

Agregar/modificar entrada de dispositivo de acceso a la red en ISE mediante Catalyst Center

Contenido

[Introducción](#)

[Antecedentes](#)

[Problema](#)

[Solución](#)

Introducción

Este documento describe el procedimiento para reconfigurar la entrada Network Access Device (NAD) en ISE que se modifica o se elimina de ISE.

Antecedentes

Puede haber varias situaciones en las que sea necesario modificar la entrada NAD de un dispositivo de red (que administra Catalyst Center). Por ejemplo:

Cuando se devuelve un dispositivo, se cambia el número de serie y se debe actualizar un nuevo número de serie en la entrada NAD de dicho dispositivo de red (Configuración avanzada de TrustSec).

De lo contrario, la autenticación de Device TrustSec no se llevaría a cabo, lo que provocaría un error al descargar los datos PAC/env.

Podría haber otra situación en la que la entrada NAD se eliminara de Identity Services Engine (ISE) (debido a un error manual por alguna otra causa). y ahora toda la autenticación del dispositivo falla porque no hay ninguna entrada NAD en ISE.

Problema

El problema en los escenarios antes mencionados es que no existe una opción predefinida en Catalyst Center para crear la entrada NAD directamente una vez que se asigna el sitio al dispositivo de red y la entrada NAD se crea por primera vez, lo que da como resultado que los usuarios tengan que configurar/modificar manualmente la entrada NAD en ISE, lo que puede llevar mucho tiempo y ser propenso a errores.

Este documento describe el procedimiento/los pasos para reconfigurar la entrada NAD (Network Access Device, Dispositivo de acceso a la red) para cualquier dispositivo de red en ISE que se modifique o se elimine de ISE NAD. Este procedimiento se aplica a cualquier dispositivo de red

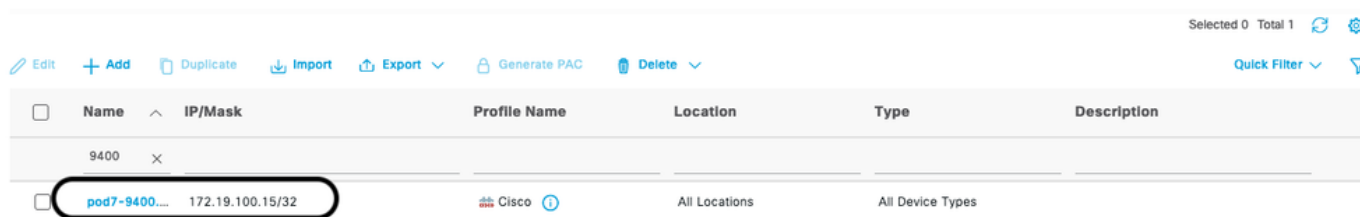
que administre Catalyst Center.

Solución

Para que Catalyst Center configure la entrada NAD en ISE, necesitamos básicamente cambiar la dirección IP de administración del dispositivo (a cualquier IP ficticia) que es backend y activa el flujo de trabajo de creación de entradas NAD.

Este procedimiento se aplica a cualquier dispositivo de red que administre Catalyst Center. La entrada NAD se creará con la dirección IP original (a medida que se active el flujo de trabajo antes del cambio en la dirección IP de administración). En este ejemplo, la configuración avanzada de TrustSec para una entrada NAD está deshabilitada en ISE :

Network Devices



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

ISE de entrada NAD para un dispositivo de red

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

La configuración avanzada de TrustSec está deshabilitada para esta entrada de NAD

Como se ve en esta imagen, la entrada NAD para el dispositivo tiene la configuración de TrustSec avanzada desactivada (generalmente cuando el centro de Catalyst crea la entrada NAD, esta sección está habilitada). Cambie la dirección IP de administración en Catalyst Center por IP ficticia, que activa el flujo de trabajo para volver a configurar la entrada NAD en ISE. Cuando cambia la dirección IP de administración, mueve la capacidad de administración del dispositivo al estado de sincronización y se debe modificar la entrada de ISE NAD.

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

Cambio de la dirección IP de administración del dispositivo de red en Catalyst Center a IP falsa

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...

El dispositivo de red entra en estado de sincronización

Devices (1) Focus: Inventory

deviceName: (*9400*)

0 Selected Add Device Tag Actions

Take a tour [Export](#)

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

El dispositivo de red se vuelve inalcanzable y no se gestiona, ya que la dirección IP de gestión es una IP ficticia y no se puede acceder a ella desde Catalyst Center

La entrada de ISE NAD para la configuración actualizada y "Advanced TrustSec Settings" está ahora habilitada:

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](#)

La configuración avanzada de TrustSec se habilitó después de actualizar la dirección IP de administración de Catalyst Center

Después de crear esto, podemos cambiar la dirección IP de administración nuevamente a su IP original.

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

Cambio de la dirección IP de administración a su IP original

Después de actualizar la dirección IP de administración a su dirección IP original, el dispositivo pasa al estado de "sincronización" y se convierte en "administrado".

Aquí hay otro escenario donde la entrada NAD fue eliminada :

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					

No data available

La entrada NAD no existe en ISE para el dispositivo de red

Como puede ver, la entrada NAD del mismo dispositivo no existe. Utilizamos el mismo procedimiento, es decir, modificamos la dirección IP de administración en Catalyst Center a IP ficticia). Después de utilizar este procedimiento, se crea la entrada NAD para el dispositivo de red con su dirección IP original.

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).