LDAP Signing auf Domänencontrollern erzwingen

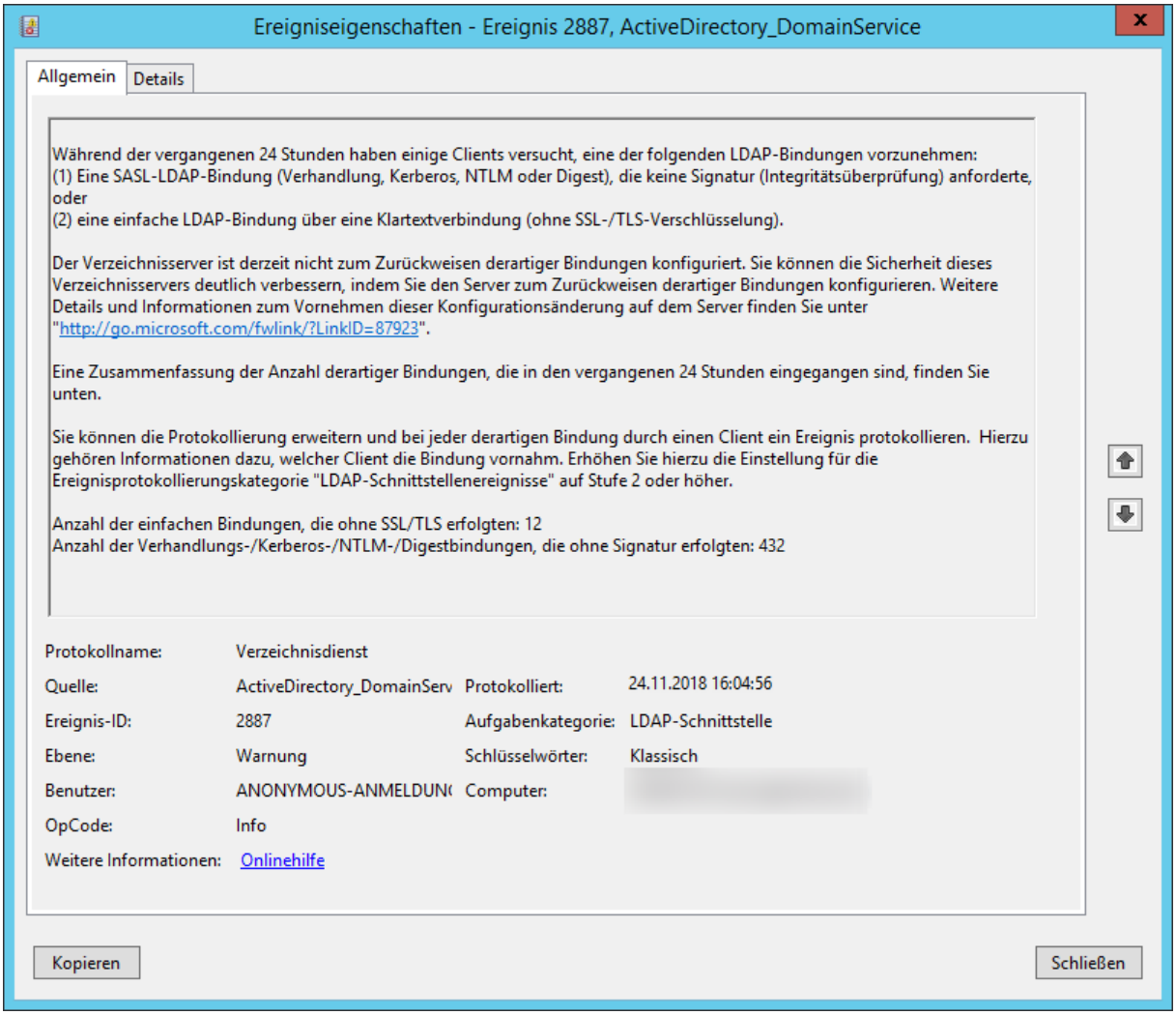
Zum Schutz der Anmeldedaten sollte das LDAP Signing (Erzwingen einer LDAP Signatur) erzwungen werden. Damit stellen wir sicher, dass Systeme und Applikationen keine Klartext-Kennwörter mehr übermitteln. Weiterhin wird mit dieser Einstellung verhindert, das künftige unsichere LDAP Bind Implementierungen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

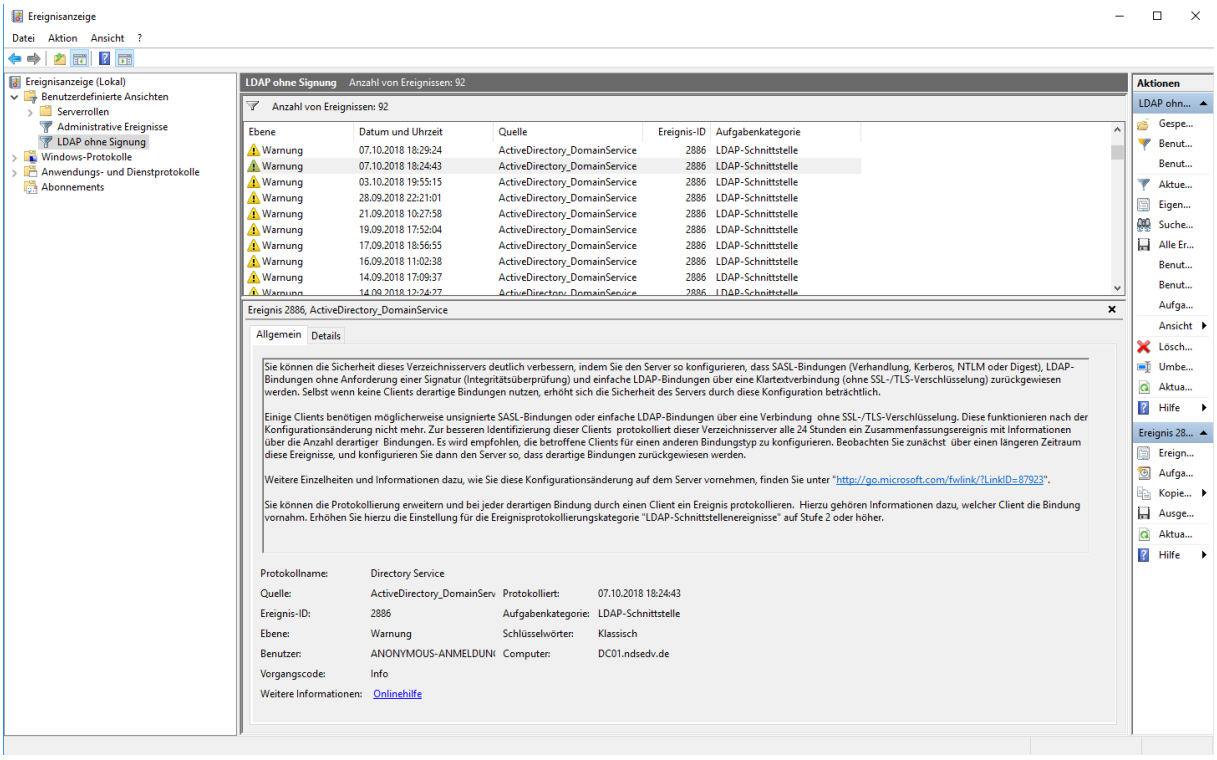
Was bringt eine komplexe Passwortrichtlinie, wenn die Daten unsicher übertragen werden können?! Im schlimmsten Fall sind es Daten von privilegierten Konten.

Das Problem:

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



LDAP Signing auf Domänencontrollern erzwingen



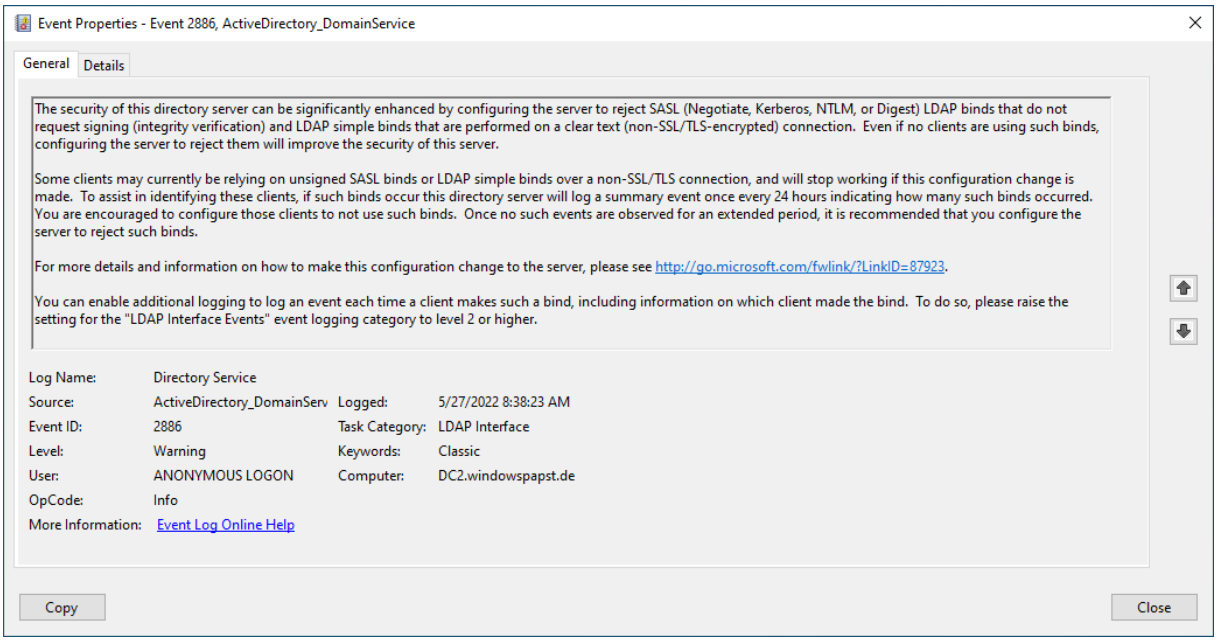
Sie können die Sicherheit dieses Verzeichnisservers deutlich verbessern, indem Sie den Server so konfigurieren, dass SASL-Bindungen (Verhandlung, Kerberos, NTLM oder Digest), LDAP-Bindungen ohne Anforderung einer Signatur (Integritätsüberprüfung) und einfache LDAP-Bindungen über eine Klartextverbindung (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 Verzeichnisserver alle 24 Stunden ein Zusammenfassungsereignis mit Informationen über die Anzahl derartiger 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-Schnittstellenereignisse" auf Stufe 2 oder höher.

Auszug aus einem englischen Betriebssystem:

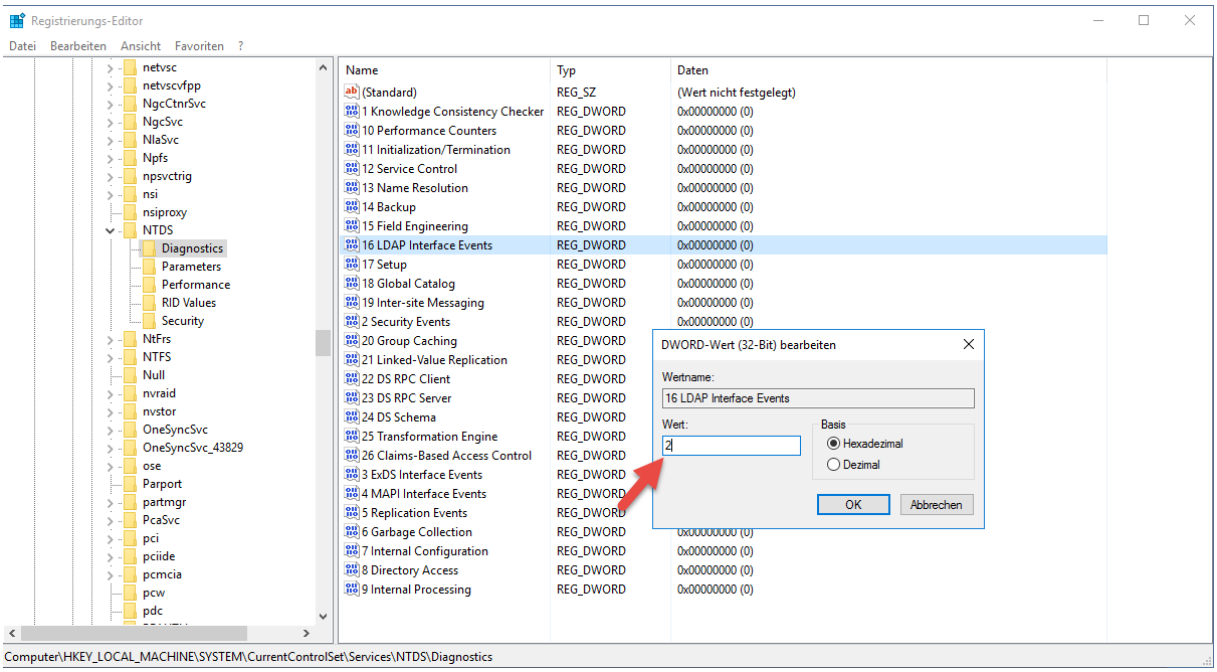


LDAP Signing auf Domänencontrollern erzwingen

Vorarbeit:

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

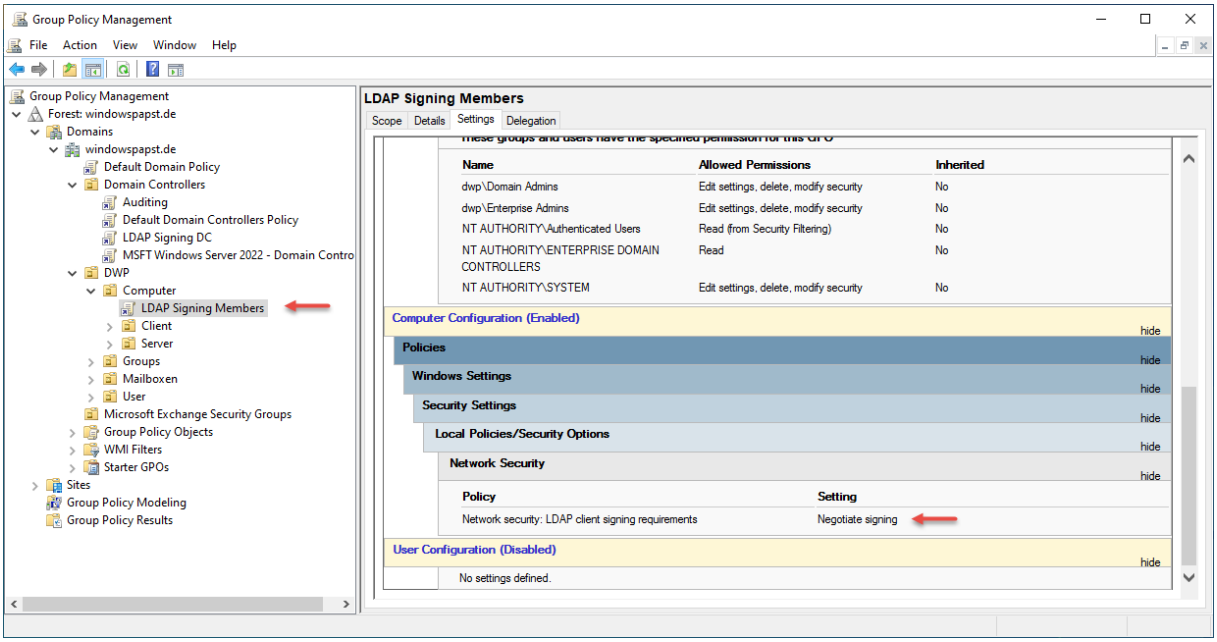
reg Add HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics /v "16 LDAP Interface Events" /t REG_DWORD /d 2



Vorgehen/Umsetzung:

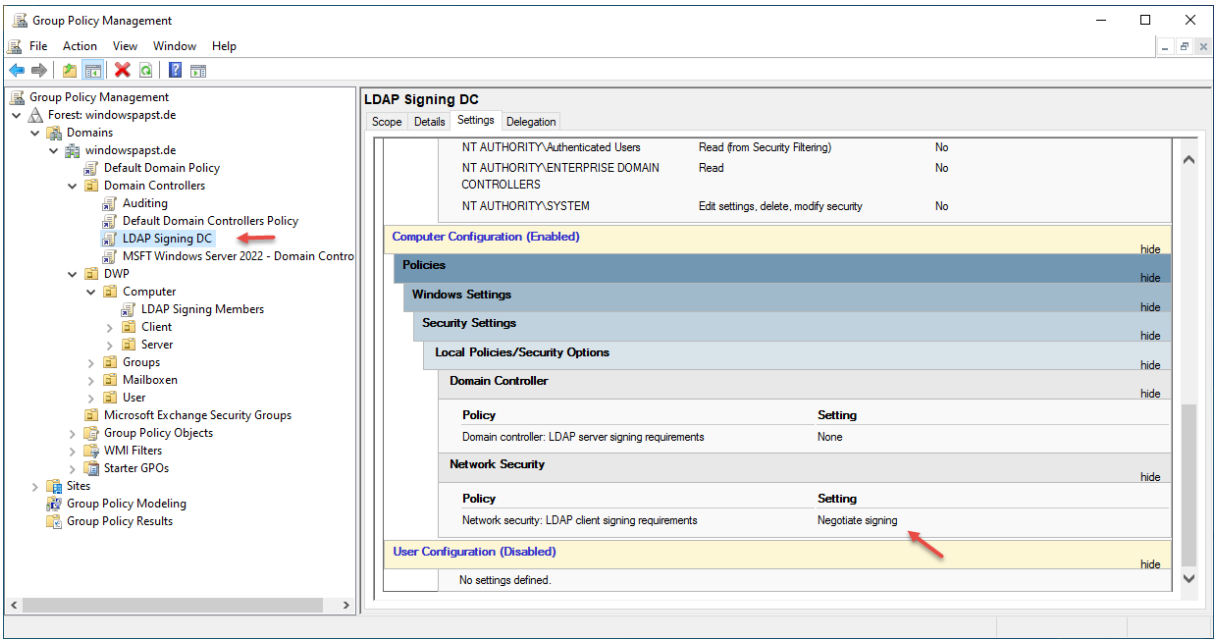
Im ersten Schritt erstellen wir zwei neue Policy namens „LDAP Signing Members & LDAP Signing DCs" mit folgenden Einstellungen:

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

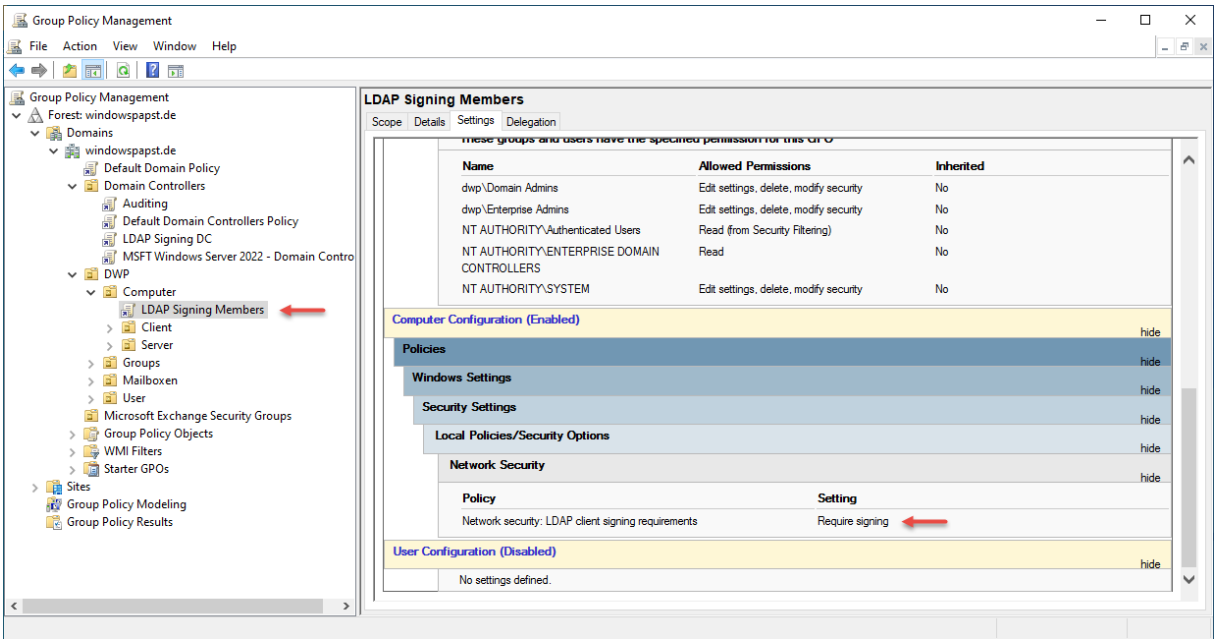


LDAP Signing auf Domänencontrollern erzwingen

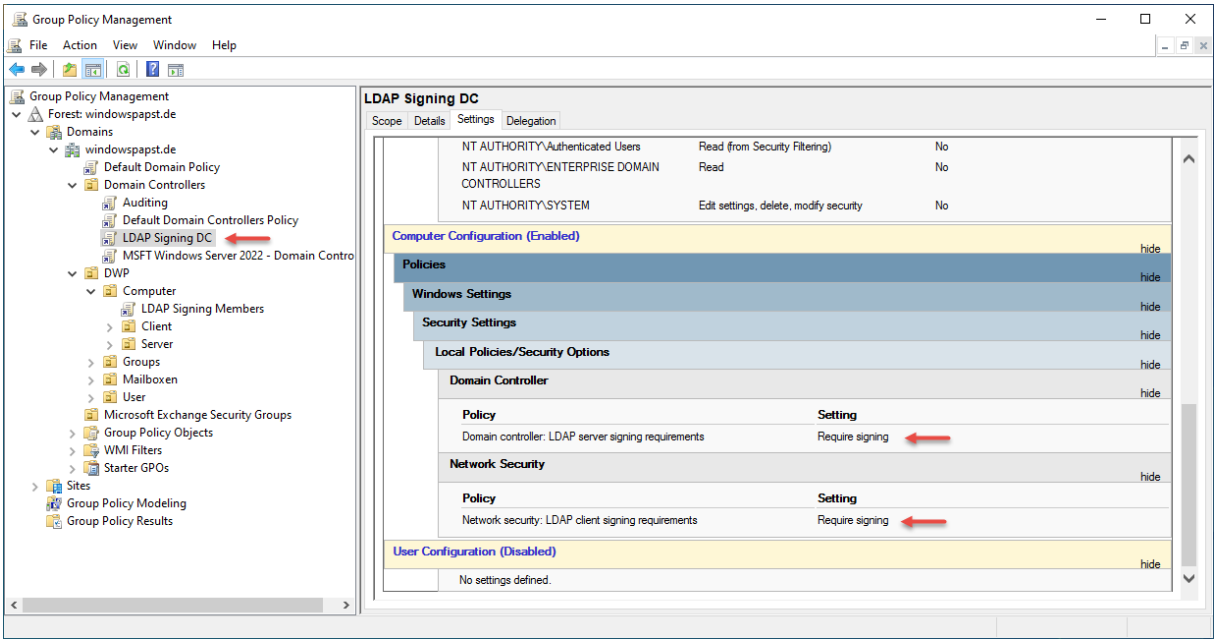
LDAP Signing DCs: LDAP Client signing requirements > **Negotiate signing**



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



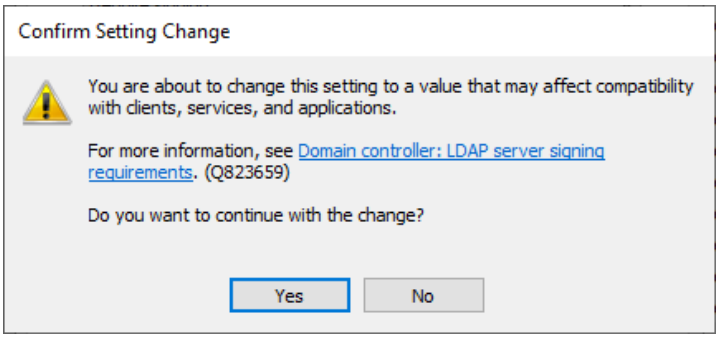
LDAP Signing auf Domänencontrollern erzwingen



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

Bei der Nutzung von GSS-API kann es zu false-positv 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 + Buit-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

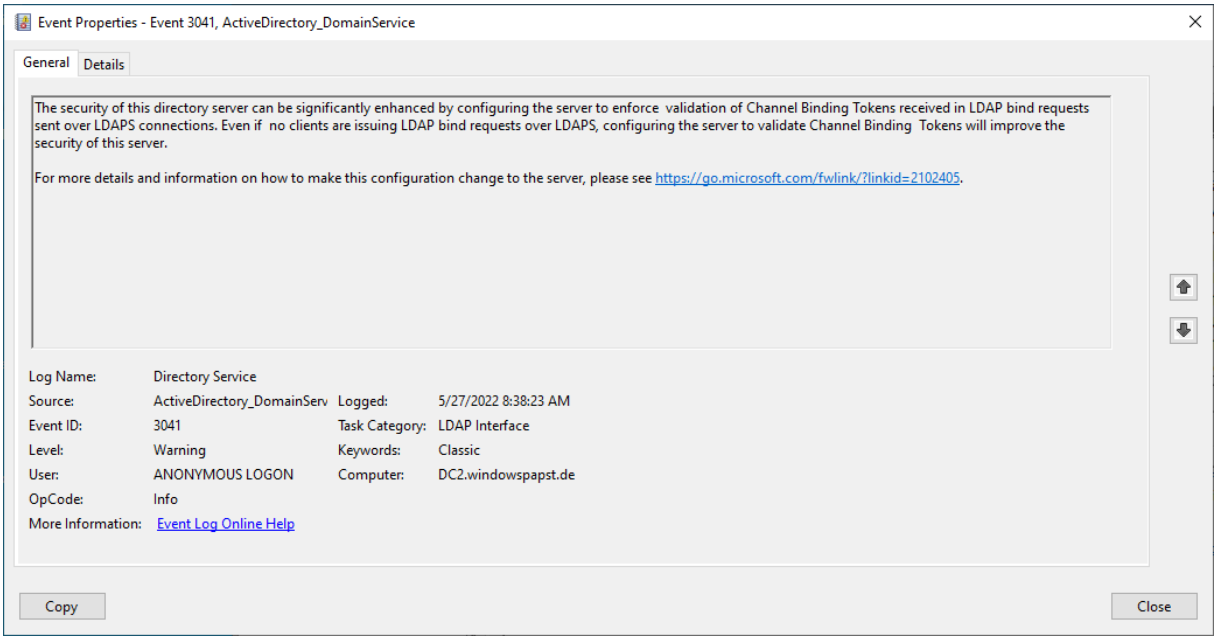
Signaturanforderungen für LDAP-Clients	Signaturanforderungen für LDAP-Server*	Ergebnis der LDAP-SASL-Bindung
Keiner	Keiner	Alle Clients können binden.
Keiner	Unterzeichnung erforderlich	Clients, die das Signieren unterstützen, können binden.
Unterzeichnung verhandeln	Keiner	Alle Clients können binden.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

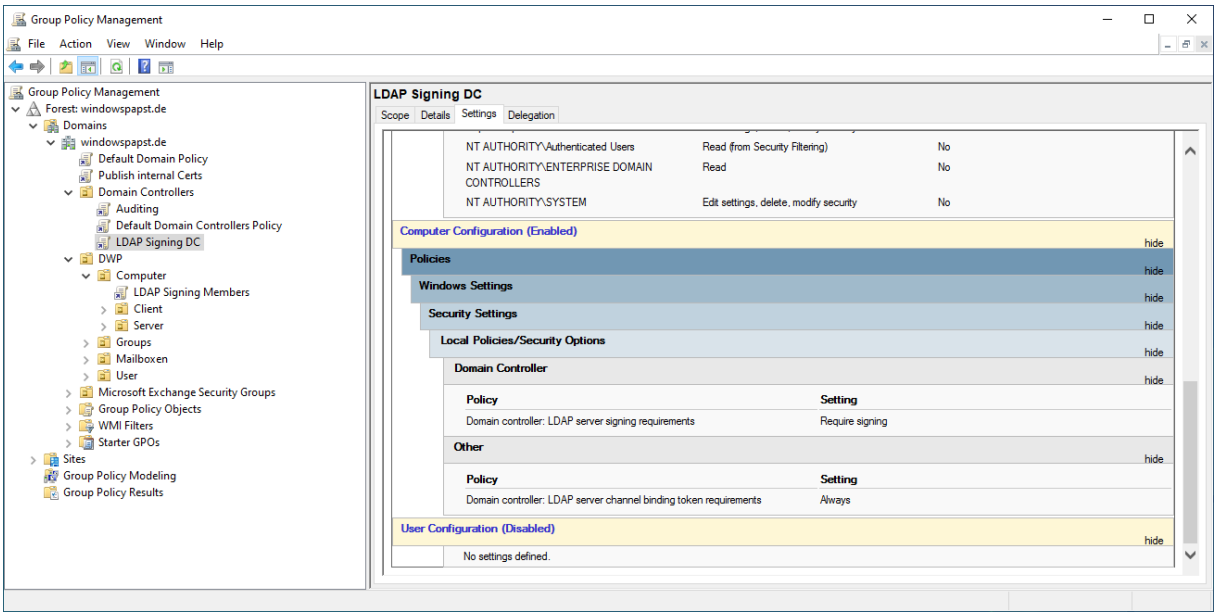


Das kann per Registry-Eintrag oder auch per GPO passieren.

```
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.