die Einstellung für die Ereignisprotokollierungskategorie "LDAP-Schnittstelleneignisse" auf Stufe 2 oder höher.

### Auszug aus einem englischen Betriebssystem:

**Event Properties - Event 2886, ActiveDirectory\_DomainService**

General Details

The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a clear text (non-SSL/TLS-encrypted) connection. Even if no clients are using such binds, configuring the server to reject them will improve the security of this server.

Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds.

For more details and information on how to make this configuration change to the server, please see <http://go.microsoft.com/fwlink/?LinkID=87923>.

You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher.

Log Name: Directory Service  
Source: ActiveDirectory\_DomainServ Logged: 5/27/2022 8:38:23 AM  
Event ID: 2886 Task Category: LDAP Interface  
Level: Warning Keywords: Classic  
User: ANONYMOUS LOGON Computer: DC2.windowspapst.de  
OpCode: Info  
More Information: [Event Log Online Help](#)

Copy Close

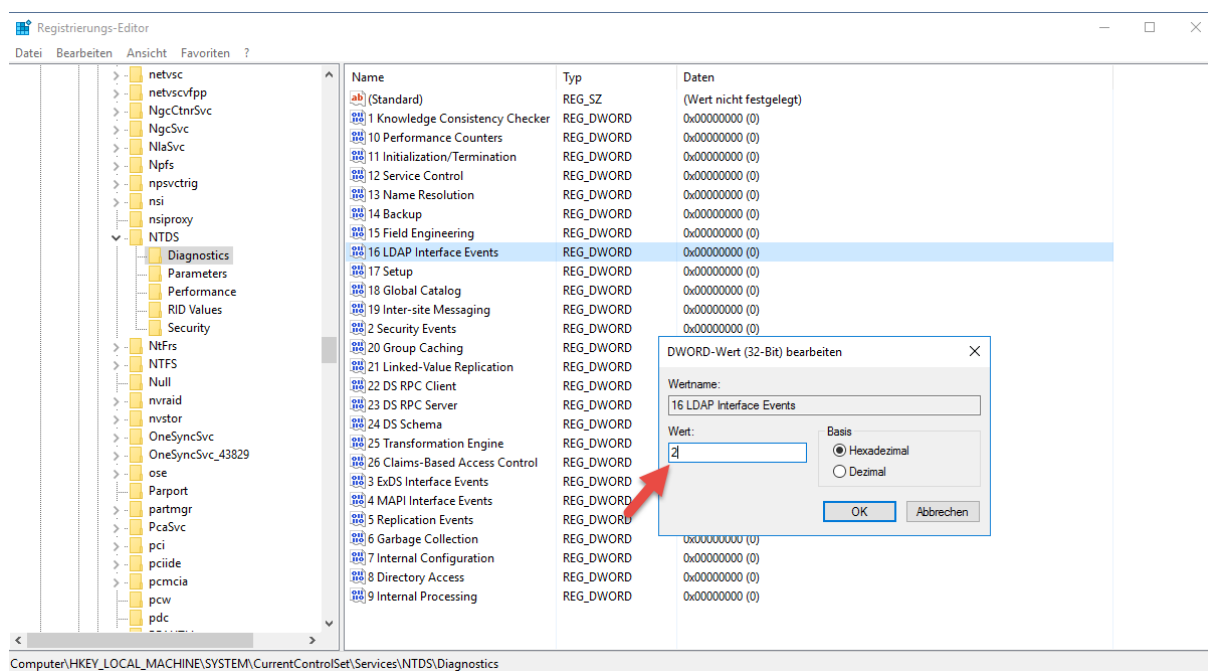


## LDAP Signing auf Domänencontrollern erzwingen

### Vorarbeit:

Systeme identifizieren die noch über Ldap simple bind kommunizieren. Dazu muss auf den Domain Controllern das Logging entsprechend aktiviert und eingestellt werden:

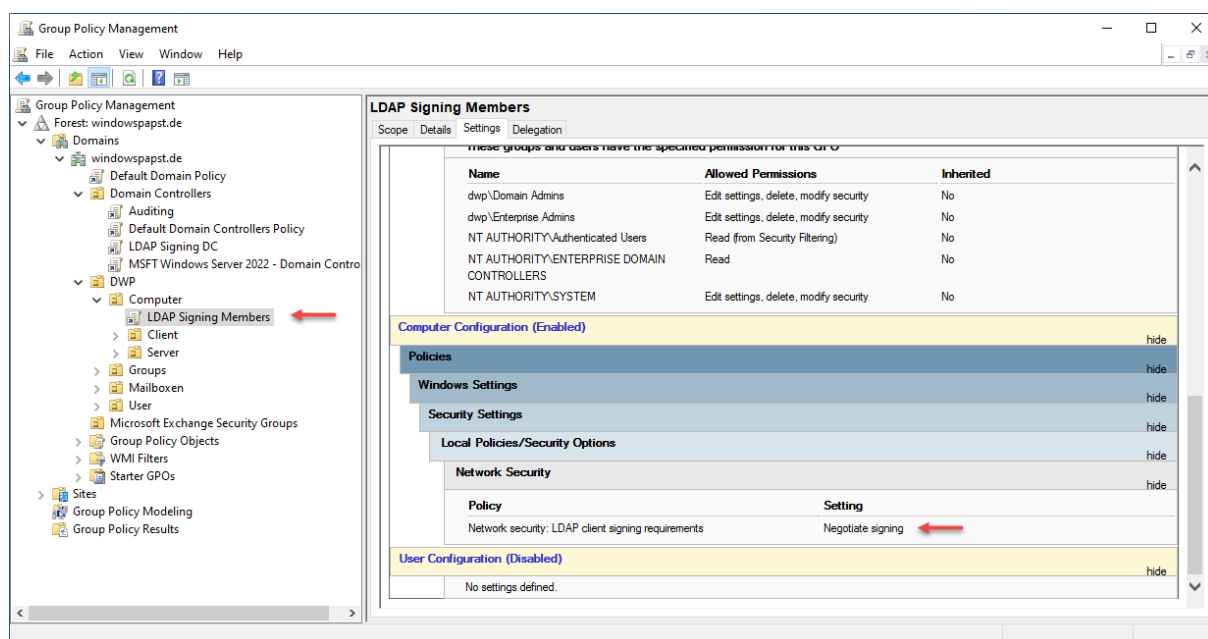
**reg Add HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics /v "16 LDAP Interface Events" /t REG\_DWORD /d 2**



### Vorgehen/Umsetzung:

Im ersten Schritt erstellen wir zwei neue Policy namens „LDAP Signing Members & LDAP Signing DCs“ mit folgenden Einstellungen:

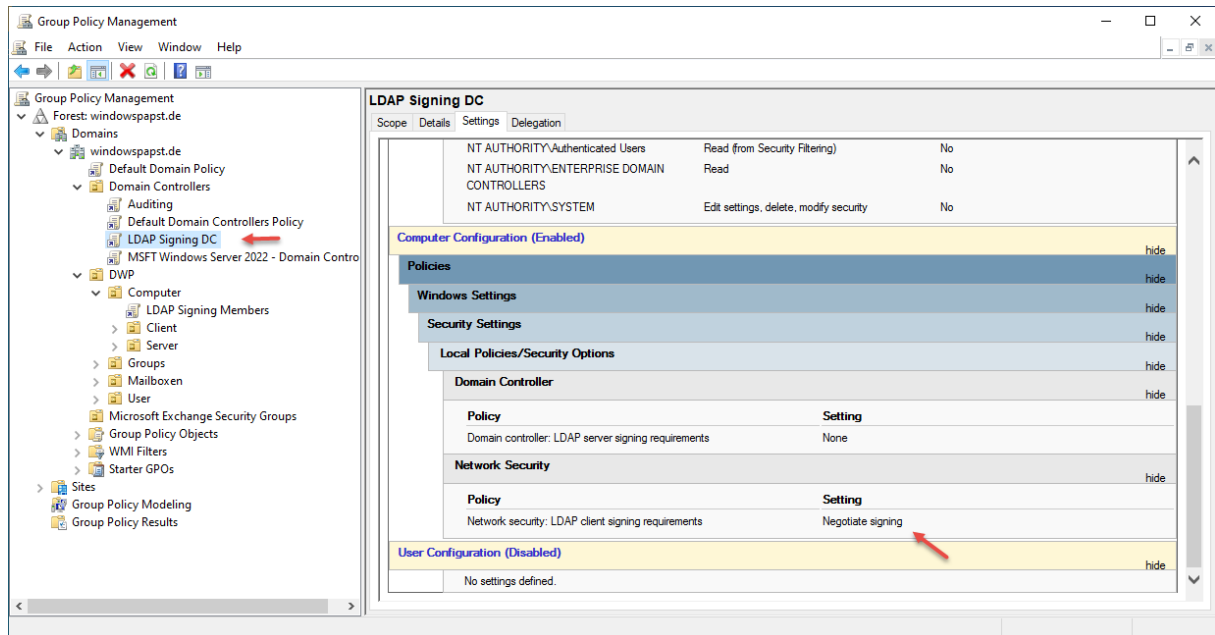
LDAP Signing Members: LDAP Client signing requirements > **Negotiate signing**.



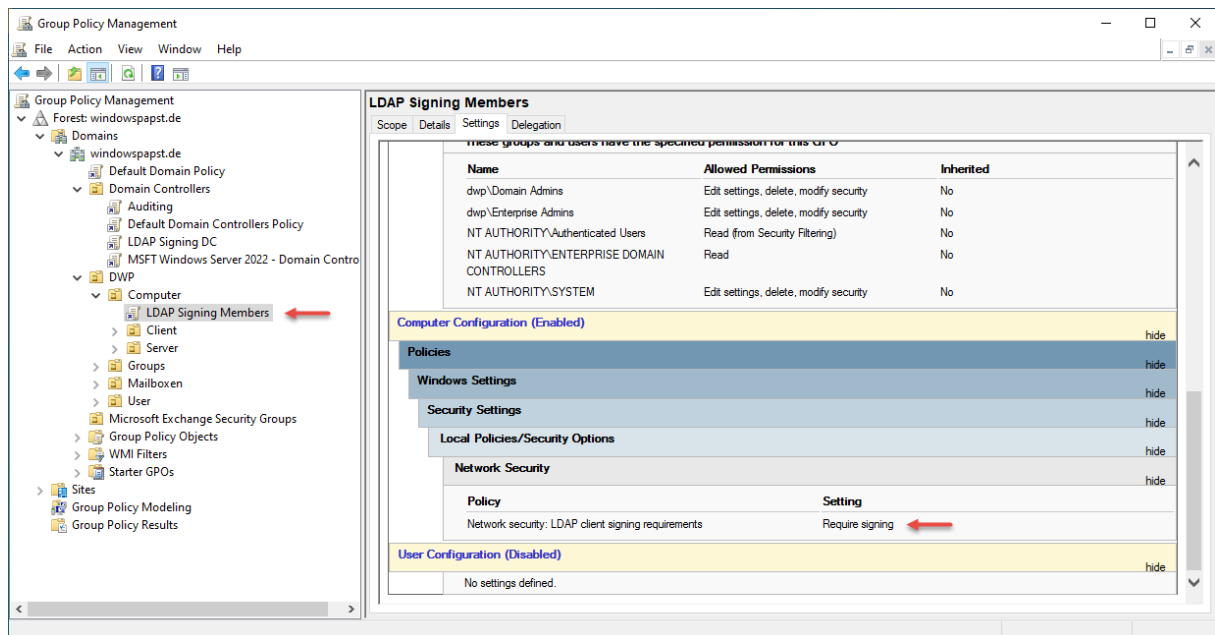


## LDAP Signing auf Domänencontrollern erzwingen

LDAP Signing DCs: LDAP Client signing requirements > **Negotiate signing**

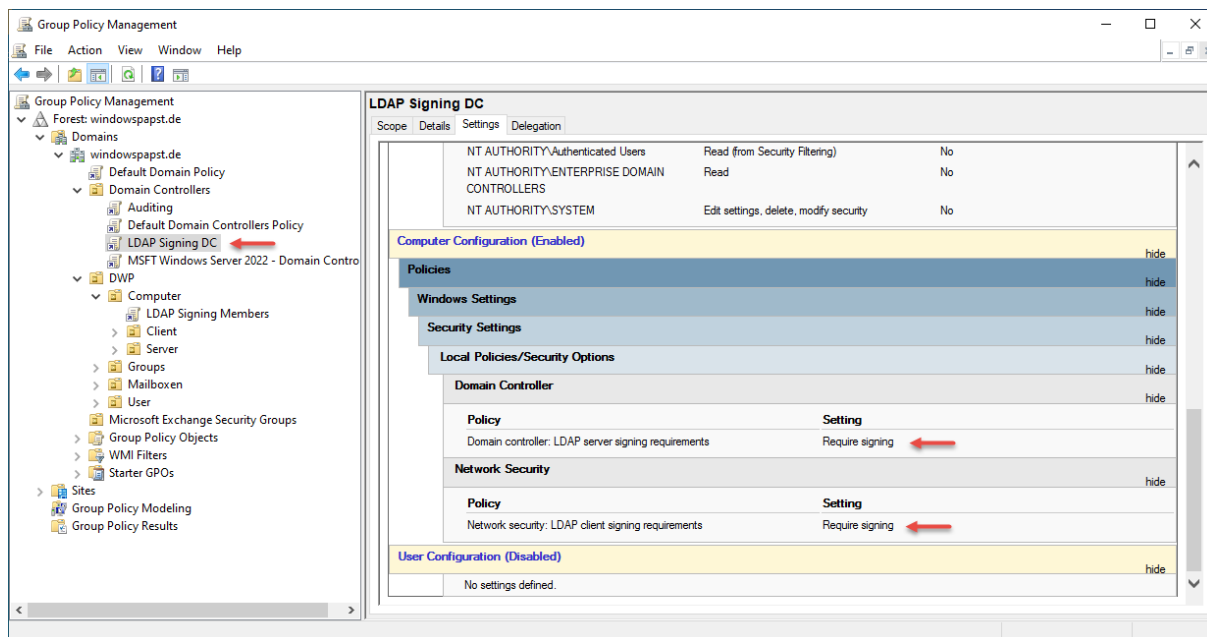


Im zweiten Schritt stellen wir nachdem alle Members (Clients & Server) ihre Policy erhalten haben, auf > **Require Signing** um.





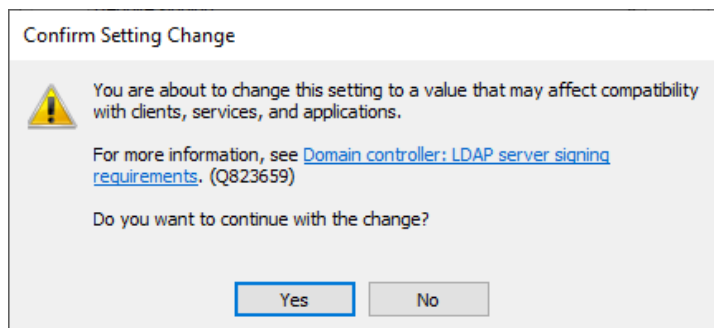
## LDAP Signing auf Domänencontrollern erzwingen



Das setzt aber voraus, dass keine Ereignisse mehr mit der ID 2889 vorkommen.

Bei der Nutzung von GSS-API kann es zu false-positiv Ereignissen kommen! Dann sollte auf SPNEGO umgestellt werden

Noch einmal der Warnhinweis, dass ab jetzt die Systeme, die nicht umgestellt wurden, keine Verbindungen mehr aufbauen könnten.



Ab jetzt ist die Datenkommunikation zwischen den (Members) Clients, Server und den Domain Controllern signiert.

LDAP Authentication	LDAP Signing NOT Configured	LDAP Signing Required	Port
Simple Bind	✓	✗	389
SimpleBind over SSL/TLS	✓	✓	636
Unsigned SASL	✓	✗	389
SASL over SSL/TLS	✓	✓	636
SASL + Built-in Encryption	✓	✓	389

Die Forcierung von LDAP-Signing erstellt eine digitale Signatur und fügt diese der Verbindung hinzu. Das stellt die Authentizität und die Integrität der übermittelten Daten sicher. Sollte kein SASL möglich sein, so muss auf LDAP/s ausgewichen werden.



## LDAP Signing auf Domänencontrollern erzwingen

### Kompatibilitätsmatrix für LDAP-Signaturen für Clients mit SASL-Bindung

Signaturanforderungen für LDAP-Clients	Signaturanforderungen für LDAP-Server*	Ergebnis der LDAP-SASL-Bindung
Keiner	Keiner	Alle Clients können binden.
Keiner	Unterzeichnung erforderlich	Clients, die das Signieren unterstützen, können binden.
Unterzeichnung verhandeln	Keiner	Alle Clients können binden.
Unterzeichnung verhandeln	Unterzeichnung erforderlich	Clients, die das Signieren unterstützen, können binden.
Unterzeichnung erforderlich	Keiner	Clients, die das Signieren unterstützen, können binden.
Unterzeichnung erforderlich	Unterzeichnung erforderlich	Clients, die das Signieren unterstützen, können binden.

### Kompatibilitätsmatrix für LDAP-Signaturen für Clients mit einfacher Bindung

Signaturanforderungen für LDAP-Clients	Signaturanforderungen für LDAP-Server*	Ergebnis der LDAP-SASL-Bindung
Keiner	Keiner	Alle Clients können binden.
Keiner	Unterzeichnung erforderlich	Fehler 0x2028 Für diesen Server ist eine sicherere Authentifizierungsmethode erforderlich. Dies ist keine kompatible Konfiguration für LDAP-Clients und LDAP-Server.
Unterzeichnung verhandeln	Keiner	Alle Clients können binden.
Unterzeichnung verhandeln	Unterzeichnung erforderlich	Fehler 0x2028 Für diesen Server ist eine sicherere Authentifizierungsmethode erforderlich.
Unterzeichnung erforderlich	Keiner	Clients, die das Signieren unterstützen, können binden.
Unterzeichnung erforderlich	Unterzeichnung erforderlich	Fehler 0x2028 Für diesen Server ist eine sicherere Authentifizierungsmethode erforderlich.

## LdapEnforceChannelBinding

Um einer weiteren wichtigen Empfehlung nachzukommen, sollte das LdapEnforceChannelBinding auf den DCs konfiguriert werden.

Event Properties - Event 3041, ActiveDirectory\_DomainService

General Details

The security of this directory server can be significantly enhanced by configuring the server to enforce validation of Channel Binding Tokens received in LDAP bind requests sent over LDAPS connections. Even if no clients are issuing LDAP bind requests over LDAPS, configuring the server to validate Channel Binding Tokens will improve the security of this server.

For more details and information on how to make this configuration change to the server, please see <https://go.microsoft.com/fwlink/?linkid=2102405>.

Log Name: Directory Service  
Source: ActiveDirectory\_DomainServ  
Event ID: 3041  
Level: Warning  
User: ANONYMOUS LOGON  
OpCode: Info  
More Information: [Event Log Online Help](#)

Logged: 5/27/2022 8:38:23 AM  
Task Category: LDAP Interface  
Keywords: Classic  
Computer: DC2.windowspapst.de

Copy Close

Das kann per Registry-Eintrag oder auch per GPO passieren.

Windows Registry Editor Version 5.00

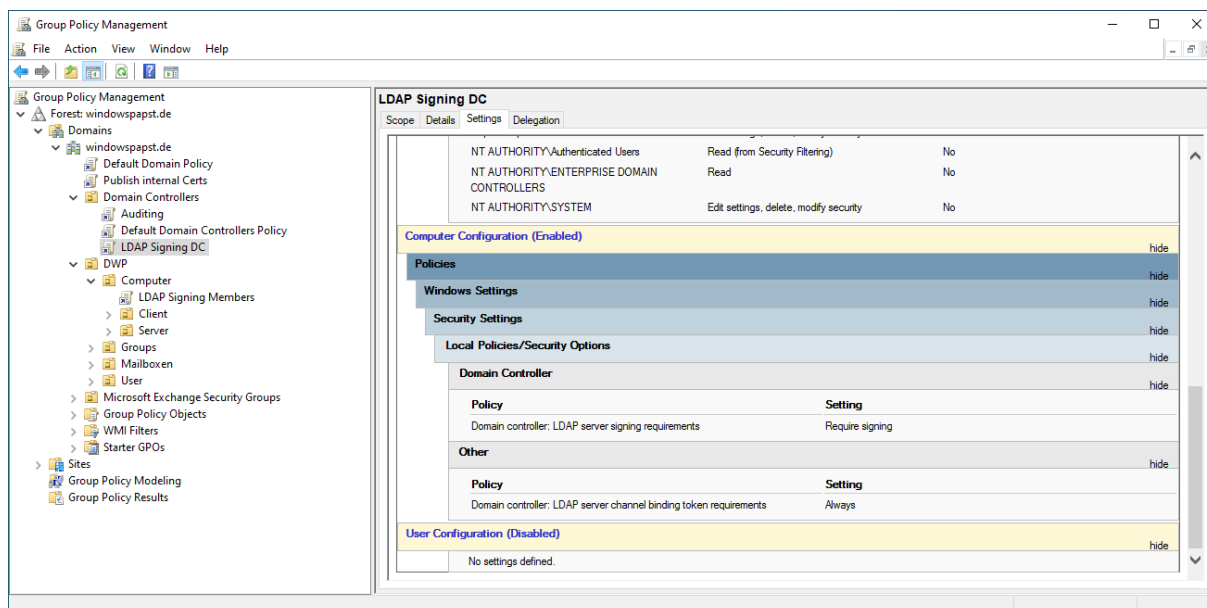
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters]

"LdapEnforceChannelBinding"=dword:00000002



## LDAP Signing auf Domänencontrollern erzwingen

### Per GPO:



**DWORD-Wert: 0** bedeutet deaktiviert. Es wird keine Kanalbindungsvalidierung durchgeführt. Dies ist das Verhalten aller Server, die nicht aktualisiert wurden.

**DWORD-Wert: 1** zeigt aktiviert an, wenn unterstützt. Alle Clients, die auf einer Version von Windows ausgeführt werden, die zur Unterstützung von Kanalbindungstoken (CBT) aktualisiert wurden, müssen dem Server Kanalbindungsinformationen bereitstellen. Clients, die eine Version von Windows ausführen, die nicht aktualisiert wurden, um CBT zu unterstützen, müssen dies nicht tun. Dies ist eine Zwischenoption, die Anwendungskompatibilität ermöglicht.

**DWORD-Wert: 2** bedeutet immer aktiviert. Alle Clients müssen Kanalbindungsinformationen bereitstellen. Der Server lehnt Authentifizierungsanforderungen von Clients ab, die dies nicht tun.

Die Aktivierung von Channel-Binding erstellt eine Brücke zwischen der Applikationsschicht und der TLS-Transportschicht (Tunnel) und erzeugt so einen eindeutigen Kanalbindungstoken. Das Token ist nur für diese **eine** Session gültig. Beim Wiederaufbau einer Session verfällt das Token und es wird ein neuer Token erstellt. Somit wird verhindert, dass das LDAP-Ticket an einer anderen Stelle eingesetzt werden kann.