

Voeg/wijzig de invoer van het netwerktoegangsapparaat in ISE door Catalyst Center toe

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Probleem](#)

[Oplossing](#)

Inleiding

In dit document wordt de procedure beschreven om de ingang (Network Access Device, NAD) in ISE-software aan te passen die is gewijzigd of verwijderd uit ISE.

Achtergrondinformatie

Er kunnen meerdere scenario's zijn waarbij de NAD-ingang voor een netwerkapparaat (dat wordt beheerd door Catalyst Center) moet worden gewijzigd. Voorbeeld:

Als een apparaat wordt geretourneerd, wordt het serienummer gewijzigd en moet een nieuw serienummer worden bijgewerkt in NAD-ingang van dat netwerkapparaat (Advanced TrustSec Settings).

Anders zou de apparaatTrustSec-verificatie niet plaatsvinden, wat resulteert in het niet downloaden van PAC/env.-gegevens.

Er zou een ander scenario kunnen zijn waar de NAD-vermelding wordt verwijderd van Identity Services Engine (ISE) (door een handmatige fout of een andere oorzaak). en nu is alle apparaatverificatie mislukt omdat er geen NAD-vermelding in ISE is.

Probleem

Het probleem in de bovengenoemde scenario's is dat er geen vooraf gedefinieerde optie in Catalyst Center is om de NAD-ingang direct te maken zodra het netwerkapparaat is toegewezen aan de site en NAD-ingang voor het eerst wordt gemaakt, wat ertoe leidt dat gebruikers de NAD-ingang in ISE handmatig moeten configureren/wijzigen, wat tijdrovend en foutgevoelig kan zijn.

In dit document worden de procedure/stappen beschreven om de NAD-ingang (Network Access Device) voor een netwerkapparaat in ISE aan te passen dat is gewijzigd of verwijderd uit ISE-

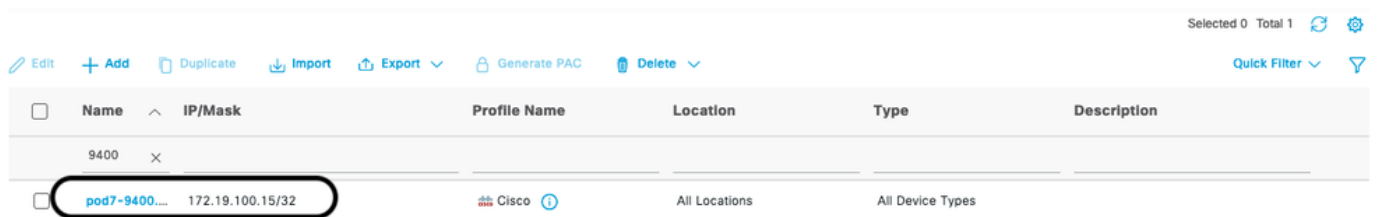
netwerktoegangsapparaat. Deze procedure is van toepassing op elk netwerkapparaat dat wordt beheerd door Catalyst Center.

Oplossing

Om Catalyst Center de NAD-vermelding in ISE te laten configureren, moeten we in principe het IP-adres van het apparaat (in een willekeurige dummy IP) wijzigen, dat backend de NAD-workflow voor het maken van vermeldingen activeert.

Deze procedure is van toepassing op elk netwerkapparaat dat wordt beheerd door Catalyst Center. De NAD-vermelding wordt aangemaakt met het oorspronkelijke IP (aangezien de workflow wordt geactiveerd vóór de wijziging in het IP-adres van het beheer). In dit voorbeeld zijn Advanced TrustSec Settings voor een NAD-vermelding uitgeschakeld in ISE:

Network Devices



Selected 0 Total 1

Edit + Add Duplicate Import Export Generate PAC Delete Quick Filter

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

NAD Entry ISE voor een netwerkapparaat

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

Geavanceerde TrustSec-instellingen zijn uitgeschakeld voor dit NAD-bericht

Zoals in deze afbeelding wordt weergegeven, heeft NAD-ingang voor het apparaat Advanced TrustSec Settings uitgeschakeld (over het algemeen wanneer Catalyst Center de NAD-ingang maakt, is deze sectie ingeschakeld). Verander het beheer IP-adres in Catalyst Center naar dummy IP die de workflow activeert om de NAD-ingang in ISE opnieuw te configureren. Wanneer u het IP-adres van het beheer wijzigt, wordt de status van de apparaatbeheerfunctie verplaatst naar Syncing en moeten de ISE- en AD-vermeldingen worden aangepast.

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**

Het IP-adres voor beheer van het netwerkapparaat in Catalyst Center wijzigen 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...

Netwerkapparaat gaat over op synchronisatiestatus

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	...

Netwerkapparaat wordt onbereikbaar en onbeheerd als IP-adres voor beheer is nep IP en niet bereikbaar via Catalyst Center

ISE-NAD-vermeldingen voor bijgewerkte en "Advanced TrustSec Settings" zijn nu ingeschakeld:

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](#)

Geavanceerde TrustSec-instellingen zijn ingeschakeld na het bijwerken van het IP-adres van het beheer vanuit Catalyst Center

Nadat dit is gemaakt, kunnen we het beheer IP adres terug naar zijn oorspronkelijke IP.

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

Het IP-adres van het beheer opnieuw wijzigen in het oorspronkelijke IP-adres

Nadat het IP-adres voor beheer is bijgewerkt naar het oorspronkelijke IP-adres, gaat het apparaat over in de "synchronisatiestatus" en wordt het "beheerd".

Hier is een ander scenario waarin NAD entry werd verwijderd:

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-ingang bestaat niet in ISE voor netwerkkapparaat

Zoals u ziet bestaat hetzelfde apparaat en item niet. We gebruiken dezelfde procedure, dat wil zeggen, wijzig het IP-adres in Catalyst Center om IP te dumpen). Na het gebruik van deze procedure wordt NAD-vermelding voor het netwerkkapparaat met het oorspronkelijke IP-adres gemaakt.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.