

Außerbetriebnahme von Kerberos von ASA 9.22

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[ASA CLI-Konfiguration - exemplarische Vorgehensweise](#)

[ASDM-Konfiguration - exemplarische Vorgehensweise](#)

[CSM-Konfiguration - exemplarische Vorgehensweise](#)

Einleitung

In diesem Dokument werden Erkenntnisse zur Kerberos-Deprecation von ASA 9.22 beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse folgender grundlegender Sicherheitskonzepte verfügen:

- Grundlegende Kenntnisse der ASA CLI
- Grundkenntnisse von AAA (Authentifizierung, Autorisierung und Abrechnung)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Alle ASA-Plattformen
- ASA CLI 9.22.1
- ASDM 7,22,1
- CSM 4,29

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

ASA CLI-Konfiguration - exemplarische Vorgehensweise

ASA CLI im Überblick:

- In der Befehlsausgabe wurden die Optionen inbold italichaus der CLI entfernt.
- Upgrades von älteren Versionen als Version 9.22, die diese Konfigurationen enthalten, führen während des Bootvorgangs zu einer Warnmeldung auf der Konsole.

ciscoasa(config)# aaa-server curb protocol ?

Befehle/Optionen für den Konfigurationsmodus:

HTTP-Form Protokoll, formularbasiert

Kerberos-Protokoll Kerberos (VERALTET)

LDAP LDAP-Protokoll

RADIUS-Protokoll

sdi-Protokoll SDI

TACACS+-Protokoll TACACS+

ciscoasa(config)# aaa-server curb-Protokoll kerberos

ciscoasa(config-aaa-server-group)#

AAA-Serverkonfigurationsbefehle:

Beenden Beenden des Konfigurationsmodus aaa-server group

Hilfe zu AAA-Serverkonfigurationsbefehlen

max-failed-attempts Geben Sie die maximale Anzahl von Fehlern an, die für einen beliebigen Server in der Gruppe zulässig sind, bevor dieser Server deaktiviert wird.

no Artikel aus aaa-server-Gruppenkonfiguration entfernen

Reaktivierungsmodus Geben Sie an, wie ausgefallene Server reaktiviert werden sollen.

validate-kdc KDC-Validierung während der Kerberos-Benutzerauthentifizierung aktivieren

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

Befehle/Optionen des exec-Modus:

delegieren Eingeschränkte Delegation von Test Kerberos

host Geben Sie dieses Schlüsselwort ein, um die IP-Adresse für den Server anzugeben.

imitieren Test Kerberos Protokoll Übergang

Kennwort Kennwort Kennwort-Schlüsselwort

Selbsttest Kerberos Selbstfahrcheinabruf

username Benutzername Schlüsselwort

ciscoasa(config)# aaa-server ldaps Protokoll ldap

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

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

aaa-server-host mode-Befehle/-Optionen:

Digest-MD5 auswählen

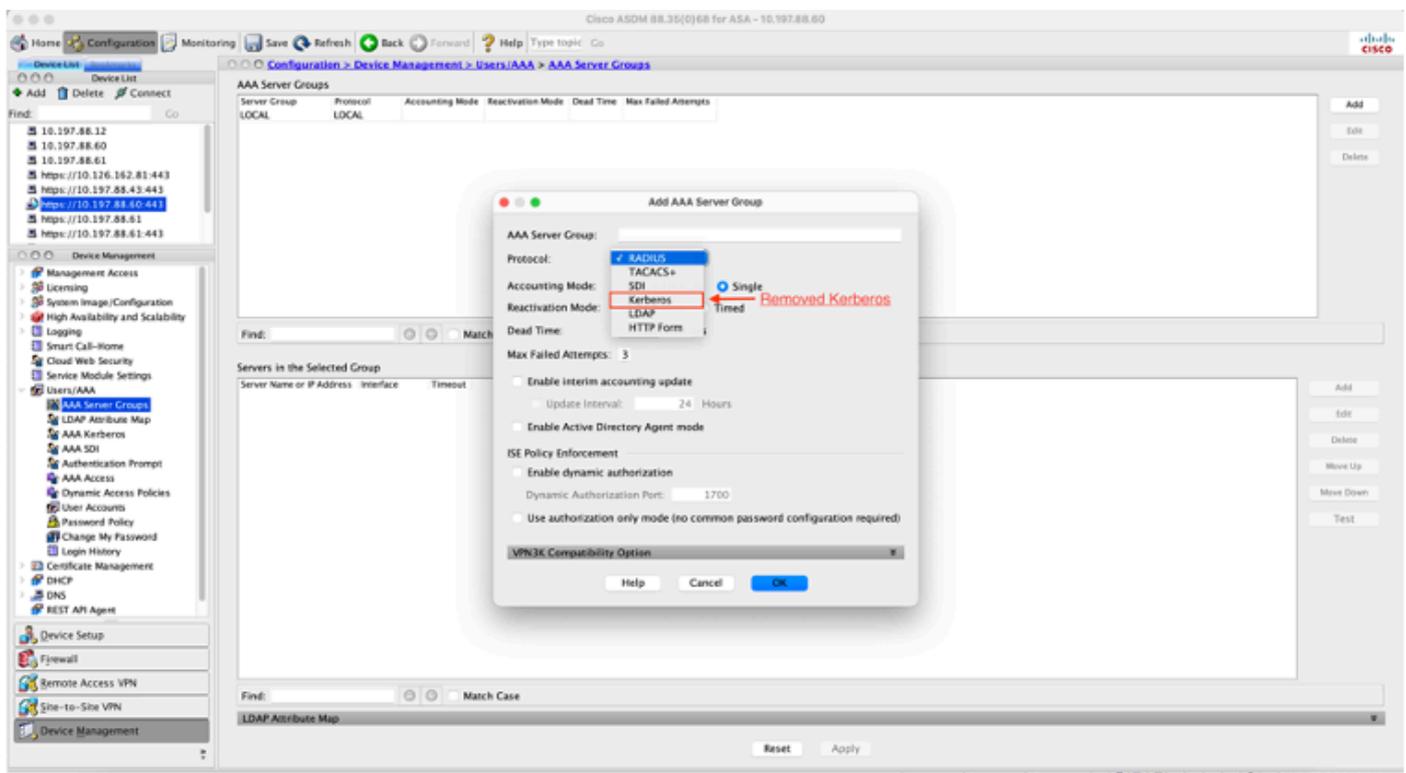
kerberos auswählen Kerberos

ciscoasa(config)# debug kerberos

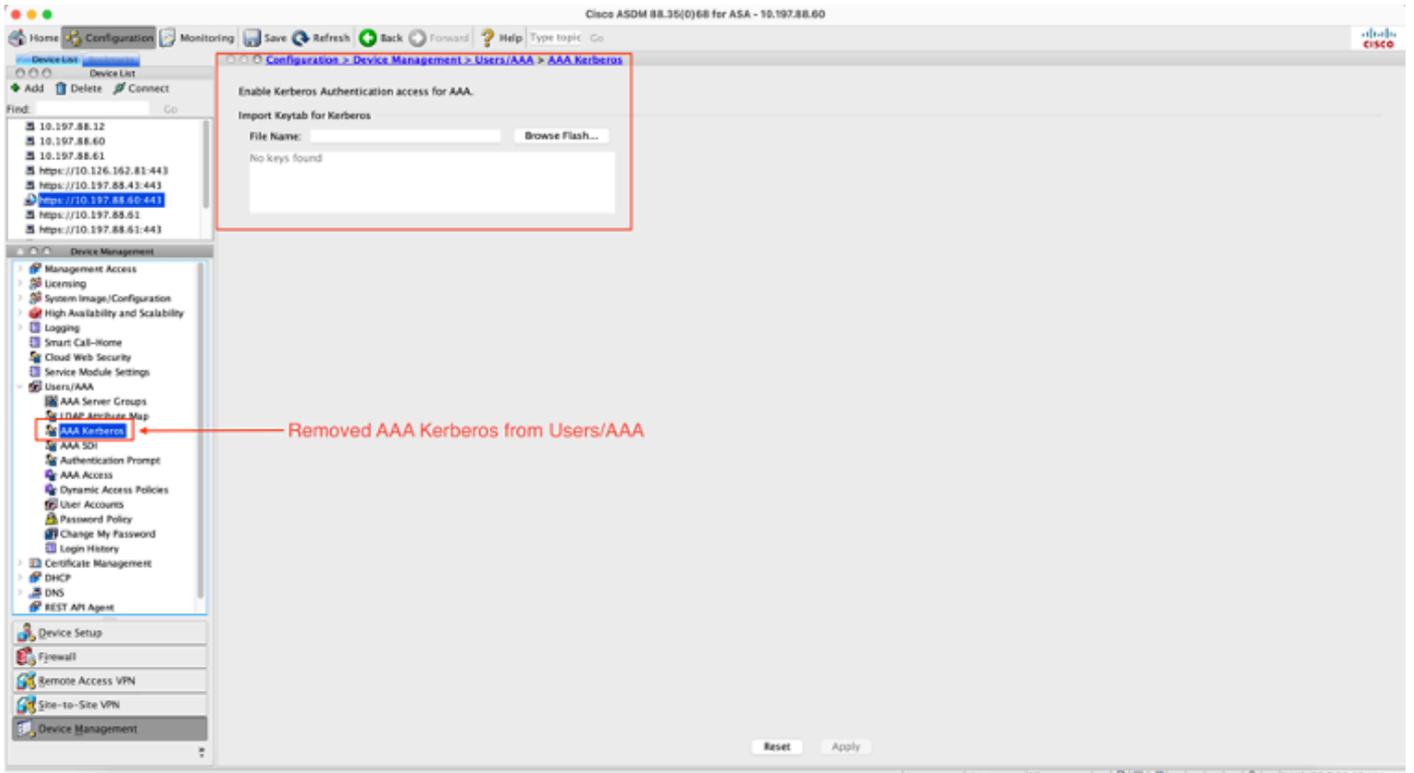
ASDM-Konfiguration - exemplarische Vorgehensweise

ASDM - Übersicht:

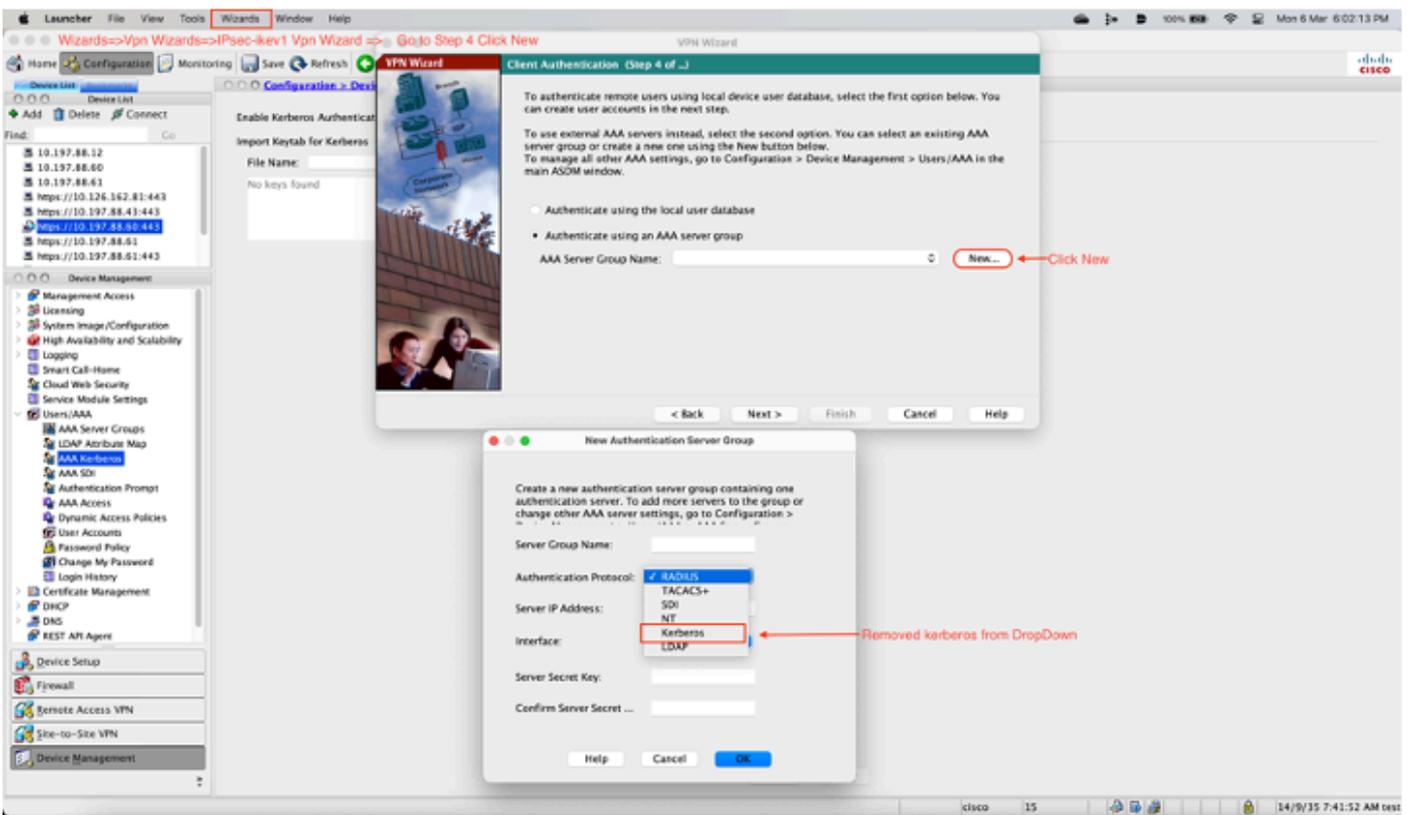
- Kerberos wird von ASDM 7.22 nicht mehr unterstützt.
- Dadurch wird die Möglichkeit für Endbenutzer vernachlässigt, AAA-Servergruppen mit dem Kerberos-Protokoll und dem LDAP-SASL-Mechanismus zu konfigurieren.
- Als Teil dieser Wertminderung wird AAA Kerberos in der Geräteverwaltung nicht mehr im TreeMenu unter Benutzer/AAA aufgeführt.
- Microsoft KCD Server wird ebenfalls nicht mehr unterstützt.



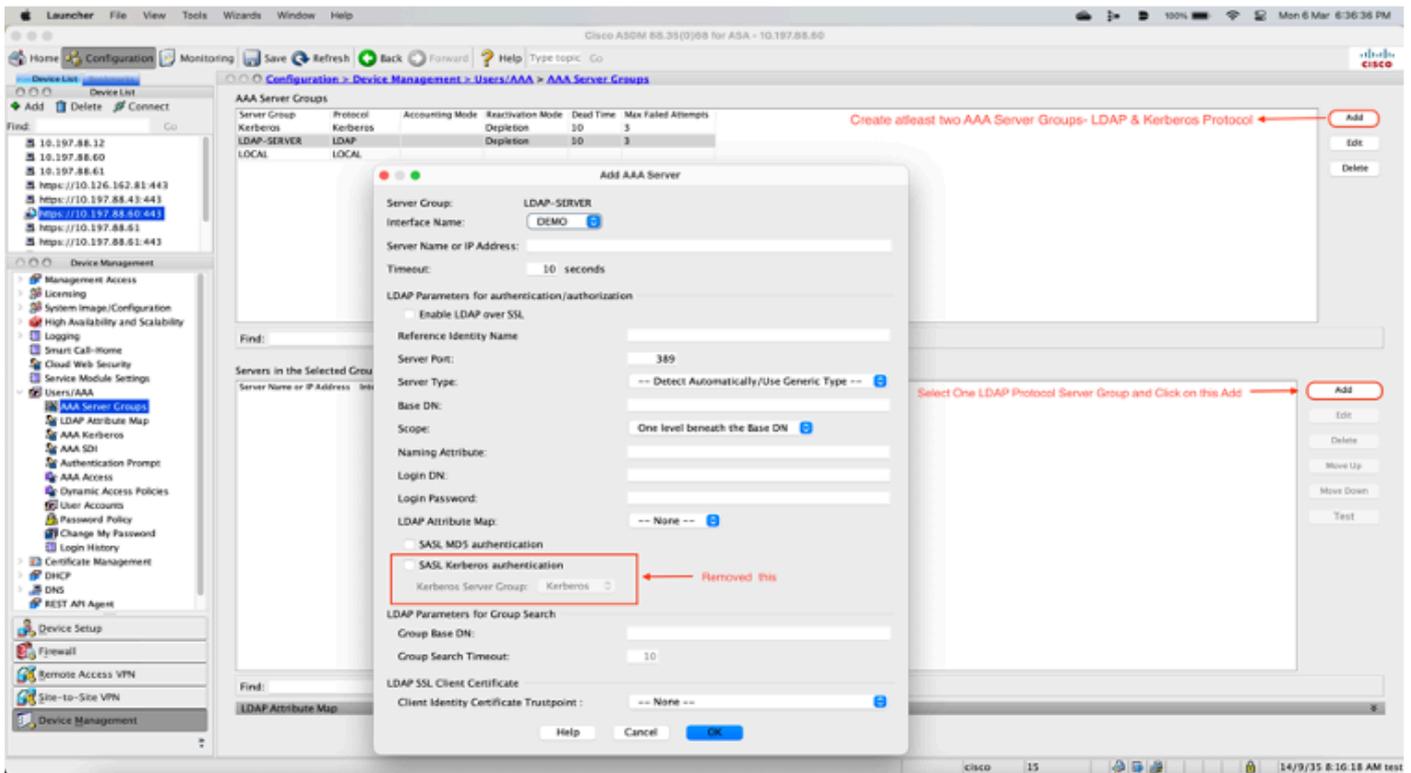
ASDM: Kerberos-Protokoll in neuer AAA-Servergruppe



ASDM: AAA Kerberos



ASDM: Kerberos-Protokoll in neuer AAA-Servergruppe

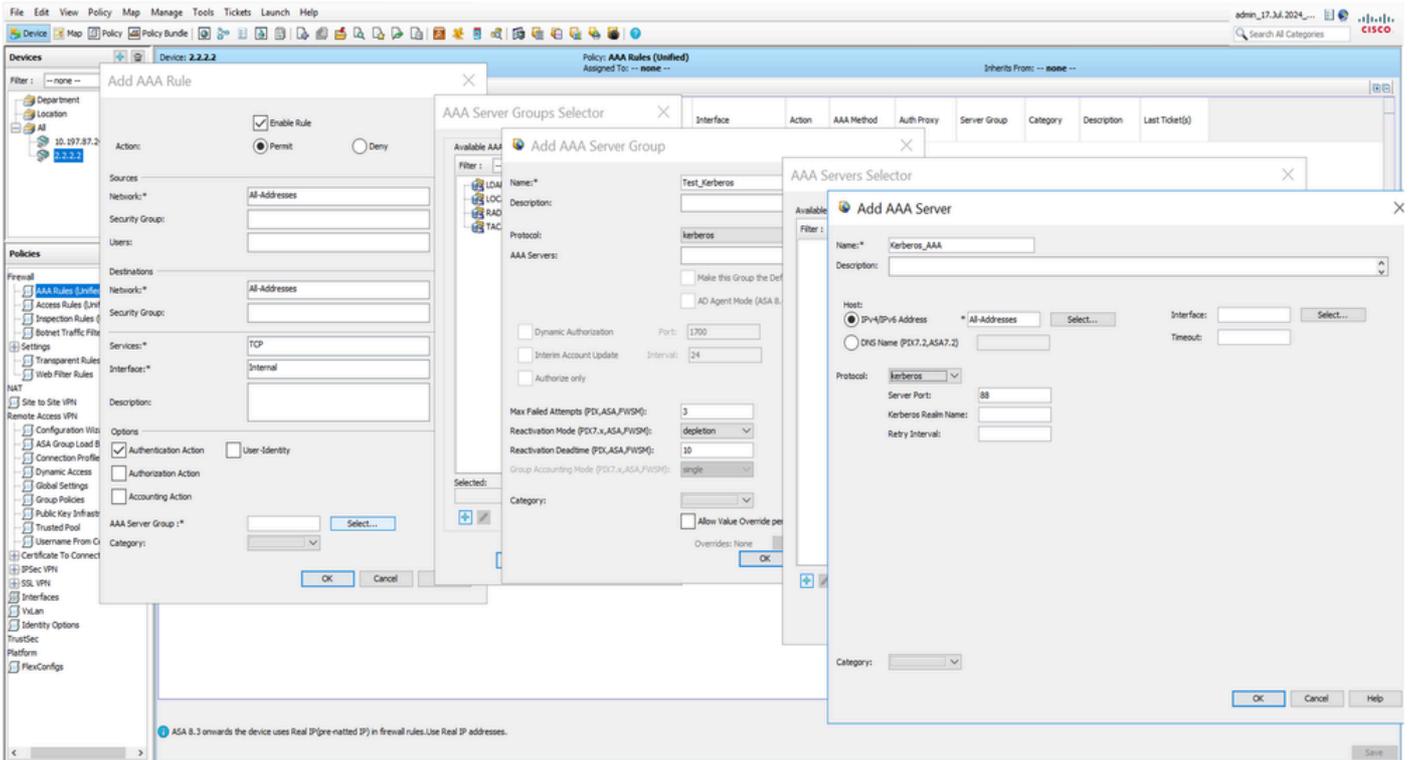


ASDM: Kerberos-Konfiguration für LDAP-SASL

CSM-Konfiguration - exemplarische Vorgehensweise

CSM im Überblick:

- Das Kerberos-Protokoll wird nicht mehr unterstützt.
- Dadurch wird die Möglichkeit für Endbenutzer vernachlässigt, AAA-Servergruppen mit dem Kerberos-Protokoll und dem LDAP-SASL-Mechanismus zu konfigurieren.
- Microsoft KCD Server wird ebenfalls nicht mehr unterstützt.
- Anstatt die Kerberos-Unterstützung aus CSM zu entfernen, wird sie in der Aktivitätsvalidierung behandelt.
- Die Aktivitätsvalidierung löst eine Fehlermeldung für die ASA-Version 9.22.1 aus, die besagt, dass das Kerberos-Protokoll ab Version 9.22.1 nicht mehr unterstützt wird.



Konfiguration des CSM-Kerberos

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

1. Speichern
2. Vorschau der Konfiguration für das Ergebnis der Aktivitätsvalidierung

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 --

Add AAA Rule

Enable Rule Permit Deny

Action: 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:

AAA Server Groups Selector

Add AAA Server Group

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

Add AAA Server

Available AAA Servers

Name: * Kerberos_AAA Description: Host: IPv4/IPv6 Address All-Addresses DNS Name (PDL,ASA7.2)

Server Port: 88 Kerberos Realm Name: Retry Interval: Timeout:

Protocol: kerberos

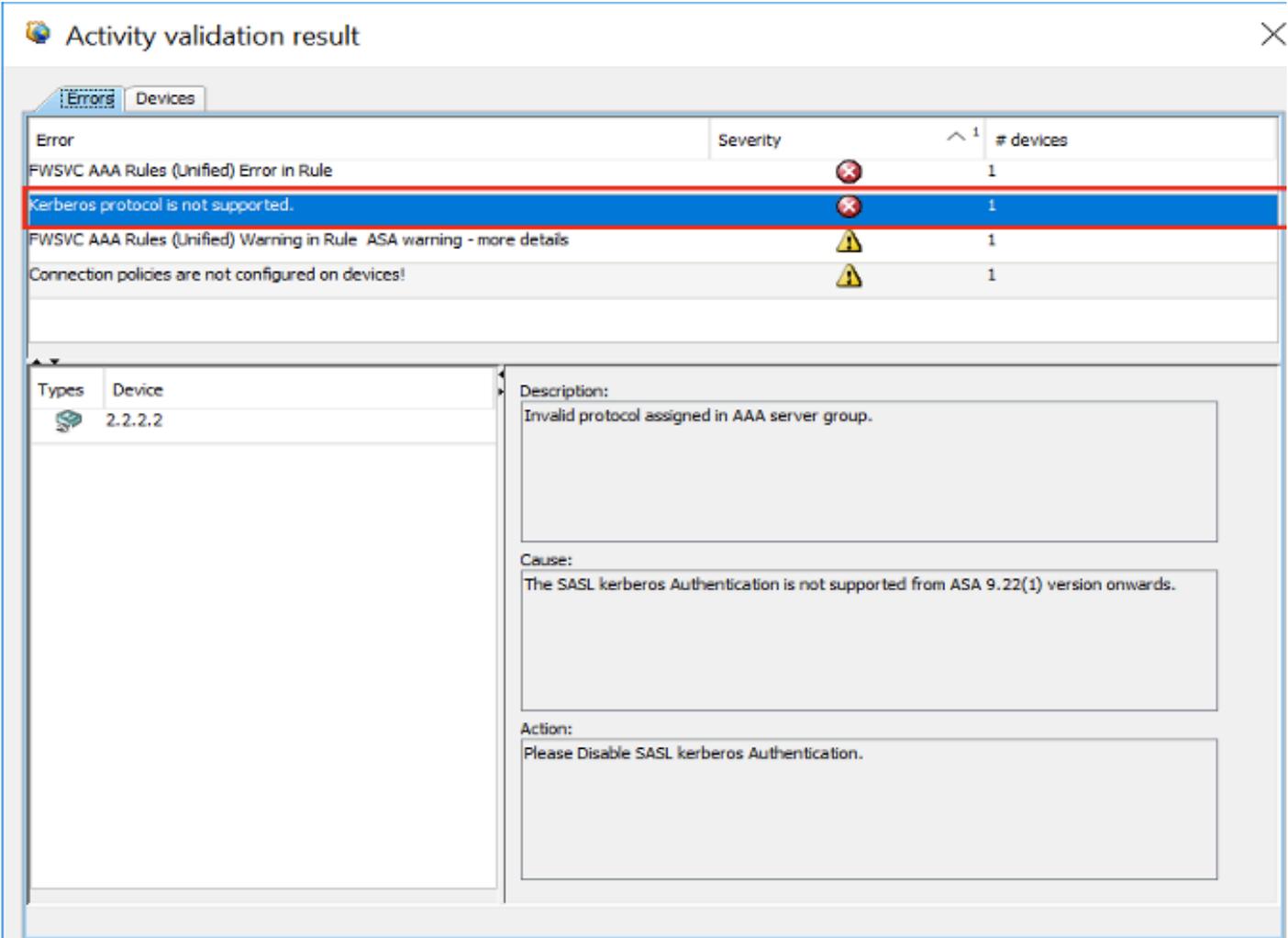
Category:

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

CSM-Kerberos-Konfiguration für LDAP-SASL

PFAD: CSM>Firewall > AAA-Regeln > AAA-Servergruppe > Hinzufügen > Protokoll > LDAP > SASL

1. Speichern
2. Vorschau der Konfiguration für das Ergebnis der Aktivitätsvalidierung



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 content area is a table with columns "Error", "Severity", and "# devices". The second row is highlighted in blue and contains the error "Kerberos protocol is not supported." with a red 'X' icon in the severity column and "1" in the "# devices" column. Below the table, there is a detailed view for the selected error. It includes a "Types" and "Device" table with one entry: "2.2.2.2". To the right of this table, there are three sections: "Description:" with the text "Invalid protocol assigned in AAA server group.", "Cause:" with the text "The SASL kerberos Authentication is not supported from ASA 9.22(1) version onwards.", and "Action:" with the text "Please Disable SASL kerberos Authentication."

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
	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.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.