# SWAでのActive Directory認証の設定

## 内容



## はじめに

このドキュメントでは、Secure Web Appliance(SWA)でActive Directory(AD)認証を設定する手順について説明します。

## 前提条件

### 要 件

次の項目に関する知識があることが推奨されます。

- SWA管理。
- 基本的なネットワーキングおよびプロキシプロトコル。
- 基本的なActive Directory管理。

次のツールをインストールしておくことを推奨します。

- 物理または仮想SWA。

- SWAグラフィカルユーザインターフェイス(GUI)への管理アクセス
- Active Directoryへの管理アクセス。

### 使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## チェックリスト

SWAをActive Directoryに接続する前に、必要なチェックがすべて完了していることを確認してください。

- SWAには、Active Directoryへの適切なネットワークアクセスがあります。詳細については、「セキュリティで保護されたWebアプライアンス用のファイアウォールの設定」を参照してください。
- SWAホスト名のDNSレコードがActive Directoryに作成されます。(CLI > sethostname)

---

注：トランスペアレントモードでは、セキュアWebアプライアンスのホスト名がリダイレクトホスト名に一致することを確認してください。

---

- SWAインターフェイスのDNSレコードは、Active Directoryに作成されます。

- Secure Web Applianceの現在の時刻をActive Directoryサーバの時刻と比較し、その差がActive Directoryサーバの[コンピュータクロック同期の最大許容値]設定で定義された値を超えていないことを確認します。

- 認証に使用するActive DirectoryドメインにSecure Web Applianceを参加させるために必要な権限とドメイン情報があることを確認します。

    - Domain AdminsグループまたはAccount Operatorsグループのメンバーであるユーザを Active Directory(AD)サーバに作成します。

    - または、必要最小限の権限でユーザを作成します。権限には、Reset Password、

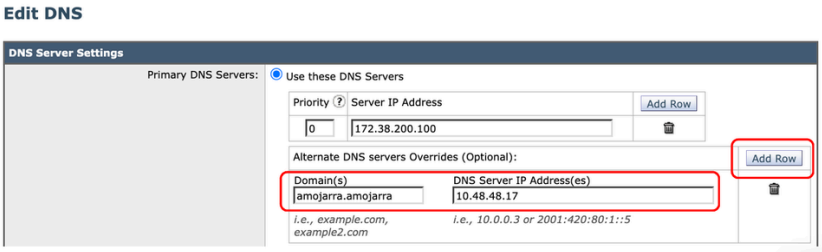
Validated write to servicePrincipalName、Write account restrictions、Write dNSHostName、およびWrite servicePrincipalNameがあります。これらの権限は、アプライアンスをドメインに参加させ、完全な機能を確保するのに十分です。

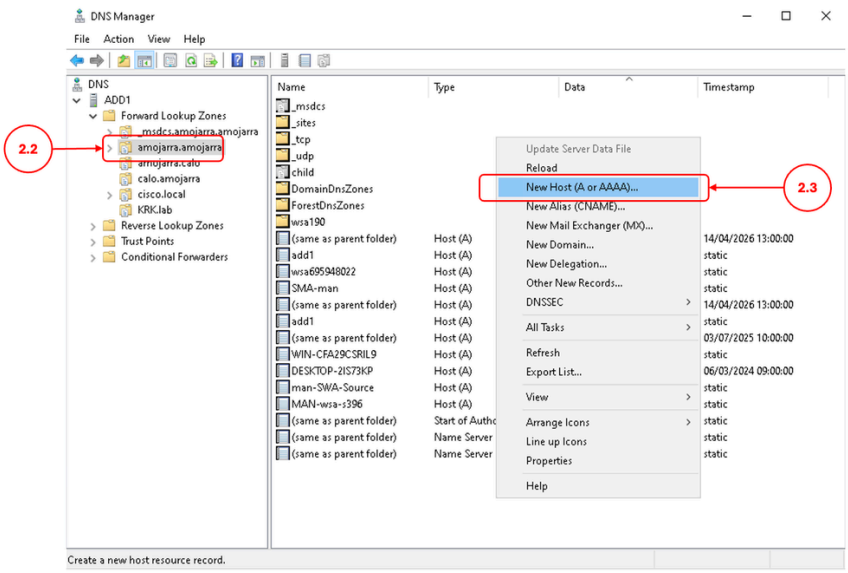
- SWAがActive Directory FQDNを解決できることを確認します。

## Active Directoryの設定

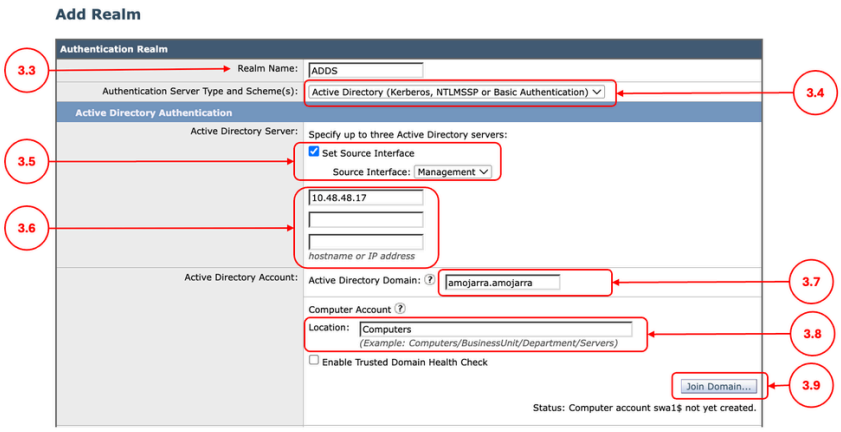
SWAでアップストリームプロキシを設定するには、次の手順を使用します。

| 手順 | 詳細 |
| --- | --- |
| ステップ 1：SWAからの情報の収集 | 手順1.1.SWAのCLIからrunsethostnameを実行し、現在のSWAホスト名を表示します。 |
| | 注：現在のホスト名を変更する場合は、新しいホスト名を入力してEnterキーを押し、commitコマンドを実行して変更を確定します。 |
| | ステップ 1.2： SWA GUIから、Networkに移動し、Interfacesを選択してインターフェイスFQDNを表示します。現在のインターフェイスFQDNを変更する場合は、Edit Settingsをクリックして変更を行い、commitをクリックします。<br>ステップ1.3:SWA GUIから、System Administrationに移動し、Time Settingsをクリックして、NTP設定が正しいことを確認します。<br>ステップ 1.4：SWA GUIから、Networkに移動し、DNSを選択します。次に、正しいDNSサーバが定義されていることを確認します。 |
| | ヒント: SWAがパブリックDNSサーバで設定されていて、Active Directoryドメインに別のDNSサーバを定義したい場合は、Edit Settingをクリックして、Alternate DNS servers Overrides (Optional)セクションでActive Directory(AD)ドメイン名とDNSサーバのIPアドレスを定義し、submitとcommitの変更をします。 |

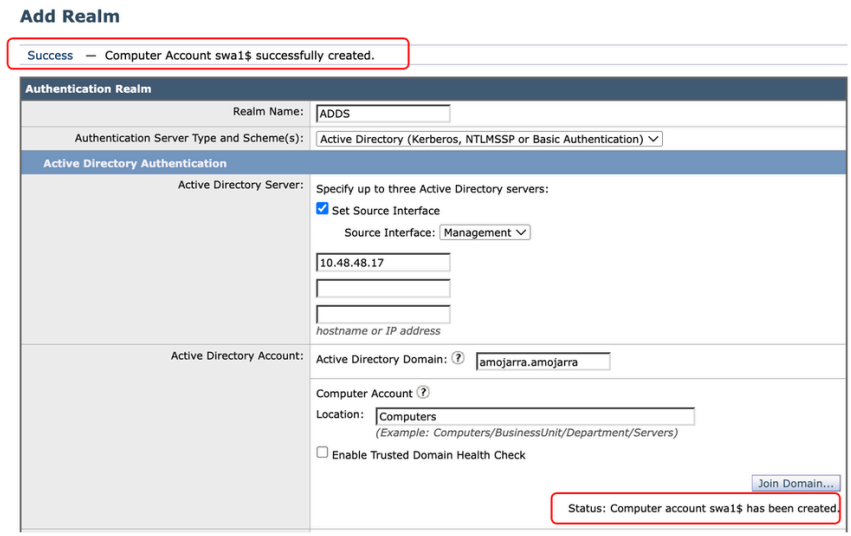
<table>
<tr><td></td><td> 

イメージ – 代替DNSサーバの追加</td></tr>
<tr><td>ステップ 2Active DirectoryでのDNSレコードの設定</td><td>ステップ 2.1： Active Directoryサーバに接続し、DNSマネージャコンソールに移動します。<br><br>ステップ 2.2：左側のパネルから目的のドメイン名を選択します。<br><br>ステップ 2.3：右側のパネルで右クリックして、New Host (A or AAAA)を選択します。<br><br> 

イメージ：新しいAレコードの作成<br><br>ステップ 2.4：SWAホスト名のDNSレコードを定義します(ステップ1.1で収集)<br><br>⚠ 注意:Active Directoryが管理インターフェイス経由でSWAに接続している場合は、管理IPアドレスを定義します。それ以外の場合は、Active Directoryがアクセスできる SWAの正しいIPアドレス ( P1インターフェイスのIPアドレスまたはP2インターフェイスのIPアドレス ) を定義します<br><br>ステップ 2.5： 各SWAインターフェイスのDNSレコードを定義します。</td></tr>
</table>

| | |
|---|---|
| | ステップ2.6.(オプション)ハイアベイラビリティを使用している場合は、定義された仮想IPアドレスを使用してハイアベイラビリティFQDNのDNSレコードを定義します。 |
| ステップ 3Active Directoryレルムの設定 | ステップ 3.1： SWAのGUIで、Networkに移動し、Authenticationを選択します。<br><br>ステップ 3.2：Add Realmをクリックします。<br><br>ステップ 3.3：レルム名を定義します。<br><br>ステップ 3.4：Authentication Server Type and Scheme(s)から、Active Directoryを選択します。<br><br>ステップ 3.5：デフォルトでは、SWAは管理インターフェイスを使用してActive Directoryに接続します。この設定を変更する場合は、Set Source Interfaceをクリックして、目的のInterfaceを選択します。<br><br>ステップ 3.6：Active Directoryドメインコントローラのホスト名またはIPアドレスを定義します。<br><br>ステップ 3.7：Active Directoryドメイン名を入力します。<br><br>ステップ3.8.(オプション)コンピュータアカウントをActive Directoryの別の組織単位(OU)に保存する場合は、目的の場所を定義します<br><br>ステップ 3.9：Join Domainをクリックします。<br><br>  <br>イメージ – レルムの追加<br><br>ステップ 3.10：ユーザ名とパスワードを入力し、Joinをクリックします。<br><br>ヒント：ドメイン名をユーザ名に含めないでください |

(たとえば、「DOMAIN\SWA_ADMIN」や「SWA_ADMIN@domain」ではなく「SWA_ADMIN」と入力します)。




イメージ：SWAがADに正常に参加した

ステップ 3.11：Submit

ステップ 3.12：変更を保存します。

# トラブルシューティング

警告: WSAとADサーバ間のクロックスキューが大きすぎます

このエラーは、Active DirectoryとSWAの間の時間が同期されていないことを示しています。ステップ1.3を使用して、SWAの時間を修正してください

```
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.*.* "Unknown hostname"障害を解決できない

このエラーは、SWAがDNSサーバ経由で自身のインターフェイスとホスト名を解決できないことを示しています。SWAに正しいDNSサーバ（ステップ1.4）が設定されていることを確認し、ス

テップ2を実行して不足しているDNSレコードを作成します。

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

ヒント:DNSサーバまたはDNSレコードを修正しても同じエラーが表示される場合は、GUI > Network > DNS > Clear DNS Cacheの順に選択し、DNSキャッシュをクリアします。

## ADD1.*.*を解決できません：「不明なホスト名」エラー

このエラーは、SWAがActive Directoryに関連するDNSレコードを解決できないことを示します。ステップ1.4を使用して、Active Directoryドメインに正しいDNSサーバを設定します。

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

ヒント:DNSサーバまたはDNSレコードを修正しても同じエラーが表示される場合は、GUI > Network > DNS > Clear DNS Cacheの順に選択し、DNSキャッシュをクリアします。

## サーバからKerberosチケットをフェッチ中のエラー：「kinit: Password incorrect」エラー

このエラーは、Active Directoryへの接続に使用されるユーザ名またはパスワードが正しくないことを示しています。

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

## ドメインに参加できません：アカウントの事前作成に失敗しました：「アクセスが不十分です」

このエラーは、コンピューターアカウントを作成するために必要な最小限の特権がユーザーに不足していることを示します。この記事の[リストの確認]セクションでユーザーの特権を確認してください。

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

## 関連情報

- AsyncOS 15.0 for Cisco Secure Web Applianceユーザガイド
- セキュアWebアプライアンス用のファイアウォールの設定
- Secure Web ApplianceでのカスタムURLカテゴリの設定：シスコ
- Cisco Webセキュリティアプライアンス(WSA)でOffice 365トラフィックを認証および復号化から除外する方法：シスコ
- セキュアなWebアプライアンスのベストプラクティスの使用：シスコ
- Secure Web Applianceでのトラフィックのブロック
- セキュアWebアプライアンスでのアップロードトラフィックのブロック
- SWAでの実行可能ファイルのダウンロードのブロック
- Secure Web ApplianceでのMicrosoft Updatesトラフィックのバイパス
- Secure Web Applianceでの認証のバイパス：シスコ

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。