

Retirada de Kerberos de ASA 9.2

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Tutorial sobre configuración de ASA CLI](#)

[Tutorial sobre configuración de ASDM](#)

[Tutorial sobre configuración de CSM](#)

Introducción

Este documento describe la información sobre la desaprobación de Kerberos desde ASA 9.22.

Prerequisites

Requirements

Cisco recomienda que conozca los conceptos básicos de seguridad:

- Conocimientos básicos de ASA CLI.
- Conocimiento básico de AAA (autenticación, autorización y contabilidad)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Todas las plataformas ASA
- ASA CLI 9.2.1
- ASDM 7.2.1
- CSM 4.29

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Tutorial sobre configuración de ASA CLI

Descripción general de ASA CLI:

- En el resultado del comando, las opciones *inbold italic* se han eliminado de la CLI.
- Las actualizaciones de versiones anteriores a la 9.22 que contienen estas configuraciones producen un mensaje de advertencia en la consola durante el arranque.

ciscoasa(config)# aaa-server curb protocol ?

configurar comandos/opciones del modo:

HTTP-form Protocol Basado en formulario HTTP

Kerberos Protocol Kerberos (DEPRECATED)

LDAP Protocol LDAP

RADIUS del protocolo RADIUS

SDI Protocol

TACACS+ Protocol TACACS+

ciscoasa(config)# aaa-server curb protocol kerberos

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

Comandos de configuración del servidor AAA:

exit Exit from aaa-server group configuration mode

Ayuda para comandos de configuración del servidor AAA

max-failed-tries (máximo de intentos fallidos) Especifique el número máximo de fallos permitidos para cualquier servidor del grupo antes de que se desactive dicho servidor

no Quitar un elemento de la configuración del grupo aaa-server

reactivation-mode (modo de reactivación) Especifique el método por el cual se reactivan los servidores fallidos

validate-kdc Habilita la validación de KDC durante la autenticación de usuario Kerberos

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

comandos/opciones del modo exec:

delegado Test Kerberos restringido delegación

host Introduzca esta palabra clave para especificar la dirección IP del servidor

suplantar transición del protocolo Test Kerberos

palabra clave password Password

recuperación de vale automático de Kerberos de prueba automática

username Username keyword

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 mode commands/options:

digest-md5 select Digest-MD5

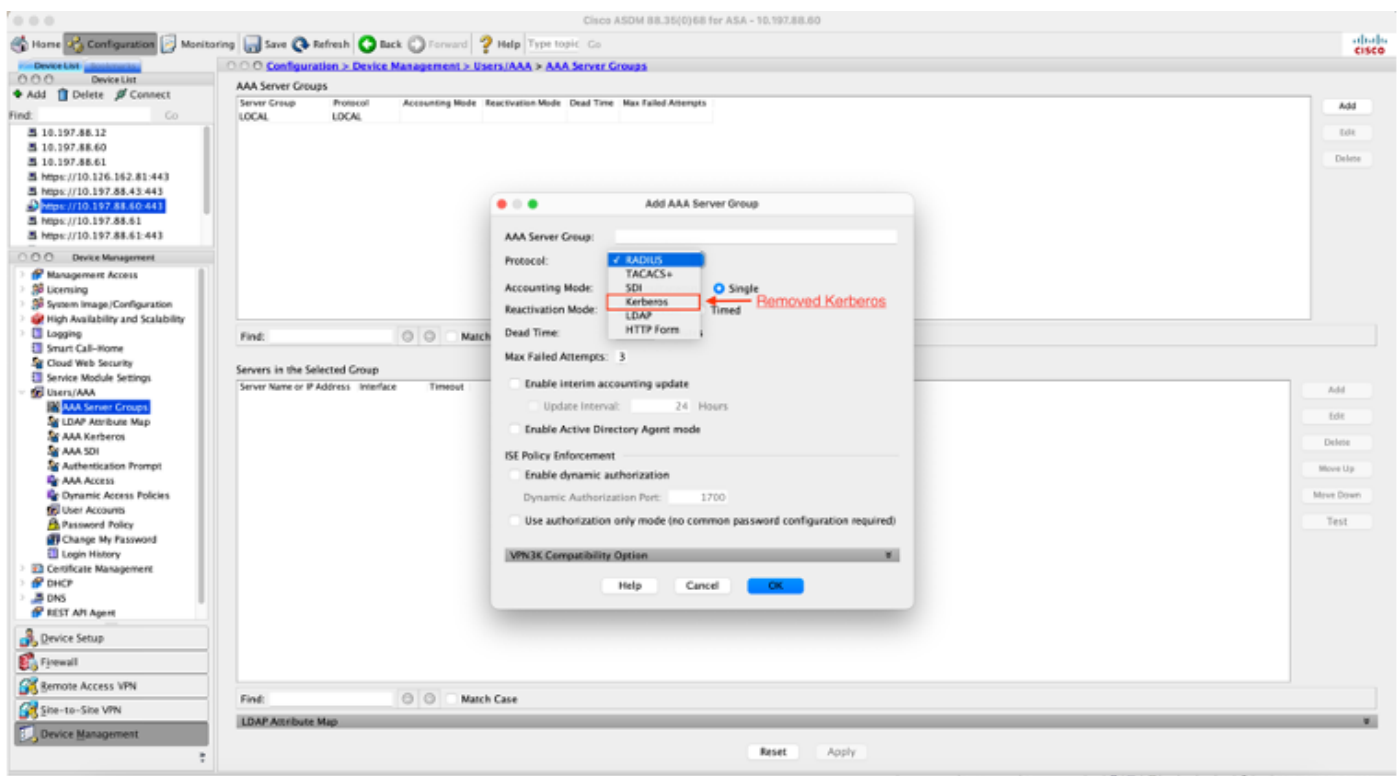
kerberos select Kerberos

ciscoasa(config)# debug kerberos

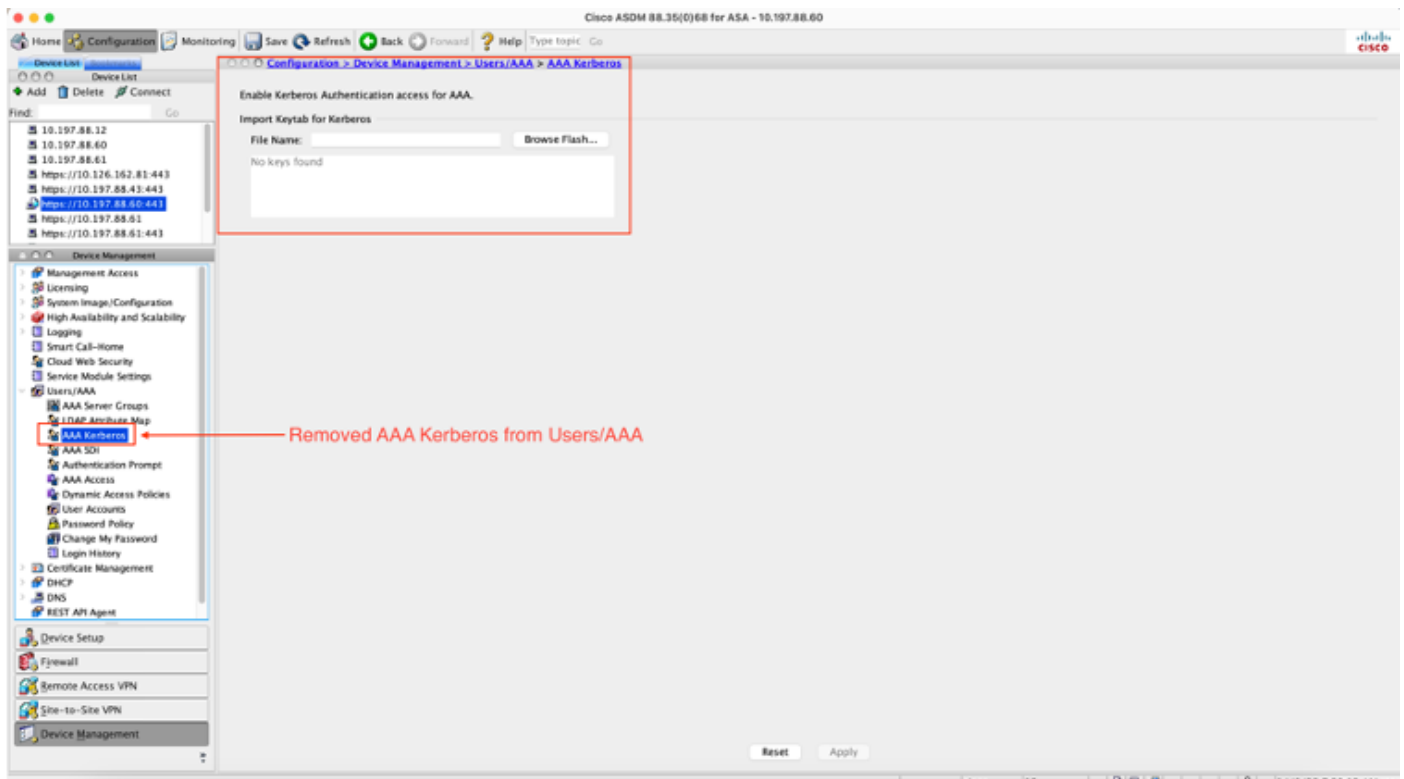
Tutorial sobre configuración de ASDM

Descripción general de ASDM:

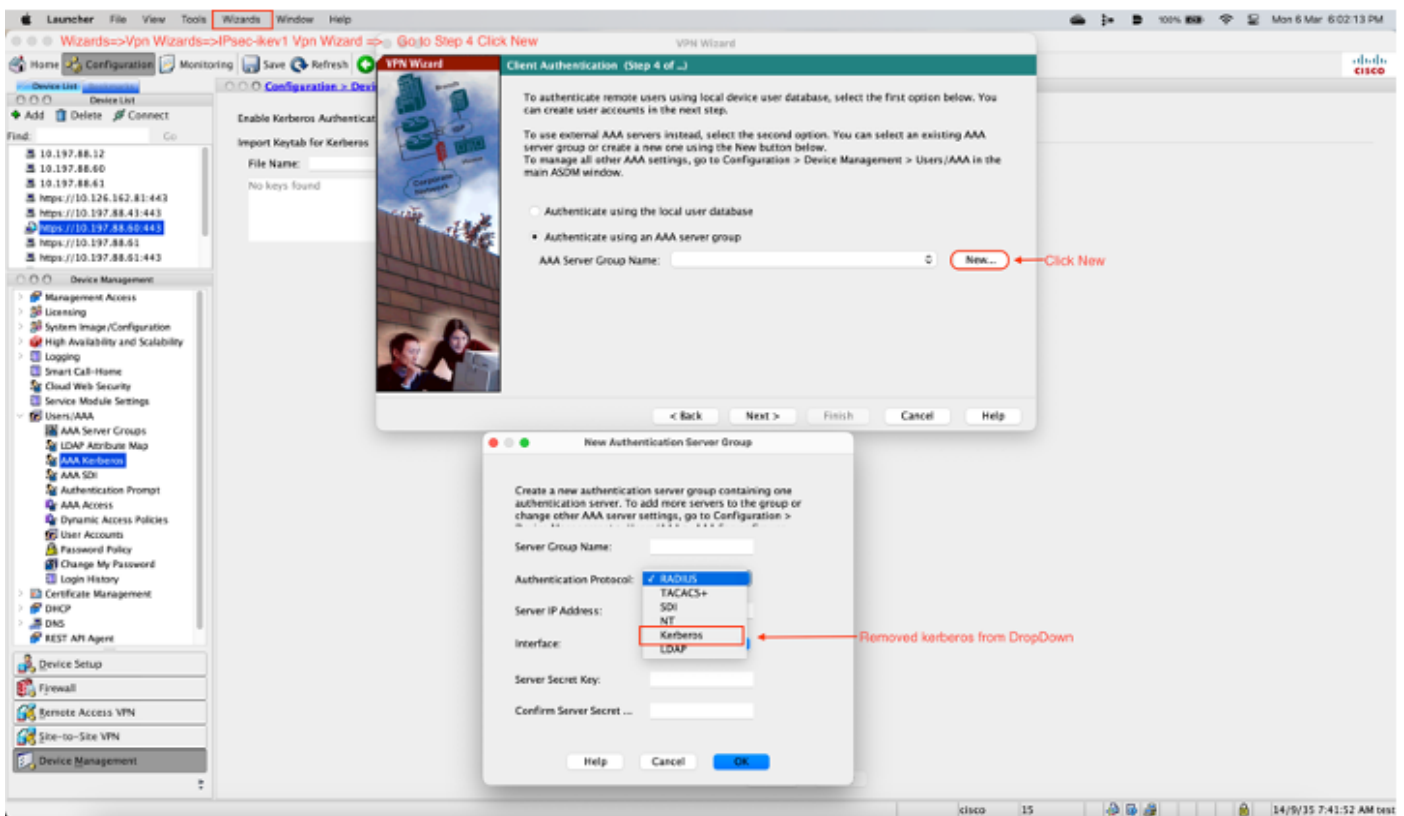
- Kerberos ya no es compatible con ASDM 7.22
- Esto desaprueba la capacidad de los usuarios finales de configurar grupos de servidores AAA con el protocolo Kerberos, así como el mecanismo LDAP SASL.
- Como parte de esta desaprobación, AAA Kerberos ya no aparece en TreeMenu bajo Users/AAA en Device Management.
- Microsoft KCD Server tampoco es compatible.



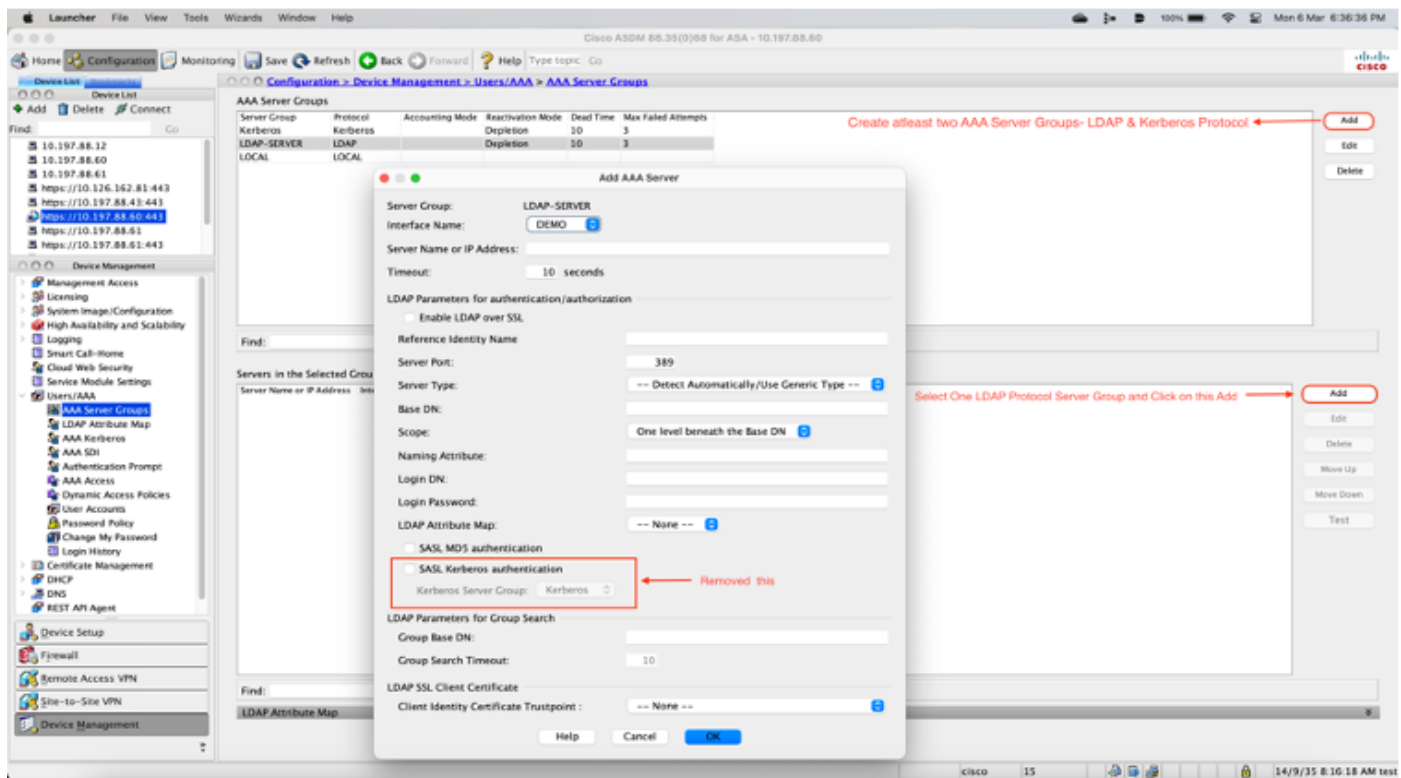
ASDM: Protocolo Kerberos en el Nuevo Grupo de Servidores AAA



ASDM: Kerberos AAA



ASDM: Protocolo Kerberos en el Nuevo Grupo de Servidores AAA



ASDM: Configuración de Kerberos para LDAP SASL

Tutorial sobre configuración de CSM

Descripción general de CSM:

- El protocolo Kerberos ya no es compatible.
- Esto desaprueba la capacidad de los usuarios finales de configurar grupos de servidores AAA con el protocolo Kerberos, así como el mecanismo LDAP SASL.
- Microsoft KCD Server tampoco es compatible.
- En lugar de quitar la compatibilidad con Kerberos de CSM, se controla en la validación de actividades.
- La Validación de la actividad arroja un mensaje de error para la versión 9.2.1 de ASA en adelante que indica que el protocolo Kerberos no se soporta a partir de la versión 9.2.1 en adelante.

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: 2.2.2.2

Policy: AAA Rules (Unified)

Inherits From: none

Filter: none

AAA Rules (Unified)

Access Rules (Unified)

Inspection Rules (Unified)

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 Infra

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:

AAA Server Groups Selector

Add AAA Server Group

Filter: *

LDAP

LOC

LDAP

RAO

TAC

Name: *

Test_Kerberos

Description:

Protocol:

AAA Servers:

Dynamic Authorization

Interim Account Update

Authorize only

Port: 1700

Interval: 24

Max Failed Attempts (PDLASA/FWSM): 3

Reactivation Mode (PDLASA/FWSM): depletion

Reactivation Deadline (PDLASA/FWSM): 10

Group Accounting Mode (PDLASA/FWSM): single

Category:

Allow Value Override per

Overrides: None

OK

AAA Servers Selector

Add AAA Server

Filter: *

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

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

Configuración de CSM Kerberos para LDAP SASL

PATH: CSM>Firewall > Reglas AAA > Grupo de servidores AAA > Agregar > Protocolo > LDAP > SASL

1. Guardar
2. Vista previa de la configuración para el resultado de validación de actividad.

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

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.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).