Wie binde ich ein On-Premises Active Directory über einen VPN-Tunnel an?

Benedikt Ladzik - 2026-08-28 - How To ...

Diese Anleitung beschreibt, wie ein On-Premises Active Directory (AD) bzw. ein LDAP-Verzeichnis sicher an Bare.ID angebunden wird. Die Integration gliedert sich in zwei logisch getrennte Phasen:

1. **Netzwerkanbindung** – Aufbau einer sicheren Verbindung zwischen der On-Premises-Umgebung und Bare.ID, in der Regel über einen gemanagten VPN-Tunnel.
2. **Verzeichnisanbindung** – Konfiguration der eigentlichen LDAP- bzw. Active-Directory-Integration (Service-Account, Suchbasen, LDAPS).

Die zweite Phase sollte erst begonnen werden, wenn die Netzwerkverbindung stabil aufgebaut und abgenommen ist.

Gesamtarchitektur

Im Zielzustand terminiert der VPN-Tunnel auf Bare.ID-Seite **direkt in den Kubernetes-Pods Deiner Bare.ID-Instanz**. Über diesen Tunnel sendet die Bare.ID-Instanz LDAP- bzw. LDAPS-Anfragen an Dein Active Directory, das Du über einen von Dir betriebenen Endpunkt – typischerweise eine dedizierte Gateway-VM – bereitstellst. So muss Dein Active Directory **nicht direkt aus dem Internet erreichbar** sein.

Ein großer Teil der Verantwortung für den stabilen Betrieb liegt auf der korrekten Netzwerk- und Firewall-Konfiguration in Deiner Umgebung.

Die VPN-Verbindung im Überblick

Die Netzwerkverbindung wird über einen gemanagten, WireGuard-basierten Tunnel des Partners XplicitTrust hergestellt. Dabei handelt es sich um eine **Point-to-Point-Verbindung (Peer-to-Peer)**: Es wird ein direkter, Ende-zu-Ende-verschlüsselter Tunnel zwischen Deiner Bare.ID-Instanz und dem von Dir betriebenen Endpunkt aufgebaut. Auf Bare.ID-Seite endet der Tunnel **direkt in den Kubernetes-Pods Deiner Instanz**; auf Deiner Seite betreibt der XplicitTrust-Agent den Endpunkt (in der Regel die Gateway-VM). Anders als bei klassischen VPNs terminiert der Tunnel also nicht an einem zwischengeschalteten zentralen VPN-Gateway, sondern reicht direkt bis zu den beteiligten Endpunkten.

Der Ansatz folgt dem Zero-Trust-Prinzip (ZTNA): Der XplicitTrust-Agent initiiert die Verbindung ausschließlich **ausgehend** aus Deinem Netzwerk heraus und hält sie aufrecht, sodass keine eingehenden Firewall-Freigaben erforderlich sind. Es wird gezielt nur die freigegebene Verbindung zum Zielsystem hergestellt, nicht der Zugriff auf ein ganzes Netzsegment.

Empfohlene Architektur (Gateway-Ansatz)

Für den produktiven Betrieb wird der Einsatz einer dedizierten Linux-VM als Gateway empfohlen. Diese VM fungiert als zentraler Übergabepunkt zwischen dem VPN-Tunnel und Deinem internen Netzwerk und betreibt den XplicitTrust-Agent. Optional kann auf derselben Instanz ein Reverse Proxy für die LDAPS-Bereitstellung betrieben werden.

Der Gateway-Ansatz bietet mehrere Vorteile:

- **Klare Netzwerksegmentierung**, da keine Installation auf Domain Controllern notwendig ist.
- **Zentrale Bündelung** von Firewall-Regeln, Logging und Zugriffskontrollen an einer Stelle, was Betrieb und Fehlersuche erleichtert.

Alternativ kann der Agent technisch auch direkt auf einem Domain Controller installiert werden. Diese Variante wird jedoch **nicht empfohlen**, da sie zu einer Vermischung von Rollen führt und höhere Anforderungen an Härtung und Betrieb stellt.

An welches System wird angebunden?

Für das Ziel der LDAP-Anfragen stehen je nach Umgebung mehrere Optionen zur Verfügung:

- **Domain Controller (DC)**: Direkte Anbindung an einen DC. Einfach umzusetzen, koppelt die Anbindung jedoch eng an die Verfügbarkeit und Last eines produktiven DC.
- **Read-Only Domain Controller (RODC)**: Anbindung an einen RODC bzw. eine read-only Replik. Lese- und Anmeldevorgänge (Bind) funktionieren hierüber, die Last auf produktiven DCs und die Angriffsfläche werden reduziert. **Wichtig:** Ein RODC eignet sich ausschließlich für den Modus „Read Only“. Da ein RODC keine Schreibvorgänge verarbeitet, schlagen schreibende Operationen – insbesondere Passwort-Resets im Modus „Writeable“ – über einen RODC fehl. Wird Passwortverwaltung über Bare.ID benötigt, muss ein **beschreibbarer Domain Controller** als Ziel verwendet werden. (Zusatzhinweis: Ein RODC kann zudem nur Konten authentifizieren, deren Passwörter gemäß seiner Password Replication Policy zwischengespeichert sind, andernfalls muss er einen beschreibbaren DC erreichen können.)
- **Reverse Proxy**: Ein dem Verzeichnis vorgelagerter Proxy (z. B. auf der Gateway-VM) terminiert LDAPS und stellt einen stabilen, gehärteten Endpunkt bereit. Eignet sich gut, um Zertifikate und Zugriffe an einer Stelle zu verwalten.

Sicherheits- und Isolationskonzept

Die VPN-Anbindung ist mandantenisoliert aufgebaut. Für jeden Bare.ID-Knoten wird ein separater VPN-Endpunkt bereitgestellt; eine gemeinsame Nutzung der VPN-Infrastruktur zwischen unterschiedlichen Kunden findet nicht statt.

Der Verbindungsaufbau erfolgt ausschließlich ausgehend aus Deinem Netzwerk heraus. Es sind keine eingehenden Verbindungen erforderlich. Dieses Modell reduziert die Angriffsfläche erheblich und vereinfacht die Integration in bestehende Sicherheitskonzepte.

Voraussetzungen

- Eine Linux-basierte virtuelle Maschine in einem Netzwerksegment, von dem aus die internen Zielsysteme erreichbar sind. Alternativ ist eine Installation direkt auf einem Domain Controller oder über Docker-Container möglich.
- Ausgehender Internetzugang auf der Maschine.
- Funktionierende grundlegende Netzwerkdienste (DNS-Auflösung und Zeit-Synchronisation), da diese indirekt für den stabilen Betrieb des Agents relevant sind.
- Ein Active Directory sowie ein Service-Account – diese werden erst für die Verzeichnisanbindung benötigt, nicht für den Aufbau des VPN-Tunnels.

Netzwerk- und Firewall-Anforderungen

Für den zuverlässigen Betrieb des XplicitTrust-Agents müssen ausgehende Firewall-Regeln korrekt konfiguriert sein.

Ausgehender HTTPS-Verkehr (TCP-Port 443) muss erlaubt sein. Er wird für Steuerungs- und Verwaltungsfunktionen des Agents benötigt (Konfigurationsabruf, Authentifizierung, Statusmeldungen). Folgende Endpunkte müssen erreichbar sein:

```
xtsa.xplicittrust.com
discoveryapi.xplicittrust.com
broker2.xplicittrust.com
relay5.xplicittrust.com
dl.xplicittrust.com
log.xplicittrust.com
```

Ausgehender UDP-Verkehr im Portbereich 51820–60000 ist erforderlich. Dieser Bereich wird für die eigentliche, WireGuard-basierte Tunnelverbindung verwendet. Wird dieser Verkehr eingeschränkt, kann es zu instabilen Verbindungen oder Verbindungsabbrüchen kommen. Die Freigabe dieses UDP-Portbereichs ist daher **nicht optional**, sondern eine zentrale Voraussetzung für den stabilen Betrieb.

Außerdem benötigt der Agent **Netzwerkzugriff auf das Zielsystem** (Dein LDAP- bzw. Active-Directory). Nimm die Freischaltung entsprechend Deiner bestehenden Infrastruktur vor (üblicherweise TCP 389 für LDAP/StartTLS bzw. TCP 636 für LDAPS).

Installation und Inbetriebnahme des XplicitTrust-Agents

Die Installation erfolgt gemäß der offiziellen Herstellerdokumentation im sogenannten „Asset Mode“. Eine detaillierte Schritt-für-Schritt-Anleitung stellt XplicitTrust bereit:

`https://docs.xplicittrust.com/install/linux-asset/`

Der Import der von Bare.ID bereitgestellten Konfigurationsdatei erfolgt über das mitgelieferte Werkzeug:

```
sudo /usr/sbin/xtna-util -import xtna-*.xtconfig
```

Weitere Installationsmöglichkeiten bestehen über einen Windows Server oder Docker.

Überprüfung der Verbindung

Nach dem Import der Konfiguration sollte die Verbindung unmittelbar überprüft werden. Der Agent stellt hierfür mehrere Diagnosefunktionen bereit:

```
sudo xtna-util -connectivity
sudo xtna-util -status
sudo xtna-util -service-status
```

Mit der Connectivity-Prüfung wird getestet, ob alle erforderlichen Endpunkte erreichbar sind und der Tunnel korrekt aufgebaut werden kann. Ein erfolgreicher Verbindungsaufbau ist daran erkennbar, dass keine Fehler gemeldet werden und der Agent als „online“ erscheint.

Ist dies nicht der Fall, liegt die Ursache in der Praxis fast immer in fehlenden Netzwerkfreigaben oder einer fehlerhaften DNS-Auflösung.

Verzeichnisanbindung (LDAP / Active Directory)

Erst nachdem die Netzwerkverbindung stabil steht, wird die eigentliche Verzeichnisanbindung konfiguriert.

Service-Account und Betriebsmodus

Für die Anbindung wird ein dedizierter Service-Account im Active Directory benötigt, mit dem sich Bare.ID am Verzeichnis anmeldet (Bind). Bare.ID basiert auf Keycloak und unterstützt drei Betriebsmodi für die Verzeichnisanbindung:

- **Read Only (empfohlen)**: Bare.ID liest Nutzer und Attribute aus dem Active Directory, schreibt jedoch nichts zurück. Profil- und Passwortänderungen sind in Bare.ID gesperrt und müssen direkt im Active Directory erfolgen. Der Service-Account benötigt nur Leserechte auf die konfigurierten Suchbasen und Attribute. Dies ist der sicherste Modus und für die meisten Anbindungen ausreichend.

- **Writeable**: In Bare.ID vorgenommene Änderungen (z. B. Profilattribute) sowie Passwort-Resets werden in das Active Directory zurückgeschrieben. Hierfür benötigt der Service-Account entsprechende Schreibrechte, die nach dem Least-Privilege-Prinzip möglichst eng delegiert werden sollten. Für AD-Passwort-Resets reicht das Recht „Kennwort zurücksetzen“ in der Praxis oft nicht aus, da beim Reset zusätzliche Attribute geschrieben werden (u. a. `pwdLastSet` und `userAccountControl`); die Delegation sollte diese einschließen.

- **Unsynced**: Nutzer werden aus dem Active Directory importiert; Änderungen (einschließlich Passwörter) werden ausschließlich lokal in Bare.ID gespeichert und **nicht** in das Active Directory zurückgeschrieben. Dieser Modus entkoppelt die lokalen Daten vom Verzeichnis und sollte nur in begründeten Ausnahmefällen verwendet werden.

  Hinweis zu Passwörtern: Passwörter werden grundsätzlich **nicht in Bare.ID gespeichert**, sondern bei der Anmeldung direkt gegen das Active Directory geprüft. Ein **Zurücksetzen oder Ändern von Passwörtern mit Rückschreiben in das Active Directory ist nur im Modus „Writeable“ möglich**. Im Modus „Read Only“ müssen Passwörter über die nativen Werkzeuge des Active Directory geändert werden; die Self-Service-Funktionen „Passwort vergessen“ bzw. „Passwort ändern“ sollten in diesem Fall deaktiviert werden, da sie für Verzeichnis-Nutzer sonst fehlschlagen.

> **Hinweis:** Damit Passwörter im Modus „Writeable“ zuverlässig zurückgeschrieben werden können, empfehlen wir eine **verschlüsselte Verbindung (LDAPS bzw. StartTLS)**. Active Directory akzeptiert Passwortänderungen in der Standardkonfiguration beispielsweise nur über eine verschlüsselte Verbindung; je nach Konfiguration Deines Verzeichnisdienstes können die Anforderungen abweichen (siehe nächster Abschnitt).

LDAPS-Zertifikatsanforderungen

Für eine verschlüsselte Verbindung zum Verzeichnisdienst empfehlen wir LDAPS (TCP 636) oder StartTLS (TCP 389). Für das vom Zielsystem (DC oder Reverse Proxy) präsentierte Serverzertifikat haben sich folgende Eigenschaften bewährt:

- Der **Common Name bzw. ein Subject Alternative Name (SAN)** sollte dem Hostnamen entsprechen, über den Bare.ID das System anspricht (FQDN).
- Das Zertifikat sollte **gültig** (nicht abgelaufen) sein und die **vollständige Zertifikatskette** ausliefern.
- **Selbstsignierte Zertifikate sowie Zertifikate interner/privater CAs werden unterstützt.** Übergib in diesem Fall das CA- bzw. Root-Zertifikat (bei selbstsignierten Zertifikaten das Zertifikat selbst) an Bare.ID. Es wird in den **Truststore Deiner Bare.ID-Instanz** aufgenommen, sodass der LDAPS-Verbindung vertraut wird.
- Für TLS-Version, Schlüssellängen und Cipher Suites empfehlen wir, Dich an den Vorgaben der BSI TR-02102-2 zu orientieren.

Die konkreten Anforderungen hängen letztlich von der Konfiguration Deines Verzeichnisdienstes ab.

Konfiguration in Bare.ID

Die Verzeichnisanbindung wird im Bare.ID-Dashboard per Self-Service als externer Login-Provider eingerichtet.

- Melde Dich mit einem Administrator-Konto bei Bare.ID auf app.bare.id an und wähle auf der Willkommensseite die Instanz aus, für die der Login-Provider verbunden werden soll.
- Klicke in der Navigation links auf “Externe Login-Provider”.
- Klicke auf den Button “Login-Provider verbinden”.

- Wähle in der Galerie den entsprechenden vorkonfigurierten Login-Provider aus.

- Wähle dort den Eintrag für LDAP.

Auf der Konfigurationsseite werden insbesondere festgelegt:

- **Verbindungs-URL**: Verbindungs-URL des Verzeichnisses (z. B. `ldaps://dc.example.local:636`) sowie Bind-DN und Passwort des Service-Accounts.
- **Bearbeitungsmodus**: Read Only, Writeable oder Unsynced (siehe oben).
- **Bind DN**: Users-DN bzw. Base DN, unter der nach Nutzern gesucht wird.
- **Attribut-Mappings**: Zuordnung der Verzeichnis-Attribute (z. B. Benutzername, E-Mail) zu den Bare.ID-Nutzerfeldern sowie ggf. Gruppen-Mappings.

> **Hinweis:** Das Attribut-Mapping steht erst nach dem erstmaligen Speichern der Login-Provider-Konfiguration zur Verfügung. Lege die Verbindung daher zunächst an und speichere sie; anschließend können die Attribut- und Gruppen-Mappings bearbeitet werden.

Diese Werte hängen von Deiner AD-Struktur ab; bei Bedarf unterstützt Bare.ID bei der Festlegung.

Abnahmekriterien

Die Anbindung gilt als erfolgreich abgeschlossen, wenn:

- der Agent dauerhaft online ist und die Diagnosefunktionen keine Fehler melden,
- die Verbindung über einen längeren Zeitraum stabil bleibt, und
- anschließend die LDAP-/LDAPS-Anbindung erfolgreich getestet wurde (Testanmeldung eines Verzeichnis-Nutzers).

Typische Fehlerbilder und Ursachen

- **Agent baut keine Verbindung auf**: In den meisten Fällen ist der ausgehende HTTPS-Verkehr blockiert oder die erforderlichen Zielsysteme sind nicht erreichbar.
- **Instabile Verbindungen**: Deuten häufig darauf hin, dass der benötigte UDP-Portbereich eingeschränkt ist oder durch NAT-/Firewall-Regeln beeinträchtigt wird.
- **Connectivity-Prüfung schlägt fehl**: Systematisch prüfen, ob DNS korrekt funktioniert, alle Zielsysteme erreichbar sind und die bereitgestellte Konfigurationsdatei korrekt importiert wurde.
- **LDAPS-Verbindung schlägt fehl**: Häufig durch einen Hostname-/SAN-Mismatch, ein abgelaufenes Zertifikat oder eine fehlende CA im Truststore verursacht.

Für weiterführende Diagnosemöglichkeiten empfiehlt sich ein Blick in die offizielle Dokumentation sowie in die vom Agent bereitgestellten Logdaten.

Rollen und Verantwortlichkeiten

- **Auf Kundenseite** liegt die Verantwortung für die Bereitstellung und den Betrieb der Gateway-VM, die korrekte Umsetzung der Netzwerk- und Firewall-Regeln, die Installation und den Betrieb des XplicitTrust-Agents, die Bereitstellung von Service-Account und LDAPS-Zertifikaten sowie die Konfiguration der Verzeichnisanbindung im Bare.ID-Dashboard.
- **Bare.ID** stellt die notwendige VPN-Konfigurationsdatei bereit, unterstützt bei der Inbetriebnahme und der Validierung der Verbindung und nimmt das bereitgestellte CA- bzw. Server-Zertifikat in den Truststore der Instanz auf.