Konfigurieren der Active Directory-Authentifizierung in SWA

Inhalt

Einleitung

In diesem Dokument werden die Schritte zum Konfigurieren der Active Directory-Authentifizierung in der Secure Web Appliance (SWA) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- SWA-Verwaltung.
- Grundlegende Netzwerk- und Proxy-Protokolle.
- Grundlegende Active Directory-Verwaltung.

Cisco empfiehlt die Installation der folgenden Tools:

- Physisches oder virtuelles SWA.

- Administrator-Zugriff auf die grafische Benutzeroberfläche (GUI) von SWA
- Administrator-Zugriff auf das Active Directory

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Checkliste

Stellen Sie vor dem Verbinden von SWA mit Active Directory sicher, dass alle erforderlichen Prüfungen durchgeführt wurden:

- SWA hat ordnungsgemäßen Netzwerkzugriff auf das Active Directory. Weitere Informationen finden Sie unter: Konfigurieren der Firewall für die sichere Web-Appliance
- Der DNS-Eintrag für den SWA-Hostnamen wird im Active Directory erstellt. (CLI > sethostname)

Anmerkung: Stellen Sie im transparenten Modus sicher, dass der Hostname der sicheren Webappliance mit dem Hostnamen der Umleitung übereinstimmt.

- DNS-Einträge für SWA-Schnittstellen werden im Active Directory erstellt.

- Vergleichen Sie die aktuelle Uhrzeit auf der sicheren Web-Appliance mit der Uhrzeit auf dem Active Directory-Server, und stellen Sie sicher, dass die Differenz den Wert nicht überschreitet, der in der Einstellung "Maximale Toleranz für die Synchronisierung der Computeruhr" auf dem Active Directory-Server definiert wurde.

- Bestätigen Sie, dass Sie über die erforderlichen Berechtigungen und Domäneninformationen verfügen, um der sicheren Webappliance zur Active Directory-Domäne beizutreten, die Sie für die Authentifizierung verwenden möchten.

    - Erstellen Sie einen Benutzer auf dem Active Directory-Server, der Mitglied der Gruppe Domänenadministratoren oder Kontooperatoren ist.

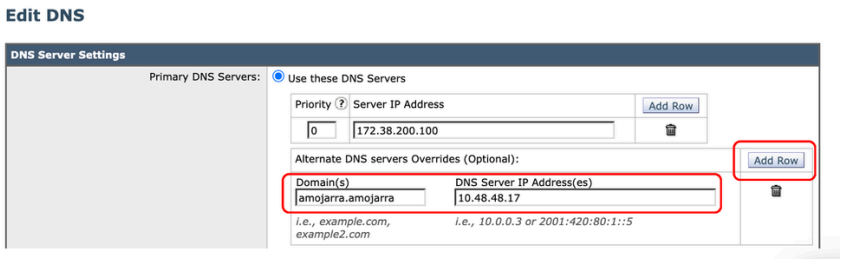
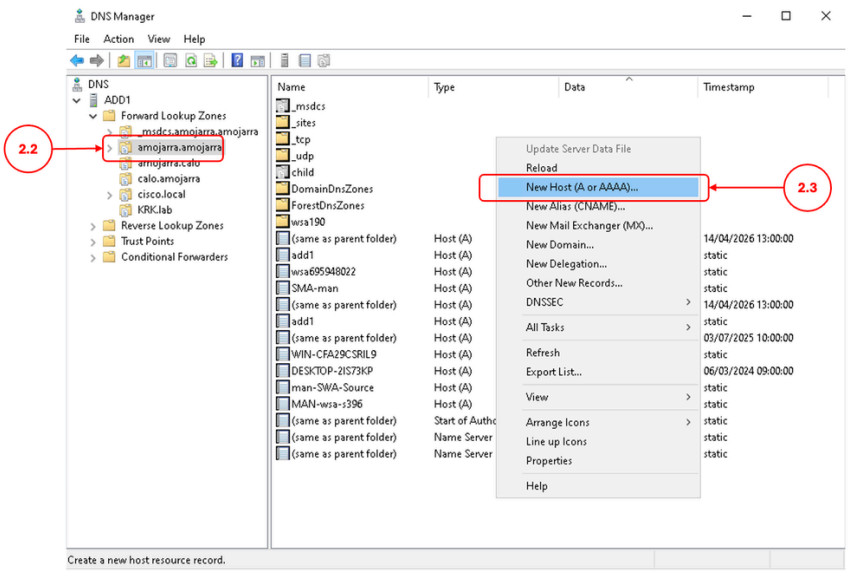
- Sie können auch einen Benutzer mit den erforderlichen Mindestberechtigungen erstellen: Zurücksetzen des Kennworts, Validierte Schreibvorgänge auf servicePrincipalName, Schreibzugriffsbeschränkungen, Write dNSHostName und Write servicePrincipalName (Schreibzugriff auf PrincipalName). Diese Berechtigungen reichen aus, um die Appliance der Domäne beizutreten und die volle Funktionalität sicherzustellen.

- Stellen Sie sicher, dass SWA den Active Directory-FQDN auflösen kann.

Konfigurieren von Active Directory

Gehen Sie folgendermaßen vor, um einen Upstream-Proxy in SWA zu konfigurieren.

Schritte	Details
Schritt 1: Sammeln Sie die Informationen von der SWA	Schritt 1.1. Geben Sie in der SWA-CLI runsethostname ein, um den aktuellen SWA-Hostnamen anzuzeigen. Anmerkung: Wenn Sie den aktuellen Hostnamen ändern möchten, geben Sie den neuen Hostnamen ein, und drücken Sie die Eingabetaste. Übertragen Sie die Änderungen dann mit dem Befehl commit. Schritt 1.2. Navigieren Sie in der SWA-GUI zu Netzwerk, wählen Sie Schnittstellen, um den Schnittstellen-FQDN anzuzeigen. Wenn Sie den aktuellen Schnittstellen-FQDN ändern möchten, klicken Sie auf Einstellungen bearbeiten, und nehmen Sie die Änderungen vor, und bestätigen Sie sie mit. Schritt 1.3: Navigieren Sie in der SWA-GUI zu Systemverwaltung, und klicken Sie auf Zeiteinstellungen. Vergewissern Sie sich, dass die NTP-Einstellungen korrekt sind. Schritt 1.4: Navigieren Sie in der SWA-GUI zu Network (Netzwerk), wählen Sie DNS aus, und stellen Sie sicher, dass der richtige DNS-Server definiert ist. Tipp: Wenn SWA mit einem öffentlichen DNS-Server konfiguriert ist und Sie einen anderen DNS-Server für Ihre Active Directory-Domäne definieren möchten, klicken Sie auf Einstellung bearbeiten, und legen Sie

	🔎 im Abschnitt Alternative DNS-Server-Überschreibungen (optional) den Active Directory-Domänennamen und die IP-Adresse des DNS-Servers fest, übermitteln Sie die Änderungen und bestätigen Sie sie.  Image: Hinzufügen alternativer DNS-Server
Schritt 2: Konfigurieren der DNS-Einträge in Active Directory	Schritt 2.1. Stellen Sie eine Verbindung mit dem Active Directory-Server her, und navigieren Sie zur DNS Manager-Konsole. Schritt 2.2. Wählen Sie den gewünschten Domänennamen im linken Bereich aus. Schritt 2.3. Klicken Sie im rechten Bereich mit der rechten Maustaste, und wählen Sie Neuer Host (A oder AAAA)  Bild - Neuen A-Datensatz erstellen Schritt 2.4: Definieren des DNS-Datensatzes für den SWA-Hostnamen (erfasst in Schritt 1.1) ⚠ Vorsicht: Wenn Active Directory über die

	⚠ Verwaltungsschnittstelle eine Verbindung mit dem SWA herstellt, definieren Sie die Management-IP-Adresse, andernfalls definieren Sie die richtige IP-Adresse des SWA, auf das Active Directory Zugriff hat (IP-Adresse der P1-Schnittstelle oder IP-Adresse der P2-Schnittstelle). Schritt 2.5: Definieren Sie den DNS-Datensatz für jede SWA-Schnittstelle. Schritt 2.6. (Optional) Wenn Sie High Availability verwenden, definieren Sie einen DNS-Eintrag für den High Availability FQDN mit der definierten virtuellen IP-Adresse.
Schritt 3: Active Directory-Bereich konfigurieren	Schritt 3.1. Navigieren Sie in der SWA-GUI zu Netzwerk, und wählen Sie Authentifizierung aus. Schritt 3.2: Klicken Sie auf Bereich hinzufügen. Schritt 3.3: Definieren eines Bereichsnamens. Schritt 3.4: Wählen Sie unter Authentication Server Type (Authentifizierungsservertyp) und Scheme(s) (Schema(s)) Active Directory aus. Schritt 3.5. Standardmäßig verwendet SWA die Verwaltungsschnittstelle, um eine Verbindung mit Active Directory herzustellen. Wenn Sie diese Einstellungen ändern möchten, klicken Sie auf Quellschnittstelle festlegen, und wählen Sie die gewünschte Schnittstelle aus. Schritt 3.6: Definieren Sie den Hostnamen oder die IP-Adresse der Active Directory-Domänencontroller. Schritt 3.7: Geben Sie den Namen der Active Directory-Domäne ein. Schritt 3.8. (Optional) Wenn Sie das Computerkonto in einer anderen Organisationseinheit (OU) im Active Directory speichern möchten, definieren Sie den gewünschten Speicherort Schritt 3.9. Klicken Sie auf Domäne beitreten.

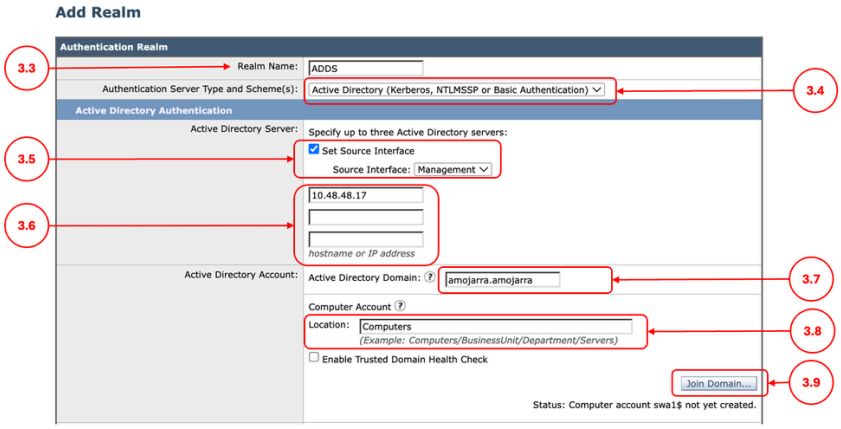


Bild - Bereich hinzufügen

Schritt 3.10: Geben Sie den Benutzernamen und das Passwort ein und klicken Sie auf Join (Teilnehmen).

Tipp: Fügen Sie dem Benutzernamen nicht den Domänennamen hinzu (geben Sie beispielsweise "SWA_ADMIN" statt "DOMAIN\SWA_ADMIN" oder "SWA_ADMIN@domain" ein).

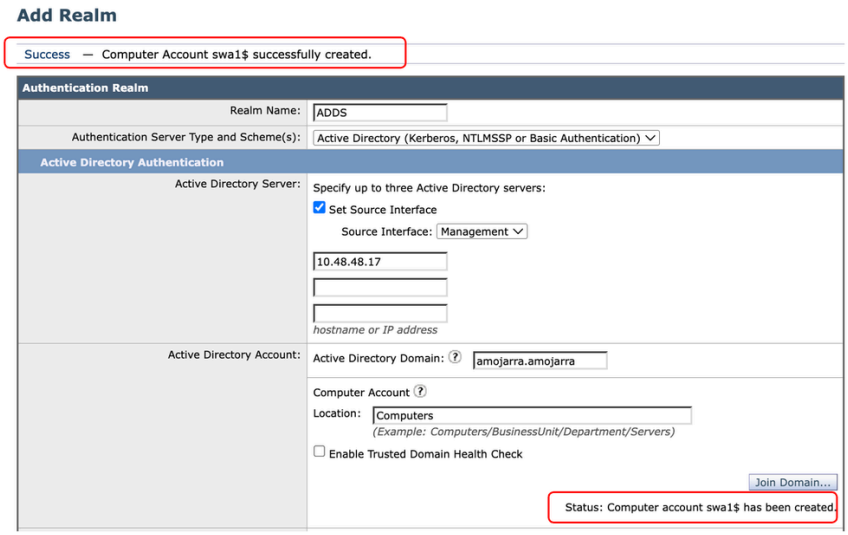


Bild - SWA erfolgreich bei der Werbeschaltung

Schritt 3.11: Senden

Schritt 3.12: Bestätigen Sie die Änderungen.

Fehlerbehebung

Warnung: Zeitdifferenz zwischen WSA- und AD-Server ist zu groß

Dieser Fehler zeigt an, dass die Zeit zwischen Active Directory und SWA nicht synchronisiert ist. Verwenden Sie Schritt 1.3, um die Uhrzeit auf der SWA zu korrigieren.

```
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.*.* "Unbekannter Hostname" konnte nicht aufgelöst werden

Dieser Fehler zeigt an, dass der SWA seine eigene Schnittstelle und den Hostnamen nicht über den DNS-Server auflösen kann. Bestätigen Sie, dass die SWA mit dem richtigen DNS-Server konfiguriert ist (Schritt 1.4), und legen Sie Schritt 2 fest, um die fehlenden DNS-Einträge zu erstellen.

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

Tipp: Wenn Sie nach dem Korrigieren des DNS-Servers oder der DNS-Einträge immer noch den gleichen Fehler erhalten, löschen Sie den DNS-Cache aus GUI > Network > DNS > Clear DNS Cache.

ADD1.*.* kann nicht aufgelöst werden: "Unbekannter Hostname" fehlgeschlagen

Dieser Fehler zeigt an, dass der SWA die DNS-Einträge für das Active Directory nicht auflösen kann. Verwenden Sie Schritt 1.4, um den richtigen DNS-Server für Ihre Active Directory-Domäne zu konfigurieren.

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

Tipp: Wenn Sie nach der Korrektur des DNS-Servers oder der DNS-Einträge immer noch den gleichen Fehler erhalten, löschen Sie den DNS-Cache aus GUI > Network > DNS > Clear DNS Cache (GUI > DNS > Löschen des DNS-Caches).

Fehler beim Abrufen der Kerberos-Tickets vom Server: "Kinit: Passwort falsch" Fehler

Dieser Fehler zeigt an, dass der Benutzername oder das Kennwort für die Verbindung mit dem Active Directory falsch sind.

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

Domäne kann nicht beitreten: Fehler beim Erstellen des Kontos: "Unzureichender Zugriff"

Dieser Fehler zeigt an, dass der Benutzer nicht über die erforderlichen Mindestberechtigungen zum Erstellen des Computerkontos verfügt. Bitte überprüfen Sie die Benutzerberechtigungen gemäß dem Abschnitt "Checkliste" in diesem Artikel.

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

Zugehörige Informationen

- Bedienungsanleitung für AsyncOS 15.0 für Cisco Secure Web Appliance
- Firewall für sichere Web-Appliance konfigurieren
- Benutzerdefinierte URL-Kategorien in einer sicheren Web-Appliance konfigurieren - Cisco
- Wie kann Office 365-Datenverkehr auf der Cisco Web Security Appliance (WSA) von der Authentifizierung und Entschlüsselung ausgenommen werden - Cisco
- Best Practices für sichere Web-Appliances - Cisco
- Blockieren von Datenverkehr in einer sicheren Web-Appliance
- Upload-Verkehr in sicherer Web-Appliance blockieren
- Download ausführbarer Dateien in SWA blockieren
- Umgehen des Datenverkehrs von Microsoft Updates in einer sicheren Web-Appliance
- Umgehung der Authentifizierung in einer sicheren Web-Appliance - Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.