

Uit bedrijf nemen van Kerberos vanaf ASA 9.22

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[ASA CLI-configuratieanalyse](#)

[ASDM-configuratieanalyse](#)

[CSM-configuratieanalyse](#)

Inleiding

In dit document wordt inzicht in de afbraak van Kerberos vanuit ASA 9.22 beschreven.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van basisbeveiligingsconcepten:

- Basiskennis van ASA CLI.
- Basiskennis van AAA (verificatie, autorisatie en accounting)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Alle ASA-platforms
- ASA CLI 9.2.1
- ASDM 7.2.1
- CSM 4.29

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

ASA CLI-configuratieanalyse

ASA CLI - Overzicht:

- In de opdrachtoutput zijn de vetgedrukte opties italichave uit de CLI verwijderd.

- Upgrades van versies voorafgaand aan 9.22 die deze configuraties bevatten resulteren in een waarschuwingsbericht op de console tijdens de opstarttijd.

ciscoasa(config)# aaa-server curb protocol?

opdrachten/opties voor configuratie-modus:

http-form Protocol HTTP-formuliergebaseerd

Kerberos Protocol Kerberos (AFGEKEURD)

LDAP-protocol LDAP

RADIUS-protocol RADIUS

SDI-protocol SDI

Tacacs+-protocol

ciscoasa(config)# aaa-server curb protocol kerberos

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

Opdrachten voor AAA-serverconfiguratie:

afsluiten uit configuratiemodus van aaa-servergroep

Help-ondersteuning voor configuratieopdrachten voor AAA-server

max-fail-pogingen Geef het maximum aantal storingen op dat is toegestaan voor elke server in de groep voordat die server wordt gedeactiveerd

no Verwijder een item uit de configuratie van de aaa-servergroep

reactiveringsmodus Hiermee geeft u de methode op waarmee defecte servers worden gereactiveerd

validate-kdc KDC-validatie inschakelen tijdens kerberos user auth

ciscoasa (config)# test aaa-server authenticatie curb?

Opdrachten/opties voor uitvoermodus:

gedelegeerde Test Kerberos beperkte delegatie

host Voer dit trefwoord in om het IP-adres voor de server op te geven

Testen Kerberos-protocolovergang nabootsen

wachtwoord wachtwoord wachtwoord wachtwoord wachtwoord

self-Test Kerberos self-ticket ophalen

Gebruikersnaam Gebruikersnaam sleutelwoord

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-mechanisme?

Opdrachten/opties voor Aa-server-host modus:

digest-md5 selecteer Digest-MD5

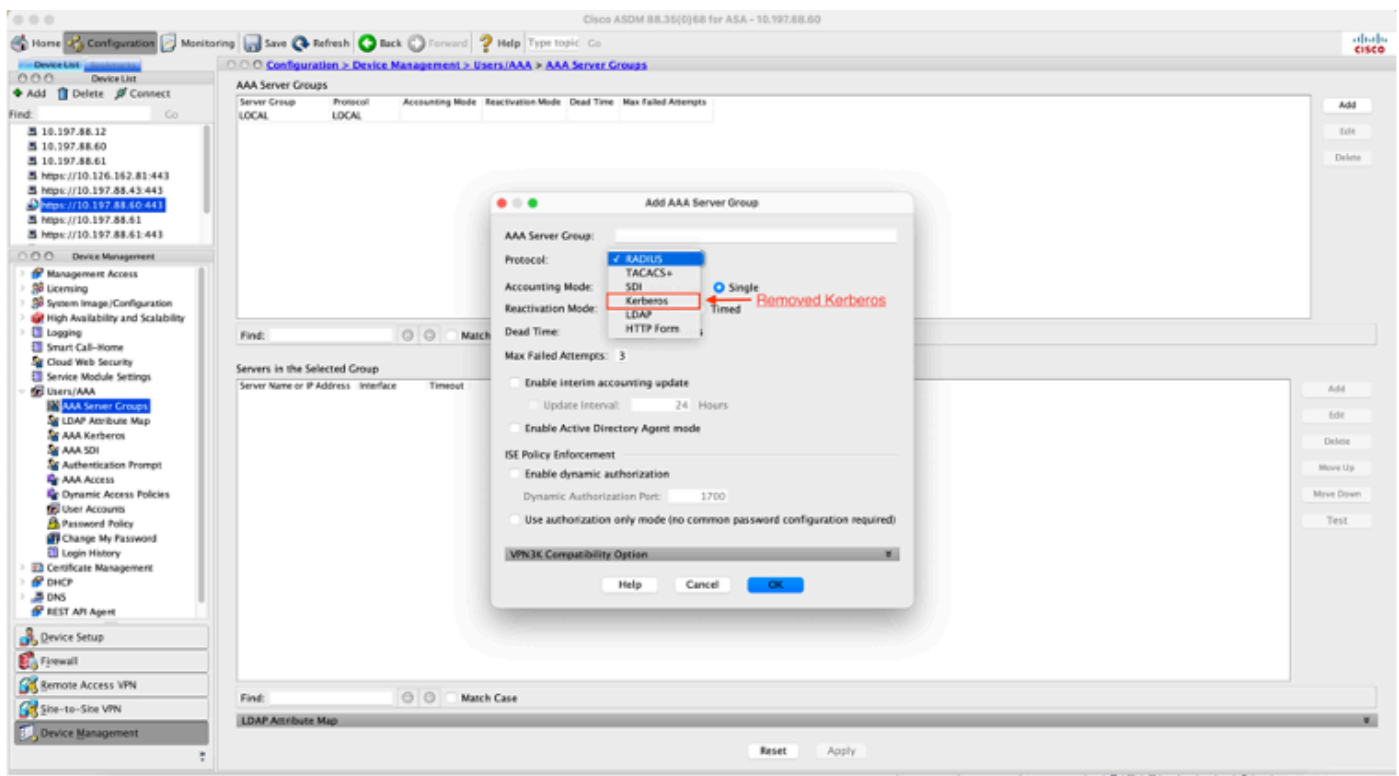
kerberos selecteren Kerberos

ciscoasa (config)# debug kerberos

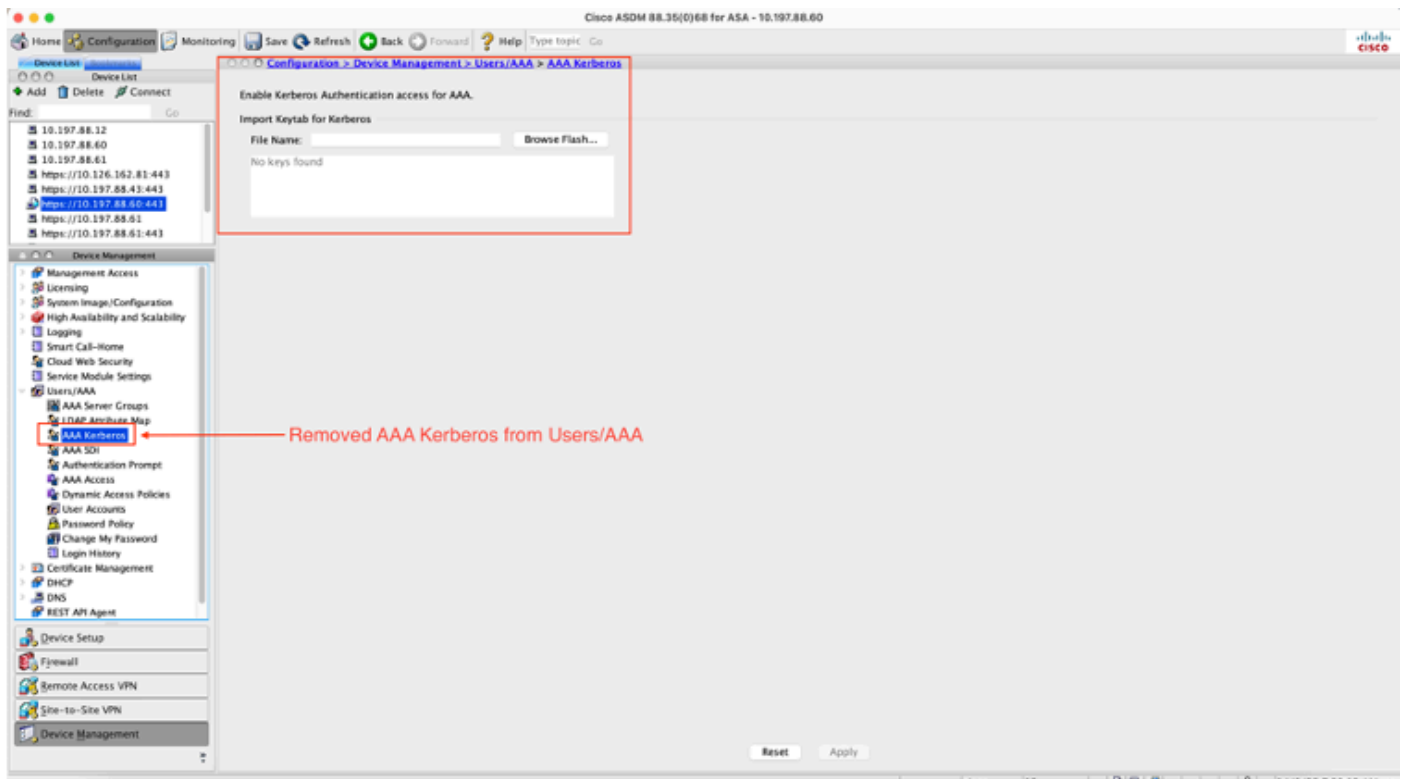
ASDM-configuratieanalyse

ASDM-overzicht:

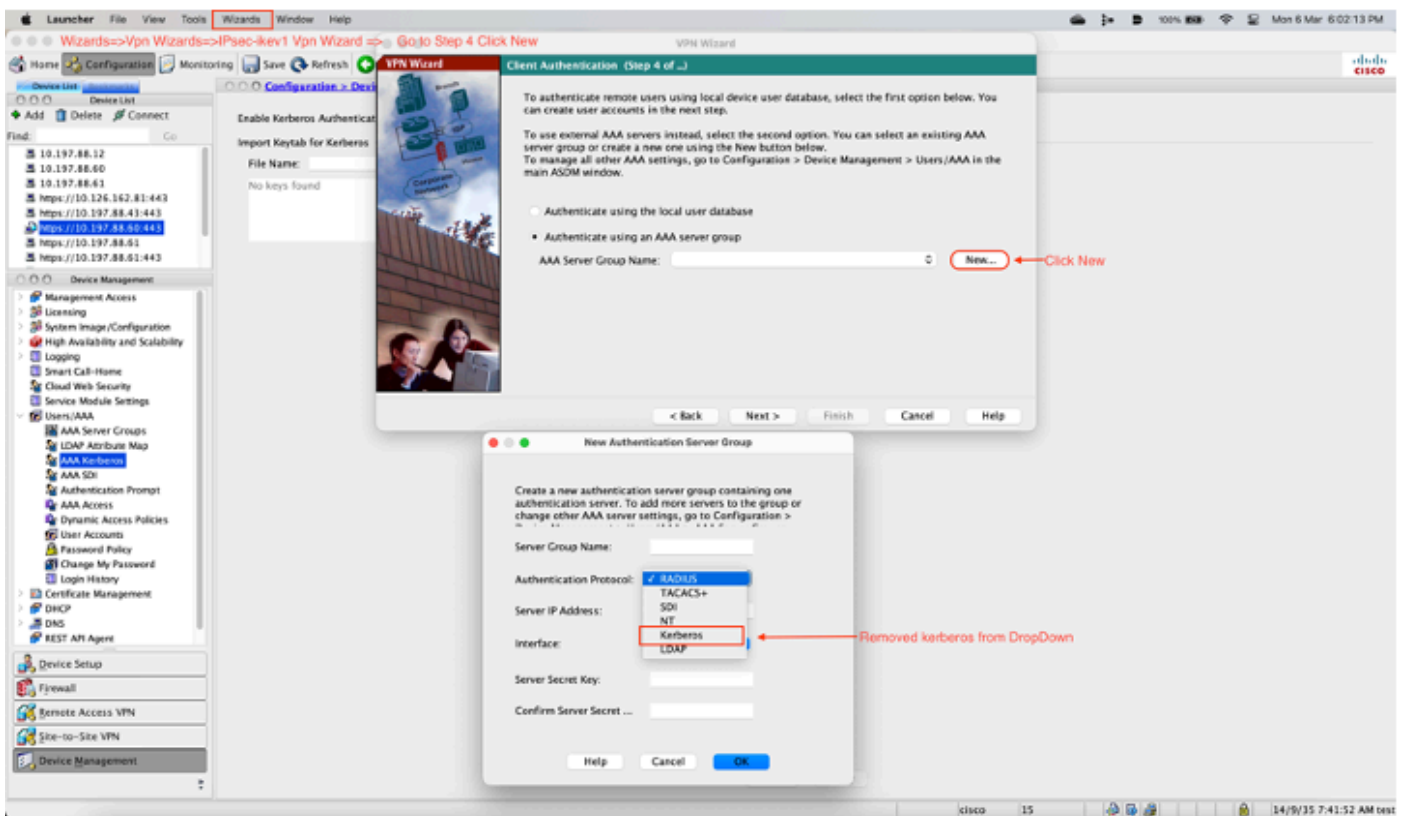
- Kerberos wordt niet meer ondersteund door ASDM 7.22
- Hierdoor wordt de mogelijkheid voor eindgebruikers om AAA-servergroepen te configureren met het Kerberos-protocol en met het LDAP SASL-mechanisme afgekeurd.
- Als deel van deze afschrijving, is AAA Kerberos niet meer vermeld in TreeMenu onder Gebruikers/AAA in Apparaatbeheer.
- Microsoft KCD Server wordt ook niet meer ondersteund.



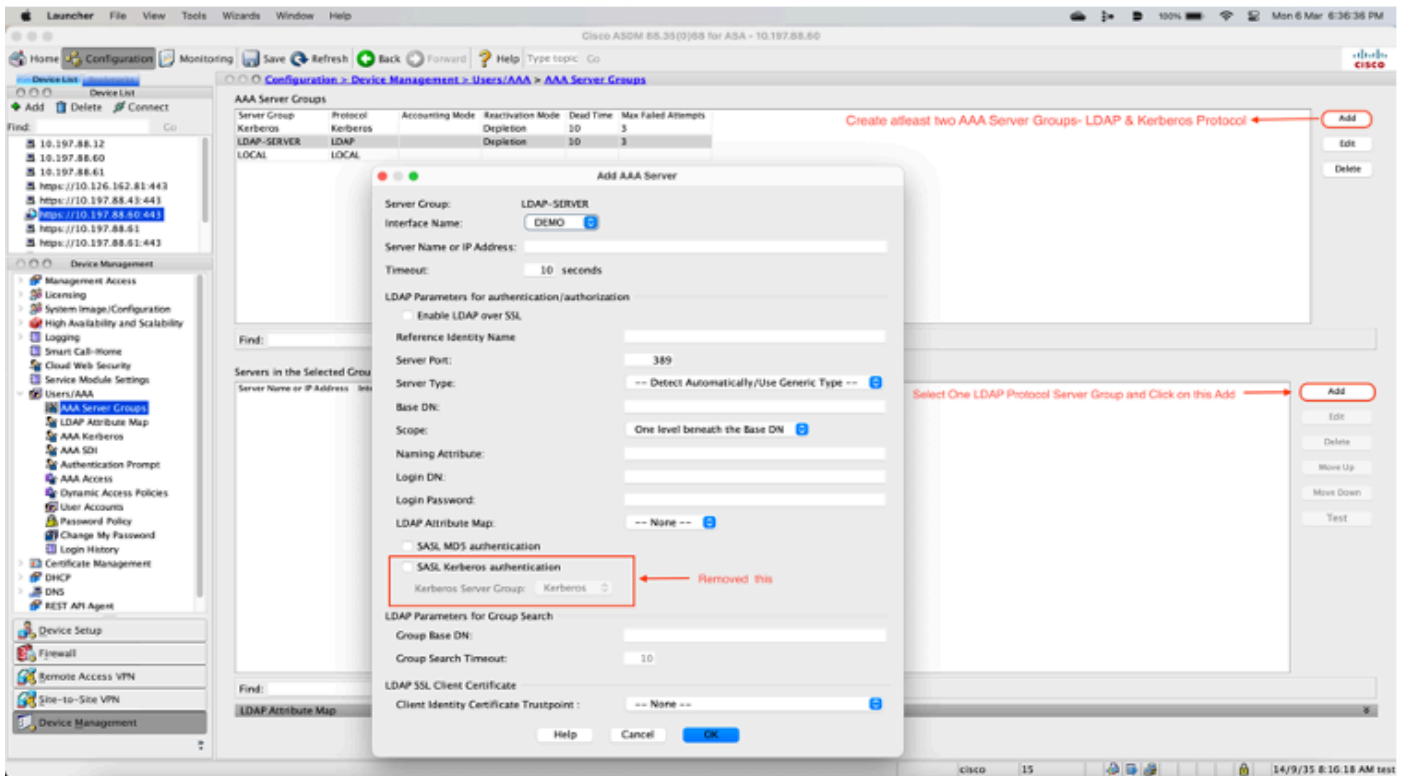
ASDM: Kerberos-protocol in nieuwe AAA-servergroep



ASDM: AAA Kerberos



ASDM: Kerberos-protocol in nieuwe AAA-servergroep

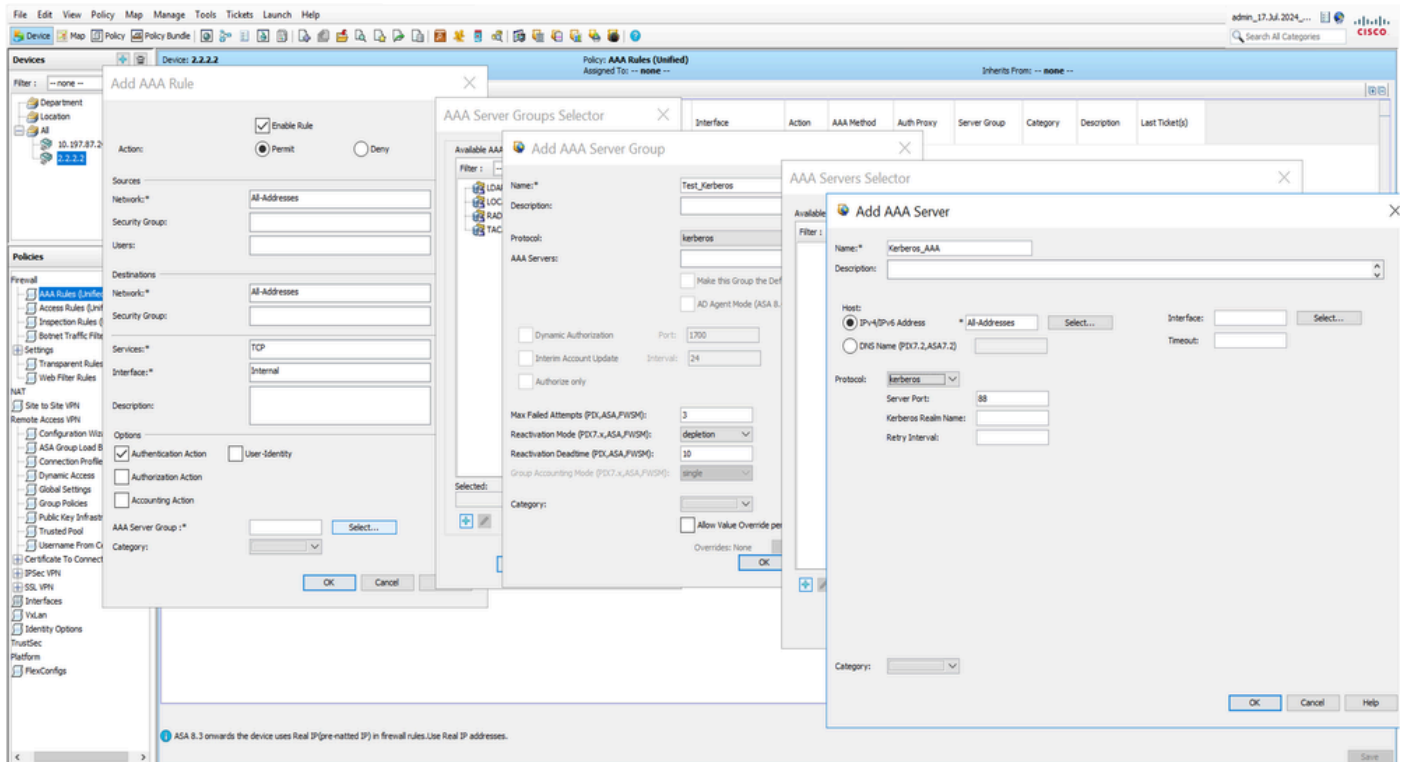


ASDM: Kerberos-configuratie voor LDAP SASL

CSM-configuratieanalyse

CSM - Overzicht:

- Kerberos-protocol wordt niet langer ondersteund.
- Hierdoor wordt de mogelijkheid voor eindgebruikers om AAA-servergroepen te configureren met het Kerberos-protocol en met het LDAP SASL-mechanisme afgekeurd.
- Microsoft KCD Server wordt ook niet meer ondersteund.
- In plaats van Kerberos-ondersteuning te verwijderen uit CSM, wordt deze verwerkt in Activiteitsvalidatie.
- Activeringsvalidatie geeft een foutmelding voor 9.22.1 ASA-versie en zegt dat Kerberos-protocol vanaf versie 9.22.1 niet wordt ondersteund.



Configuratie CSM Kerberos

PAD: CSM>Firewall > AAA-regels > AAA-servergroep > Toevoegen > Kerberos

1. Opslaan
2. Voorbeeld van Config voor resultaat van activiteitenvalidatie.

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 - more details		1
Connection policies are not configured on devices!		1

Types

Device

2.2.2.2

Description:

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...

Search All Categories

Device

Map

Policy

Policy Bundle

Tools

Tickets

Launch

Help

Devices

Device: 2.2.2.2

Policy: AAA Rules (Unified)

Assigned To: none

Inherits From: none

Filter: --none--

Department

Location

10.177.87.2

2.2.2

Policies

AAA Rules (Unified)

Access Rules (Unit)

Inspection Rules (Unit)

Botnet Traffic Filter

Settings

Transparent Rules

Web Filter Rules

NAT

Site to Site VPN

Remote Access VPN

Configuration VPN

ASA Group Load B

Connection Profile

Dynamic Access

Global Settings

Group Policies

Public Key Infrastr

Trusted Pool

Username From C

Certificate To Connect

IPSec VPN

SSL VPN

Interfaces

VLAN

Identity Options

TrustSec

Platform

FlexConfig

Add AAA Rule

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

Authorization Action

Accounting Action

AAA Server Group:

Select...

Category:

OK

Cancel

AAA Server Groups Selector

Available AAA

Filter:

LDAP

LOC

RAO

TAC

Add AAA Server Group

Name:

Test_Kerberos

Description:

Protocol:

kerberos

AAA Servers:

Dynamic Authorization

Port:

1700

Interim Account Update

Interval:

24

Authorize only

Max Failed Attempts (PDLASA/FWSM):

3

Reactivation Mode (PD17.x,ASA/FWSM):

depletion

Reactivation Deadline (PD17.x,ASA/FWSM):

10

Group Accounting Mode (PD17.x,ASA/FWSM):

single

Category:

Allow Value Override per

Overrides: None

OK

AAA Servers Selector

Available

Filter:

Add AAA Server

Name:

Kerberos_AAA

Description:

Host:

IPv4/IPv6 Address

All-Addresses

Select...

Interface:

Select...

Timeout:

Protocol:

kerberos

Server Port:

88

Kerberos Realm Name:

Retry Interval:

Category:

OK

Cancel

Help

CSM Kerberos-configuratie voor LDAP SASL

PAD: CSM>Firewall > AAA-regels > AAA-servergroep > Add > Protocol > LDAP > SASL

1. Opslaan
2. Voorbeeld van Config voor resultaat van activiteitenvalidatie.

The screenshot shows a window titled 'Activity validation result' with a close button in the top right corner. Inside the window, there are two tabs: 'Errors' and 'Devices'. The 'Errors' tab is active, displaying a table of validation errors.

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 'Kerberos protocol is not supported.'. 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.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.