Configurer l'authentification Active Directory dans SWA

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Liste De Contrôle

Configuration d'Active Directory

- Étape 1 : collecte des informations auprès de SWA
- Étape 2 : configuration des enregistrements DNS dans Active Directory
- Étape 3 : configuration du domaine Active Directory

Dépannage

- Impossible de résoudre swa1.*.* "Nom d'hôte inconnu" Échec
- Impossible de résoudre ADD1.*.* : Échec de « Nom d'hôte inconnu »
- Erreur lors de la récupération des tickets Kerberos du serveur : "kinit : Mot de passe incorrect" Échec
- Impossible de joindre le domaine : Échec de la précréation du compte : "Accès insuffisant"

Autres informations utiles

Introduction

Ce document décrit les étapes à suivre pour configurer l'authentification Active Directory dans l'appareil Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration SWA.
- Protocoles réseau et proxy de base.
- Administration Active Directory de base.

Cisco recommande d'installer les outils suivants :

- SWA physique ou virtuel.

- Accès administratif à l'interface utilisateur graphique (GUI) de SWA.
- Accès administratif à Active Directory.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Liste De Contrôle

Avant de connecter SWA à Active Directory, assurez-vous que toutes les vérifications requises ont été effectuées :

- SWA a un accès réseau approprié à Active Directory. pour plus d'informations, consultez : Configurer le pare-feu pour l'appliance Web sécurisée
- L'enregistrement DNS du nom d'hôte SWA est créé dans Active Directory. (CLI > nom_hôte).

Remarque : En mode transparent, assurez-vous que le nom d'hôte de l'appliance Web sécurisée correspond au nom d'hôte de redirection.

- Les enregistrements DNS pour les interfaces SWA sont créés dans Active Directory.

- Comparez l'heure actuelle sur l'appareil Web sécurisé avec l'heure sur le serveur Active Directory et assurez-vous que la différence ne dépasse pas la valeur définie dans le paramètre « Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur » sur le serveur Active Directory.

- Vérifiez que vous disposez des autorisations et des informations de domaine nécessaires pour joindre l'appareil Web sécurisé au domaine Active Directory que vous souhaitez utiliser pour l'authentification.

    - Créez un utilisateur sur le serveur Active Directory qui est membre du groupe Administrateurs du domaine ou Opérateurs de compte.

- Vous pouvez également créer un utilisateur avec les autorisations minimales requises : Reset Password, Validated write to servicePrincipalName, Write account restrictions, Write dNSHostName et Write servicePrincipalName. Ces autorisations sont suffisantes pour joindre l'appliance au domaine et assurer le fonctionnement complet.

- Assurez-vous que SWA peut résoudre le nom de domaine complet Active Directory.

Configuration d'Active Directory

Suivez ces étapes pour configurer l'authentification Active Directory dans SWA.

Étapes	Détails
Étape 1 : collecte des informations auprès de SWA	Étape 1.1. À partir de SWA CLI, exécutez sethostname pour afficher le nom d'hôte SWA actuel. Remarque : Pour modifier le nom d'hôte actuel, tapez le nouveau nom d'hôte et appuyez sur Entrée, puis validez les modifications en exécutant la commande commit. Étape 1.2. À partir de l'interface utilisateur graphique SWA, accédez à Network, sélectionnez Interfaces, pour afficher les interfaces FQDN. Pour modifier le nom de domaine complet des interfaces actuelles, cliquez sur Edit Settings et effectuez les modifications, puis validez. Étape 1.3. À partir de l'interface utilisateur graphique de SWA, accédez à Administration système et cliquez sur Time Settings, vérifiez que les paramètres NTP sont corrects. Étape 1.4. Dans l'interface utilisateur graphique de SWA, accédez à Network, sélectionnez DNS, vérifiez que le serveur DNS correct est défini. Conseil : Si SWA est configuré avec un serveur DNS public, pour définir un serveur DNS différent pour votre domaine Active Directory, cliquez sur Edit Setting et dans la section Alternate DNS servers Overrides (Optional), définissez le nom de domaine Active Directory et l'adresse IP du serveur DNS, puis soumettez et validez les modifications.

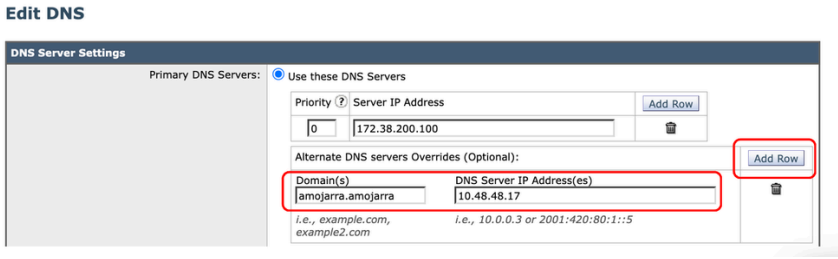
<table>
<tr><td></td><td>

Image - Ajouter d'autres serveurs DNS</td></tr>
<tr><td>Étape 2 : configuration des enregistrements DNS dans Active Directory</td><td>Étape 2.1. Connectez-vous à votre serveur Active Directory et accédez à la console Gestionnaire DNS.

Étape 2.2. Sélectionnez le nom de domaine souhaité dans le panneau de gauche.

Étape 2.3. Dans le panneau droit, cliquez avec le bouton droit et sélectionnez New Host (A ou AAAA)

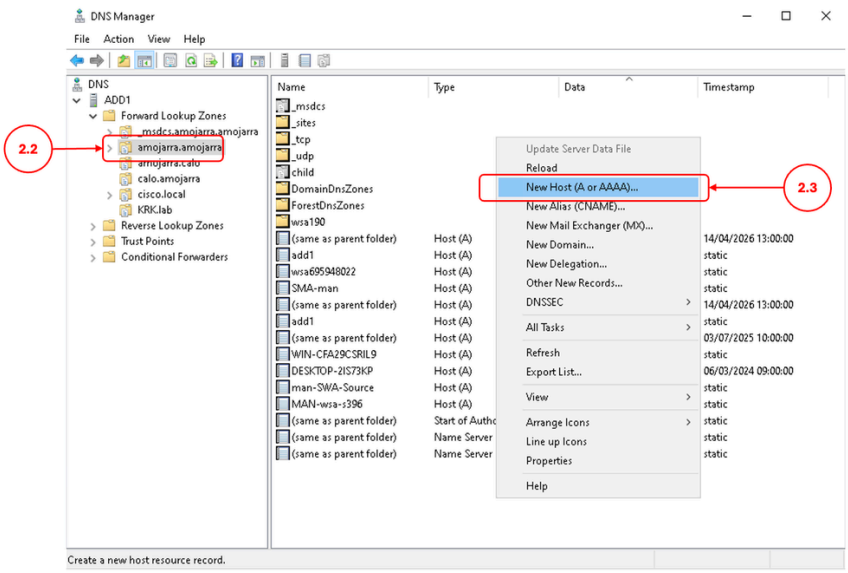
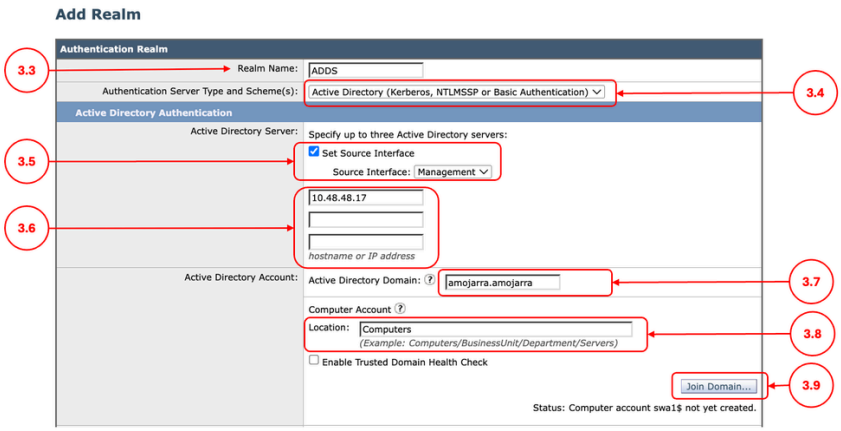


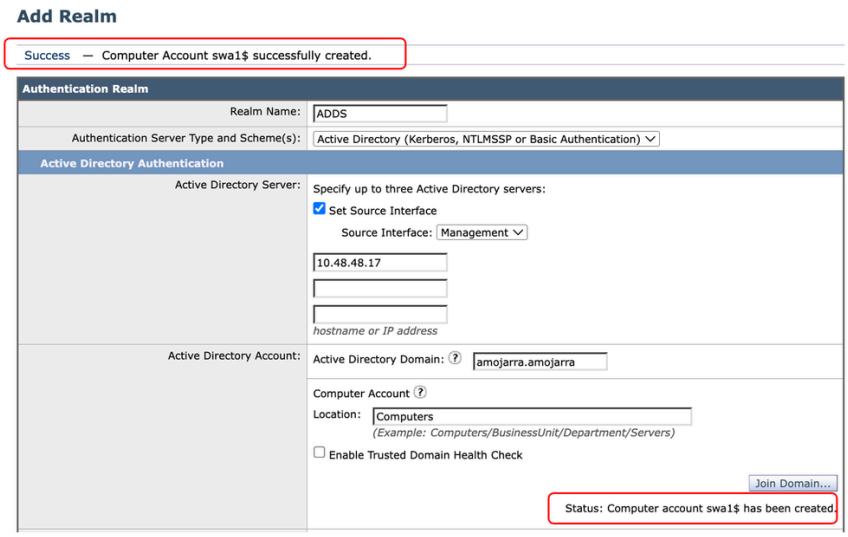
Image - Créer un nouvel enregistrement A

Étape 2.4 : définition de l’enregistrement DNS pour le nom d’hôte SWA (collecté à l’étape 1.1)

⚠ Mise en garde : Si Active Directory se connecte au SWA via l'interface de gestion, définissez l'adresse IP de gestion, sinon définissez l'adresse IP correcte du SWA auquel Active Directory a accès (adresse IP d'interface P1 ou adresse IP d'interface P2)

Étape 2.5. Définition de l’enregistrement DNS pour chaque interface SWA</td></tr>
</table>

	Étape 2.6. (Facultatif) Si vous utilisez la haute disponibilité, définissez un enregistrement DNS pour le nom de domaine complet haute disponibilité avec l'adresse IP virtuelle définie.
Étape 3 : configuration du domaine Active Directory	Étape 3.1. Dans l'interface utilisateur graphique de SWA, accédez à Network, sélectionnez Authentication. Étape 3.2. Cliquez sur Add Realm. Étape 3.3. Définition d'un nom de domaine. Étape 3.4. Dans Authentication Server Type and Scheme(s), sélectionnez Active Directory. Étape 3.5. Par défaut, SWA utilise l'interface de gestion pour se connecter à Active Directory. Pour modifier ces paramètres, cliquez sur Définir l'interface source et choisissez l'interface souhaitée. Étape 3.6. Définissez le nom d'hôte ou l'adresse IP du ou des contrôleurs de domaine Active Directory. Étape 3.7. Entrez le nom de domaine Active Directory. Étape 3.8. (Facultatif) Pour stocker le compte d'ordinateur dans une unité d'organisation (OU) différente dans Active Directory, définissez l'emplacement souhaité Étape 3.9. Cliquez sur Join Domain.  Image - Ajouter un domaine Étape 3.10. Entrez le nom d'utilisateur et le mot de passe, puis cliquez sur Join. Conseil : n'incluez pas le nom de domaine avec le nom

	d'utilisateur (par exemple, saisissez « SWA_ADMIN » plutôt que « DOMAIN\SWA_ADMIN » ou « SWA_ADMIN@domain »).  Image - SWA a rejoint AD avec succès Étape 3.11. Envoyer. Étape 3.12. Validez les modifications.

Dépannage

Avertissement : Le décalage d'horloge entre le serveur WSA et AD est trop important.

Cette erreur indique que l'intervalle de temps entre Active Directory et le SWA n'est pas synchronisé. Utilisez l'étape 1.3. pour corriger l'heure sur le SWA

```
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
```

Impossible de résoudre swa1.*.* "Nom d'hôte inconnu" Échec

Cette erreur indique que le SWA ne peut pas résoudre sa propre interface et le nom d'hôte via le serveur DNS. Vérifiez que le SWA est configuré avec le serveur DNS correct (Étape 1.4 et Étape

2) pour créer les enregistrements DNS manquants.

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

 Conseil : Si, après avoir corrigé le serveur DNS ou les enregistrements DNS, vous recevez toujours la même erreur, effacez le cache DNS à partir de GUI > Network > DNS > Clear DNS Cache.

Impossible de résoudre ADD1.*.* : Échec de « Nom d'hôte inconnu »

Cette erreur indique que le SWA ne peut pas résoudre les enregistrements DNS liés à Active Directory. Utilisez l'étape 1.4 pour configurer le serveur DNS correct pour votre domaine Active Directory.

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

 Conseil : si, après avoir corrigé le serveur DNS ou les enregistrements DNS, vous recevez toujours la même erreur, effacez le cache DNS de l'interface utilisateur graphique > Réseau > DNS > Effacer le cache DNS.

Erreur lors de la récupération des tickets Kerberos du serveur : "kinit : Mot de passe incorrect" Échec

Cette erreur indique que le nom d'utilisateur ou le mot de passe utilisé pour se connecter à Active Directory est incorrect.

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

Impossible de joindre le domaine : Échec de la précréation du compte : "Accès insuffisant"

Cette erreur indique que l'utilisateur ne dispose pas des privilèges minimaux requis pour créer le compte d'ordinateur. Vérifiez les privilèges utilisateur conformément à la section Liste de contrôle

de cet article.

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

Autres informations utiles

- Guide de l'utilisateur d'AsyncOS 15.0 pour Cisco Secure Web Appliance
- Configurer le pare-feu pour l'appliance Web sécurisée
- Configurer des catégories d'URL personnalisées dans Secure Web Appliance - Cisco
- Comment exempter le trafic Office 365 de l'authentification et du déchiffrement sur l'appareil de sécurité Web Cisco (WSA) - Cisco
- Utilisation des meilleures pratiques d'appliance Web sécurisé - Cisco
- Bloquer le trafic dans l'appliance Web sécurisée
- Bloquer le trafic de téléchargement dans l'appliance Web sécurisée
- Bloquer le téléchargement de fichiers exécutables dans SWA
- Contourner le trafic des mises à jour Microsoft dans l'appliance Web sécurisée
- Contourner l'authentification dans l'appareil Web sécurisé - Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.