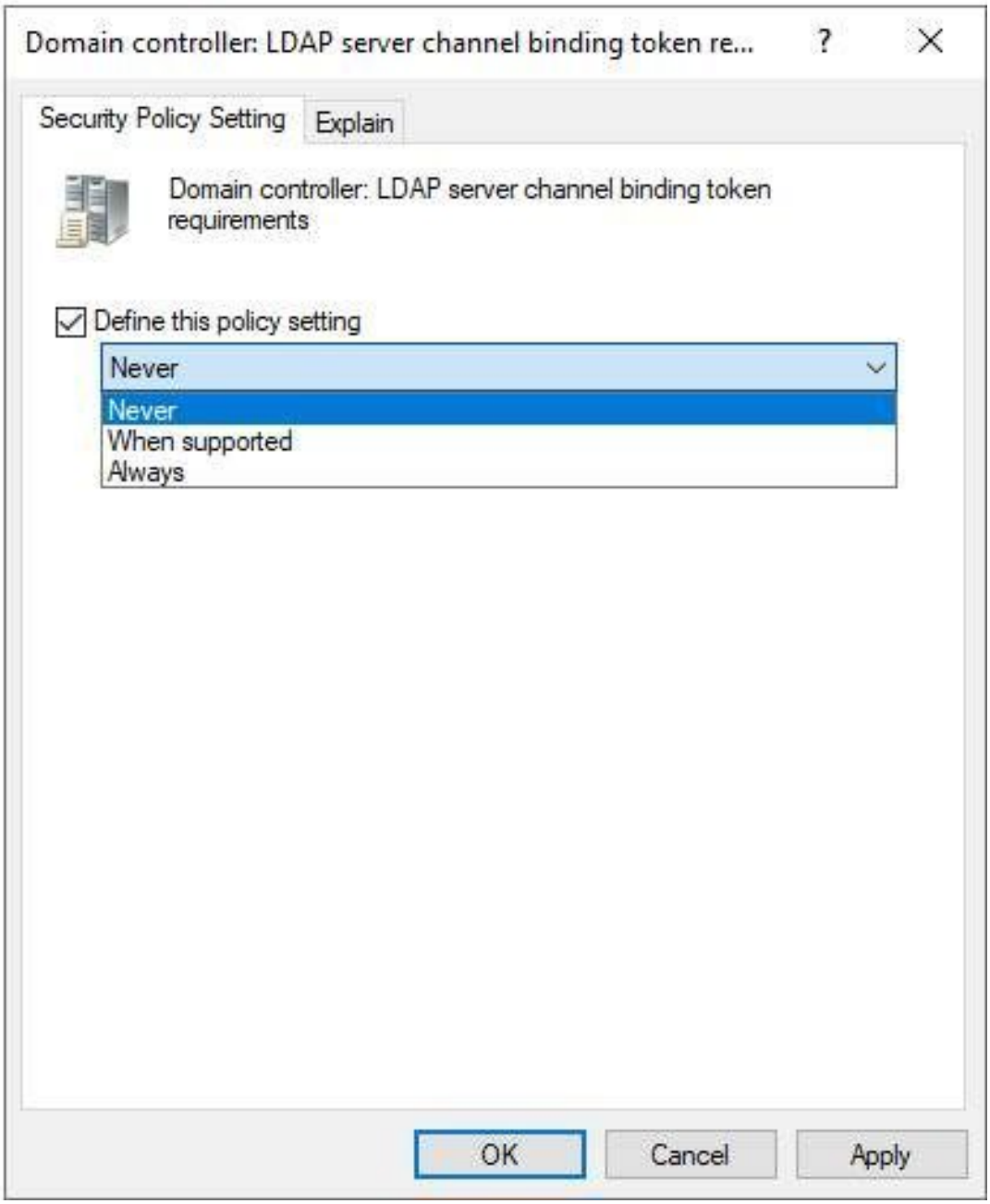
Active Directory Hardening Series - Part 5 – Enforcing LDAP Channel Binding

techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/active-directory-hardening-series---part-5—-enforcing-ldap-channel-binding/4235497



Blog Post

Hi all! - Jerry Devore back again to talk more about securing LDAP. This time I want to cover LDAP channel binding. If you have been following this series, you already know that LDAP signing should be enforced to prevent relay and MITM attacks. So, what is the purpose of enforcing LDAP channel binding? Well, channel binding can be used to prevent relay and MITM attacks against LDAP. If you don't find that explanation helpful you are not alone. A lot of people are struggling to understand why both are necessary. I hope to clear things up and give you the information you need to move forward with confidence.

To get started it would help to review the following key points from my previous post on LDAP signing.

- Simple binds are made with usernames and passwords.
- SASL binds are made using integrated authentication such as NTLM and Kerberos.

- Simple binds outside of a TLS session allow credentials and data to traverse the network in the clear and are subject to MITM attacks.
- Simple binds made over TLS leverages the session security provided by TLS which ensures the traffic is not readable and was not modified in transit.
- SASL binds can require signing which enables the client and server to exchange a session key that is used to make the communication private and ensure packets were not modified in transit.
- When SASL binds are made over TLS, the TLS session security replaces the session security offered by LDAP signing.
- Enforcing LDAP signing on the domain controller will cause SASL binds without signing and Simple Binds without TLS to be rejected.

At a glance it appears LDAP signing has all of the bases covered. However, if we think like an attacker we can find a possible loophole. What is that loophole? If a MITM can terminate the TLS session, the packets can be manipulated and put back on the wire using a new TLS session. LDAP signing is powerless to help with such an attack because the new TLS session satisfies the signing requirement. Channel binding helps close this loophole by ensuring the TLS session used to start the connection remains the TLS session for the lifetime of the session. That is accomplished by leveraging Extended Protection for Authentication (EPA) to generate a Channel Binding Token (CBT) for the session. Acquiring the CBT requires access to the client's credential which an attacker does not have in a LDAP relay scenario.

Before we move on it is important to clarify that simple binds do not use EPA or exchange CBTs. While simple binds cannot benefit from channel binding, enforcing channel binding on a domain controller will not impact simple binds over TLS. Additionally, channel binding has no impact on SASL binds that do not use TLS.

Enforcement Settings

LDAP Channel Binding support was introduced in March of 2020 and was backported as far back as Server 2008. The GPO setting for enforcement is named **Domain controller: LDAP server channel binding token requirements** which will manage the registry setting **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\LdapEnforceChannelBinding**.

Configuring the policy has the following effect:

Never: No channel binding validation is performed by the server.

When supported: Clients that advertise support for channel binding will have their connections rejected if they do not provide a valid CBT. Clients that do not support channel binding are not impacted.

Always: Any connection that does not provide a valid CBT will be rejected regardless of the client's support for channel binding.

The LdapEnforceChannelBinding registry setting does not exist until the policy is configured. As a result, channel binding is not enabled by default on domain controllers. It is also worth pointing out that changing this setting is effective immediately and does not require a reboot of the domain controller.

Client Support

There are no client side settings required to enable channel binding other than supporting EPA which was introduced in August of 2009.

Auditing

If your domain controllers are 2019 or newer you don't have to worry about having unexpected surprises when channel binding is enforced. Below is an example of a 3075 event which is recorded in the Directory Service log every time a client binds without providing a CBT. As you can see, the event captures the source IP address and the account that performed the bind.

Server 2019 and 2022 updated to November 2023 will automatically log 3075 events as long as 16 LDAP Interface Events is set to level 2 or higher. That is the same diagnostics logging setting covered in my LDAP signing article. Additionally, channel Binding on the server must be configured to **Never** or **When supported** in order for the event to be logged.

Another new event supported by 2019 and higher is 3074. Those are logged when a EPA client connection is rejected due to presenting an invalid CBT.

Server 2016 and earlier offers more limited logging via 3039 events. When a domain controller is configured to **When supported,** 3039 events capture EPA enabled clients that do not provide a valid CBT but non-EPA clients do not trigger an event. Once the server is configured to **Always,** 3039 events are logged for both EPA and non-EPA clients. Logging 3039 events requires the same LDAP diagnostic logging level as 3075 events. When channel binding is configured to **Never** no 3039 events are logged.

Keep in mind that any connection that triggers a 3039 event was rejected so they are not useful events for preemptive monitoring. If your domain controllers are not 2019 or newer you could enforce channel binding on limited number of domain controllers initially and monitor for 3039 events before making the change across the domain. Unfortunately, that approach or a full-fledged scream test are your only option if you are not going to introduce newer domain controllers.

Load Balanced LDAP… again.

As discussed previously in this series, load balancing LDAP connections to domain controllers is problematic. That is very much true when it comes to enforcing channel binding. If your load balancing solution is bridging TLS sessions (terminating the TLS session from the client and opening a new TLS session to the domain controller), enforcing channel binding will cause those connections to be rejected. If you must use a load balancer for LDAP, then the TLS session must persist from the client to the domain controller. In order to support that configuration, the FQDN of the load balancer VIP will need to be added to the Subject Alternative Name field of the certificates installed on the domain controllers. Another alternative is to configure load balanced applications to use simple binds instead of SASL.

Ok, you guys know the drill. Once again here are my **Do's and Don'ts** to help you stay employed as you enforce channel binding in your environment.

- **Do** remember that channel binding only applies to SASL binds that use TLS. SASL binds without TLS and simple binds over TLS will not be impacted by enforcing channel binding.
- **Don't** put off upgrading your domain controllers. Mainstream support for Server 2016 ended in January 2022 and extended support will end in January 2027.
- **Do** configure channel binding to **When supported** if you haven't already. That should be a low impact change given invalid CBTs are not a common issue.
- **Don't** assume the presence of legacy clients (I am looking at you XP) automatically prevents the enforcement of channel binding. It is unlikely those old clients are using TLS when making SASL binds.
- **Do** use a central logging solution to forward the 3039, 3074, 3075 events to a single location so you can efficiently manage this effort.
- **Don't** configure channel binding to **Always** until you have investigated the source of the 3075 events.
- **Don't** forget that SASL binds over TLS use TLS session security instead of session security offered by LDAP signing. That is why both LDAP signing and channel binding need to be enforced.
- **Do** check out these resources

Updated Dec 24, 2024

Version 6.0
\n\n \n\n \n \n\n \n\n \n\n\n \n\n \n\n \n\n\n\n \n \n \n\n \n\n \n\n \n\n \n\n \n\n \n\n \n\n \n\n \n\n\n\n\n \n\n \n\n \n\n\n\n \n\n \n\n