

# 从ASA 9.22中停用Kerberos

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[ASA CLI配置演练](#)

[ASDM配置演练](#)

[CSM配置演练](#)

---

## 简介

本文档介绍有关ASA 9.22中Kerberos弃用的见解。

## 先决条件

### 要求

思科建议您了解基本的安全概念：

- ASA CLI基础知识。
- AAA基础知识(身份验证、授权和记帐)

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

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

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。

## ASA CLI配置演练

ASA CLI概述：

- 在命令输出中，从CLI中删除了粗体的选项。
- 从包含这些配置的9.22之前的版本进行升级，会导致在引导期间控制台上出现警告消息。

ciscoasa(config)# aaa-server curve protocol ?

配置模式命令/选项：

http-form协议HTTP基于表单

kerberos协议Kerberos ( 已弃用 )

ldap协议LDAP

radius协议RADIUS

sdi协议SDI

tacacs+协议TACACS+

ciscoasa(config)# aaa-server curve protocol kerberos

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

AAA服务器配置命令：

exit从aaa-server group配置模式退出

aaa服务器配置命令的帮助帮助

max-failed-attempts指定组中任何服务器在停用之前允许的最大失败次数

no从aaa服务器组配置中删除项目

reactivation-mode指定重新激活故障服务器的方法

validate-kdc在kerberos用户身份验证期间启用KDC验证

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

执行模式命令/选项：

委托测试Kerberos约束委派

host输入此关键字以指定服务器的IP地址

模拟测试Kerberos协议转换

password Password关键字

自测Kerberos自检票检索

username Username关键字

ciscoasa(config)# aaa-server ldaps protocol ldap

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

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

aaa-server-host模式命令/选项：

digest-md5 select Digest-MD5

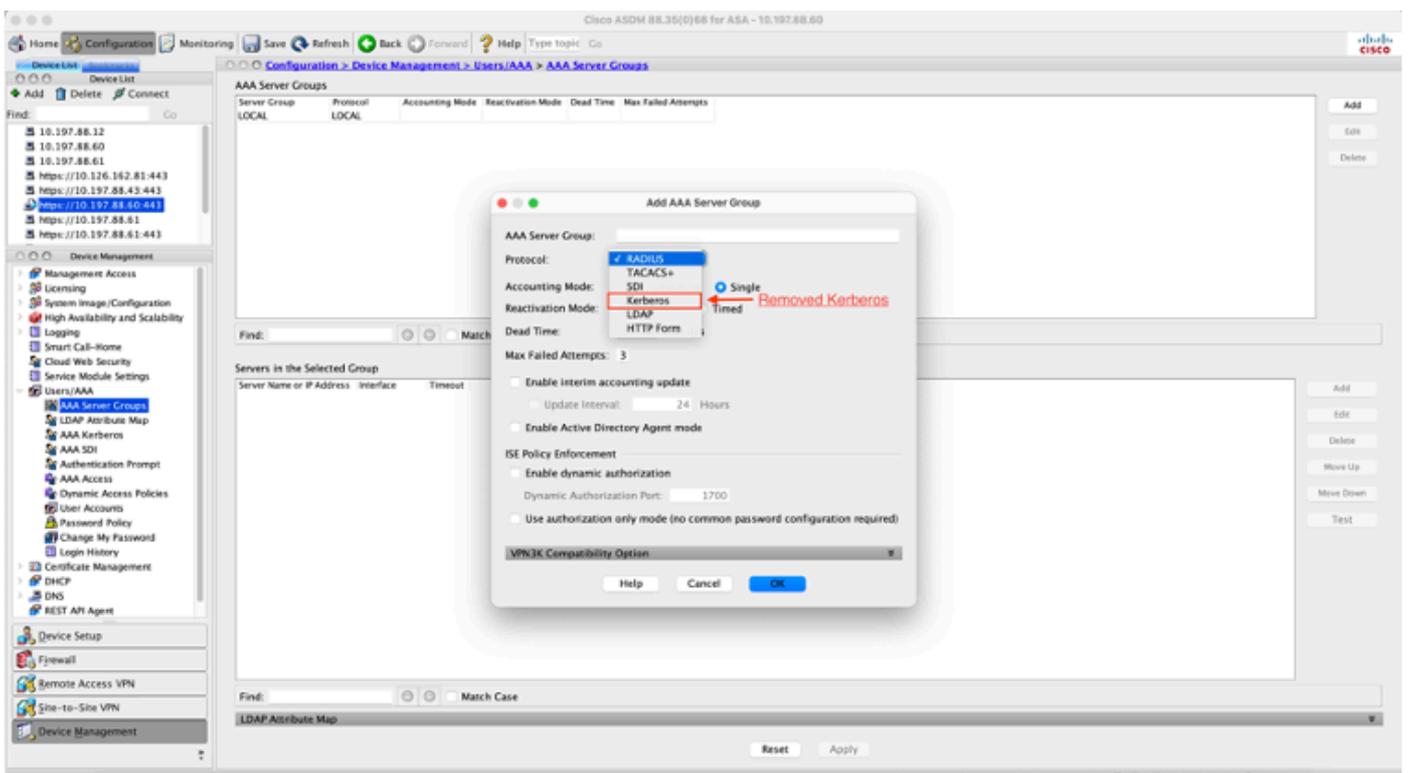
kerberos select Kerberos

ciscoasa(config)# debug kerberos

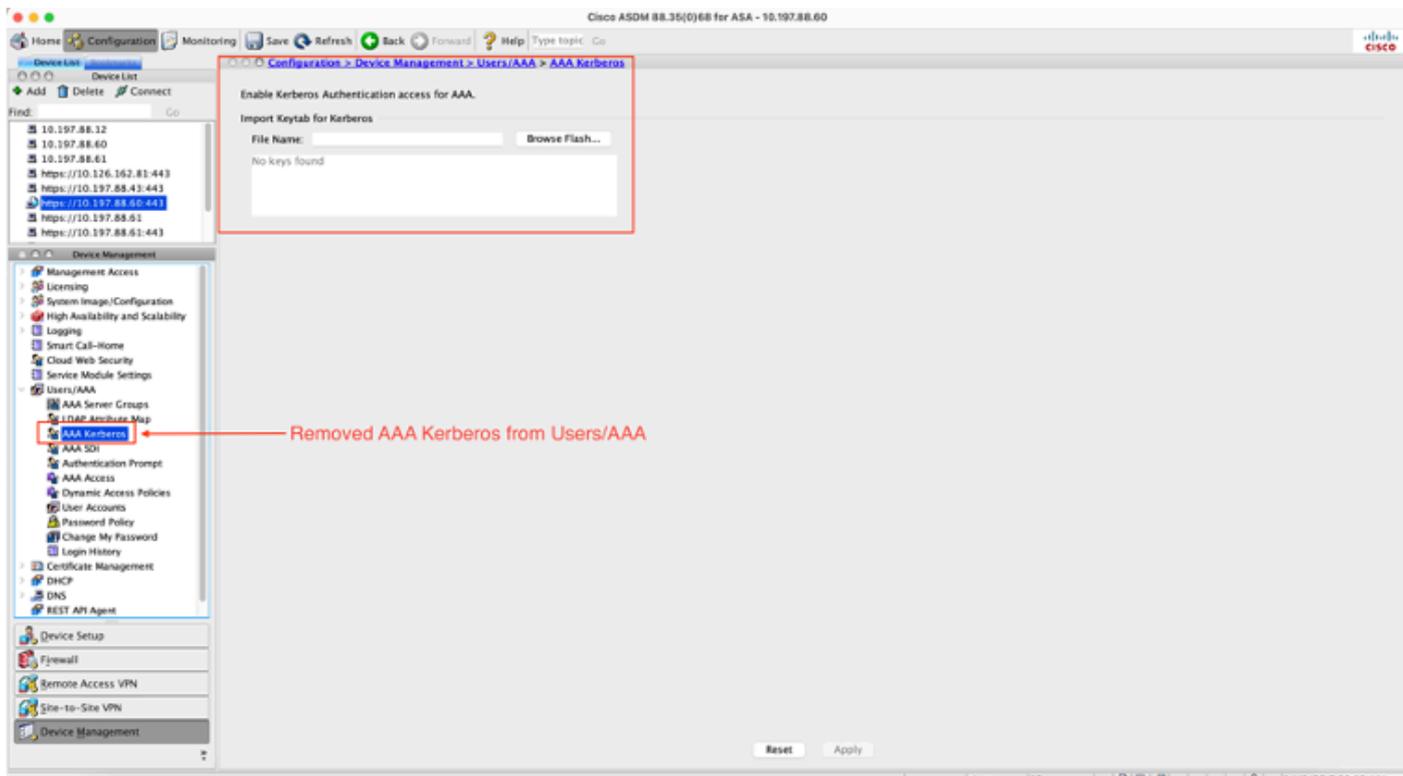
## ASDM配置演练

ASDM概述：

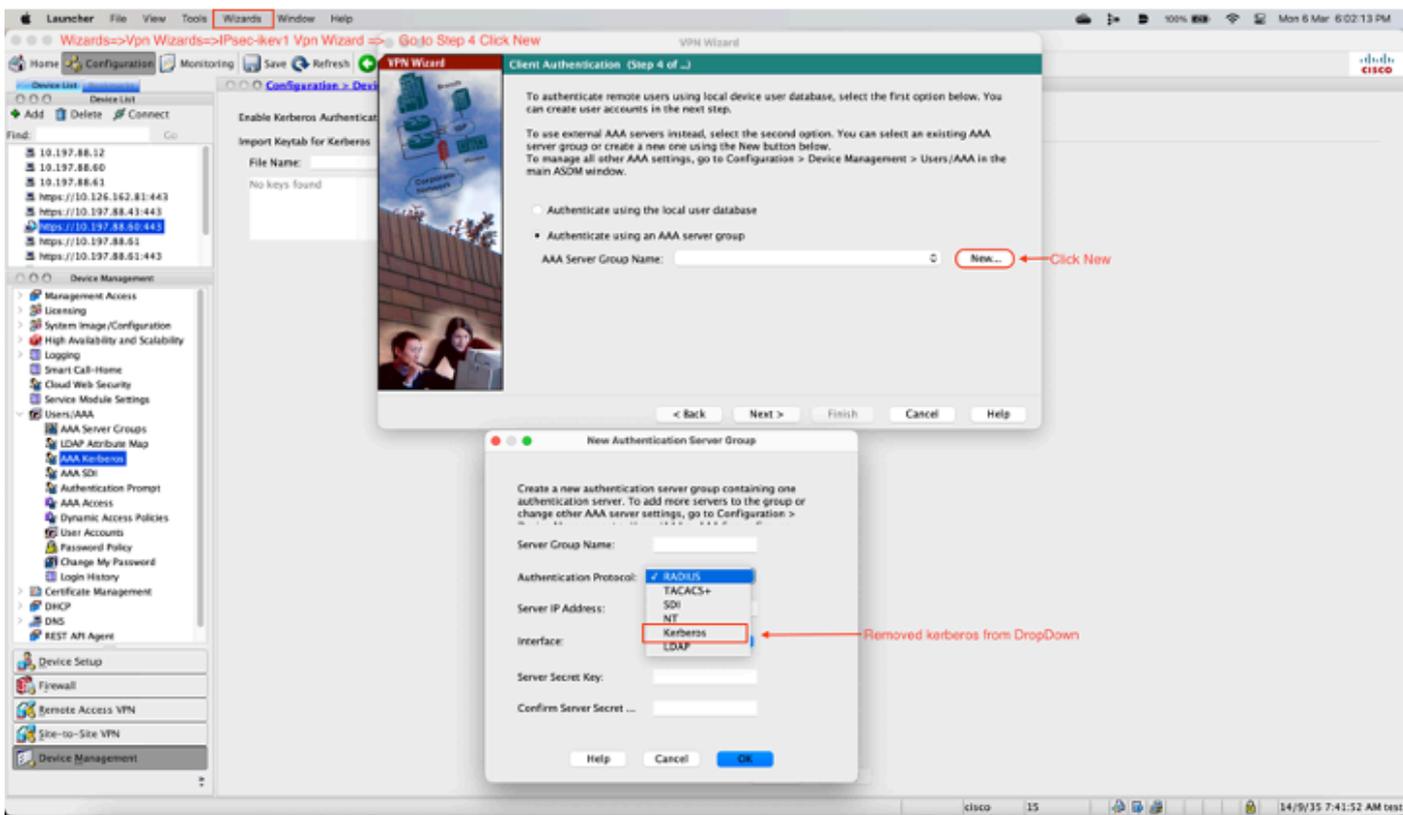
- ASDM 7.22不再支持Kerberos
- 这会降低最终用户使用Kerberos协议和LDAP SASL 机制配置AAA服务器组的能力。
- 作为此弃用的一部分，AAA Kerberos不再列在TreeMenu的Users/AAA in Device Management下。
- Microsoft KCD服务器也不再受支持。



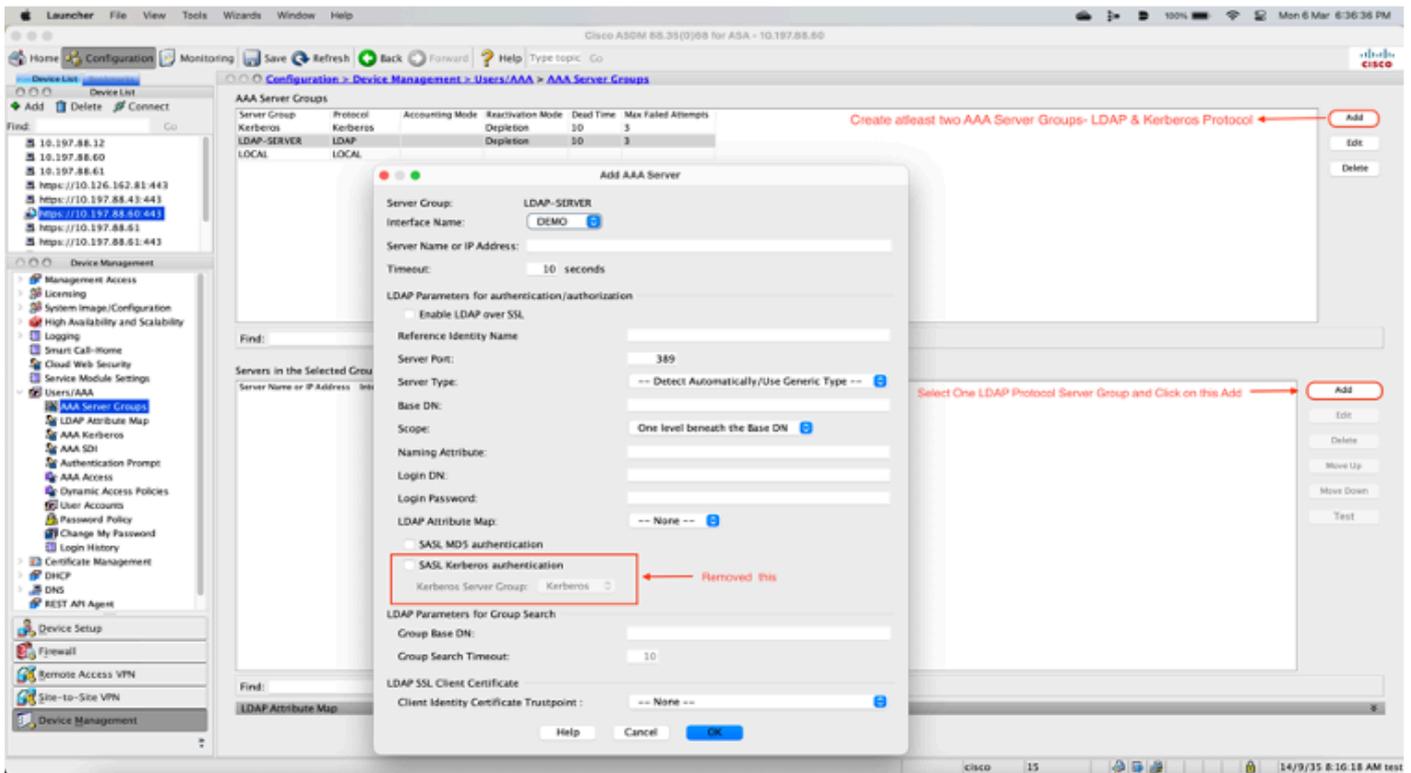
ASDM:新AAA服务器组中的Kerberos协议



ASDM:AAA Kerberos



ASDM:新AAA服务器组中的Kerberos协议

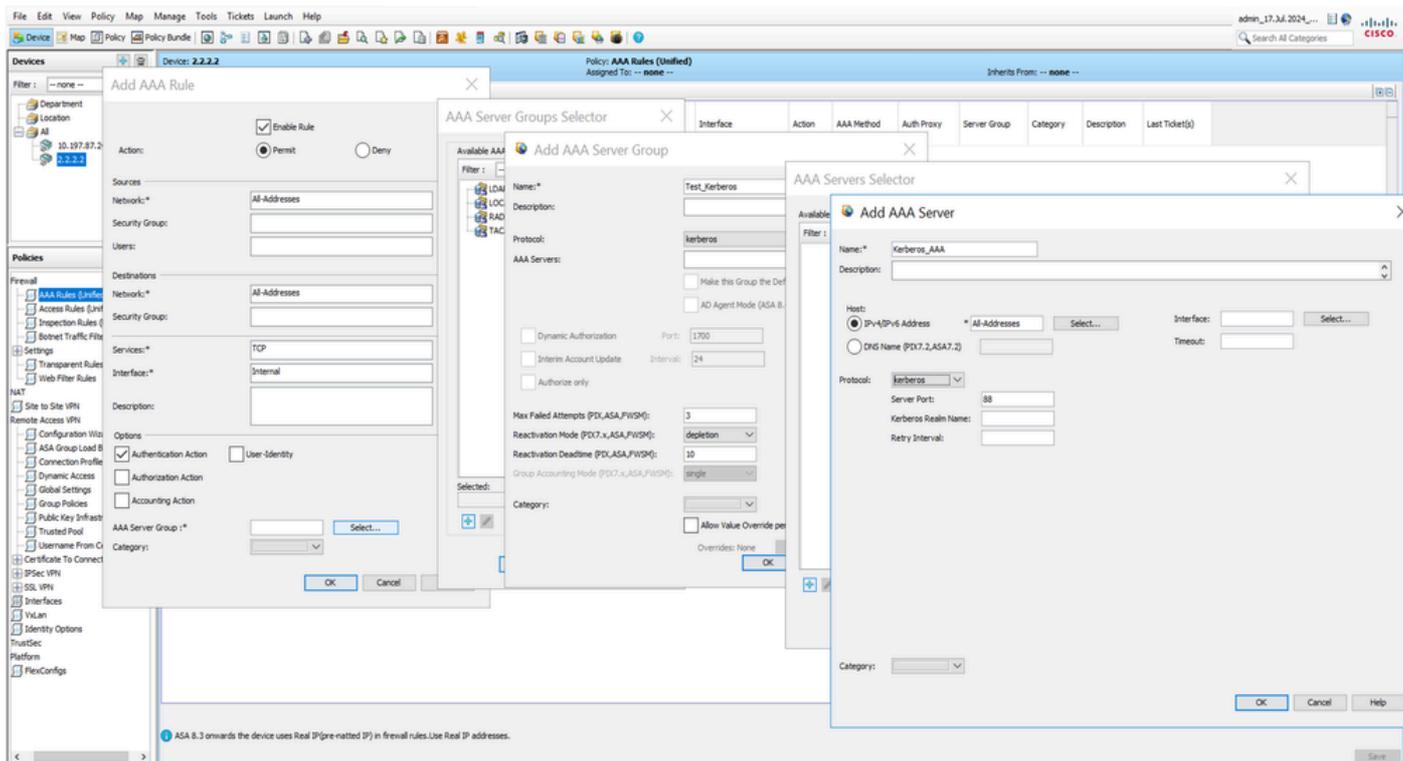


ASDM:LDAP SASL的Kerberos配置

## CSM配置演练

CSM概述：

- 不再支持Kerberos协议。
- 这会降低最终用户使用Kerberos协议和LDAP SASL 机制配置AAA服务器组的能力。
- Microsoft KCD服务器也不再受支持。
- 它不是从CSM中删除Kerberos支持，而是在活动验证中进行处理。
- 练习验证为9.22.1 ASA版本以后抛出错误消息，指出9.22.1版本以后不支持Kerberos协议。



## CSM Kerberos配置

路径：CSM>Firewall > AAA Rules > AAA Server Group > Add > Kerberos

1. 保存
2. 预览活动验证结果的配置。

### Activity validation result

Errors Devices

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

Types	Device	Description:
	2.2.2.2	Invalid protocol assigned in AAA server group.

**Cause:**  
The 'KERBEROS' Protocol is not supported from ASA 9.22(1) version onwards.

**Action:**  
Please select valid protocol.

Close Help

File Edit View Policy Map Manage Tools Tickets Launch Help

admin\_17-Jul-2024...

Devices: Device: 2.2.2.2 Policy: AAA Rules (Unified) Assigned To: -- none -- Inherits From: -- none --

Filter: -- none --

Department Location 10.107.87.2 2.2.2

AAA Rules (Unified) Add AAA Rule

Action:  Enable Rule  Permit  Deny

Sources: Network: All-Addresses Security Group: Users:

Destinations: Network: All-Addresses Security Group: Services: TCP Interface: Internal Description:

Options:  Authentication Action  User-Identity  Accounting Action AAA Server Group: \* Select... Category:

AAA Server Groups Selector

Available AAA Server Groups

Name: \* Test\_Kerberos Description: Protocol: kerberos AAA Servers:  Dynamic Authorization Port: 1700  Interim Account Update Interval: 24  Authorize only  AD Agent Mode (ASA 8.3) Max Failed Attempts (PDL,ASA,FWSM): 3 Reactivation Mode (PDL,ASA,FWSM): depletion Reactivation Deadline (PDL,ASA,FWSM): 10 Group Accounting Mode (PDL,ASA,FWSM): single Category:  Allow Value Override per Overrides: None

AAA Servers Selector

Available AAA Servers

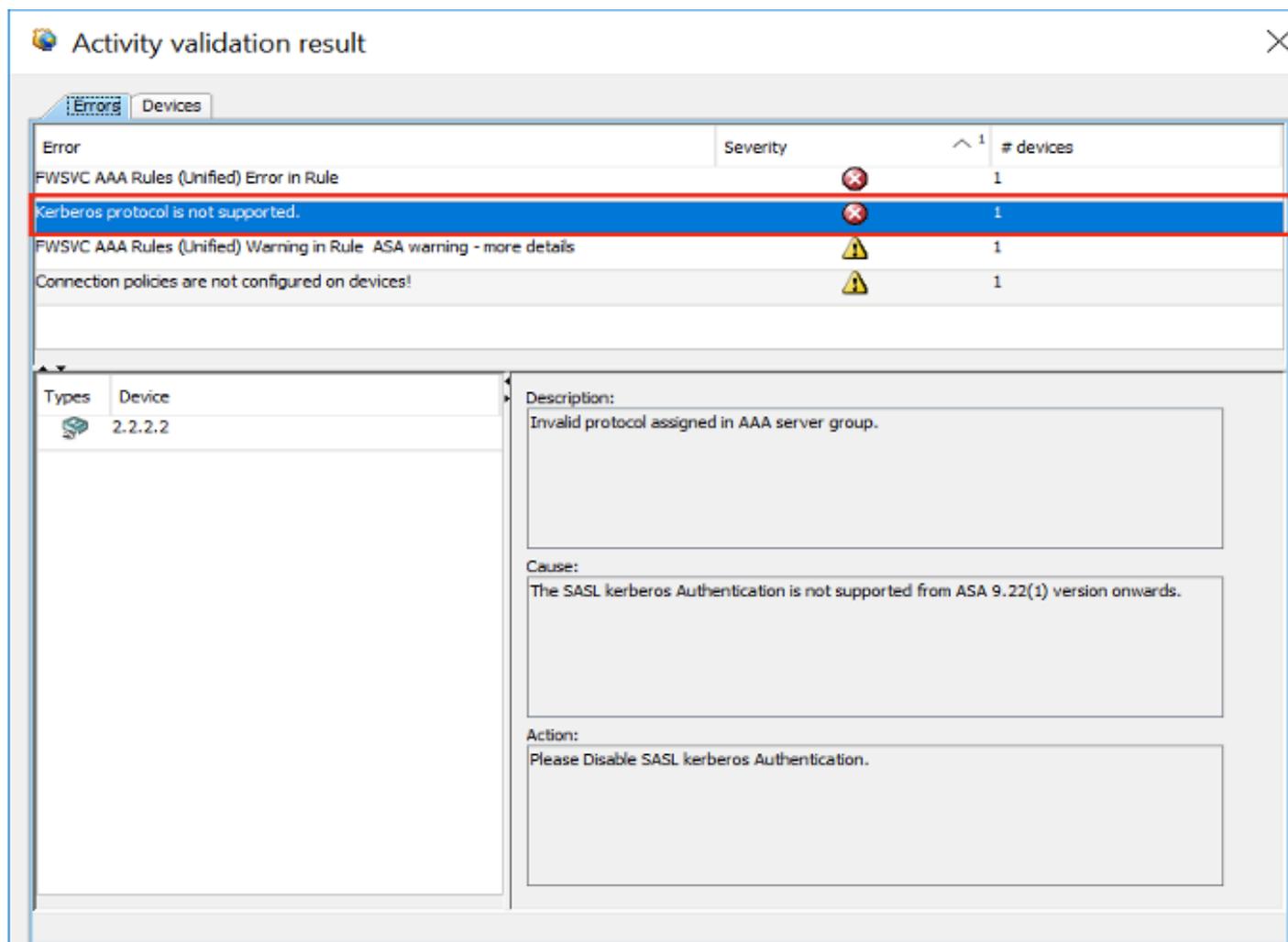
Name: \* Kerberos\_AAA Description: Host:  IPv4/IPv6 Address \* All-Addresses Select... Interface: Select...  DNS Name (PDL,ASA7.2) Timeout: Protocol: kerberos Server Port: 88 Kerberos Realm Name: Retry Interval:

ASA 8.3 onwards the device uses Real IP (pre-ratted IP) in firewall rules. Use Real IP addresses.

LDAP SASL的CSM Kerberos配置

路径：CSM>防火墙> AAA规则> AAA服务器组>添加>协议> LDAP >SASL

1. 保存
2. 预览活动验证结果的配置。



The screenshot shows a window titled "Activity validation result" with a close button in the top right corner. Below the title bar, there are two tabs: "Errors" (selected) and "Devices". The main area contains a table with the following data:

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

Below the table, there is a detailed view for the selected error. It includes a "Types" and "Device" list on the left, and a "Description", "Cause", and "Action" section on the right.

**Types**

Types	Device
	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.

## 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）。