

Eintrag für Netzwerkzugriffsggerät in der ISE nach Catalyst Center hinzufügen/ändern

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Problem](#)

[Lösung](#)

Einleitung

In diesem Dokument wird das Verfahren zur Neukonfiguration des Network Access Device (NAD)-Eintrags in der ISE beschrieben, der entweder geändert oder aus der ISE entfernt wird.

Hintergrundinformationen

Es kann mehrere Szenarien geben, in denen der NAD-Eintrag für ein Netzwerkgerät (das vom Catalyst Center verwaltet wird) geändert werden muss. Beispiele:

Wenn ein Gerät zurückgegeben wird, die Seriennummer geändert wird und eine neue Seriennummer im NAD-Eintrag des Netzwerkgeräts aktualisiert werden muss (erweiterte TrustSec-Einstellungen).

Andernfalls findet keine Geräte-TrustSec-Authentifizierung statt, was dazu führt, dass PAC-/Umschlagdaten nicht heruntergeladen werden.

In einem anderen Szenario wird der NAD-Eintrag möglicherweise aus der Identity Services Engine (ISE) gelöscht (aufgrund eines manuellen Fehlers oder aus anderen Gründen). Nun schlägt die Geräteauthentifizierung fehl, da es in der ISE keinen NAD-Eintrag gibt.

Problem

Das Problem bei den oben genannten Szenarien besteht darin, dass es in Catalyst Center keine vordefinierte Option gibt, den NAD-Eintrag direkt zu erstellen, nachdem dem Netzwerkgerät der Standort zugewiesen wurde und der NAD-Eintrag zum ersten Mal erstellt wurde. Dies führt dazu, dass Benutzer den NAD-Eintrag in der ISE manuell konfigurieren/ändern müssen, was zeitaufwendig und fehleranfällig sein kann.

In diesem Dokument werden das Verfahren bzw. die Schritte zur Neukonfiguration des NAD-Eintrags (Network Access Device) für ein beliebiges Netzwerkgerät in der ISE beschrieben, das entweder geändert oder aus der ISE NAD entfernt wird. Dieses Verfahren gilt für alle

Netzwerkgeräte, die von Catalyst Center verwaltet werden.

Lösung

Damit Catalyst Center den NAD-Eintrag in der ISE konfigurieren kann, müssen wir im Grunde die Management-IP-Adresse des Geräts (in eine beliebige Dummy-IP) ändern, da das Backend den Workflow zum Erstellen von NAD-Einträgen auslöst.

Dieses Verfahren gilt für alle Netzwerkgeräte, die von Catalyst Center verwaltet werden. Der NAD-Eintrag wird mit der ursprünglichen IP erstellt (da der Workflow vor der Änderung der Management-IP-Adresse ausgelöst wird). In diesem Beispiel sind die erweiterten TrustSec-Einstellungen für einen NAD-Eintrag in der ISE deaktiviert:

Network Devices

Name	IP/Mask	Profile Name	Location	Type	Description
9400	x				
pod7-9400...	172.19.100.15/32	Cisco	All Locations	All Device Types	

NAD-Eintrag ISE für ein Netzwerkgerät

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Servers

Network Devices

Default Device

Device Security Settings

TACACS Authentication Settings

SNMP Settings

SNMP Version 2c

SNMP RO Community ** [Show](#)

SNMP Username

Security Level

Auth Protocol

Auth Password [Show](#)

Privacy Protocol

Privacy Password [Show](#)

Polling Interval 0 seconds(Valid Range 600 to 86400 or zero)

Link Trap Query

MAC Trap Query

Originating Policy Services Node Auto

Advanced TrustSec Settings

Erweiterte TrustSec-Einstellungen sind für diesen NAD-Eintrag deaktiviert.

Wie in diesem Bild zu sehen ist, sind die erweiterten TrustSec-Einstellungen für den NAD-Eintrag des Geräts deaktiviert (in der Regel ist dieser Abschnitt aktiviert, wenn Catalyst Center den NAD-Eintrag erstellt). Ändern Sie die Management-IP-Adresse in Catalyst Center in Dummy-IP, wodurch der Workflow zur Neukonfiguration des NAD-Eintrags in der ISE ausgelöst wird. Wenn Sie die Management-IP-Adresse ändern, wird die Gerätemanagement-Funktion in den Synchronisierungsstatus verschoben, und der ISE NAD-Eintrag muss geändert werden.

Devices (1) Focus: Inventory

deviceName: (*9400*)

1 Selected [Add Device](#) [Tag](#) [Actions](#)

Device Name	IP Address
pod7-9400.dr.com	172.19.100.15

1 Records

Edit Device

Credentials **Management IP** Resync Interval Device Role

Device IP / DNS Name*
172.19.100.100

- Please ensure that the new IP address is reachable from Cisco DNA Center and device credentials are correct, otherwise the device may go to an unmanaged state.
- Please ensure that the device is re-provisioned if the management interface has changed and IP address of the same has been updated. Failure to do so will cause reachability issues from the device to the network servers.

Device Controllability is **Enabled**. Config changes will be made on network devices during discovery/inventory or when device is associated to a site. [Learn More](#)

[Cancel](#) [Update](#)

Ändern der Management-IP-Adresse für das Netzwerkgerät in Catalyst Center in Dummy IP

Devices (1) Focus: Inventory

deviceName: (*9400*)

0 Selected [Add Device](#) [Tag](#) [Actions](#)

Device Name	IP Address	Device Family	Reachability	EoX Status	Manageability
pod7-9400.dr.com	172.19.100.100	Switches and Hubs (WLC Capable)	Reachable	Not Scanned	Managed Syncing...

Netzwerkgerät wechselt in Synchronisierungsstatus

Devices (1) Focus: Inventory

deviceName: (*9400*)

0 Selected [Add Device](#) [Tag](#) [Actions](#)

As of: Jul 7, 2024 7:13 PM

Device Name	IP Address	Device Family	Reachability	EoX Status	Manageability	Compliance	Health Score	Site
pod7-9400.dr.com	172.19.100.100	Switches and Hubs (WLC Capable)	Unreachable	Not Scanned	Managed Inventory Sync...	Non-Compliant	No Health	.../E

Netzwerkgerät wird nicht erreichbar und nicht verwaltet, da die Management-IP-Adresse eine Dummy-IP-Adresse ist und nicht vom Catalyst Center aus erreichbar ist

ISE NAD-Eintrag für aktualisierte und "Advanced TrustSec Settings" ist jetzt aktiviert :

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RA

Network Devices

Default Device

Device Security Settings

SNMP Username _____

Security Level _____ ▾

Auth Protocol _____ ▾

Auth Password _____ [Show](#)

Privacy Protocol _____ ▾

Privacy Password _____ [Show](#)

Polling Interval seconds(Valid Range 600 to 86400 or zero)

Link Trap Query

MAC Trap Query

Originating Policy Services Node ▾

▾ **Advanced TrustSec Settings**

▾ Device Authentication Settings

Use Device ID for TrustSec Identification

Device Id

Password [Show](#)

Erweiterte TrustSec-Einstellungen wurden nach der Aktualisierung der Management-IP-Adresse von Catalyst Center aktiviert.

Nachdem dies erstellt wurde, können wir die Management-IP-Adresse wieder in ihre ursprüngliche IP-Adresse ändern.

Provision / Inventory

Search: deviceName: (*9400*)

1 Selected

Device Name	IP Address
pod7-9400.dr.com	172.19.100.15

1 Records

Edit Device

Credentials | **Management IP** | Resync Interval | Device Role

Device IP / DNS Name*
172.19.100.15

- Please ensure that the new IP address is reachable from Cisco DNA Center and device credentials are correct, otherwise the device may go to an unmanaged state.
- Please ensure that the device is re-provisioned if the management interface has changed and IP address of the same has been updated. Failure to do so will cause reachability issues from the device to the network servers.

Device Controllability is **Enabled**. Config changes will be made on network devices during discovery/inventory or when device is associated to a site. [Learn More](#)

Cancel Update

Zurücksetzen der Management-IP-Adresse auf die ursprüngliche IP

Nach der Aktualisierung der Management-IP-Adresse auf die ursprüngliche IP-Adresse wechselt das Gerät in den Synchronisierungsstatus und wechselt in den Status "Managed".

In einem anderen Szenario wurde der NAD-Eintrag gelöscht:

Network Devices

Selected 0 Total 0

Edit + Add Duplicate Import Export Generate PAC Delete Quick Filter

Name	IP/Mask	Profile Name	Location	Type	Description
9400	x				

No data available

NAD-Eintrag in der ISE für das Netzwerkgerät nicht vorhanden

Wie Sie sehen, ist der gleiche Eintrag für das Gerät NAD nicht vorhanden. Wir gehen genauso vor, d. h. ändern Sie die Management-IP-Adresse in Catalyst Center in Dummy (IP). Nach diesem Verfahren wird ein NAD-Eintrag für das Netzwerkgerät mit seiner ursprünglichen IP-Adresse erstellt.

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.