

從ASA 9.22中停用Kerberos

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[ASA CLI配置演練](#)

[ASDM配置演練](#)

[CSM配置演練](#)

簡介

本文檔介紹了有關ASA 9.22中Kerberos棄用的見解。

必要條件

需求

思科建議您瞭解基本的安全概念：

- ASA CLI基礎知識。
- AAA基本知識(驗證、授權和記帳)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 所有ASA平台
- ASA CLI 9.22.1
- ASDM 7.22.1
- CSM 4.29

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。

ASA CLI配置演練

ASA CLI概述：

- 在命令輸出中，**斜體**選項已從CLI中刪除。
- 從包含這些配置的9.22之前的版本進行升級，會導致在引導期間在控制檯上出現警告消息。

ciscoasa(config)# aaa-server curve protocol ?

配置模式命令/選項：

http格式協定基於HTTP格式的

kerberos協議Kerberos (不建議使用)

ldap協定LDAP

radius通訊協定RADIUS

sdi通訊協定SDI

tacacs+通訊協定TACACS+

ciscoasa(config)# aaa-server限制協定kerberos

ciscoasa(config-aaa-server-group)# ?

AAA伺服器配置命令：

退出Exit from aaa-server group configuration mode

有關AAA伺服器配置命令的幫助幫助

max-failed-attempts指定在停用組中任何伺服器之前允許的最大失敗次數

no從aaa伺服器組配置中刪除專案

reactivation-mode指定重新啟用故障伺服器的方法

validate-kdc在kerberos使用者身份驗證期間啟用KDC驗證

ciscoasa(config)# test aaa-server authentication current ?

exec模式命令/選項：

委託測試Kerberos約束委派

host輸入此關鍵字以指定伺服器的IP地址

模擬測試Kerberos協定轉換

password Password關鍵字

自測試Kerberos自檢票檢索

username Username關鍵字

ciscoasa(config)# aaa-server ldaps protocol ldap

ciscoasa(config-aaa-server-group)# aaa-server ldaps host x.x.x

ciscoasa(config-aaa-server-host)# sasl-mechanism ?

aaa-server-host mode commands/options:

digest-md5 select Digest-MD5

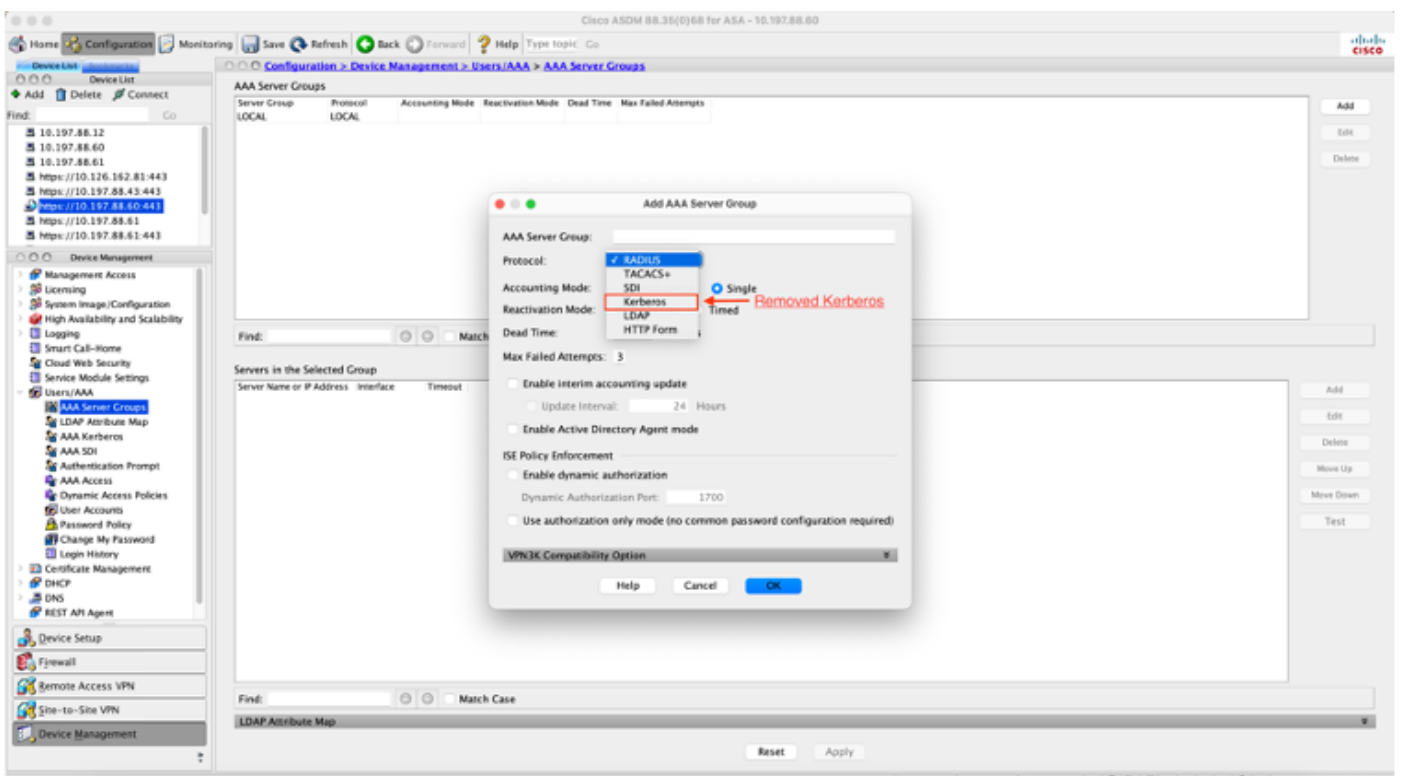
kerberos select Kerberos

ciscoasa(config)# debug kerberos

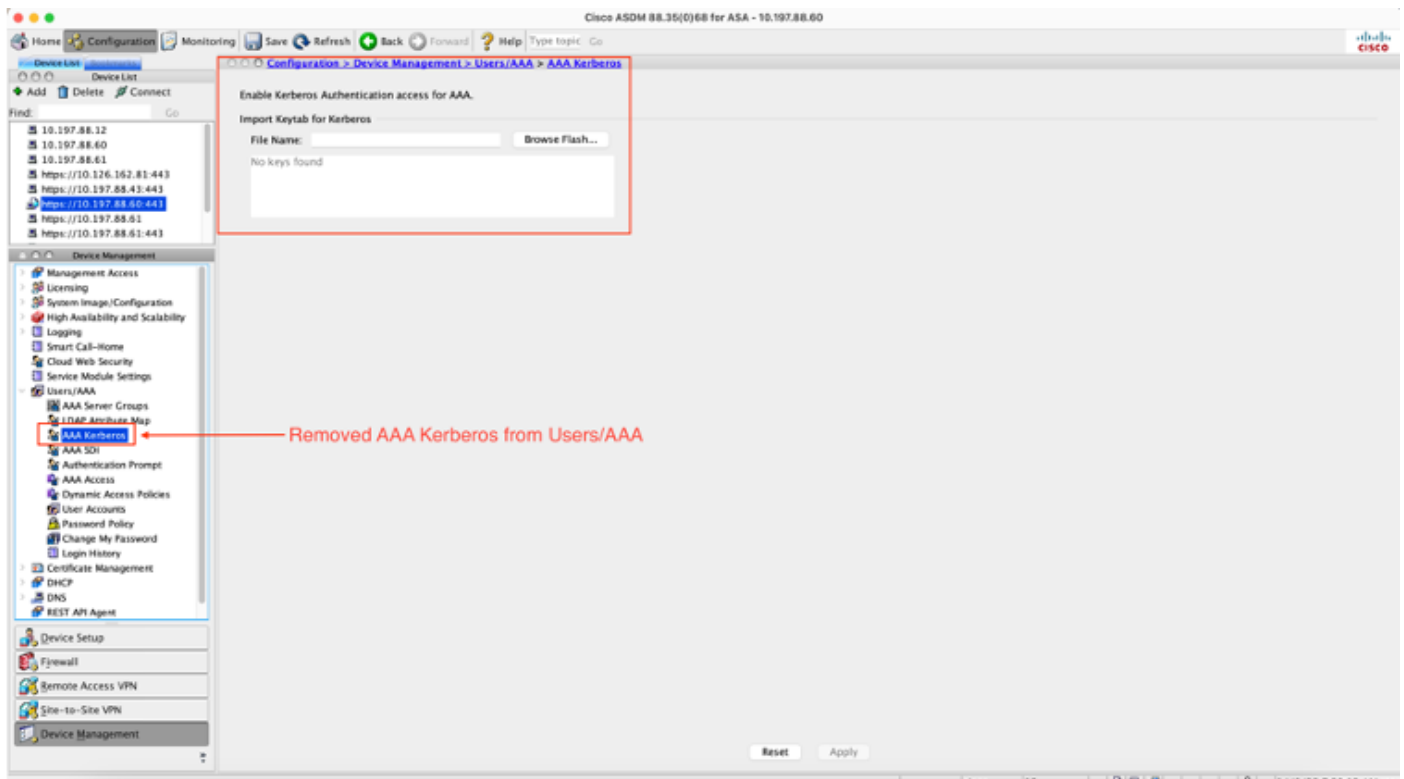
ASDM配置演練

ASDM概述：

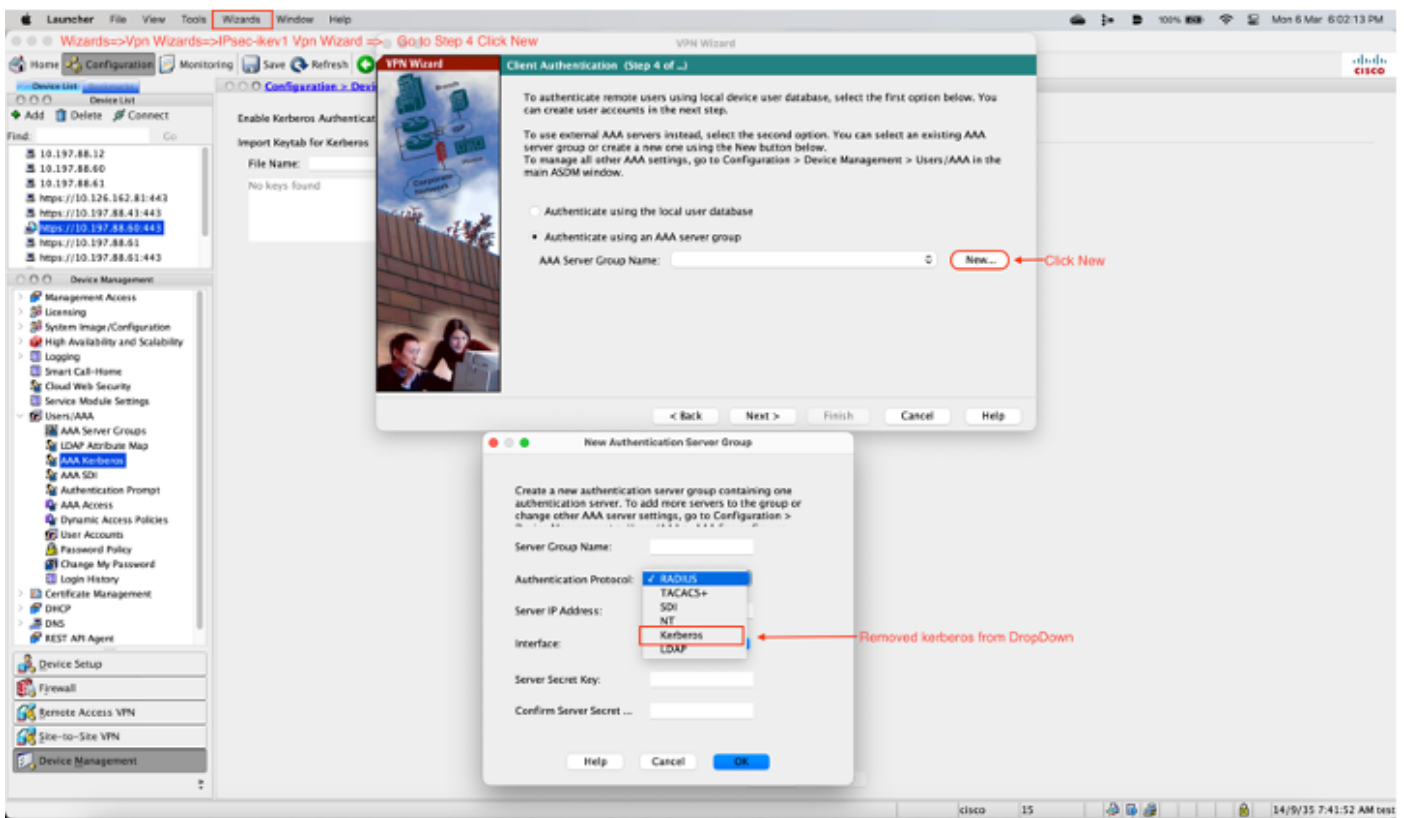
- ASDM 7.22不再支援Kerberos
- 這會降低終端使用者使用Kerberos協定和LDAP SASL機制配置AAA伺服器組的能力。
- 作為此棄用的一部分，AAA Kerberos不再列在TreeMenu中的Users/AAA in Device Management。
- Microsoft KCD Server也不再受支援。



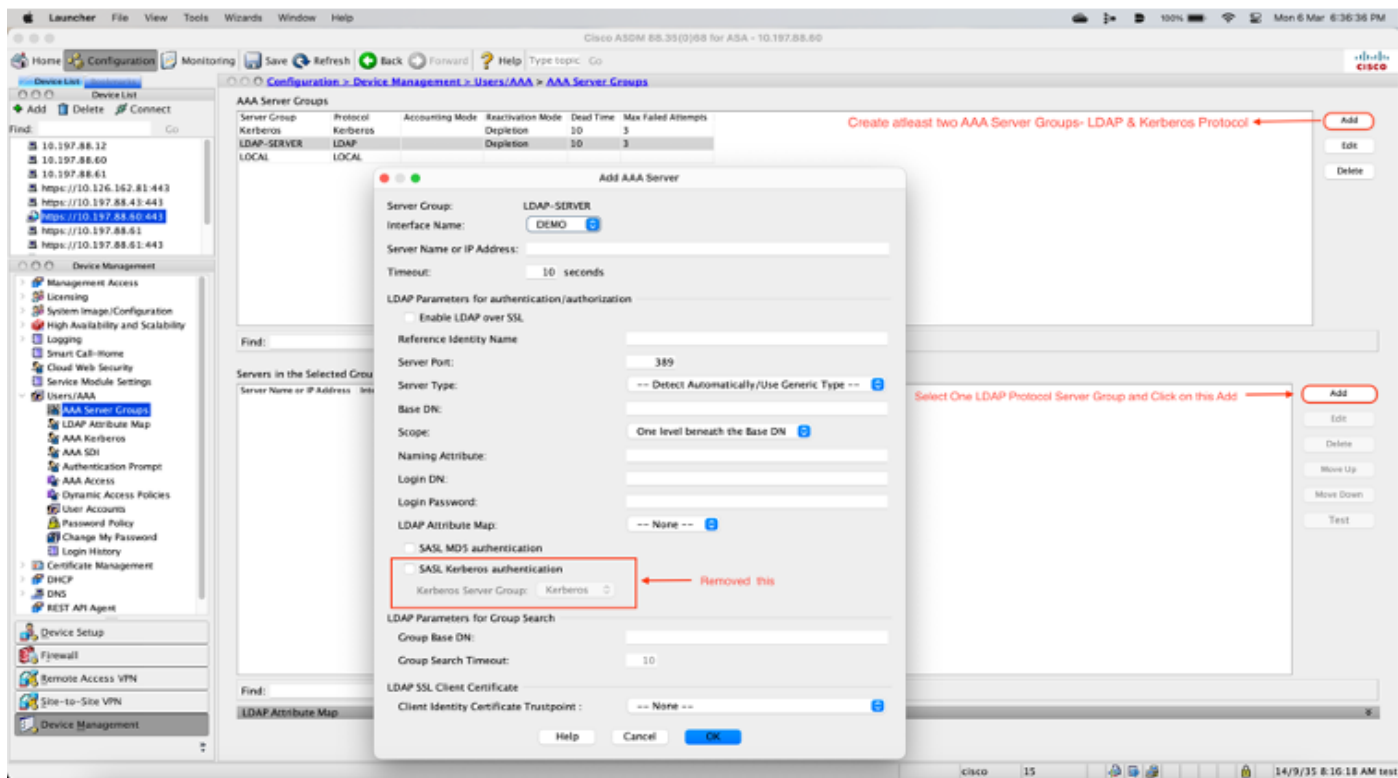
ASDM:新AAA伺服器組中的Kerberos協定



ASDM:AAA Kerberos



ASDM:新AAA伺服器組中的Kerberos協定

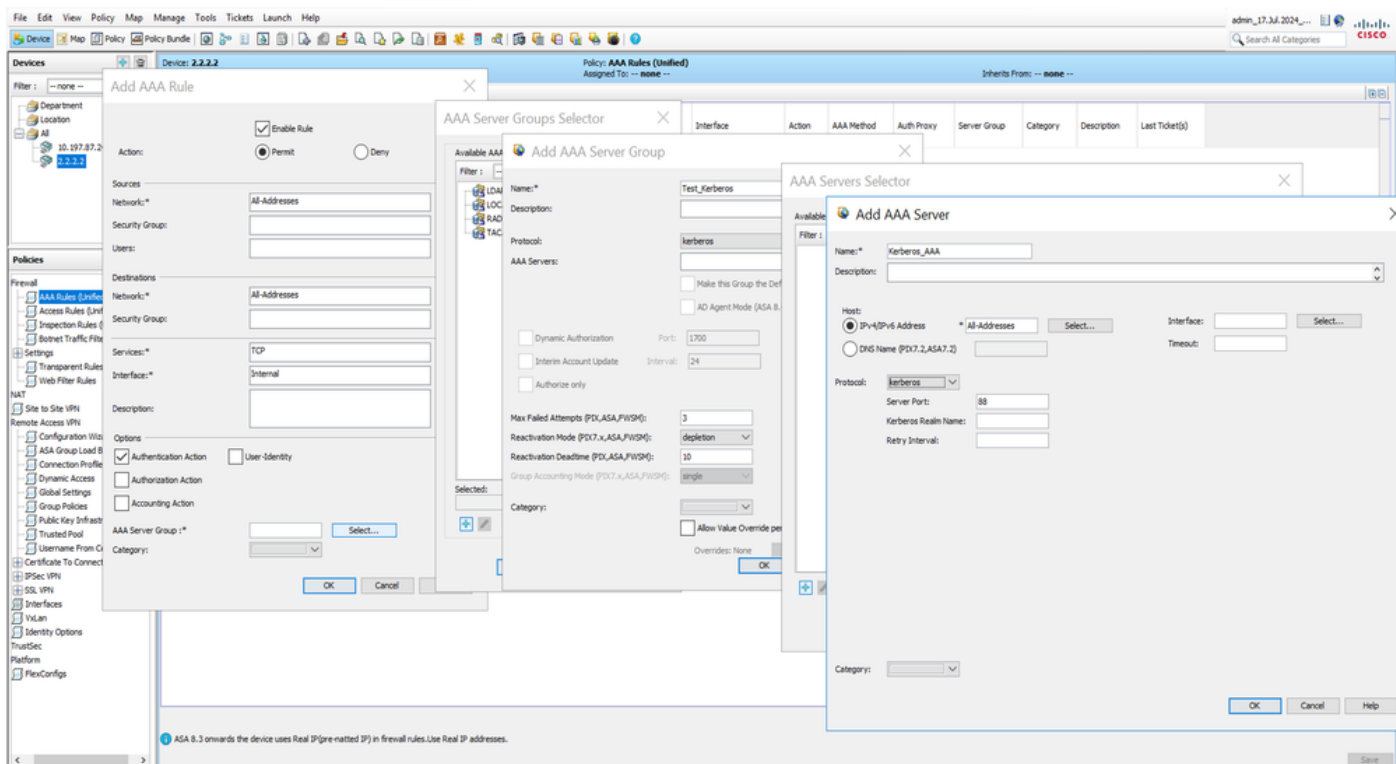
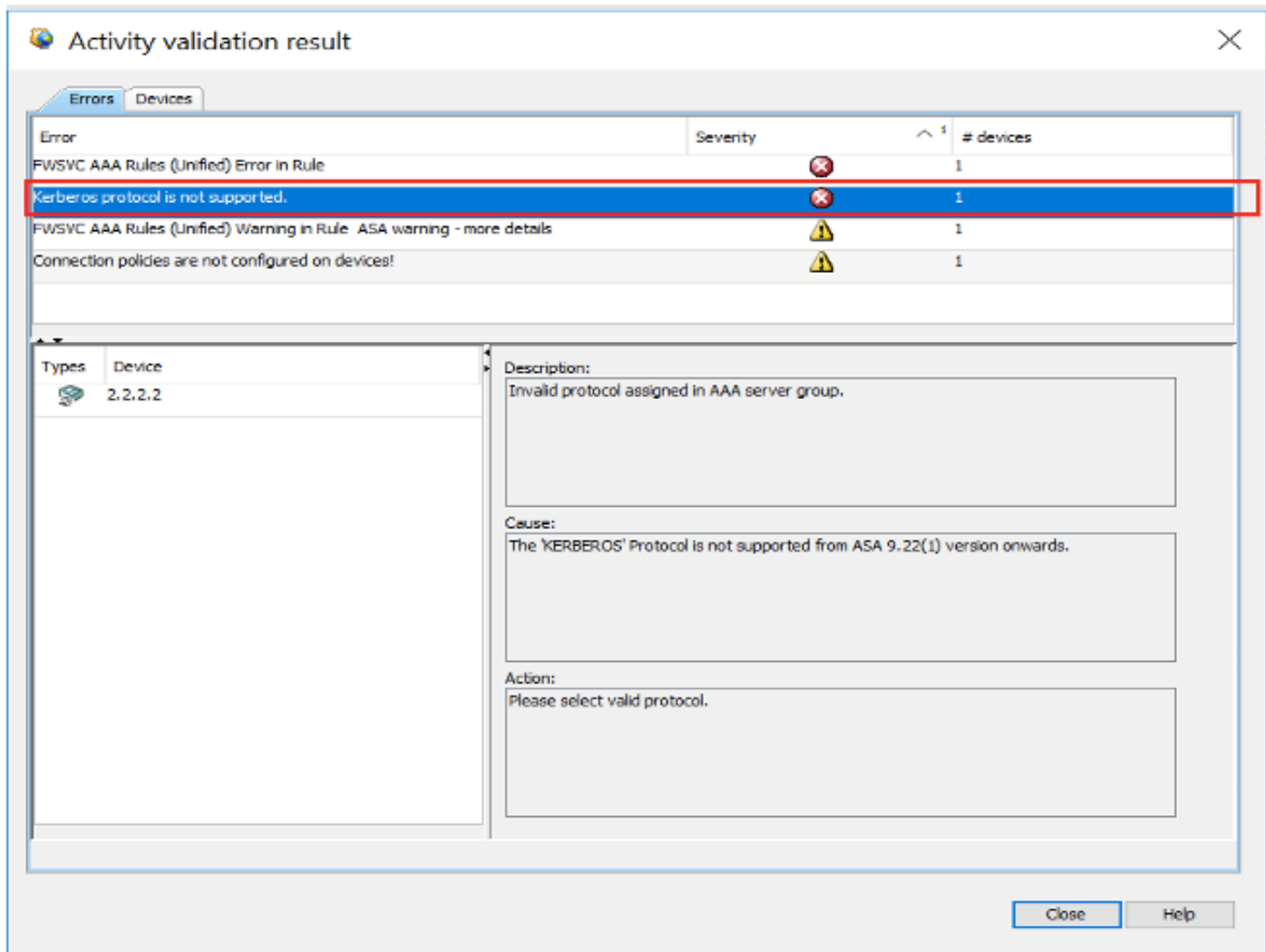


ASDM:LDAP SASL的Kerberos配置

CSM配置演練

CSM概述：

- 不再支援Kerberos協定。
- 這會降低終端使用者使用Kerberos協定和LDAP SASL機制配置AAA伺服器組的能力。
- Microsoft KCD Server也不再受支援。
- 不是從CSM中刪除Kerberos支援，而是在「活動驗證」中進行處理。
- 活動驗證會為9.22.1 ASA版本以後引發錯誤消息，指出9.22.1版本以後不支援Kerberos協定。



LDAP SASL的CSM Kerberos配置

路徑：CSM>防火牆> AAA規則> AAA伺服器組>新增>協定> LDAP >SASL

1. 儲存
2. 預覽活動驗證結果的配置。

Activity validation result

ErrorsDevices

Error	Severity	# devices
FWSVC AAA Rules (Unified) Error in Rule		1
Kerberos protocol is not supported.		1
FWSVC AAA Rules (Unified) Warning in Rule ASA warning - more details		1
Connection policies are not configured on devices!		1

TypesDevice

2.2.2.2

Description:

Invalid protocol assigned in AAA server group.

Cause:

The SASL kerberos Authentication is not supported from ASA 9.22(1) version onwards.

Action:

Please Disable SASL kerberos Authentication.

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）。