在SWA中配置Active Directory身份验证

目录

简介

先决条件

- 要求
- 使用的组件

核对清单

配置Active Directory

- 步骤1.从SWA收集信息
- 步骤2.在Active Directory中配置DNS记录
- 步骤3.配置Active Directory领域

故障排除

- 无法解析swa1.*.*“未知主机名”故障
- 无法解析ADD1.*.* :“未知主机名”故障
- 从服务器获取Kerberos票证时出错：“kinit:“密码不正确”失败
- 无法加入域：未能预创建帐户："访问不足"

相关信息

简介

本文档介绍在安全网络设备(SWA)中配置Active Directory身份验证的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- SWA管理。
- 基本网络和代理协议。
- 基本Active Directory管理。

思科建议您安装以下工具：

- 物理或虚拟SWA。

- 对SWA图形用户界面(GUI)的管理访问。
- 对Active Directory的管理访问。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

核对清单

在将SWA连接到Active Directory之前，请确保已完成所有必需的检查：

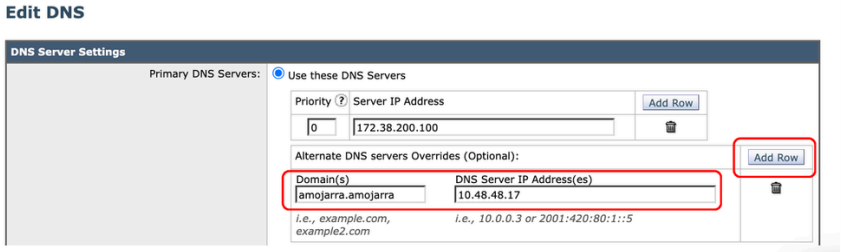
- SWA对Active Directory具有适当的网络访问权限。有关更多信息，请访问：为安全Web设备配置防火墙。
- SWA主机名的DNS记录在Active Directory中创建。(CLI > sethostname)

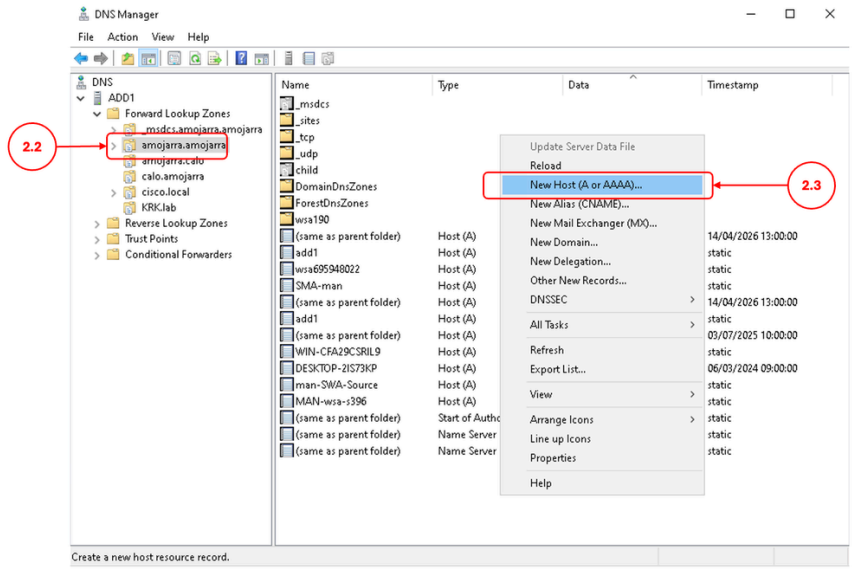
注意：在透明模式下，确保安全Web设备主机名与重定向主机名匹配。

- SWA接口的DNS记录在Active Directory中创建。
- 比较安全Web设备上的当前时间与Active Directory服务器上的时间，并确保差异不超过Active Directory服务器上的“计算机时钟同步的最大容差”设置中定义的值。
- 确认您具有将安全Web设备加入要用于身份验证的Active Directory域所需的必要权限和域信息。
    - 在Active Directory服务器上创建属于Domain Admins或Account Operators组成员的用户。
    - 或者，创建具有最低所需权限的用户：Reset Password、Validated write to servicePrincipalName、Write account restrictions、Write dNSHostName和Write servicePrincipalName。这些权限足以将设备加入域并确保其功能完整。
- 确保SWA可以解析Active Directory FQDN。

配置Active Directory

使用以下步骤在SWA中配置上游代理。

步骤	详细信息
步骤1.从SWA收集信息	第1.1步：从SWA CLI,runsethostname查看当前SWA主机名。 注意：如果要更改当前主机名，请键入新主机名并按Enter，然后执行commit命令提交更改。 第1.2步：从SWA GUI中，导航到Network，选择Interfaces，以查看接口FQDN。如果要更改当前接口FQDN，请单击Edit Settings，然后进行更改，然后提交请。 第1.3步：从SWA GUI，导航到系统管理，然后单击时间设置，确保NTP设置正确。 第1.4步：从SWA GUI中，导航到网络，选择DNS，确保定义了正确的DNS服务器。 提示：如果SWA配置有公共DNS服务器，并且您希望为Active Directory域定义不同的DNS服务器，请单击Edit Setting，并在Alternate DNS servers Overrides(Optional)部分定义Active Directory域名和DNS服务器IP地址，然后submit和commit更改。  映像 — 添加备用DNS服务器
步骤2.在Active Directory中配置DNS记录	步骤2.1.连接到Active Directory服务器并导航到DNS Manager控制台。 第2.2步：从左侧面板中选择所需的域名。 第2.3步：在右侧面板中，右键单击并选择New Host(A or AAAA)



图像 — 创建新的A记录

第2.4步：为SWA主机名定义DNS记录(在第1.1步中收集)

⚠ 警告：如果Active Directory通过管理接口连接到SWA，请定义管理IP地址，否则定义Active Directory有权访问的SWA的正确IP地址（P1接口IP地址或P2接口IP地址）

步骤2.5.定义每个SWA接口的DNS记录。

第2.6步(可选)如果使用高可用性，请使用定义的虚拟IP地址定义高可用性FQDN的DNS记录。

步骤3.配置Active Directory领域

第3.1步：在SWA GUI中，导航到网络，选择Authentication。

第3.2步：点击添加领域。

步骤3.3.定义领域名称。

第3.4步：从身份验证服务器类型和方案选择Active Directory。

第3.5步。默认情况下，SWA使用管理接口连接到Active Directory，如果您想更改此设置，请点击Set Source Interface并选择所需的接口。

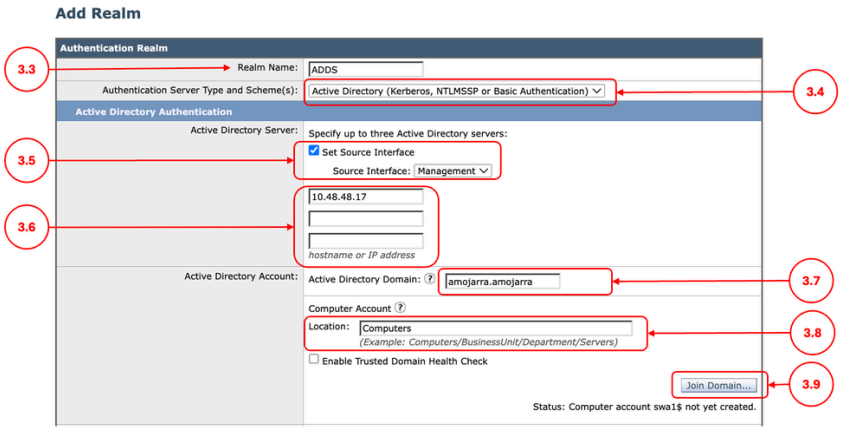
第3.6步：定义Active Directory域控制器的主机名或IP地址。

第3.7步。输入Active Directory域名。

第3.8步(可选)如果要将计算机帐户存储在Active Directory中

的其他组织单位(OU)中，请定义所需的位置

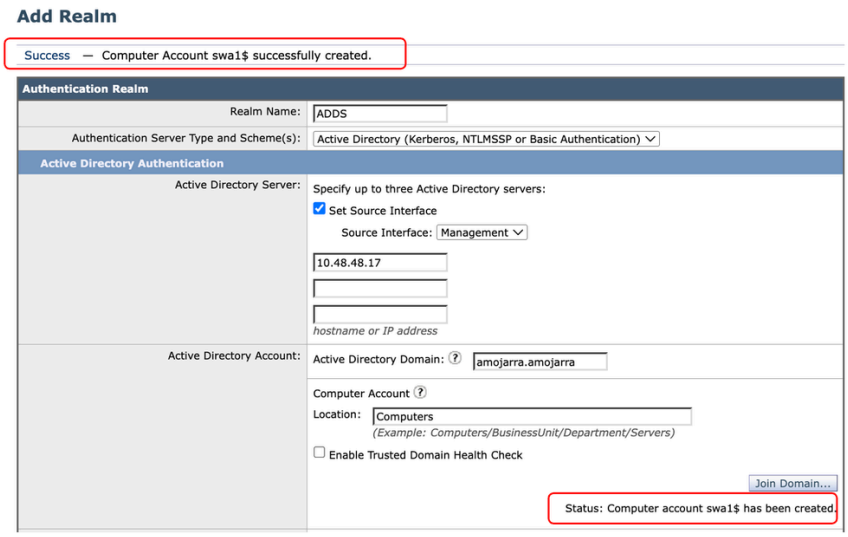
第3.9步。点击加入域。



图像 — 添加领域

第3.10步。输入用户名和密码，然后点击加入。

提示：请勿在用户名中包含域名(例如，输入“SWA_ADMIN”而不是“DOMAIN\SWA_ADMIN”或“SWA_ADMIN@domain”)。



映像 — SWA已成功加入AD

步骤3.11.提交

步骤3.12.提交更改。

故障排除

警告：WSA和AD服务器之间的时钟偏差过大

此错误表示Active Directory和SWA之间的时间不同步。使用步骤1.3更正SWA上的时间

```
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
```

无法解析swa1.*.*“未知主机名”故障

此错误表示SWA无法通过DNS服务器解析自己的接口和主机名。确认SWA配置了正确的DNS服务器（第1.4步），并使用第2步创建缺失的DNS记录。

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

提示：如果在更正DNS服务器或DNS记录后仍然收到相同的错误，请从GUI > Network > DNS > Clear DNS Cache清除DNS缓存。

无法解析ADD1.*.* :“未知主机名”故障

此错误表示SWA无法解析与Active Directory相关的DNS记录。使用步骤1.4为Active Directory域配置正确的DNS服务器。

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

提示：如果在更正DNS服务器或DNS记录后仍然收到相同的错误，请从GUI > Network > DNS > Clear DNS Cache清除DNS缓存。

从服务器获取Kerberos票证时出错：“kinit:“密码不正确”失败

此错误表示用于连接到Active Directory的用户名或密码不正确。

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

无法加入域：未能预创建帐户："访问不足"

此错误表示用户缺少创建计算机帐户所需的最低权限。请根据本文的“核对表”部分检查用户权限。

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

相关信息

- 思科安全Web设备AsyncOS 15.0用户指南
- 为安全Web设备配置防火墙
- 在安全Web设备中配置自定义URL类别 — 思科
- 如何免除Office 365流量在思科网络安全设备(WSA)上的身份验证和解密 — 思科
- 使用安全Web设备最佳实践 — 思科
- 阻止安全网络设备中的流量
- 阻止安全Web设备中的上传流量
- 阻止SWA中的可执行文件下载
- 绕过安全Web设备中的Microsoft更新流量
- 绕过安全Web设备中的身份验证 — 思科

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。