

So richten Sie die LDAP-Authentifizierung auf HiOS-Geräten ein

- 2023-12-18 - HiOS

In dieser Lektion wird beschrieben, wie Sie die LDAP-Authentifizierung auf HiOS-Geräten konfigurieren.

Nützliche Tools: LDAP-Browser, z. Softerra LDAP Browser

Installation eines Active Directory Server

Informationen zur Installation von Windows AD Server 2012 finden Sie unter folgendem Link:

<http://social.technet.microsoft.com/wiki/contents/articles/12370.windows-server-2012-set-up-your-first-domain-controller-step-by-step.aspx>

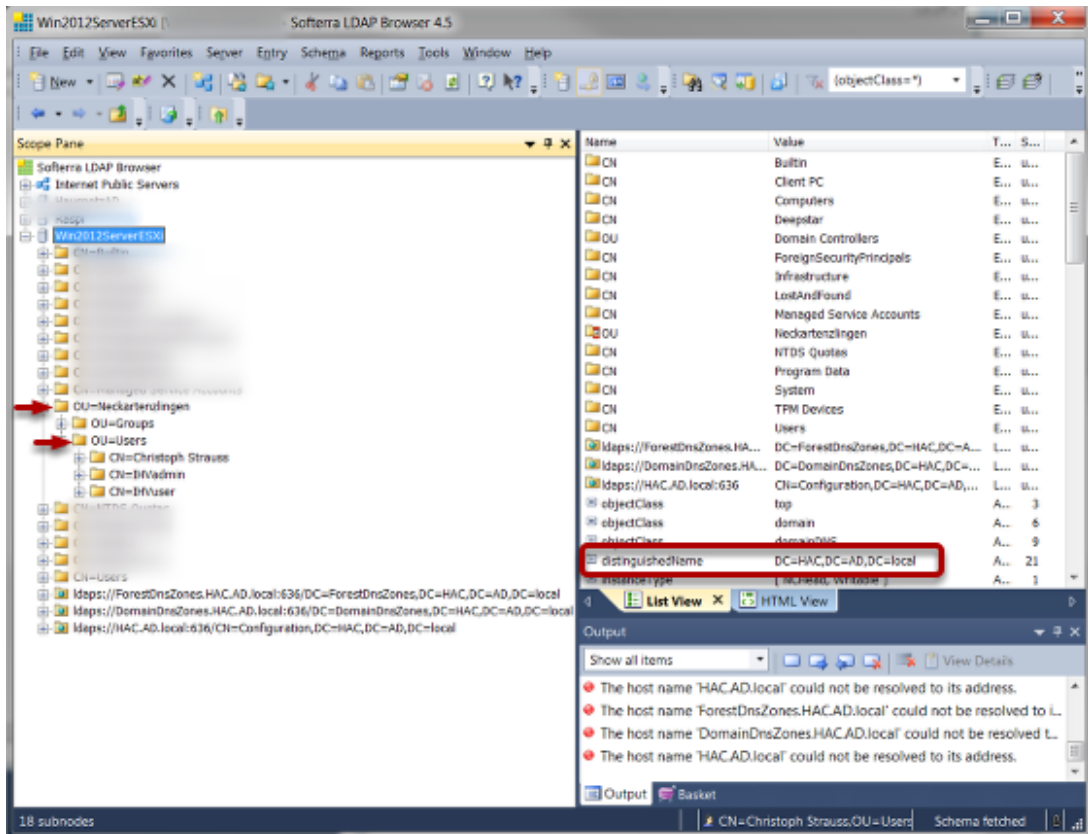
Informationen zur Installation von Windows AD Server 2016 finden Sie unter folgenden Link:

<https://ittutorials.net/microsoft/windows-server-2016/setting-up-active-directory-ad-in-windows-server-2016/>

Anweisungen zum Einrichten des Microsoft AD-Zertifikatdienstes finden Sie hier:

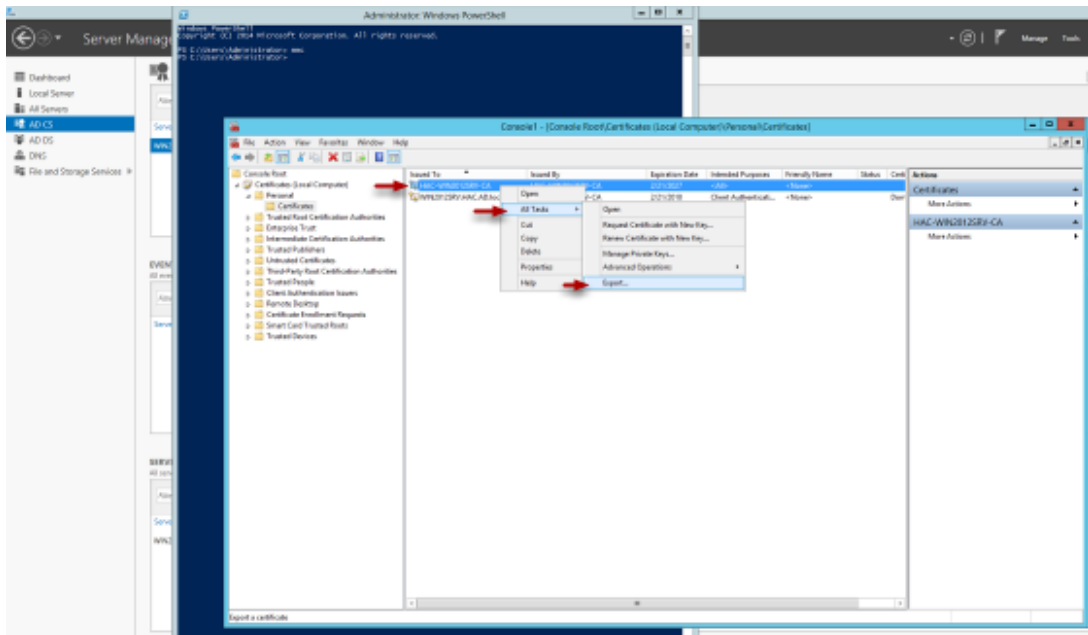
<https://www.virtuallyboring.com/setup-microsoft-active-directory-certificate-services-ad-cs/>

Durchsuchen Sie den LDAP-Server



Verwenden Sie einen LDAP-Browser und durchsuchen Sie die Struktur Ihres AD-Servers.

So rufen Sie das Active Directory-CA-Zertifikat vom Server ab

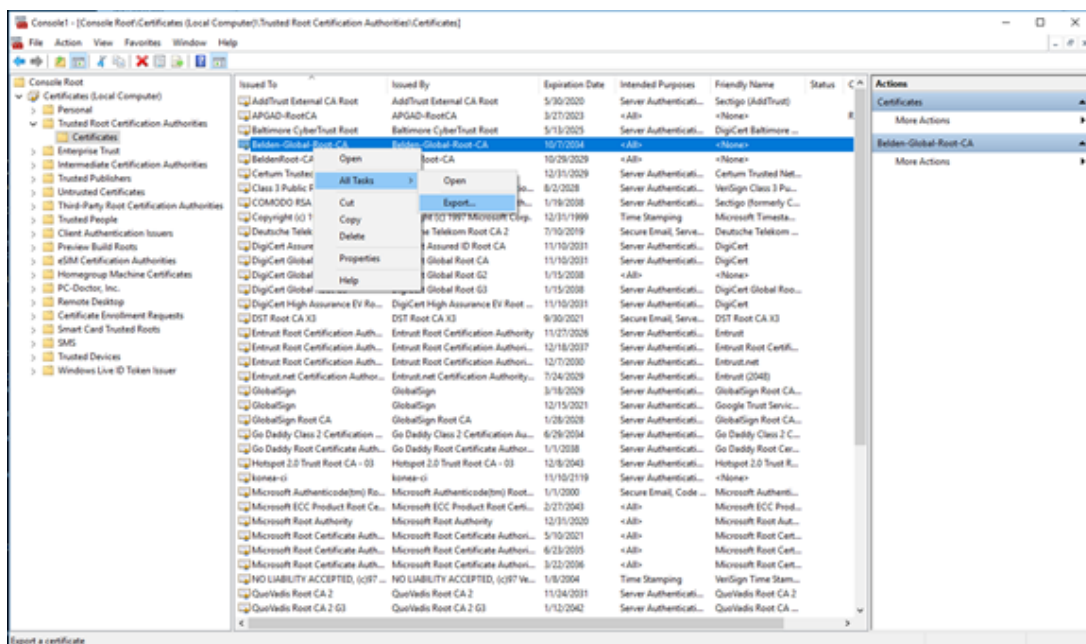


1. Stellen Sie eine Remote-Desktop-Verbindung her oder melden Sie sich an der Konsole eines DC an.
2. Starten Sie über Powershell die Microsoft Management Console, indem Sie MMC eingeben

und die Eingabetaste drücken

3. Wählen Sie im Menü FILE die Option ADD/REMOVE SNAP-IN
4. Wählen Sie CERTIFICATES und klicken Sie auf die Schaltfläche ADD
5. Wählen Sie COMPUTER ACCOUNT
6. Wählen Sie LOCAL COMPUTER
7. Klicken Sie auf FINISH
8. Klicken Sie auf OK
9. Erweitern Sie die CERTIFICATES
10. Erweitern Sie PERSONAL
11. Wählen Sie den DC im rechten Fenster.
12. Klicken Sie mit der rechten Maustaste auf den DC
13. Wählen Sie ALL TASKS - EXPORT
14. Klicken Sie auf NEXT (2 mal).
15. Wählen Sie Base-64-codiertes X.509 (.CER) aus und klicken Sie auf NEXT
15. Benennen Sie die Zertifikatsdatei (befindet sich auf dem DC)
16. Kopieren Sie die Datei und importieren Sie sie bei Bedarf

So rufen Sie das Active Directory-CA-Zertifikat von einem Client ab



To retrieve the AD server certificate from a client device:

1. open the Microsoft Management Console - Window-key+R and type mmc
2. Select File - Add/Remove Snap-in (CTRL+M) and add 'Certificates' for Computer account
3. Select Certificates (Local Computer) - Trusted Root Certification Authorities - Certificates from the tree structure
4. Highlight the Belden-Global-Root-CA certificate and select All Tasks - Export from the context menu (right click)
5. In the certificate export wizard select Base-64 encoded X.509 (.CER) format to export in file.

Authentifizierungsliste

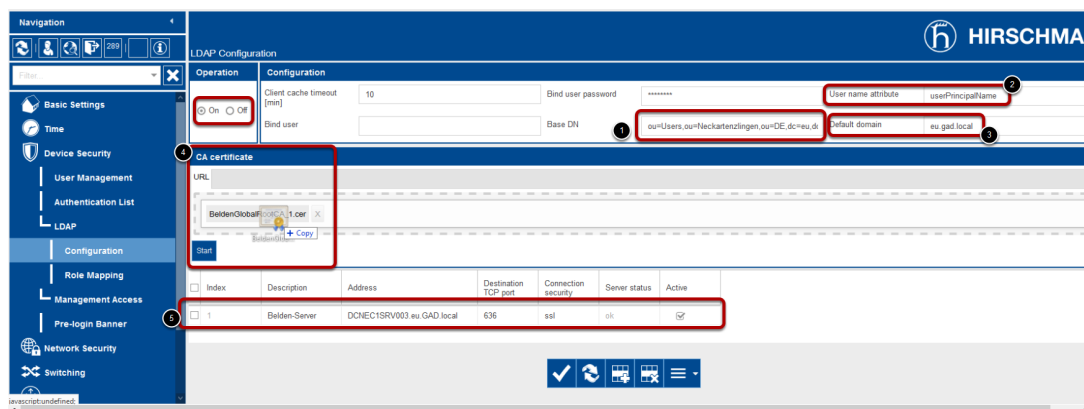


Name	Policy 1	Policy 2	Policy 3	Policy 4	Policy 5	Dedicated applications	Active
defaultDot1x8021AuthList	radius	reject	reject	reject	reject	8021x	<input checked="" type="checkbox"/>
defaultLdapAuthList	local	ldap	reject	reject	reject	SSH, Telnet, Webinterface	<input checked="" type="checkbox"/>
defaultV24AuthList	local	reject	reject	reject	reject	Console(V.24)	<input checked="" type="checkbox"/>

Ändern Sie die Richtlinien für die Authentifizierungsliste in LDAP.

Zum Testen setzen Sie LDAP an zweiter Stelle, bis Sie Ihre Konfigurationsarbeiten überprüft haben.

LDAP-Konfiguration



LDAP Configuration

Operation: On Off

Configuration:

Client cache timeout [min]: 10

Bind user password: *****

User name attribute: usePrincipalName

Bind user: [empty]

Base DN: ou=Users,ou=Heckertentzlingen,ou=DE,dc=eu,dc

Default domain: eu.gad.local

CA certificate: BeldenGlobalRootCA1.cer

Index	Description	Address	Destination TCP port	Connection security	Server status	Active
1	Belden-Server	DN:DC1SRV03.eu.GAD.local	636	ssl	ok	<input checked="" type="checkbox"/>

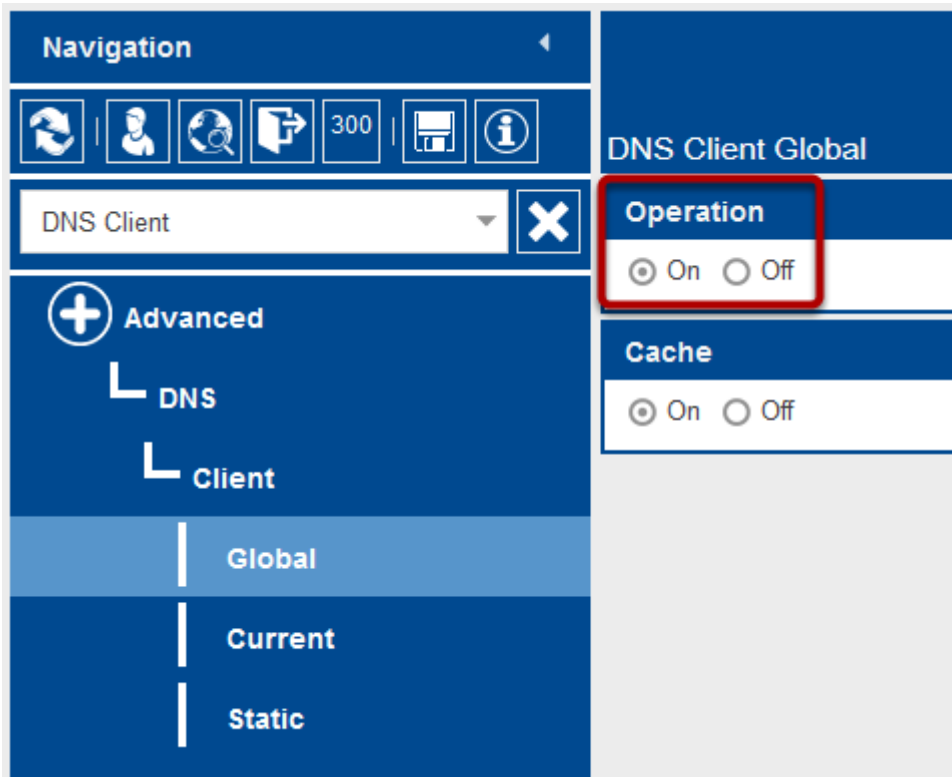
Operation: On

Konfiguration:

1. Base DN
2. User Name Attribute
3. Default domain
4. CA Certificate: Laden Sie das Serverzertifikat hoch, wenn Sie SSL oder TLS verwenden

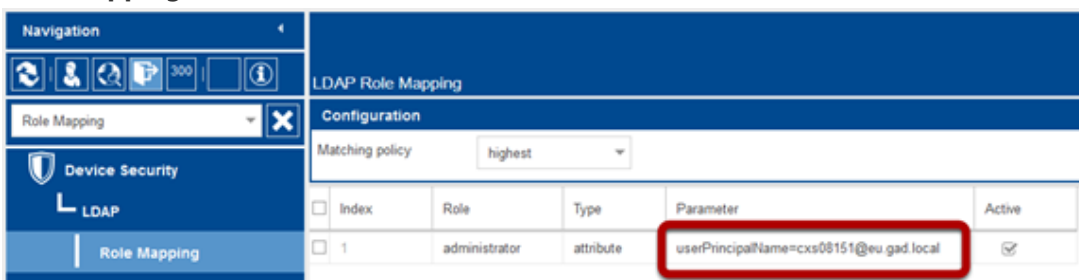
- Geben Sie den AD server, die Portnummer(normalerweise 389 or 636) an. In diesem Beispiel verwenden wir aufgrund des verwendeten Zertifikats einen Servernamen. Stellen Sie sicher, dass Sie auch den DNS-Client aktivieren (nächster Schritt)

Enable DNS Client



Aktivieren Sie den DNS-Client

Role Mapping



Erstellen Sie eine neue Rollenzuordnung.

Auswählbare Rollen sind nicht unauthorized, guest, auditor, operator und administrator

Ordnen Sie diese Rollen AD-Attributen oder -Gruppen zu.