

Smantellamento di Kerberos dall'appliance ASA

9.2

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Procedura dettagliata per la configurazione di ASA CLI](#)

[Procedura dettagliata per la configurazione di ASDM](#)

[Procedura dettagliata per la configurazione del modulo CSM](#)

Introduzione

Questo documento descrive le informazioni dettagliate sull'obsolescenza di Kerberos da ASA 9.2.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti base sulla sicurezza:

- Conoscenze base della CLI di ASA.
- Conoscenze base di AAA (autenticazione, autorizzazione e accounting)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Tutte le piattaforme ASA
- ASA CLI 9.2.1
- ASDM 7.2.1
- CSM 4.29

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Procedura dettagliata per la configurazione di ASA CLI

Panoramica della CLI di ASA:

- Nell'output del comando, le opzioni in **bold italic** sono state rimosse dalla CLI.
- Gli aggiornamenti dalle versioni precedenti alla 9.22 che contengono queste configurazioni generano un messaggio di avviso sulla console durante il tempo di avvio.

cisco-asa(config)# aaa-server curb protocol?

configurare i comandi/le opzioni della modalità:

http-form Protocollo HTTP basato su form

Kerberos, protocollo Kerberos (DEPRECATO)

LDAP protocollo LDAP

Radius Protocollo RADIUS

SDI Protocollo sdi

Protocollo TACACS+ TACACS+

cisco-asa(config)# kerberos protocollo curb aaa-server

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

Comandi di configurazione del server AAA:

uscire dalla modalità di configurazione gruppo aaa-server

Guida ai comandi di configurazione del server AAA

max-failed-try Specifica il numero massimo di errori consentiti per qualsiasi server del gruppo prima che il server venga disattivato

no Rimuovere un elemento dalla configurazione del gruppo aaa-server

modalità di riattivazione Specificare il metodo di riattivazione dei server in errore

validate-kdc Abilita la convalida KDC durante l'autenticazione utente Kerberos

cisco asa(config)# test aaa-server authentication curb?

comandi/opzioni modalità di esecuzione:

delega Delega vincolata Kerberos test

host Immettere questa parola chiave per specificare l'indirizzo IP del server

rappresentazione della transizione del protocollo Kerberos di test

password Parola chiave Password

test automatico recupero ticket Kerberos

username Parola chiave Username

cisco asa(config)# protocollo ldap aaa-server

cisco-asa(config-aaa-server-group)# host aaa-server ldap x.x.x

cisco-asa(config-aaa-server-host)# sasl-mechanism ?

comandi/opzioni modalità host-server-aaa:

digest-md5 select Digest-MD5

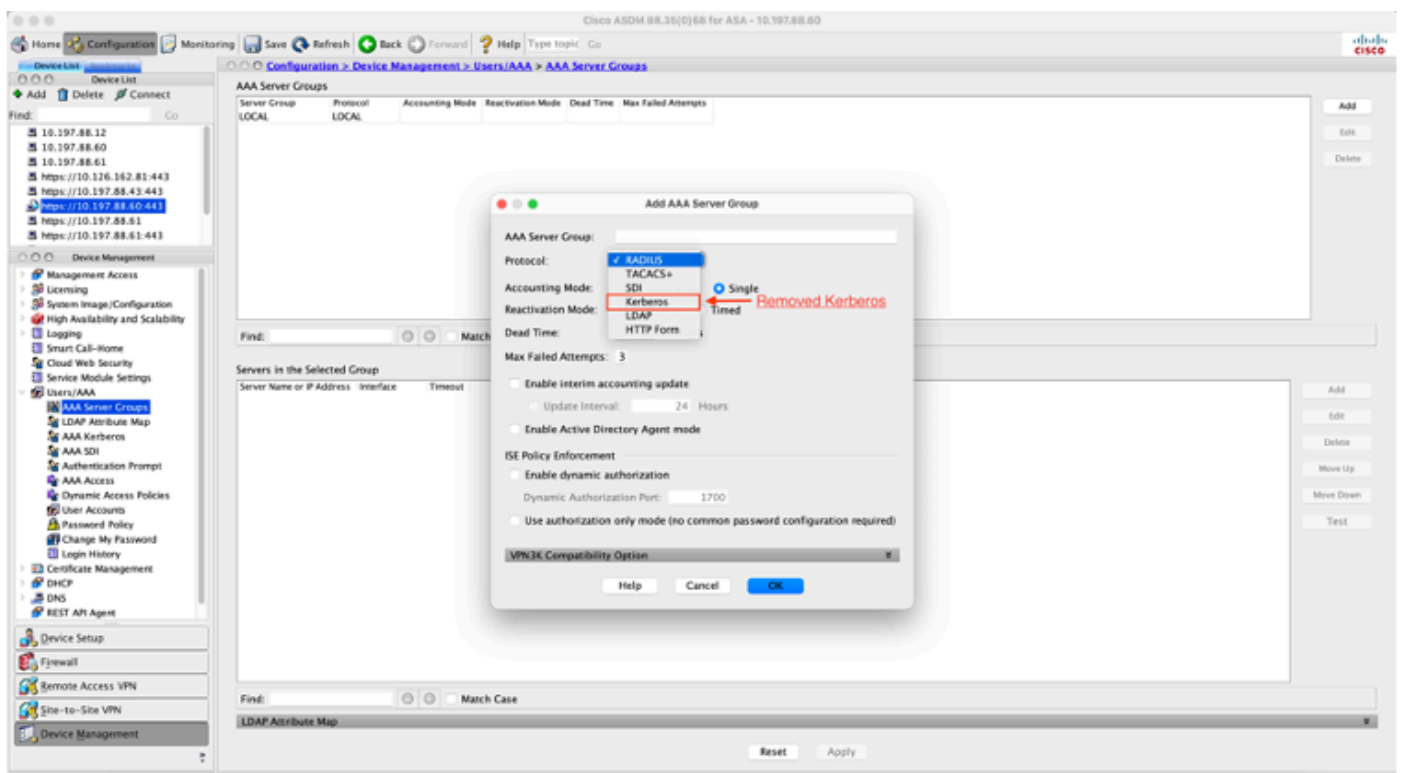
Kerberos selezione Kerberos

cisco(config)# debug kerberos

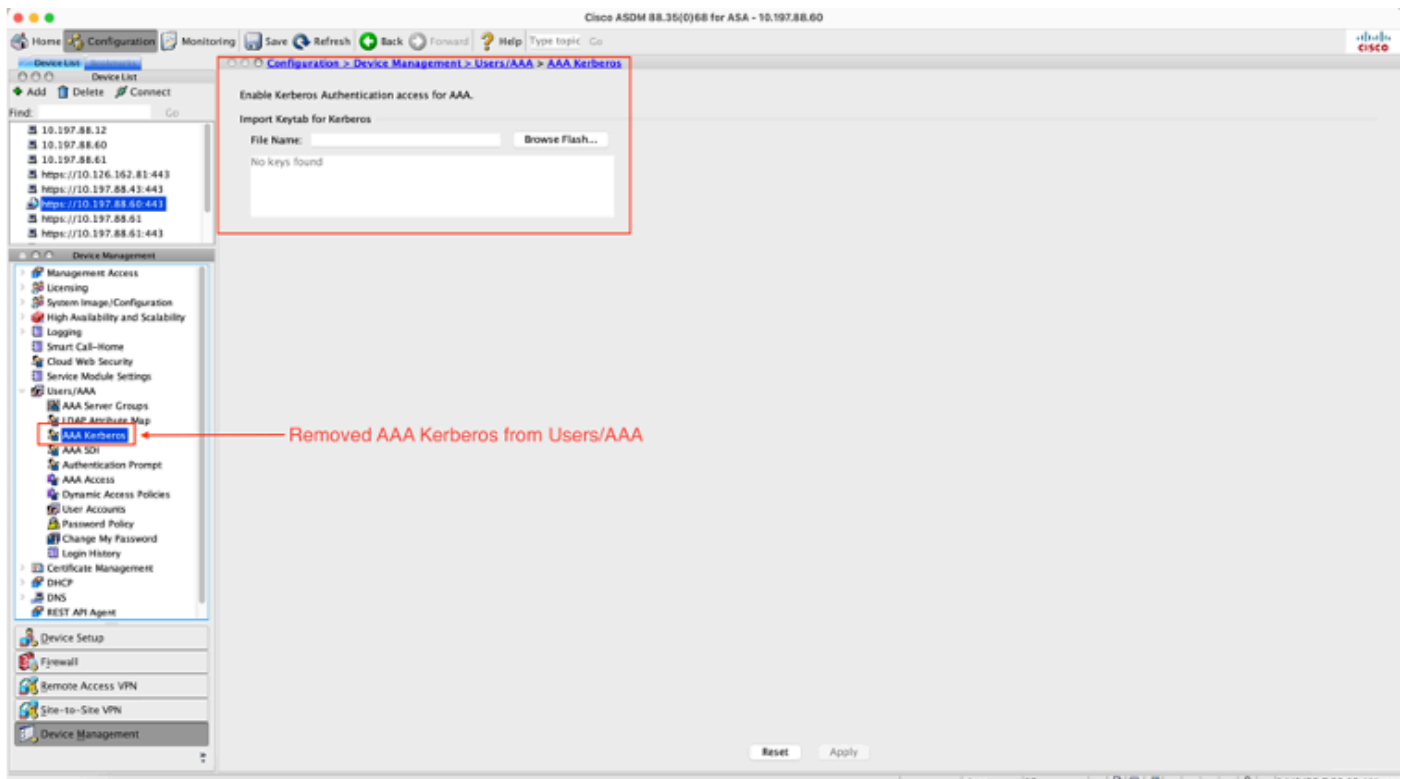
Procedura dettagliata per la configurazione di ASDM

Panoramica di ASDM:

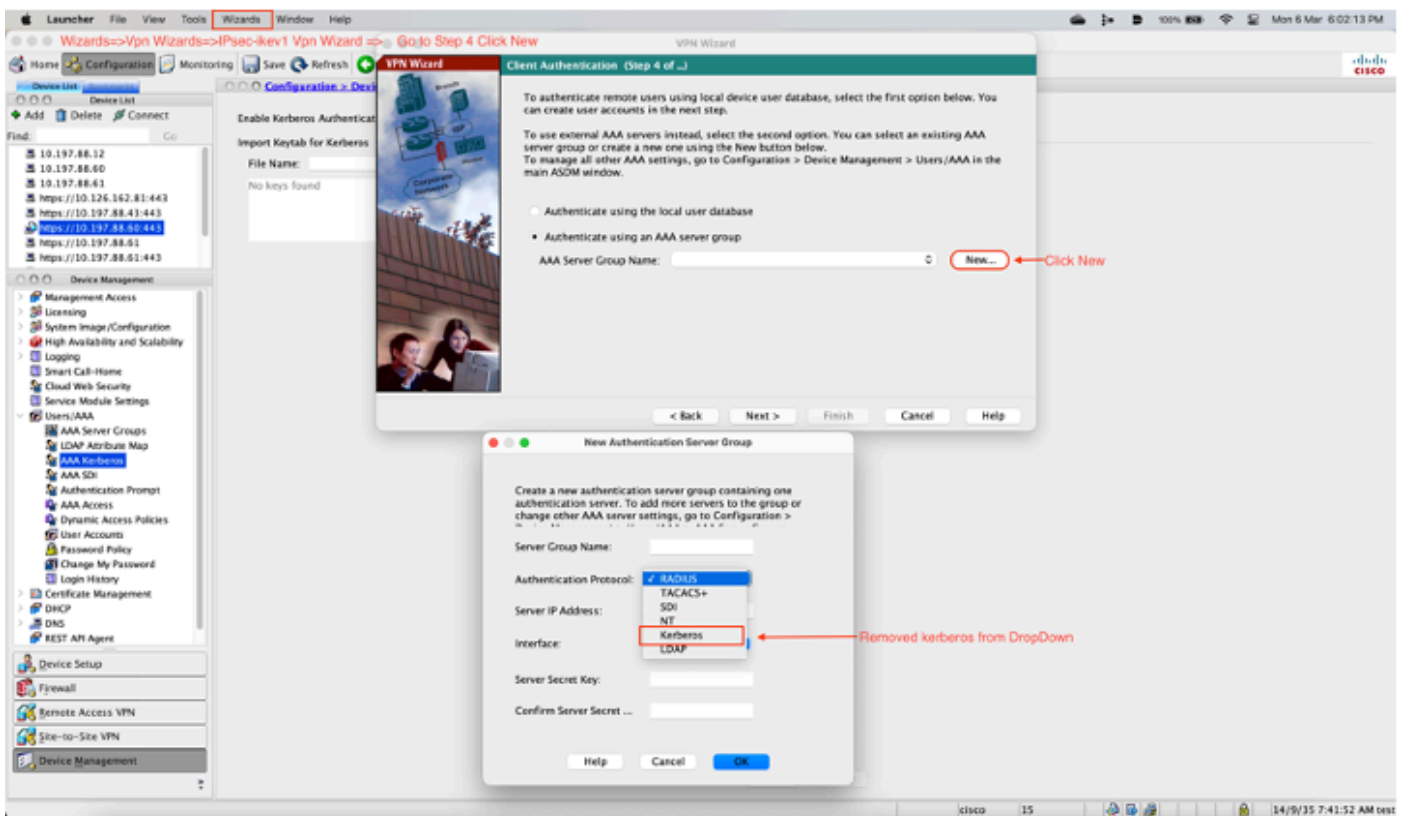
- Kerberos non è più supportato da ASDM 7.2
- In questo modo, gli utenti finali non possono più configurare i gruppi di server AAA con il protocollo Kerberos e con il meccanismo LDAP SASL.
- Come parte di questa deprecazione, AAA Kerberos non è più elencato in TreeMenu sotto Users/AAA in Device Management.
- Microsoft KCD Server non è più supportato.



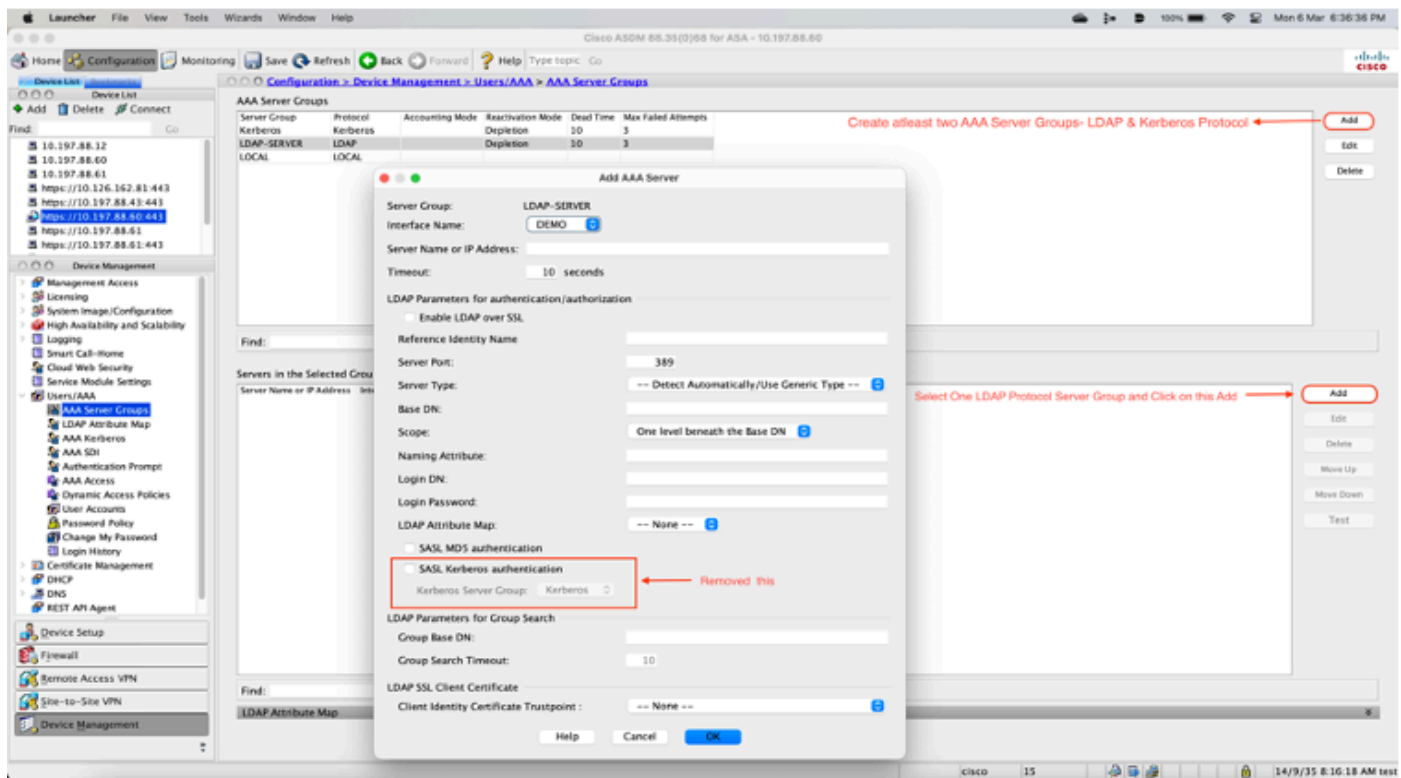
ASDM: Protocollo Kerberos nel nuovo gruppo di server AAA



ASDM: AAA Kerberos



ASDM: Protocollo Kerberos nel nuovo gruppo di server AAA

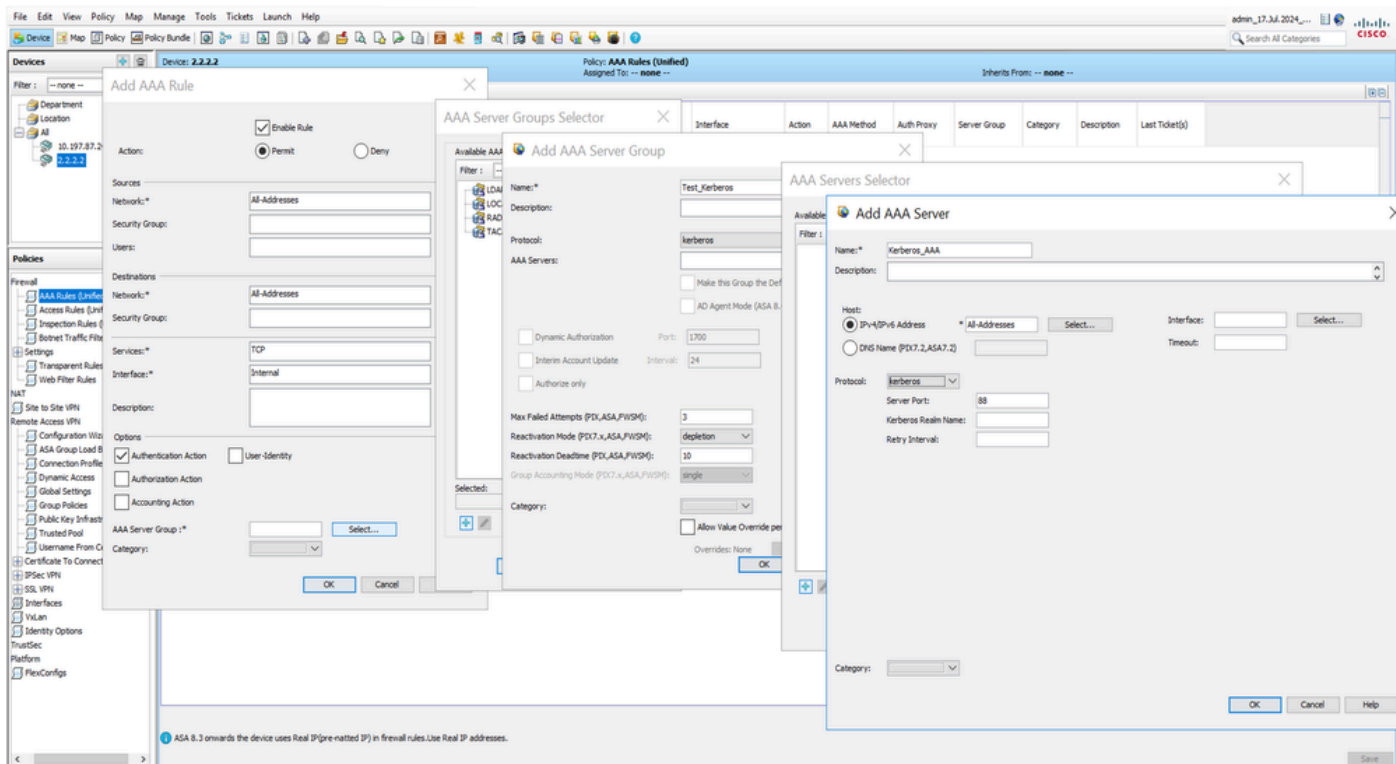


ASDM: Configurazione Kerberos per SASL LDAP

Procedura dettagliata per la configurazione del modulo CSM

Panoramica di CSM:

- Protocollo Kerberos non più supportato.
- In questo modo, gli utenti finali non possono più configurare i gruppi di server AAA con il protocollo Kerberos e con il meccanismo LDAP SASL.
- Microsoft KCD Server non è più supportato.
- Anziché rimuovere il supporto Kerberos da CSM, viene gestito in Convalida attività.
- La convalida dell'attività genera un messaggio di errore per la versione 9.22.1 dell'ASA e successive: il protocollo Kerberos non è supportato a partire dalla versione 9.22.1.



Configurazione CSM Kerberos

PERCORSO: CSM>Firewall > Regole AAA > Gruppo server AAA > Aggiungi > Kerberos

1. Salva
2. Antepima configurazione per risultato convalida attività.

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 '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

AAA Server Groups Selector

Add AAA Server Group

AAA Servers Selector

Add AAA Server

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

Configurazione CSM Kerberos per SASL LDAP

PERCORSO: CSM>Firewall > Regole AAA > Gruppo server AAA > Aggiungi > Protocollo > LDAP > SASL

1. Salva
2. Anteprima configurazione per risultato convalida attività.

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.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).