Active Directory Sync

Niklas Leide - 2024-08-20 - Användarsynk

Notera att Skolons AD-synkmodul har passerat end-of-life och uppdateras inte längre. Vi rekommenderar alla kunder som har en AD-synk installerad att ta kontakt med oss för att ersätta med en synktyp som uppdateras löpande.

AD Synkmodul

Det här dokumentet kommer gå igenom hur AD Synkmodulen fungerar, först övergripande och sedan i mer teknisk detalj. Därefter går dokumentet igenom vilka krav som finns för att kunna integrera AD Synkmodulen.

Övergripande

AD Synkmodulen är ett program som installeras på en member server hos huvudmannen, därefter schemaläggs det när Synkmodulen ska skicka ut data från AD:t till Skolon. Synkmodulen kommer att kommunicera med Skolon via Skolons API.

Modulen bygger på LDAP-protokollet och kommer skicka information från AD:t gällande användare (elever och lärare), skoltillhörigheter, grupper och grupptillhörigheter.

Detalj

AD Synkmodul tillhandahålls i form av **sex filer**; en .exe-fil som schemaläggs på er member server och kör synken i valt intervall (exempelvis varje natt), en .config-fil som håller inställningar för det specifika AD:t. Förutom nämnda filer följer också fyra dll:er för loggning och anslutning till AD:t samt Skolon.

Krav

Struktur på AD

AD Synkmodulen läser användardata från OU, elever respektive lärare kan ligga i samma eller var sitt OU. För att avgöra vilken eller vilka skolor en användare tillhör används ett attribut på användaren. Vilka attribut som krävs samt vilka som finns tillgängliga beskrivs i under **AD Attribut**.

Skoltillhörighet

Vilken eller vilka skolor en användare tillhör bestäms av ett attribut på användaren. Om användaren tillhör flera skolor separeras de med kommatecken “,”. Exempelvis kan ett attribut innehålla: *<skolId1>,<skolId2>.* Vilket attribut som innehåller skolorna och vilken separator som ska användas konfigureras i config-filen.

Skolorna i attributet ska representeras med skolID, ett skolID är en unik identifierare för skolan. Varje skolID som används måste kommuniceras till Skolon för att koppla ihop till rätt skola och autentiseras.

Mer information finns under **Inställningar**.

Användartyp

Om lärare och elever ligger i samma OU krävs ett attribut på användaren som avgör om det är en lärare eller elev. Vilket attribut det är och vilka värden som motsvarar elev respektive lärare kan ställas in i config-filen med hjälp av ett filter. Detta behövs inte om lärare och elever ligger i olika OU.

OBS! I nuvarande version (5.1.1) krävs det att man anger något i filtret även om det inte behövs. Ange i så fall ett filter som alltid är sant.

Klasser och undervisningsgrupper

Det finns två olika sätt att skapa grupper i Skolon.

Modell 1

Modell 1 bygger på att varje användares klass- och grupptillhörigheter läses som attribut på användaren. För klasser används ett attribut som innehåller skolId sammanslaget med klassens namn i en kommaseparerad sträng enligt:

<skolId>-<klassnamn>,<skolId>-<klassnamn>,...

För elever består listan endast av en klass medan en lärare kan tillhöra flera.

På motsvarande sätt hanteras undervisningsgrupper med en kommaseparerad sträng enligt:

<skolId>-<gruppnamn>,<skolId>-<gruppnamn>,...

I detta fallet kan både lärare och elever tillhöra flera grupper.

SkolId som används gör att lärare och elever kan tillhöra flera olika skolor och tillhöra klasser och grupper på respektive skola. Vilket ID som ska användas som skolId bestäms beroende på vad som finns tillgängligt i miljön och kan väljas i konfigurationen. Grundprincipen är att det ska kunna identifiera en unik skola.

Istället för att använda kommaseparerade listor kan man använda multi-value attribut.

OBS! Vid många grupptillhörigheter kan attributet ha en begränsning i antal tecken som gör att alla medlemskap kommer med. Detta kan ni utöka med hjälp av att ändra i ert AD Schema.

Modell 2

Modell 2 bygger på att synken läser in grupperna från grupp-objekt i AD:t. Objektet behöver då innehålla ett member-attribut som är ett multi-value-attribut med användares distinguished names (dn). Gruppens namn blir i detta fallet objektets namn (cn). ID för gruppen (som gör den unik) är objectGUID. Både member-attribut, cn och objectGUID finns som standard på grupp-objekt i AD.

För att avgöra om gruppen är en klass eller undervisningsgrupp samt vilken skola gruppen tillhör används filter. Man kan ange ett filter för undervisningsgrupper och ett för klasser för varje skola.

Exempelvis kan man ange ett filter som söker efter grupper under en organizationalUnit (skola) med ett attribut groupType=CLASS för att hitta alla klasser för en skola.

Det finns möjlighet att formatera om namnen på klasser och grupper genom att använda regex. Då anges ett regex för att söka och ett för att ersätta utifrån resultatet.

OBS! I nuvarande version (5.1.1) krävs det att man anger något i filtret även om det inte behövs. Ange i så fall ett filter som alltid är sant.

AD Attribut
Nedan beskrivs objekten som behöver finnas i AD för respektive modell samt vilka attribut som krävs och är frivilliga.

4.2.1 Elever

Beskrivning	Attribut i AD
Obligatoriska attribut	
ID	SID (security identifier)
Förnamn	givenName

Efternamn	sn
SkolId (kan vara flera)	<konfigureras>
Rekommenderade attribut	
E-post	<konfigureras>
Klass (används för modell 1)	<konfigureras>
Grupper (används för modell 1)	<konfigureras>
Årskurs (F = förskola, 0-10 = grundskola, 11-14 = gymnasie, V = vuxenutbildning)	<konfigureras>
Valfria attribut	
Hemtelefon	homephone
Mobiltelefon	mobile
Adress	postalAddress
Postnummer	postalCode
Ort	l

Lärare

Från OU:t kan särskild personal filtreras ut att tas med i synken. Då anges vilket attribut som ska läsas och vilket värde attributet ska ha för att tas med. Exempelvis kan avdelning kan användas för att inte få med alla användare.

Beskrivning	**Attribut i AD**
Obligatoriska attribut	
ID	SID (security identifier)
Förnamn	givenName
Efternamn	sn
SkolId	<konfigureras>
Rekommenderade attribut	
E-post	<konfigureras>
Klasser (används för modell 1)	<konfigureras>

Grupper (används för modell 1)	<konfigureras>
Valfria attribut	
Hemtelefon	homephone
Mobiltelefon	mobile
Adress	postalAddress
Postnummer	postalCode
Ort	l

Grupper

Grupper gäller endast för modell 2. Gruppens namn hämtas från objektnamnet men kan manipuleras med regex.

Beskrivning	**Attribut i AD**
Obligatoriska attribut	
Medlemslista (lista med dn)	members
Grupptyp (klass eller undervisningsgrupp)	<konfigureras>

Inställningar

Vid installation av AD Synkmodul behövs ett antal grundinställningar, alla inställningar sköts i .config-filen som följer med vid leverans. Inställningarna berör exempelvis konfiguration av AD-struktur och mappning av attributen i det specifika AD:t. All konfiguration sköts via .config-filen som följer med vid leverans.

Förutom konfigurationen för AD:t behöver en mapp för loggning sättas upp och autensieringsparametrar från Skolon fyllas i. Autensieringsparametrarna tillhandahålls av Skolon och består av ett ClientId och en ClientSecret.

En annan viktig del är skolans identifierare mot Skolon. Detta kan antingen vara exempelvis en av skolenhetskoderna som används på skolan eller en egen skolnyckel. En skolnyckel är en godtycklig identifierare som väljs i samråd mellan skolan och Skolon. Oavsett vilken identifierare som väljs är det viktigt att bekräfta valet med Skolon då nyckeln måste aktiveras för den specifika skolans autensieringsparametrar.

Rättigheter

För att kunna synka upp data till Skolon krävs följande rättigheter. Användaren som kör .exe-filen behöver ha rättighet att läsa från AD samt ha skriv- och borttagningsrättigheter

till mappen för loggar (se mer info för konfiguration i **Inställningar**).

Miljö
För att kunna köra AD Synkmodul krävs .Net Framework 4.6 eller senare samt OLEDB Provider Microsoft.ACE.OLEDB.12.0.

Det krävs även att modulen har internetåtkomst för att kunna skicka data till Skolon API:et. Data skickas endast ut på port 443 (SSL).

Säkerhet

Data överförs från AD till Skolon och innefattar information om personer, grupper och skolor. Selektionen av data konfigureras av huvudman i AD-synken för att enkelt kunna filtrera bort data som inte är tillämplig.

Synk av data initieras av huvudman genom att schemalägga körning av AD-synken. Vanligen körs synken varje natt.

Anslutningar upprättas endast inifrån nätverket där AD-synken körs; nätverket/servern där AD-synken körs behöver alltså inte öppnas upp för anslutningar utifrån.

All överföring av data sker krypterat med protokollet TLS.

Autentiseringen baseras på OAuth2-standarden där varje synk har en egen uppsättning av nycklar (client ID och client secret) som tillsammans med skolID identifierar en skola. För varje synktillfälle autentiseras AD-synken och använder under synksessionen en sessionsbaserad token (access token).

Taggar
AD
Användarsynk
Onboarding