

Wat is het verschil tussen NTLM en LDAP-verificatie?

Inhoud

[vraag](#)

[Omgeving](#)

[Clientervaring](#)

[basisch](#)

[NTLM \(SSP\)](#)

[Security](#)

[basisch](#)

[NTLM \(SSP\)](#)

vraag

Wat is het verschil tussen NTLM en LDAP-verificatie?

Omgeving

Cisco web security applicatie (WSA), alle versies van AsyncOS

Verificatie met de WSA kan worden uitgesplitst in de volgende mogelijkheden:

Cliënt > WSA	WSA > Verificatieserver	Type verificatieserver
Basisauthenticatie	LDAP-verificatie	LDAP-server
Basisauthenticatie	LDAP-verificatie	Actieve Map-server met LDAP
Basisauthenticatie	NTLM Basis-verificatie	Active Directory server (NTLM Basic)
NTLM-verificatie	NTLMSSP-verificatie	Active Directory Server (NTLMSSP)

Opmerking: NTLMSSP wordt gewoonlijk NTLM genoemd.

Het opmerkelijke verschil tussen basisauthenticatie en NTLM - authenticatie is hieronder.

Clientervaring

basisch

De client wordt altijd gevraagd naar aanmeldingsgegevens. Nadat de referenties zijn ingevoerd, zullen browsers gewoonlijk een aanvinkvakje aanbieden om de bijgeleverde geloofsbrieven te onthouden. Elke keer dat de browser wordt gesloten, zal de client opnieuw oproepen of de eerder opgeslagen aanmeldingsgegevens opnieuw verzenden.

Opmerking: NTLM Basic gebruikt basisauthenticatie van de cliënt en zal dus dezelfde eigenschappen hebben.

NTLM (SSP)

- De client zal transparant authenticeren met behulp van zijn Windows-aanmeldingsgegevens.
- De enige gevallen waarin de cliënt voor geloofsbrieven zal vragen zijn als de geloofsbrieven van Windows eerst mislukken (dit zal voorkomen als de cliënt lokaal aan de computer en niet aan het domein wordt ingelogd gebruikt voor authenticatie) of als de cliënt geen WSA vertrouwt.

Security

basisch

Credentials worden met gewone tekst onveilig verstuurd. Een eenvoudige pakketvastlegging tussen de client en de WSA zal de gebruikersnaam EN het wachtwoord van de gebruiker onthullen.

NTLM (SSP)

Credentials worden veilig verstuurd via een handdruk die drie kanten op zou gaan (verteerbare Stijlenauthenticatie). Het wachtwoord wordt NOOIT via de bedrading verzonden.

Het NTLM-proces ziet er als volgt uit:

1. De client stuurt een NTLM-onderhandelingspakket. Dit vertelt de WSA dat de cliënt voornemens is NTLM-verificatie te doen.
2. De WSA stuurt een NTLM Challenge string naar de client.
3. De client gebruikt een algoritme gebaseerd op zijn wachtwoord om de uitdaging aan te passen en stuurt de uitdagingsreactie naar de WSA.
4. De AD server verifieert dan dat de client het juiste wachtwoord gebruikt gebaseerd op het al dan niet aanpassen van de challenge string.