ASA 9.22からのKerberosの使用停止

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

ASA CLI設定のウォークスルー

ASDM設定のウォークスルー

CSM設定のチュートリアル

はじめに

このドキュメントでは、ASA 9.22からのKerberos廃止に関する考察を説明します。

前提条件

要件

次の基本的なセキュリティの概念に関する知識があることが推奨されます。

- ASA CLIに関する基礎知識
- AAA(認証、許可、アカウンティング)に関する基本的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- すべてのASAプラットフォーム
- ASA CLI 9.22.1
- ASDM 7.22.1
- CSM 4.29

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ASA CLI設定のウォークスルー

ASA CLIの概要

- コマンド出力で、太字の斜体のオプションがCLIから削除されています。

- これらの設定を含む9.22より前のバージョンからのアップグレードでは、ブート時にコンソールに警告メッセージが表示されます。

ciscoasa(config)# aaa-server curb protocol ?

設定モードコマンド/オプション：

httpフォームプロトコルHTTPフォームベース

kerberosプロトコルKerberos（廃止）

ldapプロトコルLDAP

radiusプロトコルRADIUS

sdiプロトコルSDI

tacacs+プロトコルTACACS+

ciscoasa(config)# aaa-server curb protocol kerberos

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

AAAサーバ設定コマンド：

exit aaa-server groupコンフィギュレーションモードを終了します。

aaaサーバ設定コマンドのヘルプ

max-failed-attemptsグループ内のサーバが非アクティブになるまでに許容される最大エラー数を指定します

no aaa-serverグループ設定から項目を削除します。

reactivation-mode障害が発生したサーバを再アクティブ化する方法を指定します

validate-kdc:kerberosユーザ認証中にKDC検証を有効にします

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

execモードのコマンド/オプション：

委任テストKerberos制約付き委任

host：サーバのIPアドレスを指定します

偽装テストKerberosプロトコルの移行

password passwordキーワード

セルフテストKerberosセルフチケット取得

usernameユーザ名キーワード

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コマンド/オプション：

digest-md5選択Digest-MD5

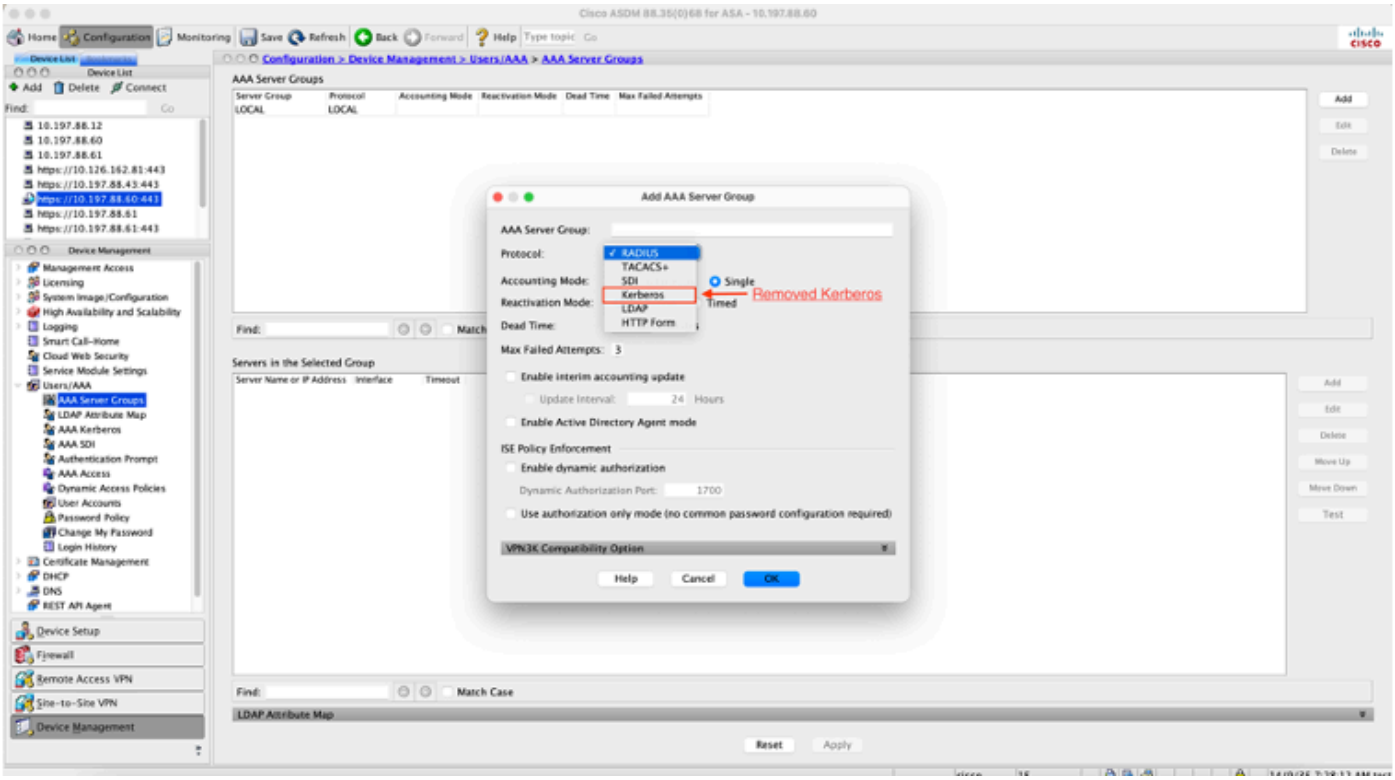
kerberos:Kerberosの選択

ciscoasa(config)# debug kerberos

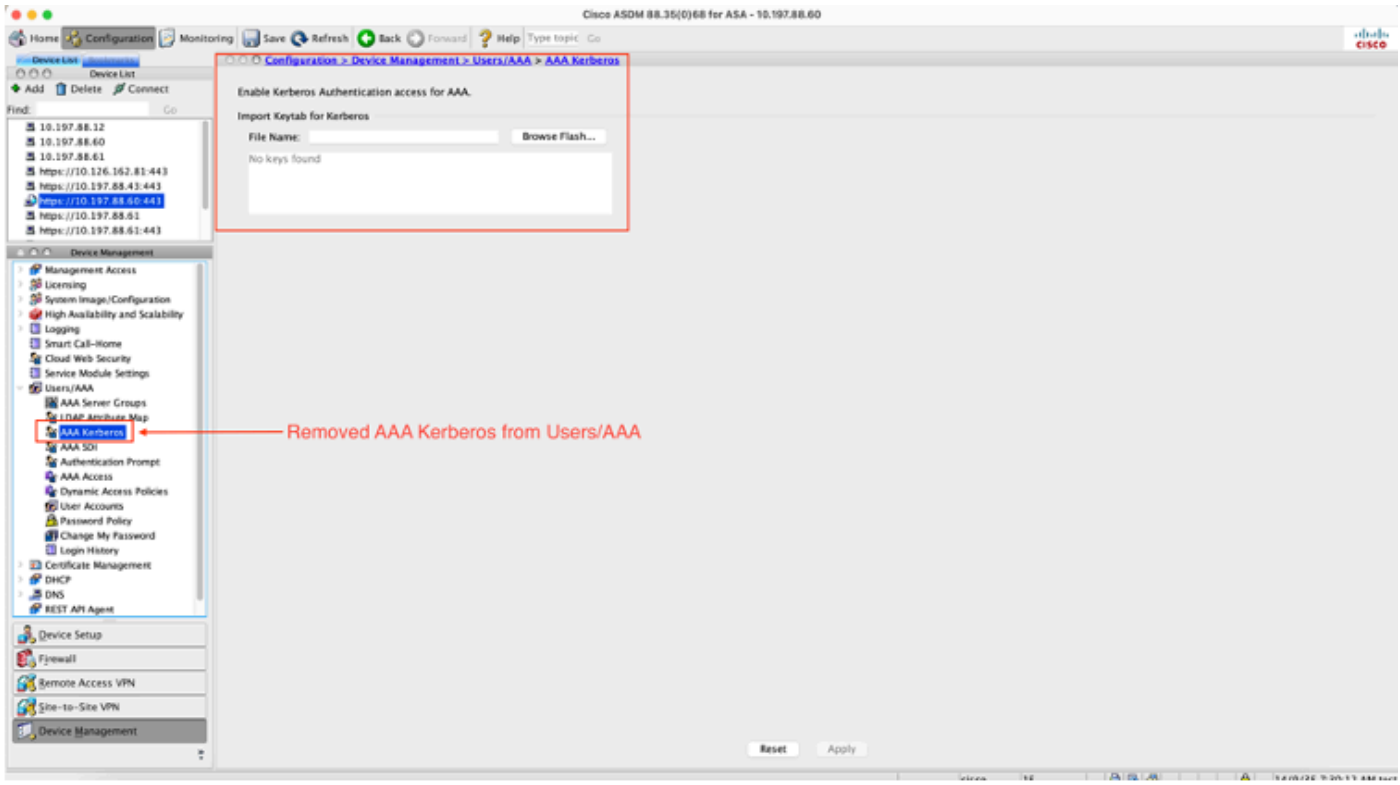
ASDM設定のウォークスルー

ASDMの概要

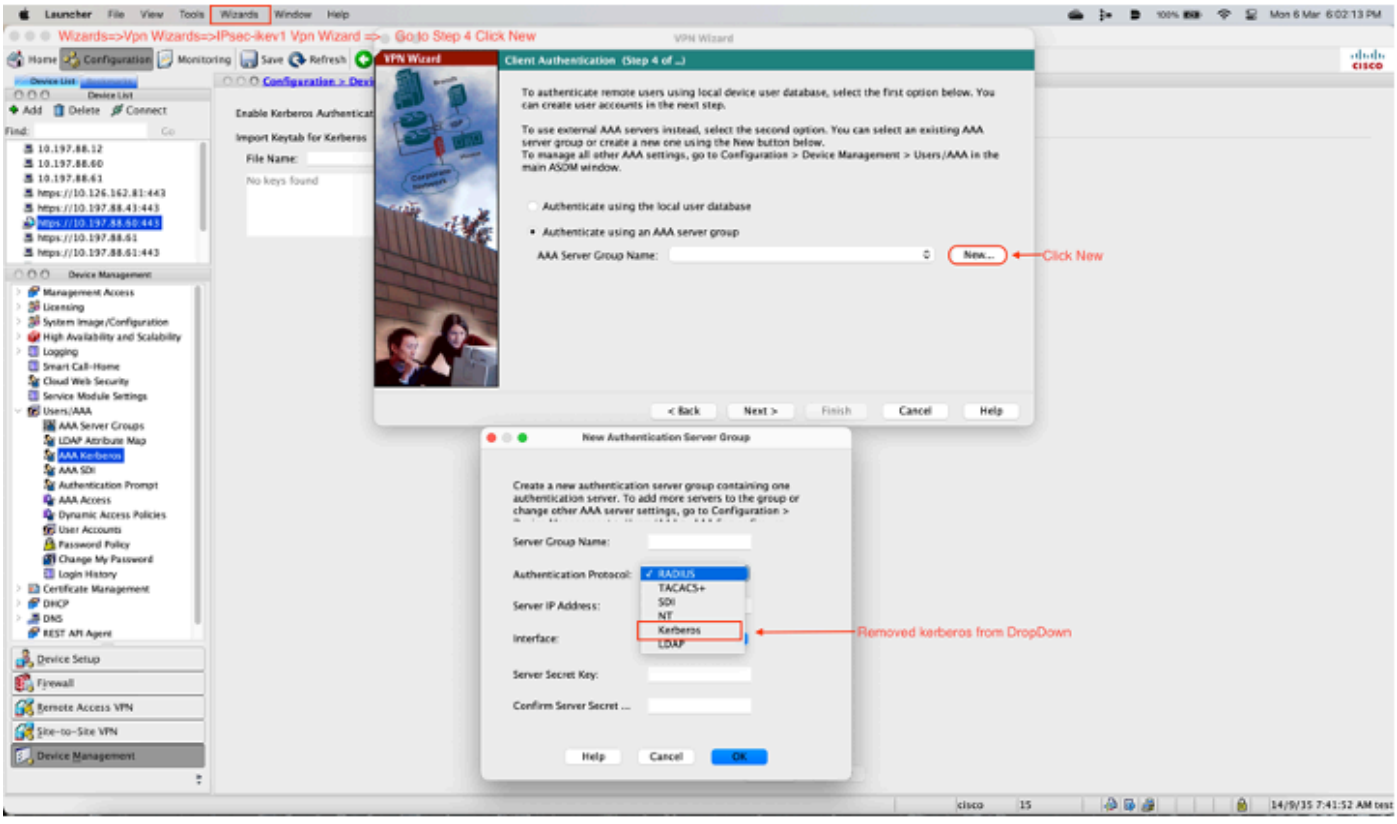
- KerberosはASDM 7.22ではサポートされなくなりました
- これは、エンドユーザがKerberosプロトコルとLDAP SASLメカニズムを使用してAAAサーバグループを設定する機能を廃止します。
- この廃止の一環として、AAA KerberosはDevice ManagementのUsers/AAAの下のTreeMenuにリストされなくなりました。
- Microsoft KCD Serverもサポートされなくなりました。



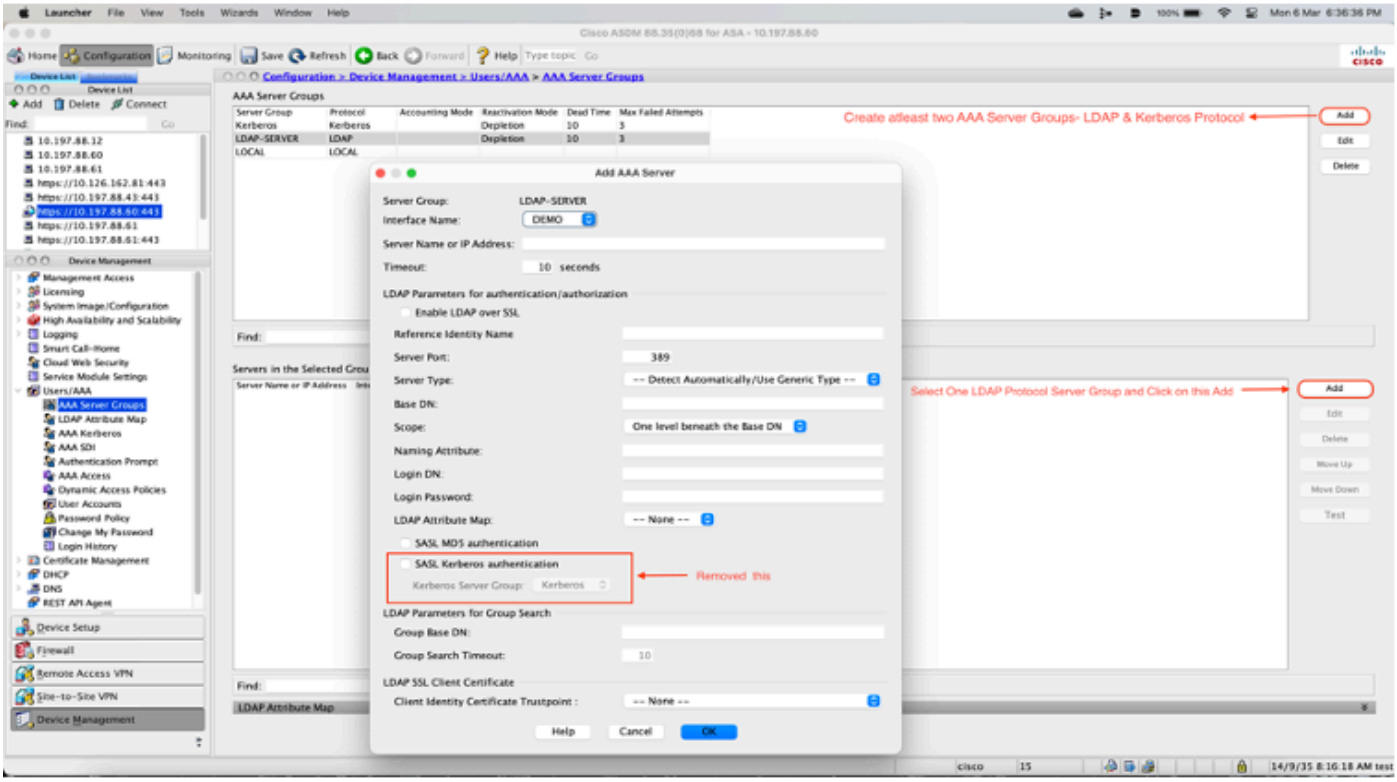
ASDM：新しいAAAサーバグループのKerberosプロトコル



ASDM:AAA Kerberos



ASDM：新しいAAAサーバグループのKerberosプロトコル

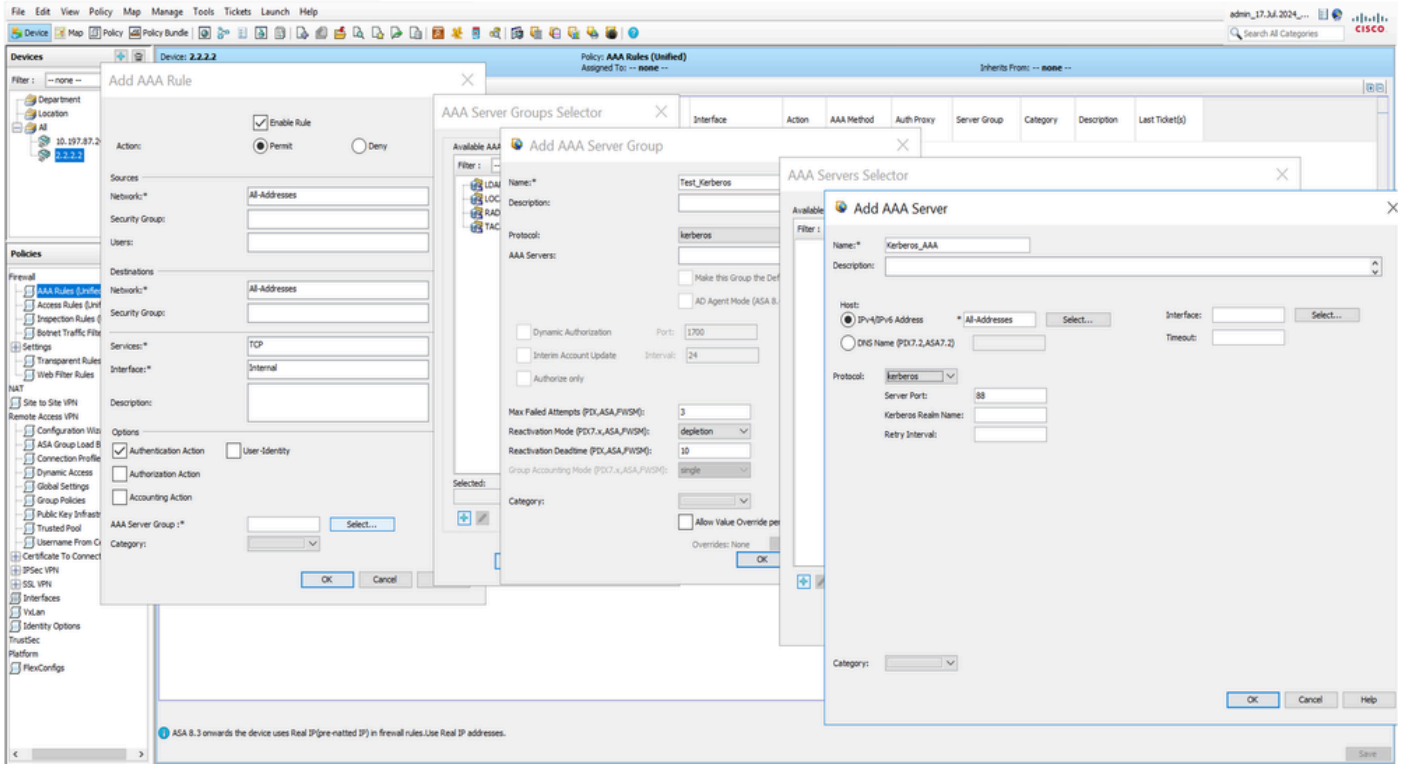


ASDM:LDAP SASLのKerberos設定

CSM設定のチュートリアル

CSM概要：

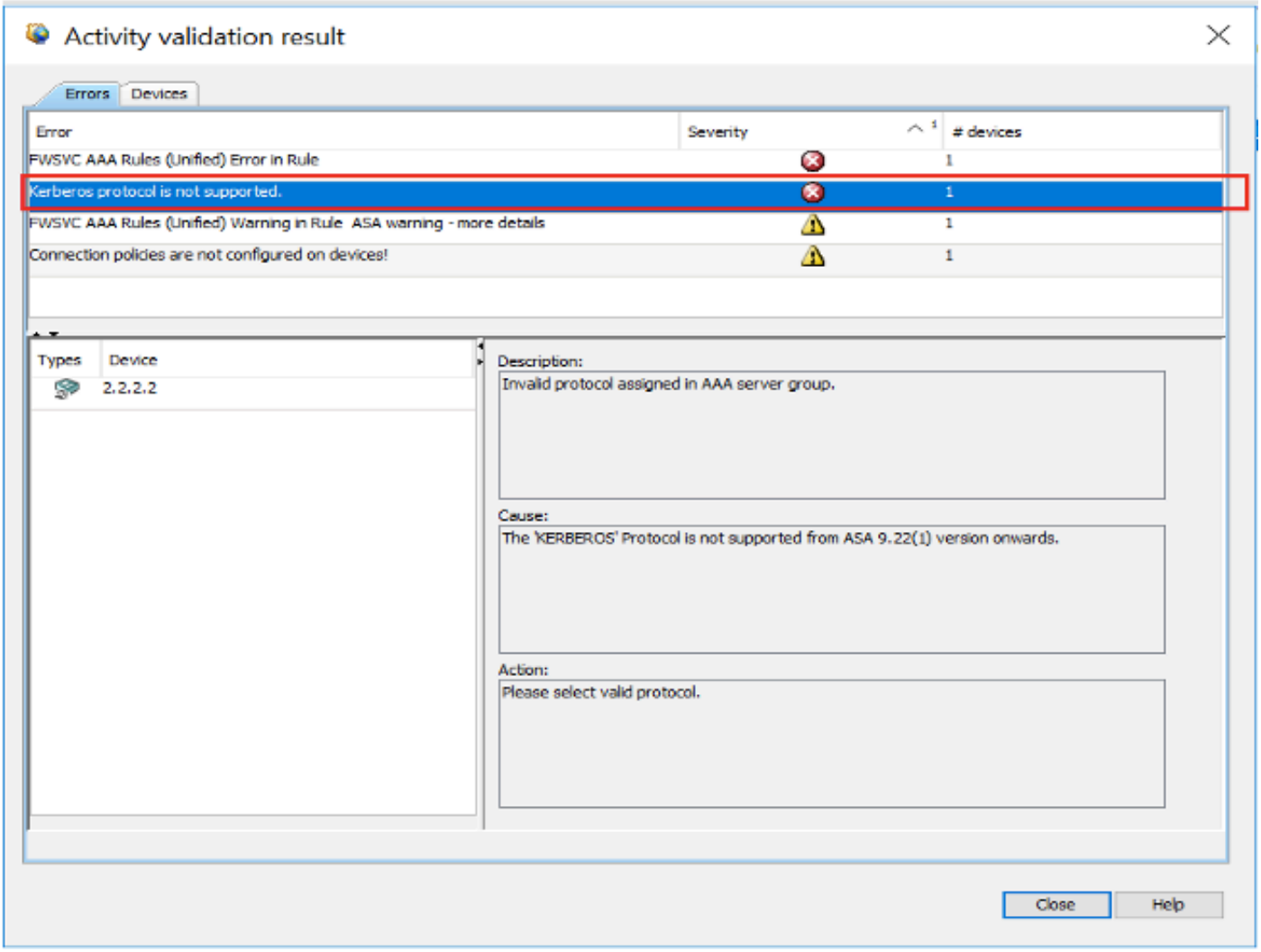
- Kerberosプロトコルはサポートされなくなりました。
- これは、エンドユーザがKerberosプロトコルとLDAP SASLメカニズムを使用してAAAサーバグループを設定する機能を廃止します。
- Microsoft KCD Serverもサポートされなくなりました。
- CSMからKerberosサポートを削除する代わりに、アクティビティ検証で処理されます。
- アクティビティ検証では、9.22.1以降のASAバージョンでは「Kerberosプロトコルは9.22.1以降ではサポートされていません」というエラーメッセージが表示されます。

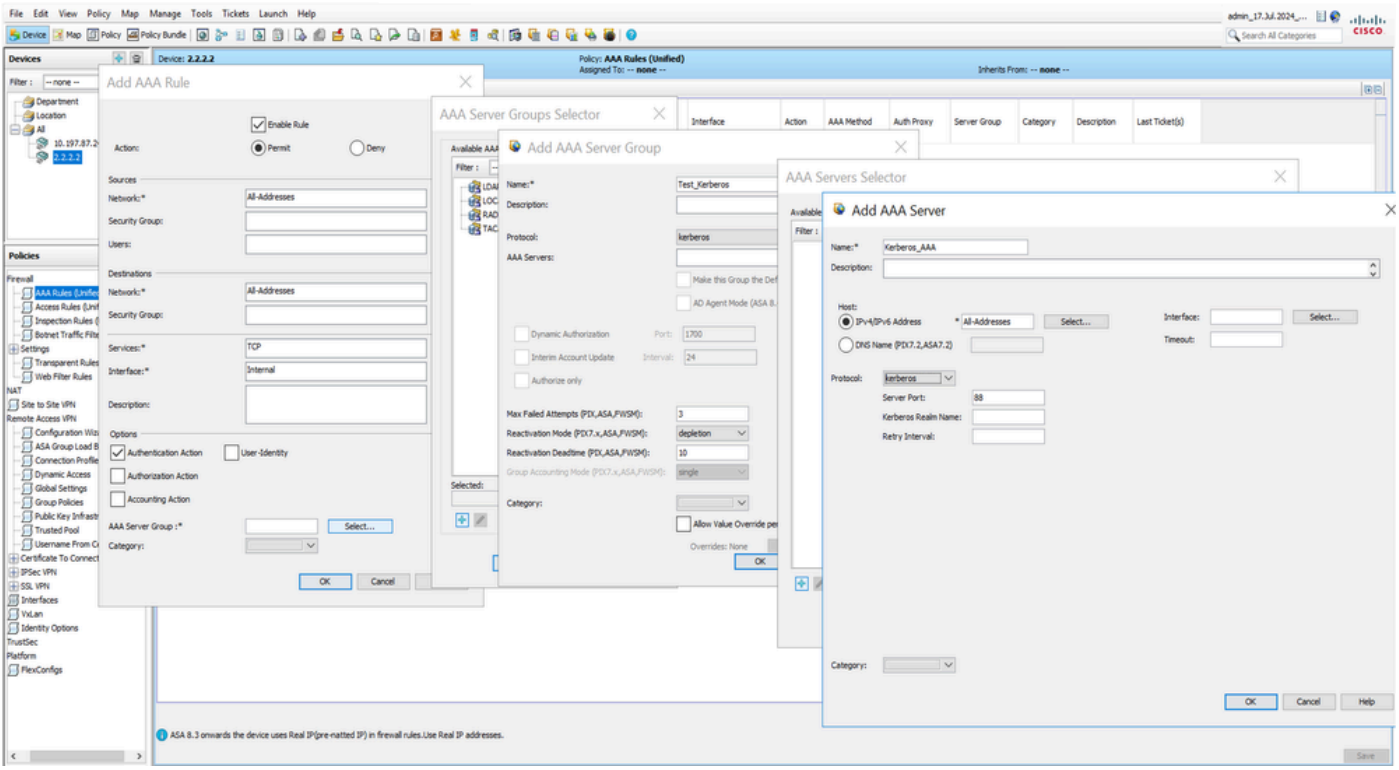


CSM Kerberosの設定

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

1. 保存します。
2. アクティビティ検証結果の構成をプレビューします。

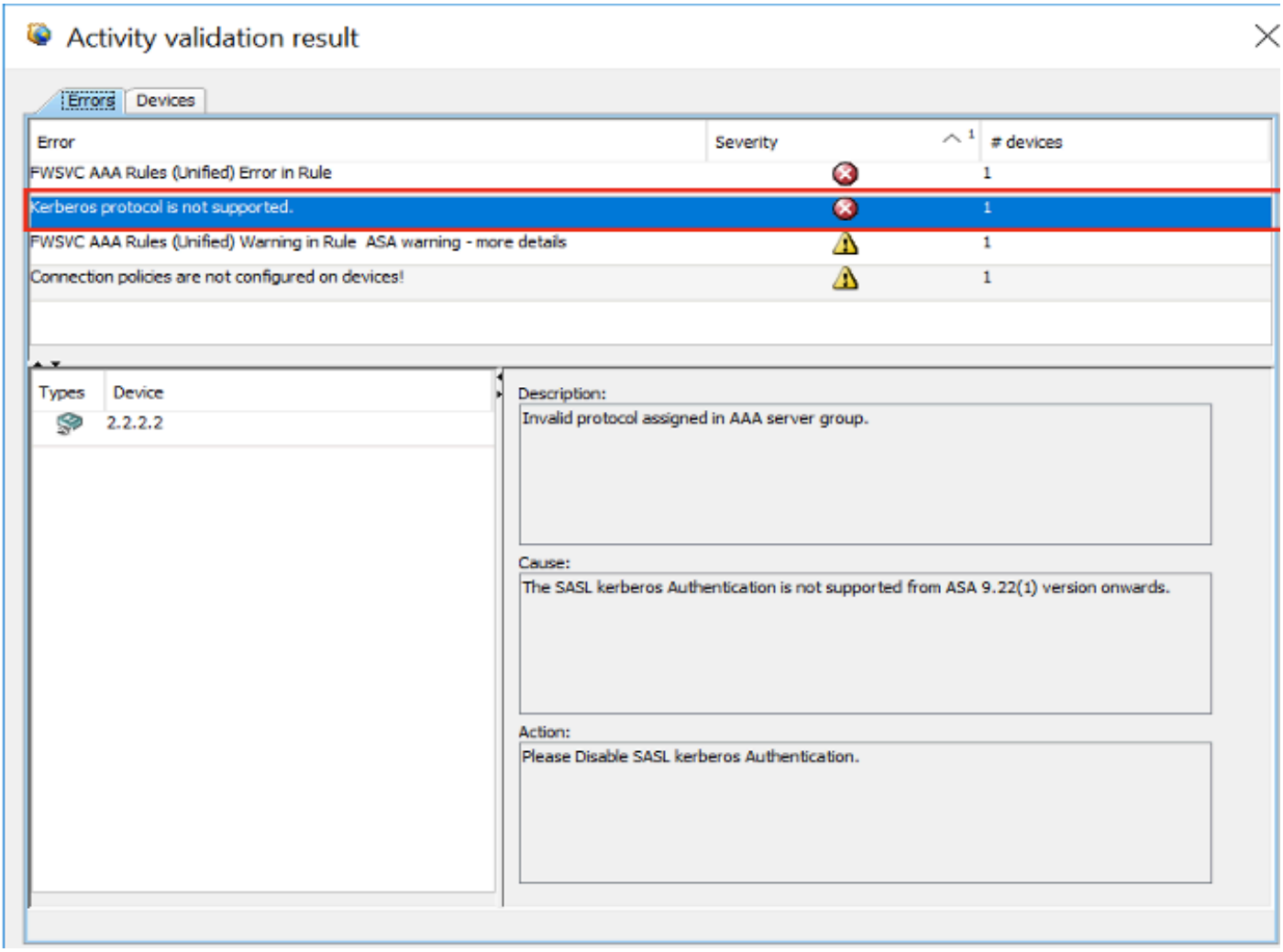




LDAP SASL用のCSM Kerberos設定

パス：CSM>Firewall > AAA Rules > AAA Server Group > Add >Protocol > LDAP >SASL

1. 保存します。
2. アクティビティ検証結果の構成をプレビューします。



翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。