在SWA中配置Active Directory身份驗證

目錄

簡介

本文檔介紹在安全Web裝置(SWA)中配置Active Directory身份驗證的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- SWA管理。
- 基本網路和代理協定。
- 基本Active Directory管理。

思科建議您安裝以下工具：

- 物理或虛擬SWA。

- 對SWA圖形使用者介面(GUI)的管理訪問。
- 對Active Directory的管理訪問許可權。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

核對表

在將SWA連線到Active Directory之前，請確保已完成所有必需的檢查：

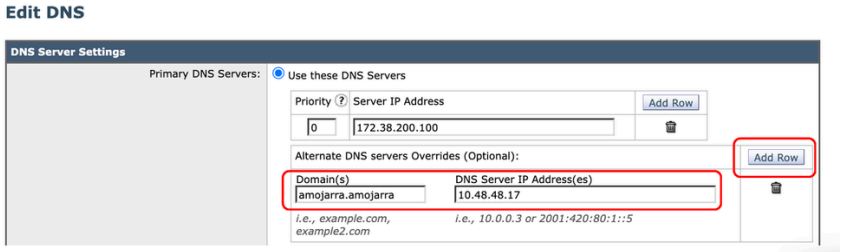
- SWA具有對Active Directory的正確網路訪問許可權。欲知更多資訊，請訪問：為安全Web裝置配置防火牆。
- 在Active Directory中建立SWA主機名的DNS記錄。(CLI > sethostname)

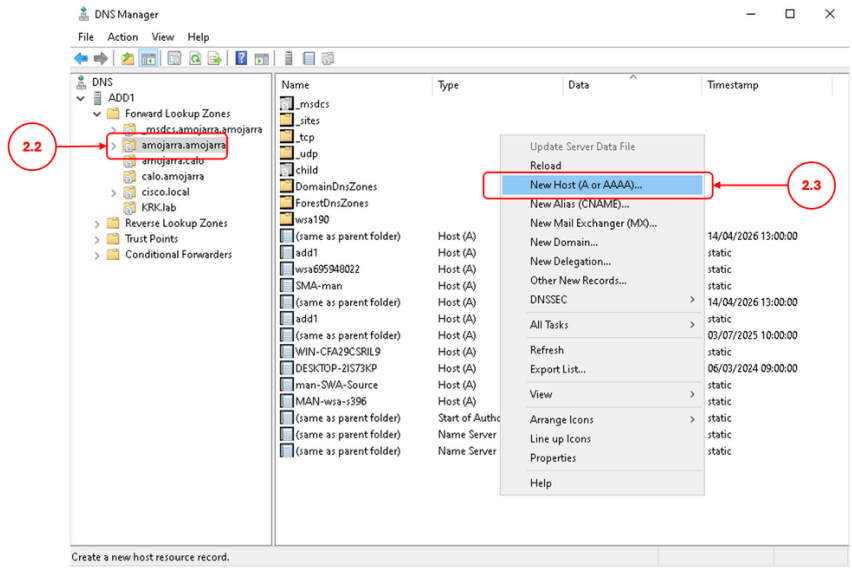
附註：在透明模式下，確保Secure Web Appliance主機名與Redirect Hostname匹配。

- SWA介面的DNS記錄在Active Directory中建立。
- 將安全Web裝置上的當前時間與Active Directory伺服器上的時間進行比較，並確保差異不超過Active Directory伺服器上的「電腦時鐘同步的最大容差」設定中定義的值。
- 確認您具有將Secure Web Appliance加入要用於身份驗證的Active Directory域所需的必要許可權和域資訊。
    - 在Active Directory伺服器上建立作為Domain Admins或Account Operators組成員的使用者。
    - 或者，建立具有最低所需許可權的使用者：Reset Password、Validated write to servicePrincipalName、Write account restrictions、Write dNSHostName和WriteservicePrincipalName。這些許可權足以將裝置加入域並確保其功能完整。
- 確保SWA可以解析Active Directory FQDN。

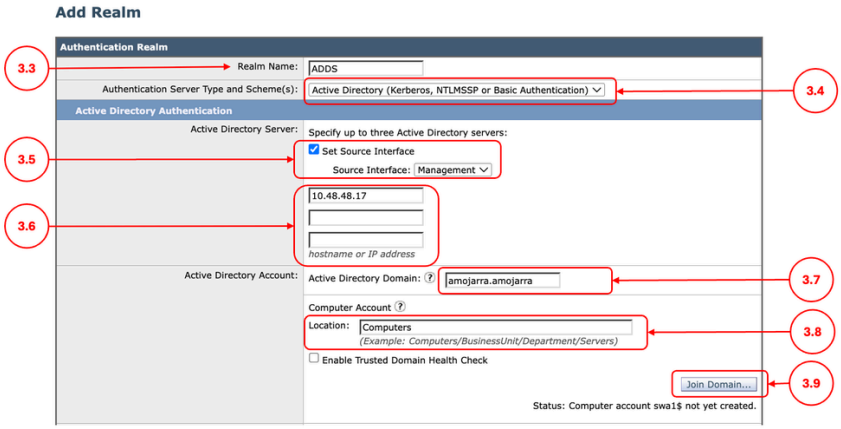
配置Active Directory

使用以下步驟在SWA中配置上游代理。

步驟	詳細資料
步驟1.從SWA收集資訊	步驟1.1.從SWA CLI中，runsethostname檢視當前SWA主機名。 附註：如果要更改當前主機名，請鍵入新主機名並按Enter鍵，然後執行commit命令提交更改。 步驟1.2.從SWA GUI導航到Network，選擇Interfaces以檢視介面FQDN。如果要更改當前介面FQDN，請按一下Edit Settings並進行更改，然後commit。 步驟1.3.從SWA GUI中，導覽至System Administration，然後點選Time Settings，確保NTP設定正確。 步驟1.4.在SWA GUI中，導航到Network，選擇DNS，確保定義了正確的DNS伺服器。 提示：如果SWA配置了公共DNS伺服器，並且您要為Active Directory域定義不同的DNS伺服器，請按一下Edit Setting，然後在備用DNS伺服器覆蓋（可選）部分定義Active Directory域名和DNS伺服器IP地址，然後submit和commit更改。  映像 — 新增備用DNS伺服器
步驟2.在Active Directory中配置DNS記錄	步驟2.1.連接到Active Directory伺服器並導航到DNS Manager控制台。 步驟2.2.從左側面板中選擇所需的Domain name。 步驟2.3.在右側面板中，按一下右鍵並選擇New Host（A或AAAA）

	 影象 — 建立新的A記錄 步驟2.4.定義SWA主機名的DNS記錄(在步驟1.1中收集) ⚠ 注意：如果Active Directory通過管理介面連線到SWA，請定義管理IP地址，否則定義Active Directory有權訪問的SWA的正確IP地址（P1介面IP地址或P2介面IP地址） 步驟2.5. 定義每個SWA介面的DNS記錄。 步驟2.6.(可選)如果您正在使用高可用性，請使用定義的虛擬IP地址定義高可用性FQDN的DNS記錄。
步驟3.配置Active Directory領域	步驟3.1.從SWA GUI導航到Network，選擇Authentication。 步驟3.2.單擊Add Realm。 步驟3.3.定義領域名稱。 步驟3.4.從Authentication Server Type and Scheme(s)中選擇Active Directory。 步驟3.5。預設情況下，SWA使用管理介面連線到Active Directory，如果您想更改此設定，請按一下Set Source Interface並選擇所需的介面。 步驟3.6.定義Active Directory域控制器的主機名或IP地址。 步驟3.7.輸入Active Directory域名。 步驟3.8.(可選)如果要將電腦帳戶儲存在Active Directory中的其他組織單位(OU)中，請定義所需的位置

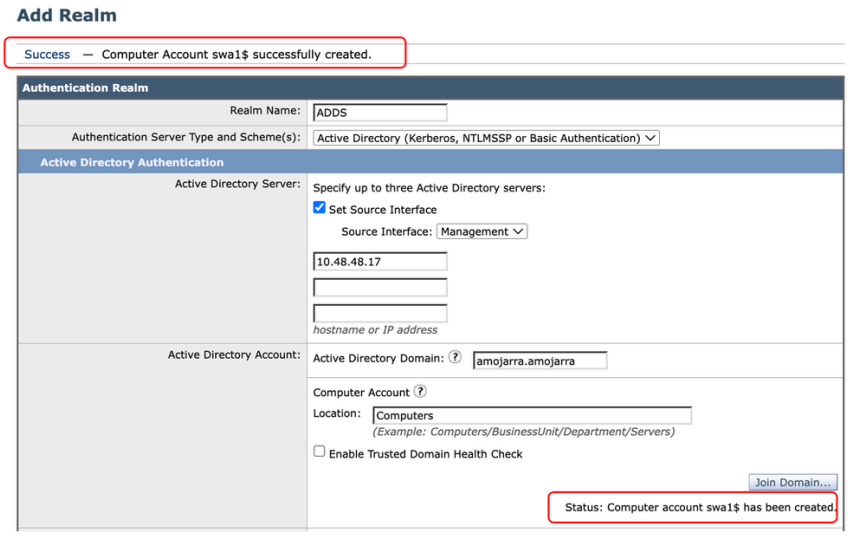
步驟3.9。單擊Join Domain。



影象 — 新增領域

步驟3.10.輸入用戶名和密碼，然後點選加入。

提示：請勿將域名與使用者名稱一起包含(例如，輸入「SWA_ADMIN」而不是「DOMAIN\SWA_ADMIN」或「SWA_ADMIN@domain」)。



影象 — SWA已成功加入AD

步驟3.11.提交

步驟3.12.提交更改。

疑難排解

警告：WSA和AD伺服器之間的時鐘偏差過大

此錯誤表示Active Directory和SWA之間的時間不同步。使用步驟1.3更正SWA上的時間

```
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
```

無法解決swa1.*.* "Unknown hostname"故障

此錯誤表示SWA無法通過DNS伺服器解析其自身的介面和主機名。確認已使用正確的DNS伺服器（步驟1.4）配置了SWA，並且執行了步驟2以建立缺失的DNS記錄。

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


提示：如果在更正DNS伺服器或DNS記錄之後您仍然收到相同的錯誤，請從GUI > Network > DNS > Clear DNS Cache清除DNS快取。

無法解析ADD1.*.*：「未知主機名」故障

此錯誤表示SWA無法解析與Active Directory相關的DNS記錄。使用步驟1.4為您的Active Directory域配置正確的DNS伺服器。

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


提示：如果在更正DNS伺服器或DNS記錄之後，您仍然收到相同的錯誤，請從GUI > Network > DNS > Clear DNS Cache清除DNS快取。

從伺服器獲取Kerberos票證時出錯：「kinit:Password incorrect" Failure

此錯誤表示用於連線到Active Directory的使用者名稱或密碼不正確。

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

無法加入域：未能預建立帳戶："訪問不足"

此錯誤表示使用者缺少建立電腦帳戶所需的最低許可權。請根據本文的「核對表」部分檢查使用者許可權。

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

相關資訊

- Cisco Secure Web Appliance AsyncOS 15.0使用手冊
- 為安全Web裝置配置防火牆
- 在Secure Web Appliance中配置自定義URL類別 — Cisco
- 如何免除Office 365流量在思科網路安全裝置(WSA)上進行身份驗證和解密 — 思科
- 使用安全Web裝置最佳實踐 — 思科
- 阻止安全Web裝置中的流量
- 阻止安全Web裝置中的上傳流量
- 在SWA中阻止執行檔下載
- 繞過安全Web裝置中的Microsoft更新流量
- 繞過安全Web裝置中的身份驗證 — Cisco

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。