

Active Directory-verificatie configureren in SWA

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Checklist](#)

[De Active Directory configureren](#)

[Stap 1. Verzamel de informatie van SWA](#)

[Stap 2. De DNS-records configureren in Active Directory](#)

[Stap 3. Active Directory Realm configureren](#)

[Probleemoplossing](#)

[SWA1 kan niet worden opgelost.*: * Fout met onbekende hostnaam](#)

[ADD1 kan niet worden opgelost.*: "Unknown hostname"-fout](#)

[Fout bij ophalen van Kerberos-tickets van server: "kinit: wachtwoord incorrect" Fout](#)

[Kan niet deelnemen aan domein: account niet vooraf gemaakt: "onvoldoende toegang"](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de stappen voor het configureren van Active Directory-verificatie in Secure Web Appliance (SWA).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SWA-beheer.
- Basisprotocollen voor netwerken en proxy's.
- Basis Active Directory-beheer.

Cisco raadt u aan deze hulpprogramma's te installeren:

- Fysieke of virtuele SWA.
- Administratieve toegang tot de grafische gebruikersinterface (GUI) van SWA.
- Toegang tot de Active Directory.

Gebruikte componenten


Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Checklist

Voordat u SWA verbindt met Active Directory, moet u controleren of alle vereiste controles zijn uitgevoerd:

- SWA heeft goede netwerktoegang tot de Active Directory. voor meer informatie kunt u terecht op: [Firewall configureren voor Secure Web Appliance](#).
- DNS-record voor SWA-hostnaam wordt gemaakt in de Active Directory. (CLI > sethostname)

 Opmerking: zorg er in de transparante modus voor dat de hostnaam van de Secure Web Appliance overeenkomt met de hostnaam voor omleiden.



- DNS-records voor SWA-interfaces worden gemaakt in de Active Directory.
- Vergelijk de huidige tijd op de Secure Web Appliance met de tijd op de Active Directory-server en zorg ervoor dat het verschil niet groter is dan de waarde die is gedefinieerd in de instelling "Maximale tolerantie voor kloksynchronisatie van de computer" op de Active Directory-server.
- Bevestig dat u over de benodigde machtigingen en domeingegevens beschikt om u aan te melden bij de Secure Web Appliance voor het Active Directory-domein dat u wilt gebruiken voor verificatie.
 - Maak een gebruiker aan op de Active Directory-server die lid is van de groep Domeinbeheerders of Accountbeheerders.
 - U kunt ook een gebruiker maken met de minimaal vereiste machtigingen: Wachtwoord

opnieuw instellen, Gevalideerd schrijven naar servicePrincipalName, accountbeperkingen schrijven, Write dNSHostName en Write servicePrincipalName. Deze machtigingen zijn voldoende om het toestel aan het domein toe te voegen en de volledige functionaliteit te garanderen.

- Zorg ervoor dat SWA de Active Directory FQDN kan oplossen.

De Active Directory configureren

Gebruik deze stappen om een upstream-proxy in SWA te configureren.

Stappen	Details
Stap 1. Verzamel de informatie van SWA	<p>Stap 1.1. Van SWA CLI, runsethostname om de huidige SWA-hostnaam te bekijken.</p> <p> Opmerking: Als u de huidige hostnaam wilt wijzigen, typt u de nieuwe hostnaam en drukt u op Enter en legt u vervolgens wijzigingen vast door de opdracht commit uit te voeren.</p> <p>Stap 1.2. Navigeer vanuit de SWA GUI naar Netwerk, selecteer Interfaces, om de FQDN-interfaces te bekijken. Als u de huidige FQDN-interfaces wilt wijzigen, klikt u op Instellingen bewerken en voert u de wijzigingen in opdracht uit.</p> <p>Stap 1.3. Vanuit de SWA GUI, navigeer naar Systeembeheer en klik op Tijdinstellingen, zorg ervoor dat de NTP-instellingen correct zijn.</p> <p>Stap 1.4. Navigeer vanuit SWA GUI naar Netwerk, selecteer DNS, zorg ervoor dat de juiste DNS-server is gedefinieerd.</p> <p> Tip: Als SWA is geconfigureerd met een openbare DNS-server en u wilt een andere DNS-server definiëren voor uw Active Directory-domein, klikt u op Instelling bewerken en selecteert u in de sectie Alternatieve DNS-servers overschrijvingen (optioneel) de Active Directory-domeinnaam en het IP-adres van de DNS-server, dient u wijzigingen in en legt u deze vast.</p>

Edit DNS

DNS Server Settings

Primary DNS Servers: Use these DNS Servers

Priority (?)	Server IP Address	
0	172.38.200.100	<input type="button" value="Add Row"/>

Alternate DNS servers Overrides (Optional):

Domain(s)	DNS Server IP Address(es)	
amojarra.amojarra	10.48.48.17	<input type="button" value="Add Row"/>

i.e., example.com, example2.com i.e., 10.0.0.3 or 2001:420:80:1::5

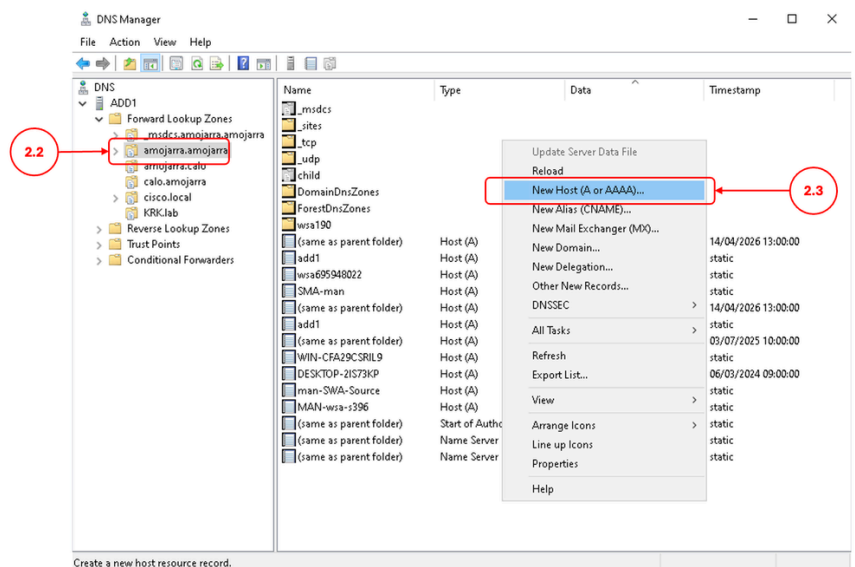
Afbeelding - Alternatieve DNS-servers toevoegen

Stap 2. De DNS-records configureren in Active Directory

Stap 2.1. Maak verbinding met uw Active Directory-server en navigeer naar de DNS Manager-console.

Stap 2.2. Selecteer de gewenste domeinnaam in het linkerdeelvenster.

Stap 2.3. Klik met de rechtermuisknop in het rechterdeelvenster en kies Nieuwe host (A of AAAA)



Afbeelding - Een nieuw A-record maken

Stap 2.4. Het DNS-record definiëren voor de SWA-hostnaam (verzameld in stap 1.1)



Waarschuwing: Als de Active Directory via de beheerinterface verbinding maakt met de SWA, definieert u het IP-adres voor beheer, anders definieert u het juiste IP-adres van de SWA waartoe Active Directory toegang heeft (IP-adres voor P1-interface of IP-adres voor P2-interface)

Stap 2.5. Definieer het DNS-record voor elke SWA-interface.

Stap 2.6. (Optioneel) Als u High Availability gebruikt, definieert u een DNS-record voor de FQDN met hoge beschikbaarheid met het gedefinieerde virtuele IP-adres.

Stap 3. Active Directory Realm configureren

Stap 3.1. Navigeer vanuit de SWA GUI naar Netwerk, selecteer Verificatie.

Stap 3.2. Klik op Rijk toevoegen.

Stap 3.3. Definieer een domeinnaam.

Stap 3.4. Kies Active Directory uit het type en schema(s) van de verificatieserver.

Stap 3.5. Standaard gebruikt SWA de beheerinterface om verbinding te maken met de Active Directory. Als u deze instellingen wilt wijzigen, klikt u op Broninterface instellen en kiest u de gewenste interface.

Stap 3.6. Definieer de hostnaam of het IP-adres van de Active Directory Domain Controller(s).

Stap 3.7. Voer de naam van het Active Directory-domein in.

Stap 3.8. (Optioneel) Als u de computeraccount wilt opslaan in een andere organisatie-eenheid (OU) in de Active Directory, moet u de gewenste locatie definiëren

Stap 3.9. Klik op Domein aanmelden.

Afbeelding - Realm toevoegen

Stap 3.10. Voer de gebruikersnaam en het wachtwoord in en klik op Deelnemen.



Tip: Vermeld de domeinnaam niet bij de



gebruikersnaam (voer bijvoorbeeld "SWA_ADMIN" in plaats van "DOMAIN\SWA_ADMIN" of "SWA_ADMIN@domain").

Add Realm

Success — Computer Account swa1\$ successfully created.

Afbeelding - SWA is met succes aan het AD toegevoegd

Stap 3.11. voorleggen

Stap 3.12. Verbind de veranderingen.

Probleemoplossing



Waarschuwing: de scheve klok tussen WSA- en AD-server is te groot

Deze fout geeft aan dat de tijd tussen de Active Directory en de SWA niet is gesynchroniseerd. Gebruik stap 1.3 om de tijd op de SWA te corrigeren


Warning: Clock skew between WSA 'Thu Apr 16 08:25:17 2026' and AD server 'Wed Apr 15 08:30:30 2026' is
Warning: Clock skew between WSA 'Thu Apr 16 08:25:17 2026' and AD server 'Wed Apr 15 08:30:30 2026' is

SWA1 kan niet worden opgelost.*. * Fout met onbekende hostnaam

Deze fout geeft aan dat de SWA zijn eigen interface en de hostnaam niet via de DNS-server kan oplossen. Bevestig dat de SWA is geconfigureerd met de juiste DNS-server (stap 1.4) en zie stap

2 om de ontbrekende DNS-records te maken.


Failure: Unable to resolve 'swa1.amojarra.amojarra' : Unknown hostname

 Tip: Als u na het corrigeren van de DNS-server of DNS-records nog steeds dezelfde fout ontvangt, wist u de DNS-cache van GUI > Netwerk > DNS > DNS-cache wissen.

ADD1 kan niet worden opgelost.*.*: "Unknown hostname"-fout

Deze fout geeft aan dat de SWA de DNS-records met betrekking tot de Active Directory niet kan oplossen. Gebruik stap 1.4 om de juiste DNS-server voor uw Active Directory-domein te configureren.

Failure: Unable to resolve 'ADD1.amojarra.amojarra' : Unknown hostname

 Tip: Als u na het corrigeren van de DNS-server of DNS-records nog steeds dezelfde fout ontvangt, wist u de DNS-cache van GUI > Netwerk > DNS > DNS-cache wissen.

Fout bij ophalen van Kerberos-tickets van server: "kinit: wachtwoord incorrect" Fout

Deze fout geeft aan dat de gebruikersnaam of het wachtwoord dat is gebruikt om verbinding te maken met de Active Directory onjuist is.

Failure: Error while fetching Kerberos Tickets from server '10.48.48.17' : kinit: Password incorrect

Kan niet deelnemen aan domein: account niet vooraf gemaakt: "onvoldoende toegang"

Deze fout geeft aan dat de gebruiker niet over de minimaal vereiste rechten beschikt om de computeraccount aan te maken. Controleer de gebruikersrechten volgens de sectie Checklist in dit artikel.

Failure: Error while joining WSA onto server '10.48.48.17' : ads_print_error: AD LDAP ERROR: 50 (Insuff

Gerelateerde informatie

- [Gebruikershandleiding voor AsyncOS 15.0 voor Cisco Secure Web Appliance](#)
- [Firewall configureren voor Secure Web Appliance](#)
- [Aangepaste URL-categorieën configureren in Secure Web Appliance - Cisco](#)
- [Hoe Office 365-verkeer vrij te stellen van verificatie en decodering op Cisco Web Security Appliance \(WSA\) - Cisco](#)
- [Best practices voor veilige webapparaten gebruiken - Cisco](#)
- [Verkeer blokkeren in Secure Web Appliance](#)
- [Uploadverkeer blokkeren in Secure Web Appliance](#)
- [Executable File Download blokkeren in SWA](#)
- [Microsoft Updates-verkeer omzeilen in Secure Web Appliance](#)
- [Verificatie omzeilen in Secure Web Appliance - Cisco](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.