Resolución de Problemas de Conectividad entre Cisco DNA Center y Nuestros Dispositivos de Red (Troubleshooting)

Comunidad de Cisco

Fernando Santillán – Technical Consulting Engineer – DNA Center TAC
Eduardo Cardeña – Technical Consulting Engineer – DNA Center TAC

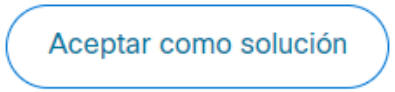
Jueves 30 de noviembre de 2023

Conecte, Interactúe, ¡Colabore!

Soluciones

¡Acepte las soluciones correctas y felicite a quienes le ayudaron! Los foros de discusión tienen muchas entradas, de las cuales no todas cuentan con una respuesta correcta o válida.

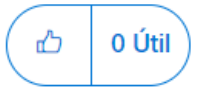
Ayude a otros usuarios a encontrar las respuestas correctas en el motor de búsqueda de la comunidad indicando que la duda fue resuelta al activar la opción “Aceptar como solución”.

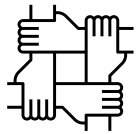


Agradecimientos

¡Resalte el esfuerzo de otros miembros!

Los votos útiles motivan a otros miembros que colaboran en la comunidad, a seguir ayudándonos a contestar las preguntas abiertas, y ofreciéndoles la oportunidad de ganar premios además de ser una muestra valiosa de ¡nuestro reconocimiento!





Spotlight Awards

¡Nuevos ganadores en español!

Destaca por tu esfuerzo y compromiso para mejorar la comunidad y ayudar a otros miembros. Los Premios Spotlight se otorgan trimestralmente para destacar a los miembros más destacados.

¡Ahora también puedes nominar a un candidato! Haga clic aquí

Community Spotlight awards

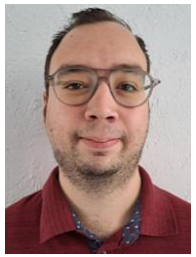
Fernando Santillán

Technical Consulting Engineer

Fernando es egresado del Instituto Politécnico Nacional (IPN) de la Escuela Superior de Ingeniería Mecánica y Eléctrica, con cinco años de experiencia en equipos IoT (CGR, CGS, IE e IR) y en la solución DNA Center y equipos Catalyst, así como Docker y Kubernetes.

Actualmente ocupa el puesto de Customer Support Engineer con dos años como líder de equipo para TAC.

Eduardo Cardeña



Technical Consulting Engineer

Eduardo es egresado de la Universidad Veracruzana con título en Instrumentación Electrónica, con seis años de experiencia en tecnología Cisco (R&S, Wireless, Collaboration y DNA Center).

Anteriormente, Eduardo trabajó como Ingeniero de Implementación y Soporte con varios partners de Cisco.

Posee la certificación CCNP Enterprise con especialidad en redes inalámbricas.

Descargue la presentación

https://bit.ly/CL4doc-nov23

slido

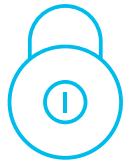
Join at

slido.com

#2370 995

Passcode: **iibnaw**

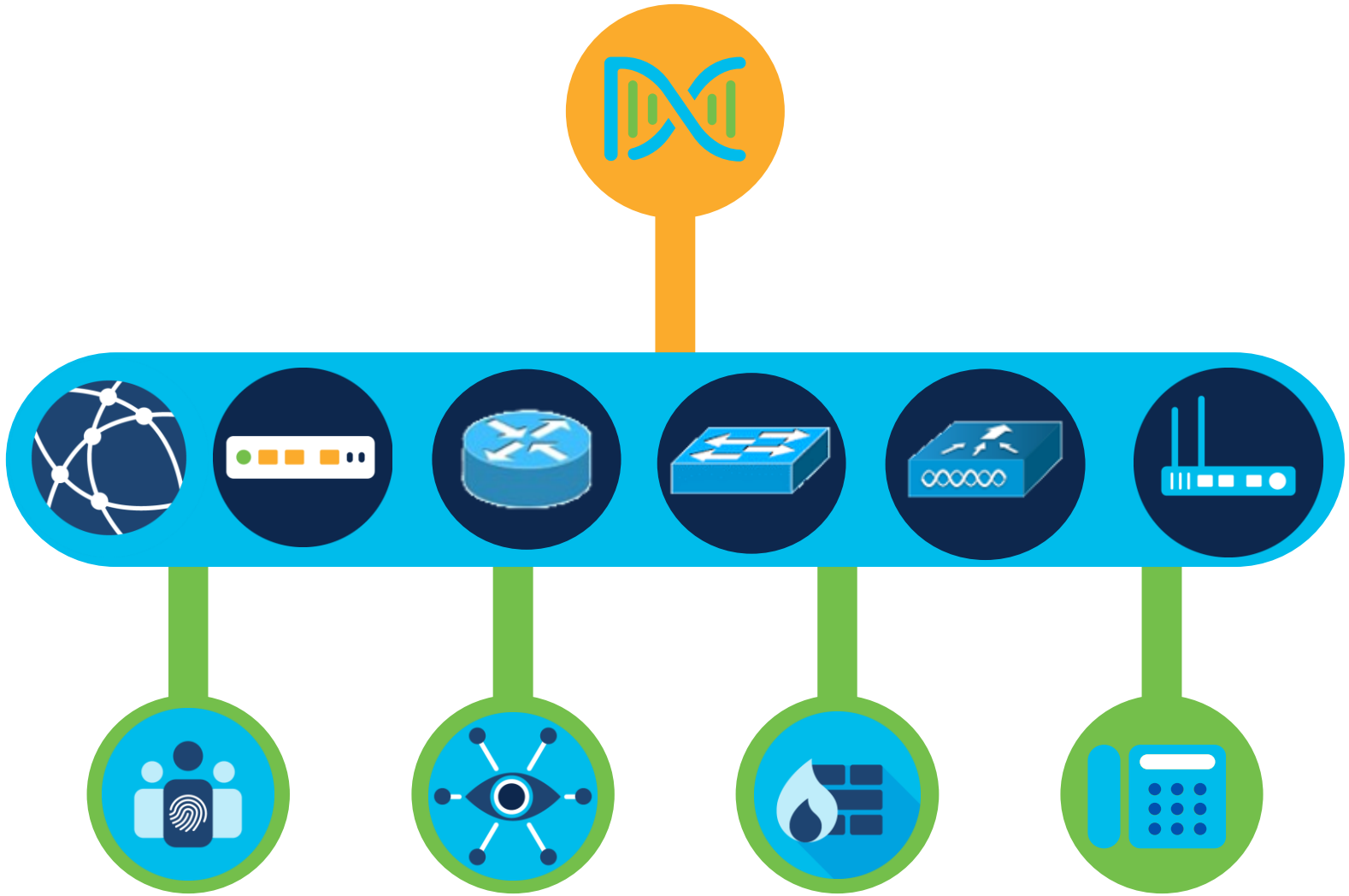
Agenda



1. Tipos de Incidentes
2. Alertas
3. Herramientas de Troubleshooting
4. Automation para Troubleshooting
5. Demostración

Tipos de Incidentes

Tipos de Dispositivos



Requisitos

Para la recopilación parcial de inventario en Cisco DNA Center, se debe contar los siguientes valores:

- Versión SNMP
- SNMP community strings de solo lectura
- SNMP community strings de escritura
- Valor de reintento de SNMP
- Valor de tiempo de espera de SNMP

Para la recopilación completa de inventario en Cisco DNA Center, se debe contar los siguientes valores:

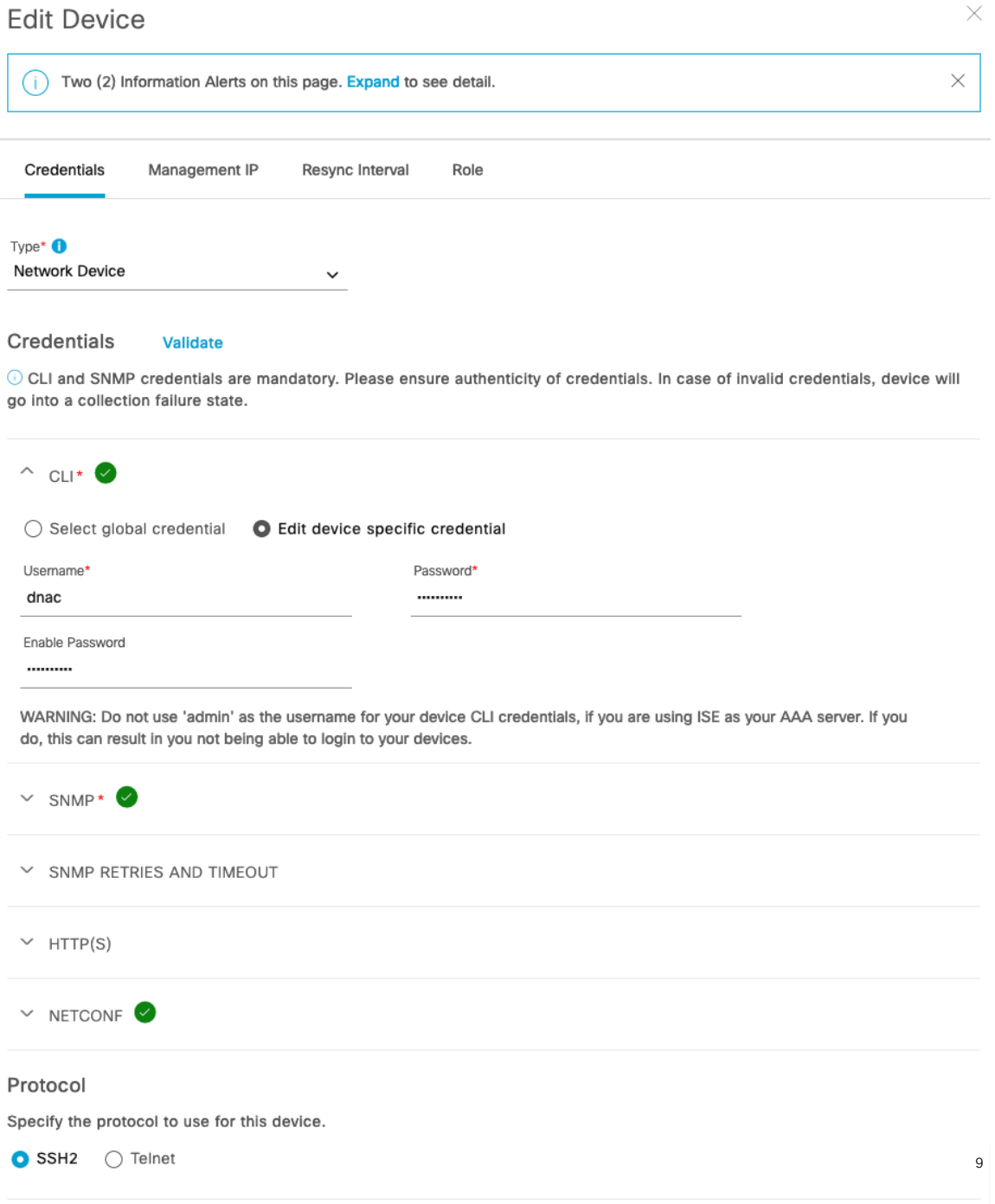
- Dirección IP del dispositivo
- Versión SNMP
- SNMP community strings de solo lectura
- SNMP community strings de escritura
- Valor de reintento de SNMP
- Valor de tiempo de espera de SNMP
- Nombre de usuario de CLI
- Contraseña de CLI
- Contraseña de “enable” de CLI
- Valor de tiempo de espera de la CLI

Validar credenciales

CLI Credentials

SNMP Credentials

NETCONF



Tipos de Incidentes

Threshold-based

- Problemas basados en umbrales.
- Problemas detectados por Assurance.

Conectividad

- Ping
- SSH
- Netconf

Problemas basados en IA

- Problemas detectados por Cisco AI Network Analytics.
- Se activan en función a parámetros preestablecidos.

Problemas de conexión

- Tiempo excesivo, Fallos excesivos, Tiempo de asociación excesivo, Fallos de asociación excesivos, Tiempo de autenticación excesivo, Fallos de autenticación excesivos, Tiempo DHCP excesivo y Fallos DHCP excesivos.

Telemetría

- Rendimiento total de radio, Rendimiento de aplicaciones multimedia, Rendimiento de aplicaciones de nube, Rendimiento de aplicaciones de colaboración y Rendimiento de aplicaciones sociales.

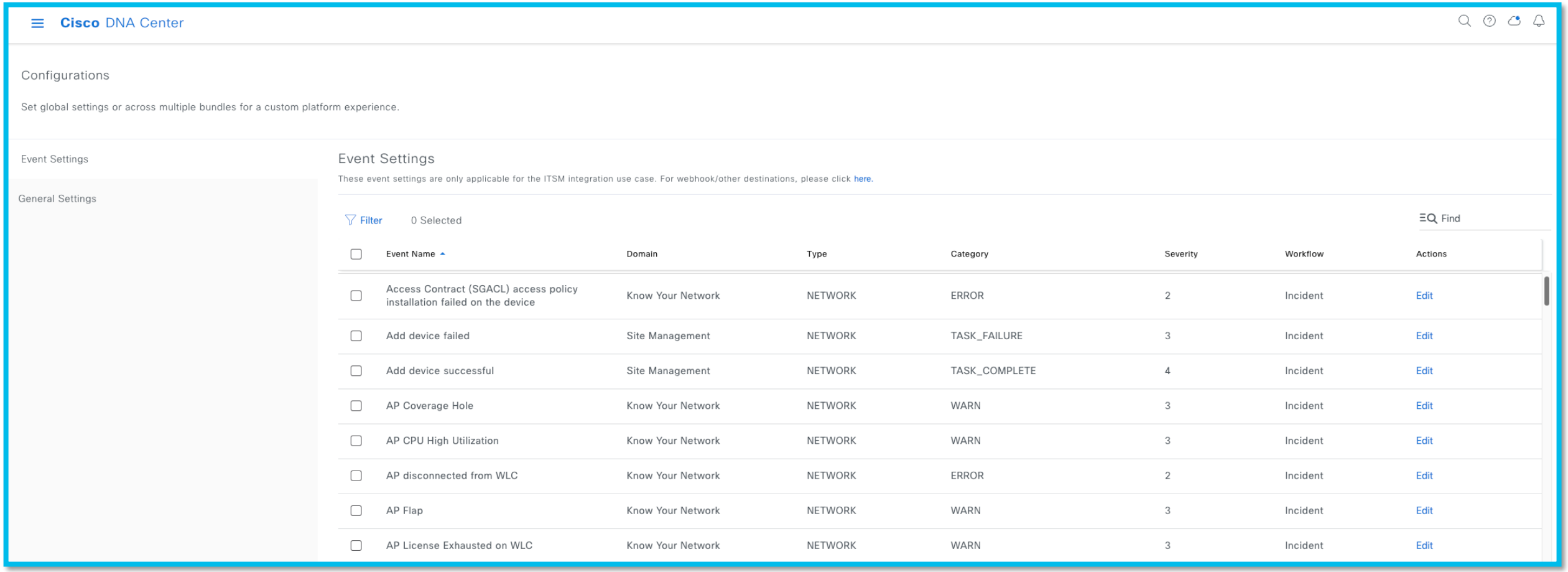
L2 Loop & PoE

- Problemas detectados por Assurance que puede solucionar mediante el flujo de trabajo de MRE.

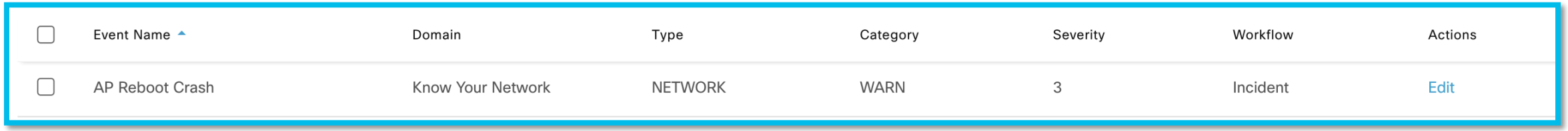
Alertas

Configuración de Eventos

- Navegue al menú de Cisco DNA Center > Platform > Manage



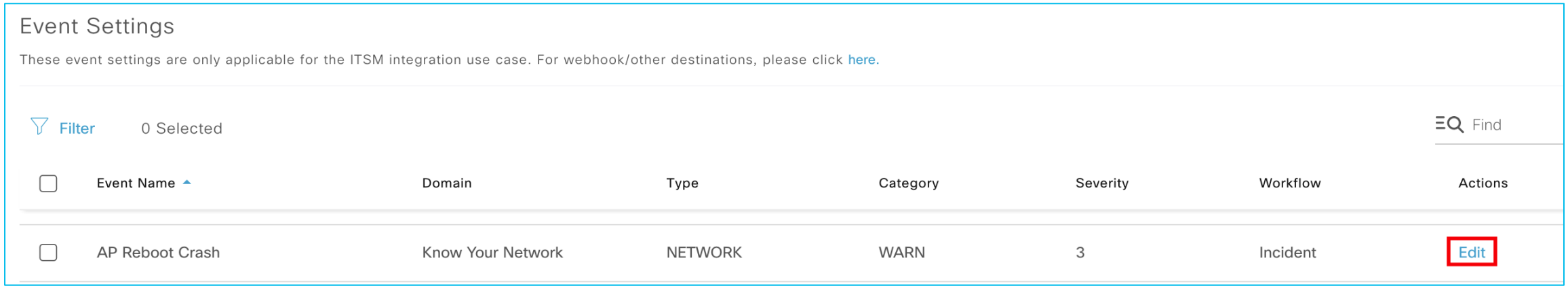
Configuración de Eventos

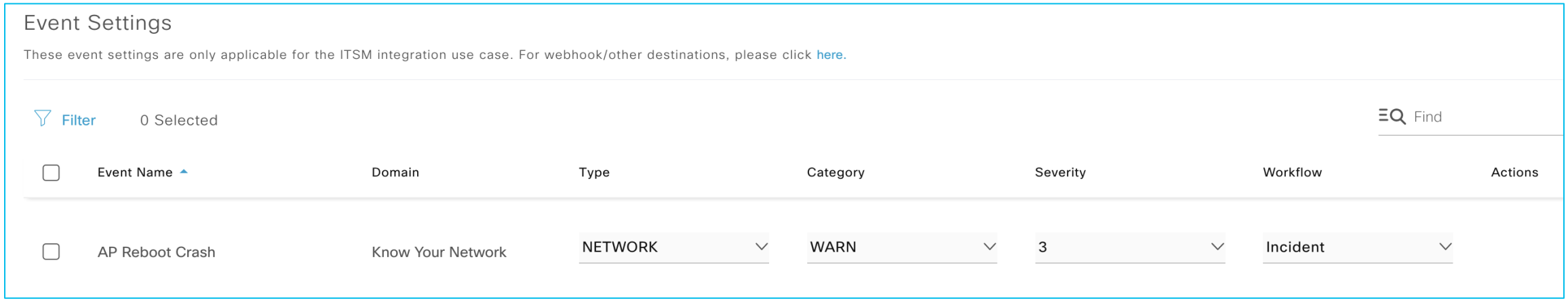


Event Name	Domain	Type	Category	Severity	Workflow	Actions
AP Reboot Crash	Know Your Network	NETWORK	WARN	3	Incident	Edit

- **Nombre del evento**: Nombre del evento en Cisco DNA Center.
- **Dominio**: Dominio del evento en Cisco DNA Center.
- **Tipo**: Network, App, System, Security, or Integrations.
- **Categoría**: Error, Warn, Info, Alert, Task Progress, Task Complete
- **Severidad**: Del 1 al 5 (donde 1 es el más crítico).
- **Flujo de trabajo**: Incident, Problem, Event, or RFC
- **Actions**: Configurar el evento.

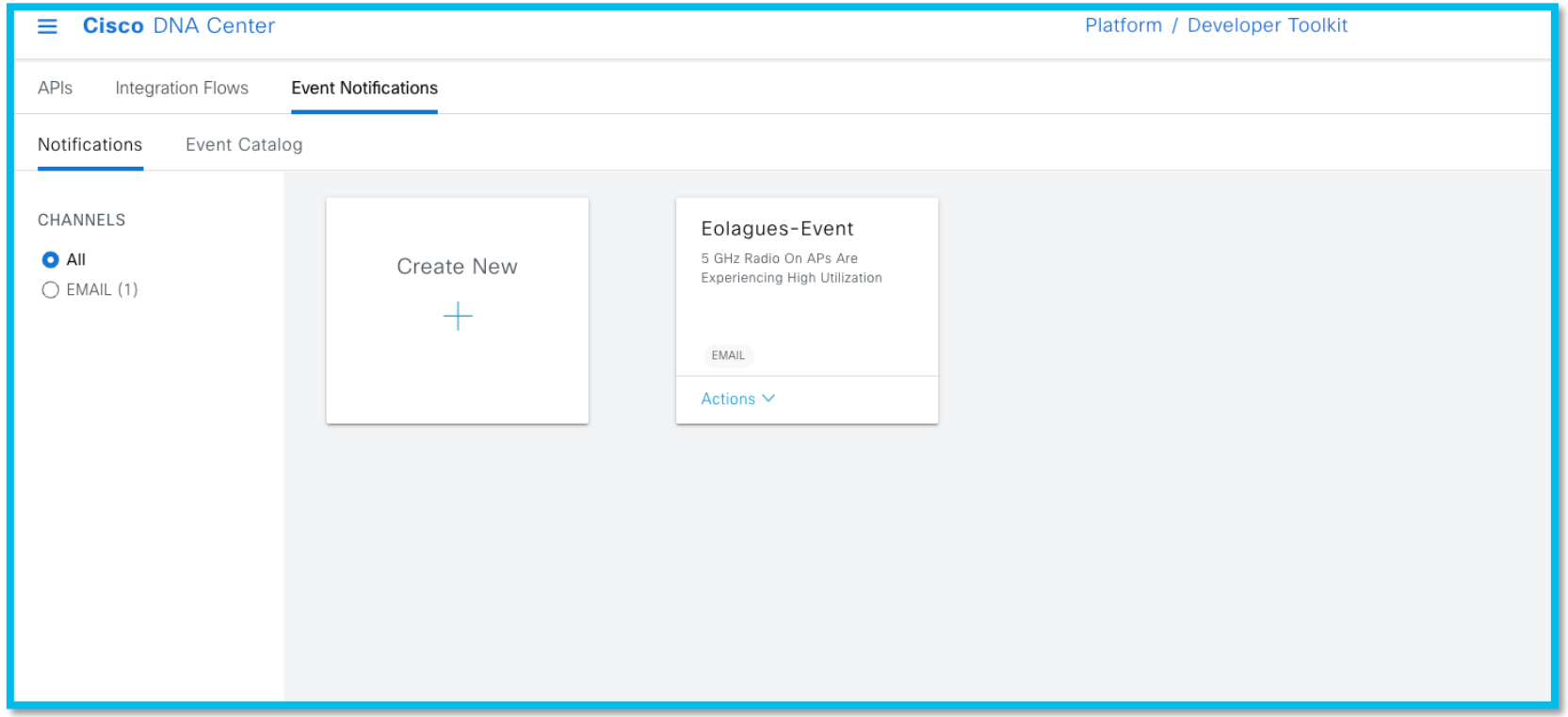
Configuración de Eventos





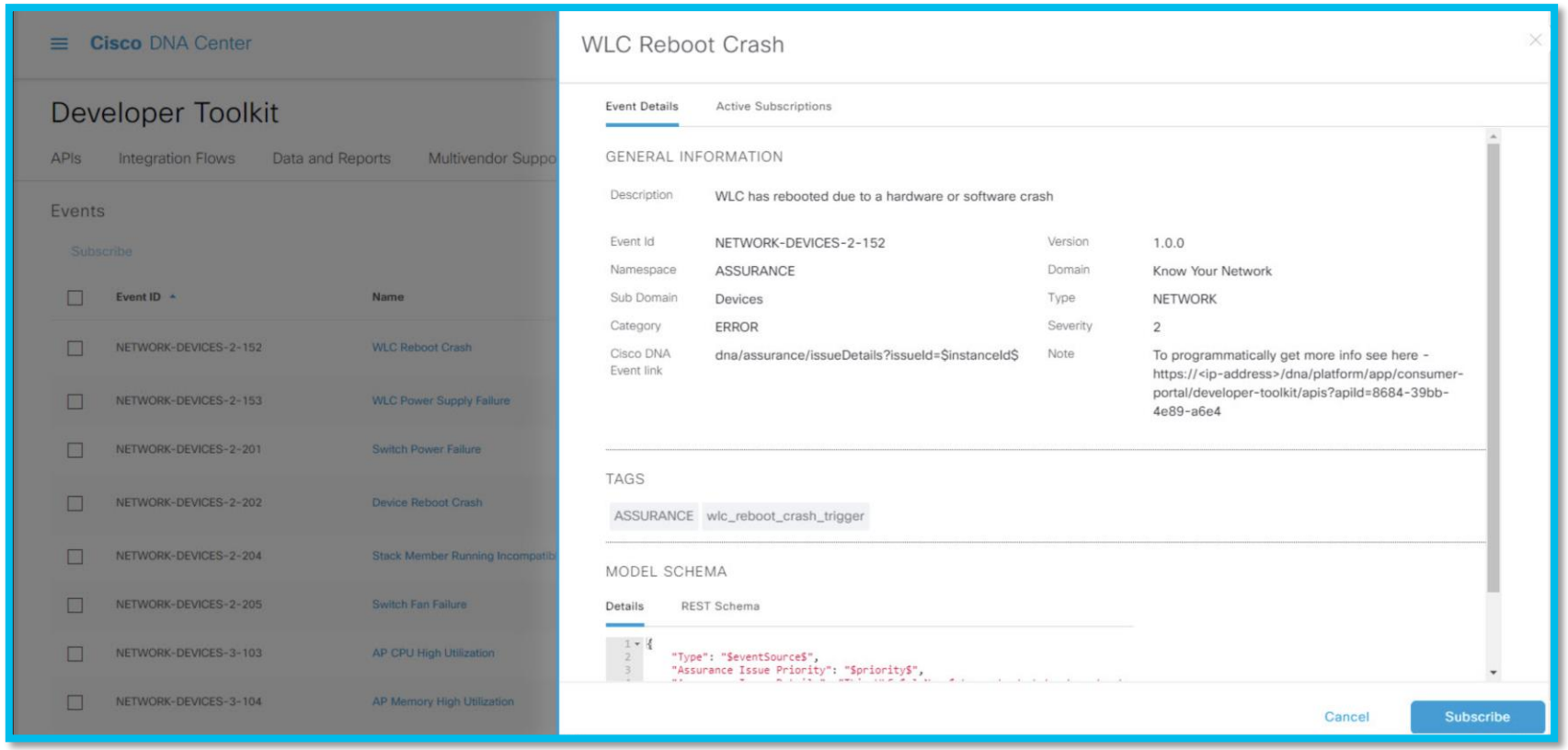
Eventos

- Puede suscribirse a un evento mediante la ventana Eventos en la GUI de Cisco DNA Center. Navegue a Menú > Platform > Developer Toolkit > Event Notifications.

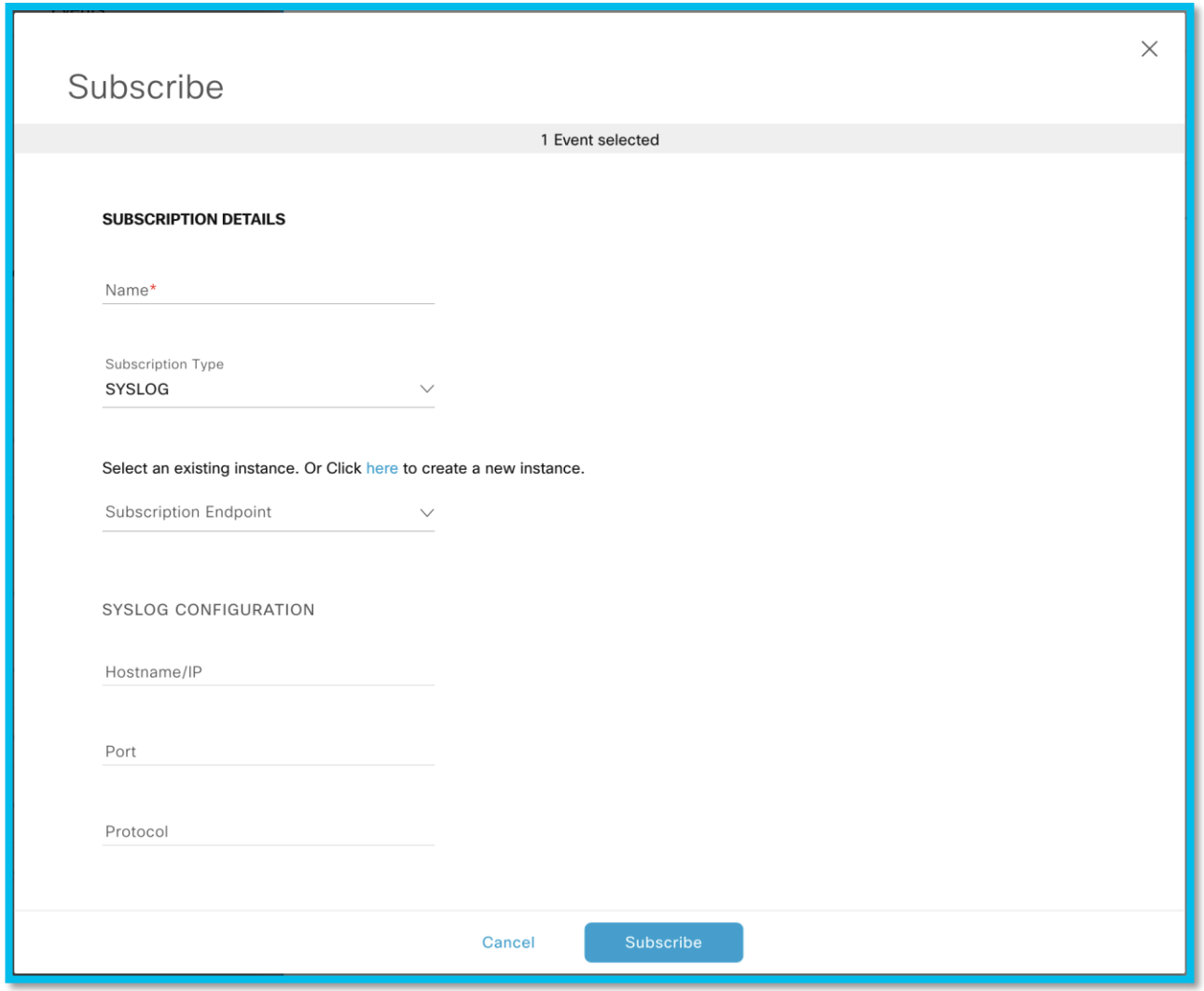


Eventos

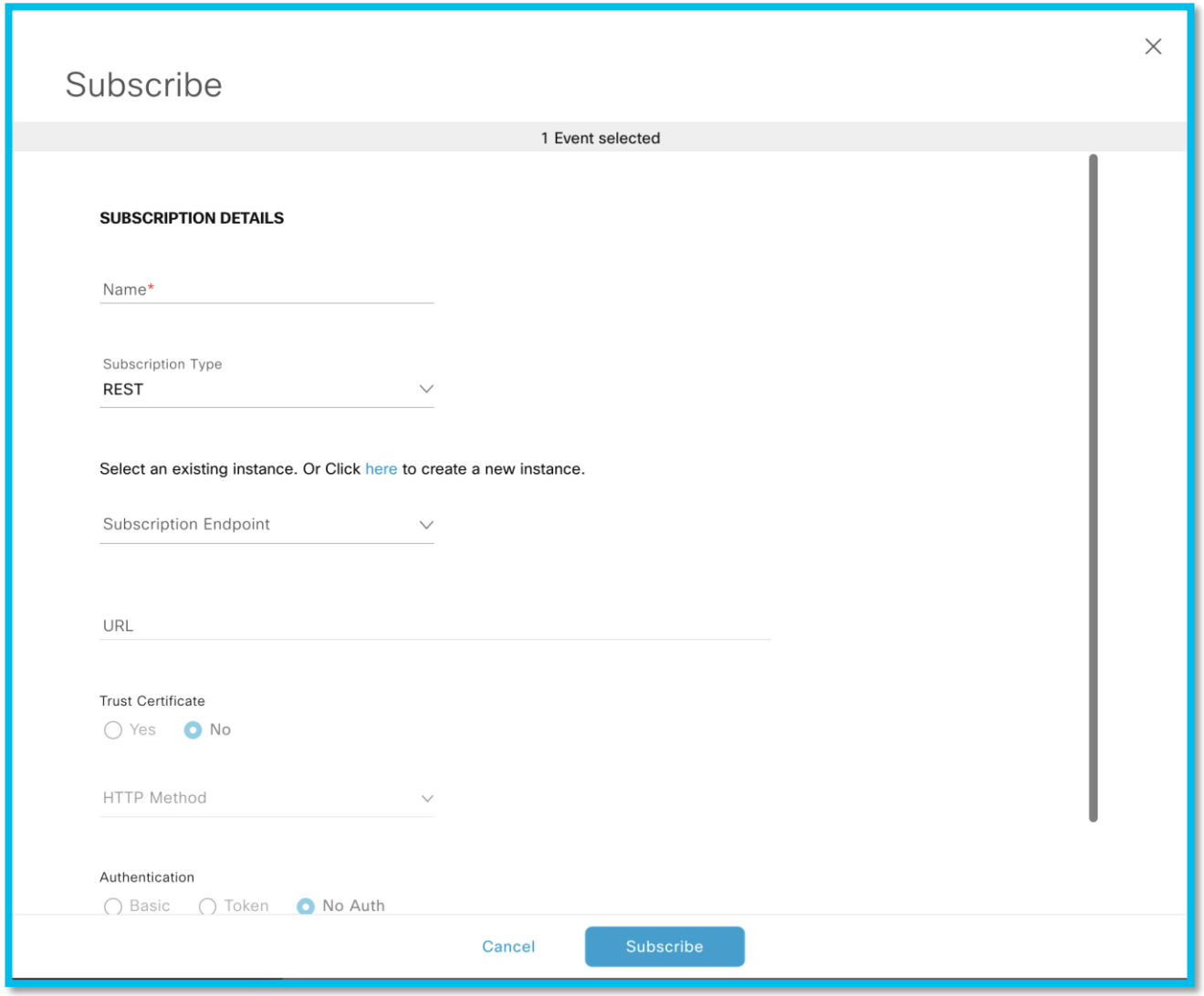
- Haga clic en un enlace Nombre para abrir un panel deslizante de suscripción de eventos.



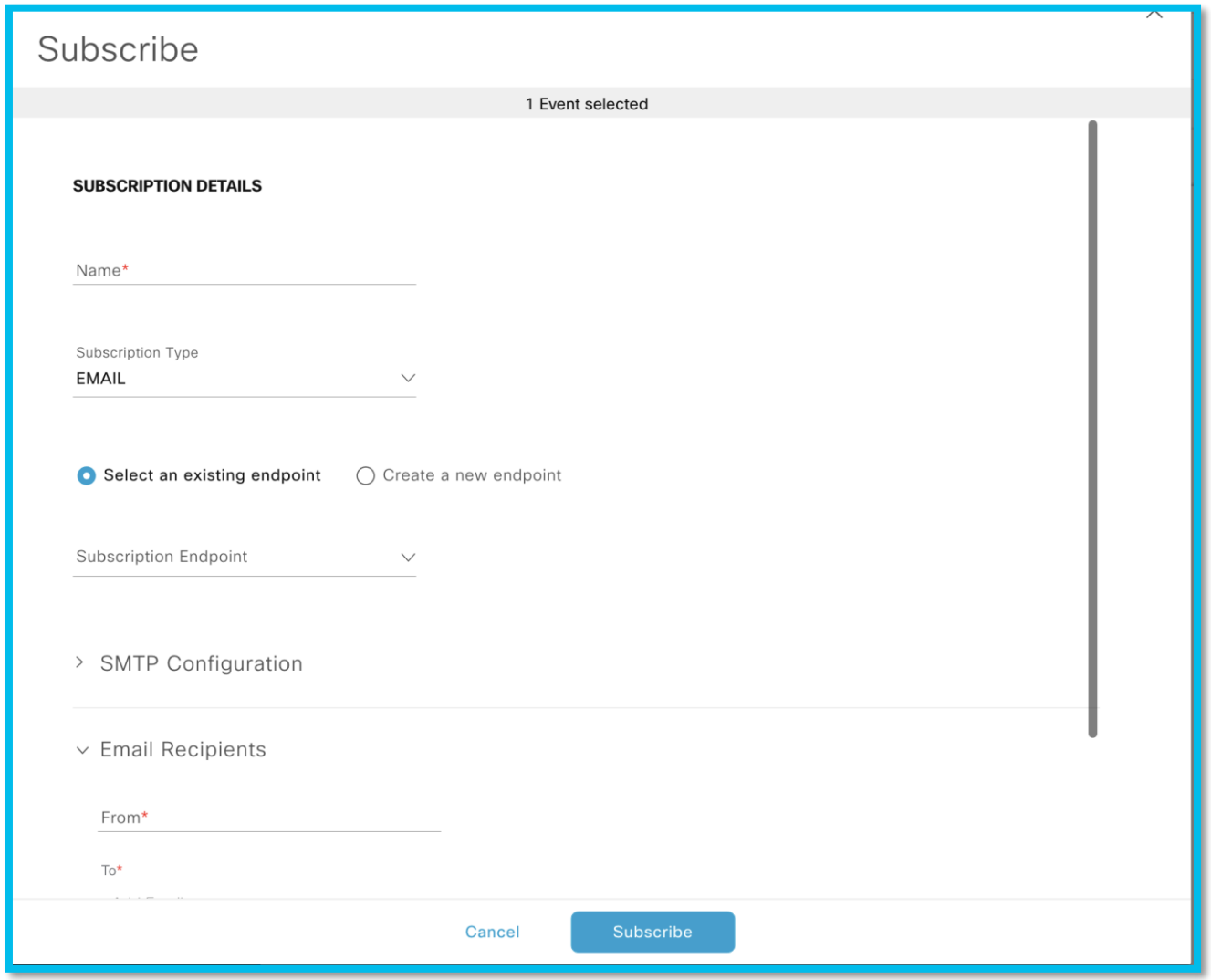
Events – Syslog



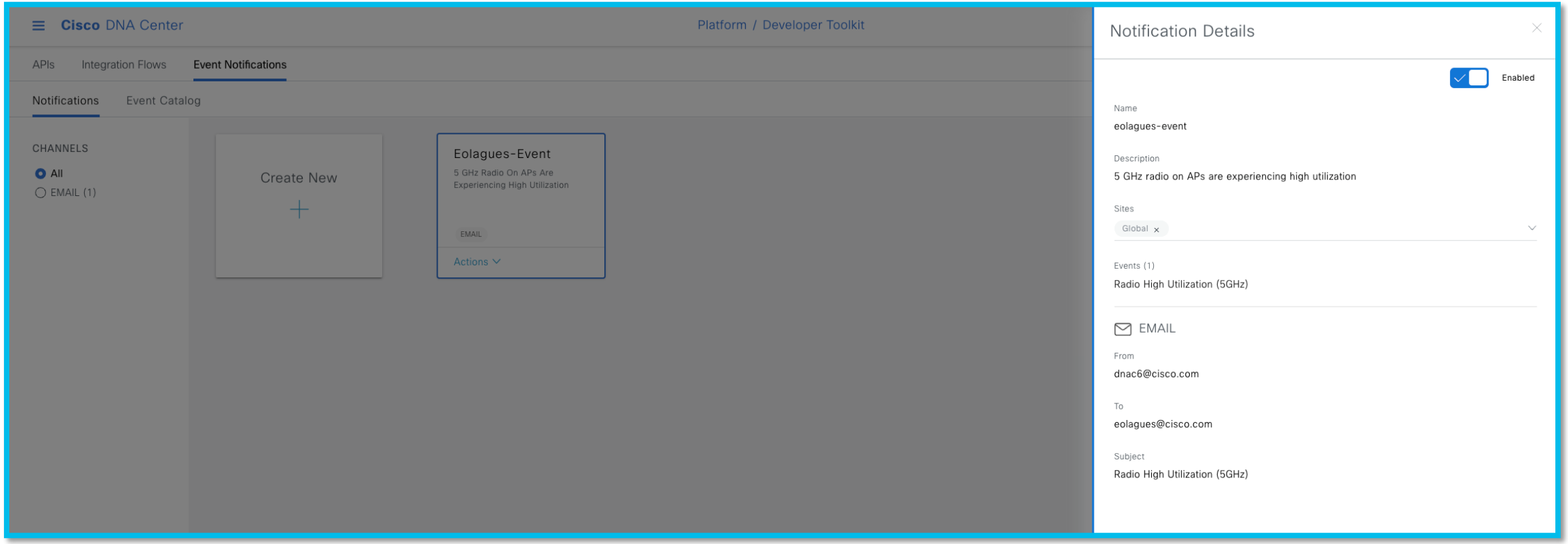
Events – REST API (Webhook)



Events – Email

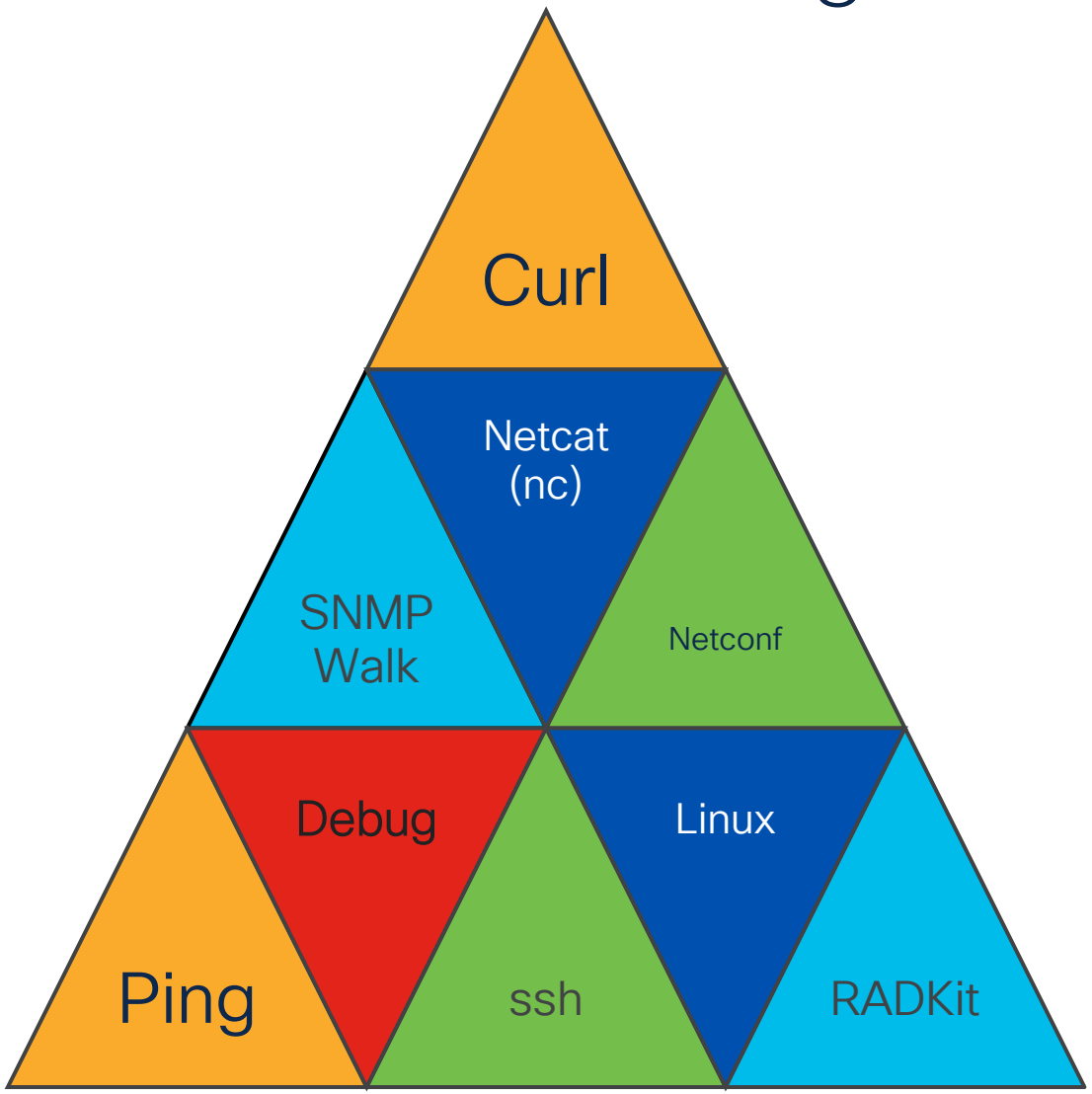


Events



Herramientas de Troubleshooting

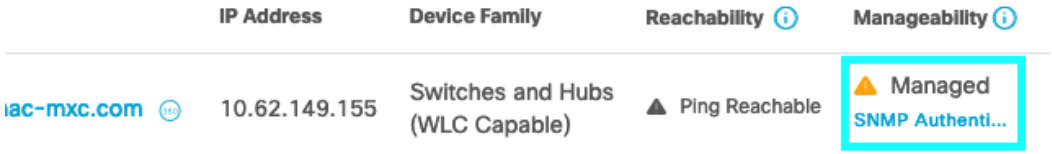
Herramientas de troubleshooting de red.

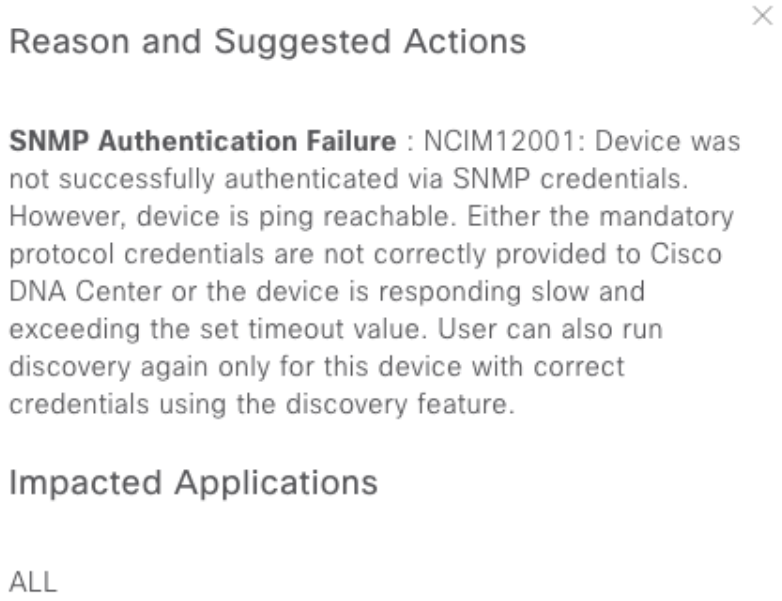


SNMPWALK

SNMPWALK

- SNMP walk es una aplicación SNMP que utiliza solicitudes SNMP GETNEXT para recopilar datos SNMP de dispositivos habilitados para SNMP de red e infraestructura, como conmutadores y enrutadores.
- Realizar un recorrido SNMP puede ayudarlo a solucionar problemas de estadísticas faltantes o inexactas para dispositivos de red y otros dispositivos sondeados a través de SNMP al confirmar la comunicación SNMP con dispositivos remotos y qué identificadores de objeto (OID) están respondiendo.





SNMPWALK para SNMPv2

`snmpwalk -v 2c -c “community-name” “device IP address”`

- -v 2c Versión de SNMP
- -c Nombre de la comunidad configurado en el dispositivo

```
# snmpwalk -v 2c -c d_dnacread 192.168.37.230
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco IOS Software [Gibraltar], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version
16.12.1a, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Sun 04-Aug-19 06"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.1537
iso.3.6.1.2.1.1.3.0 = Timeticks: (622140492) 72 days, 0:10:04.92
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "CSR1K_APPX.Pod2.com"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 78
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.2.1.0 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.2.1 = STRING: "GigabitEthernet1"
```

SNMPWALK para SNMPv3

```
snmpwalk -v3 -l <noAuthNoPriv|authNoPriv|authPriv> -u <username> [-a <MD5|SHA>] [-A <authphrase>] [-x DES] [-X
<privaphrase>] <ipaddress>[:<dest_port>] [oid]
```

```
snmpwalk -v3 -l authPriv -u dnac -a SHA -A Mexico123 -x AES -X Mexico123 172.30.1.72
```

```
# snmpwalk -v3 -l authPriv -u dnac -a SHA -A Mexico123 -x AES -X Mexico123 172.30.1.72
Iso.3.6.1.2.1.1.1.0 = STRING: “Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software
(CAT9K_IOSXE)”, Version 17.3.3, RELEASE SOFTWARE (fc7) Technical Support:
http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Thu 04-Mar-21 12:32 by mcpre”
iso.3.6.1.2.1.1.2.0 =  OID: iso.3.6.1.4.1.9.1.2494
iso.3.6.1.2.1.1.3.0 = Timeticks: (42498183) 4 days, 22:03:01.83
iso.3.6.1.2.1.1.4.0 = “”
iso.3.6.1.2.1.1.5.0 = STRING: “Border2-CN.Pod8.com”
iso.3.6.1.2.1.1.6.0 = “”
iso.3.6.1.2.1.1.7.0 = INTEGER: 6
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00


# snmpwalk -v3 -l authPriv –u dnac3 -a SHA -A Mexico123 -x AES -X Mexico123 172.30.1.72
snmpwalk: Unknnown user name

# snmpwalk -v3 -l authPriv –u dnac3 -a MD5 -A Mexico123 -x AES -X Mexico123 172.30.1.72
snmpwalk: Authentication failure (incorrect password, community or key)
```

Join at
slido.com
#2370 995

Passcode:
iibnaw

Seleccione la oración que solo tenga afirmaciones correctas sobre el siguiente SNMPWALK:
 # snmpwalk -v3 -l authPriv -u user_admin -a SHA -A Tac123 -x AES -X Tac123 172.30.1.72

a) El usuario para la prueba SNMPWALK es super_admin y el tipo de autenticación es SHA
0%

b) El usuario para la prueba SNMPWALK es user_admin y el tipo de autenticación es MD5
0%

c) El usuario para la prueba SNMPWALK es user_admin y el tipo de autenticación es SHA
0%

d) SNMPWALK es versión 2 y el tipo de autenticación es SHA
0%

NETCONF

NETCONF

NETCONF (Network Configuration Protocol) es un protocolo de gestión de red definido en RFC 6241 diseñado para la configuración, gestión y recuperación de datos operativos de dispositivos de red.

El protocolo NETCONF está basado en servidor u orientado a la conexión y consiste de 4 capas de operación.

NETCONF generalmente se implementa usando SSH como transporte

Como modelo de datos principal, NETCONF puede hacer uso de modelos de datos específicos de redes basados en YANG. Los dispositivos de red compatibles con YANG tendrán construcciones de red fácilmente disponibles en formato YANG para modelar datos RPC generales.

Capas de Operación de NETCONF

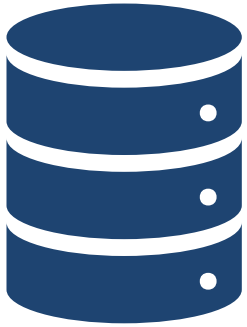
El protocolo NETCONF está basado en servidor u orientado a la conexión y consiste de 4 capas de operación.

Layer	Example
Transporte	SSHv2
Mensajes	<rpc>, <rpc-reply>
Operaciones	<get>, <copy-config>, <edit-config>
Contenido	XML (YANG)

Configuración de NETCONF

- Con "netconf-yang" se habilita netconf-yang en el dispositivo globalmente
- Se requieren listas de métodos AAA, ya que NETCONF utilizará exclusivamente las listas de métodos AAA "predeterminadas", incluso si el acceso SSH/Telnet es manejado por otras listas AAA.
- Asegúrese de que el nombre de usuario local almacenado en el dispositivo esté configurado para un nivel de privilegio de 15, que es necesario para el funcionamiento del Cisco DNA Center.
- El puerto predeterminado es 830

NETCONF en DNA Center



Recopilación de datos de estado de la aplicación

Informe RUM (Licenciamiento)

Active poll

0

Join at

slido.com

#2370 995

Passcode:

iibnaw

¿Cómo contribuye NETCONF a la funcionalidad de Cisco DNA Center para la gestión de redes?

a) NETCONF se utiliza para definir el diseño visual de la interfaz de usuario de Cisco DNA Center.

0%

b) NETCONF ayuda a automatizar el aprovisionamiento y la configuración de los dispositivos de red en la infraestructura.

0%

c) NETCONF proporciona monitorización en tiempo real del tráfico y rendimiento de la red dentro del Cisco DNA Center.

0%

d) NETCONF es el principal responsable de gestionar la autenticación de usuarios y el control de acceso en el Cisco DNA Center.

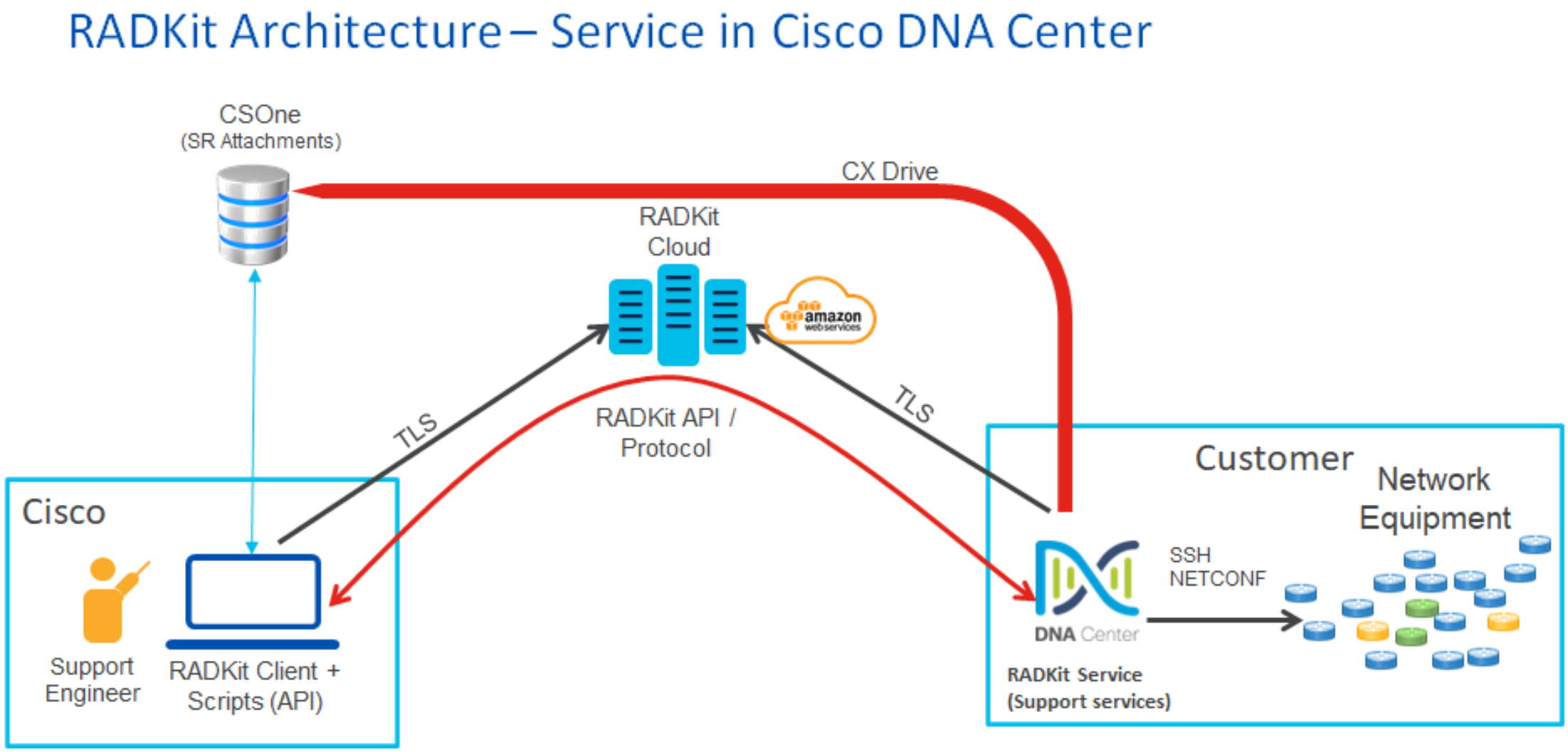
0%

RADKit

RADKit en Cisco DNA Center

- Cisco RADKit proporciona conectividad interactiva segura a terminales remotas e interfaces de usuario web.
- Las funciones de Cisco RADKit están integradas en Cisco DNA Center y se denominan Autorización de Soporte Remoto.
- Cuando los usuarios utilizan la función de Autorización de Soporte Remoto, pueden hacer que el TAC de Cisco acceda remotamente a su entorno Cisco DNA Center para ayudarles a recopilar información o solucionar problemas.

RADKit en Cisco DNA Center



RADKit Service & Client

RADKit consta de tres elementos principales:

- **RADKit Service**: una aplicación ligera instalada de lado del Cliente que se utiliza como puente a los dispositivos de red. Es compatible con muchos protocolos de gestión estándar como SSH, telnet, Netconf, HTTP/REST, Swagger/OpenAPI y proxy SOCKS.
- **RADKit Client** - un front-end que permite a un Ingeniero Cisco consultar o acceder remotamente a los dispositivos de red de un Cliente a través de un Servicio RADKit.
- **RADKit Cloud** - actúa como transporte entre el RADKit Client y el Service. Proporciona cifrado TLS, servicios CA y autenticación Cisco SSO y basada en certificados para Clientes y Servicios.

Automation para Troubleshooting

Herramientas embebidas en Cisco DNA Center

Security Advisories	Utiliza los avisos del Equipo de Respuesta a Incidentes de Seguridad de Productos Cisco (PSIRT) y nos muestra los dispositivos con vulnerabilidades.
Inventory Insights	Muestra dispositivos con configuración errónea según sus vecinos, mejores prácticas o en caso de tener links inactivos. Mantiene histórico de datos.
Network Reasoner	Le permite solucionar rápidamente diversos problemas de su red de forma proactiva.
Command Runner	Permite enviar comandos de diagnóstico a los dispositivos seleccionados. Actualmente, se permiten los comandos show y otros comandos de solo lectura.

Active poll

0

Join at

slido.com

#2370 995

Passcode:

iibnaw

¿Cuál es el criterio primario de revisión que utiliza la herramienta de Avisos de Seguridad (Security Advisories) para generar las alertas?

a) La versión del dispositivo

0%

b) El SN del dispositivo

0%

c) La configuración activa del dispositivo

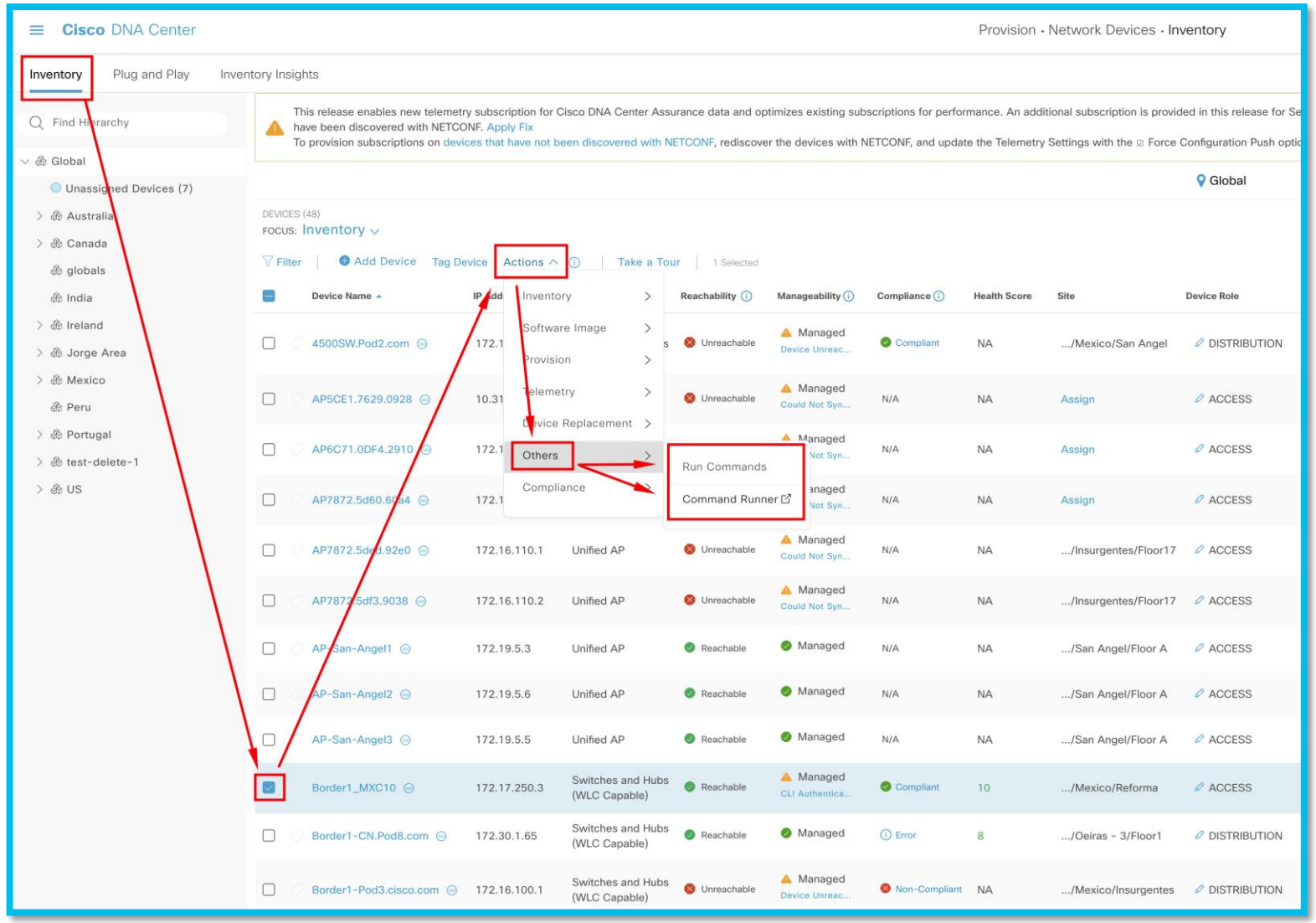
0%

d) El último aprovisionamiento del dispositivo

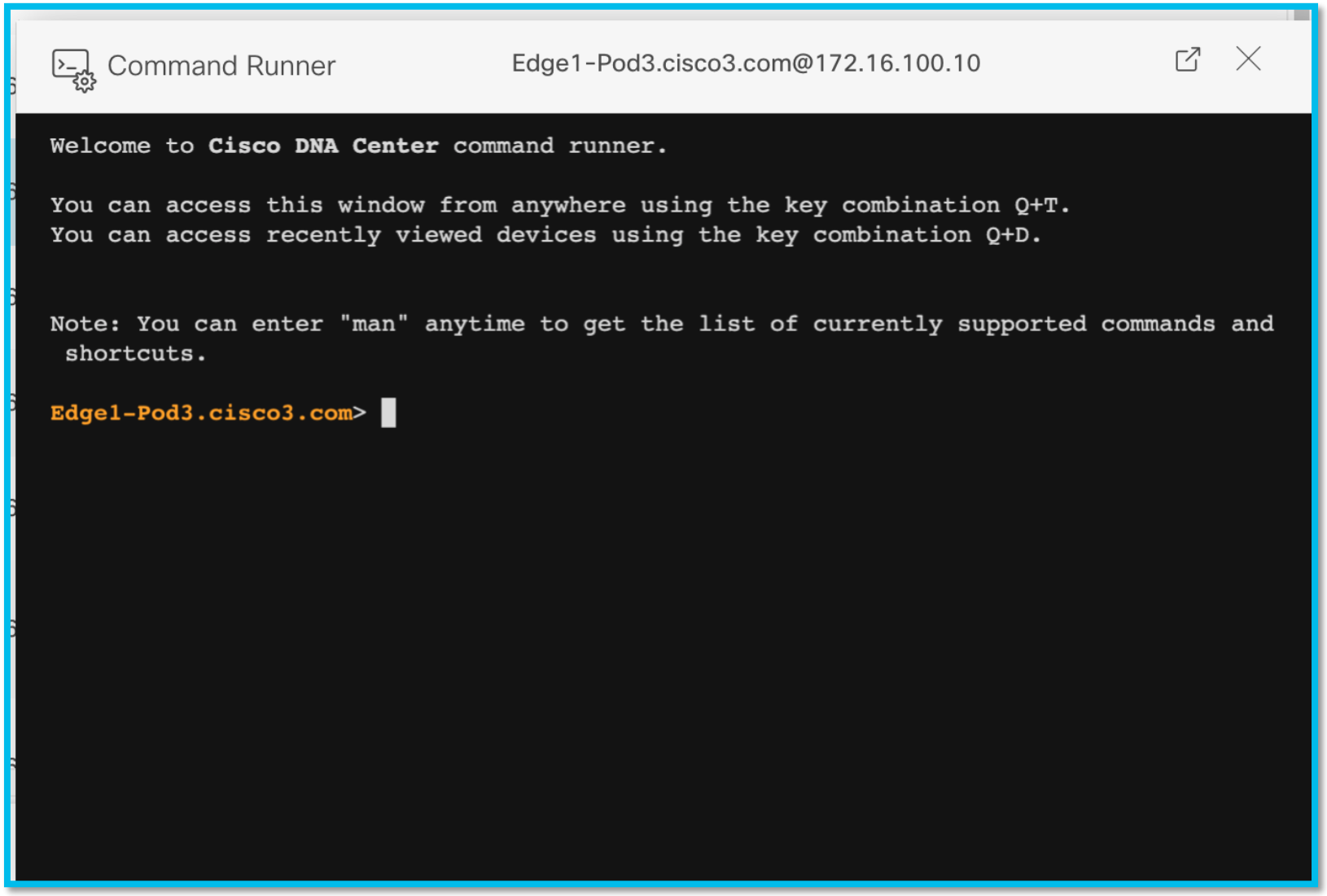
0%

Command Runner

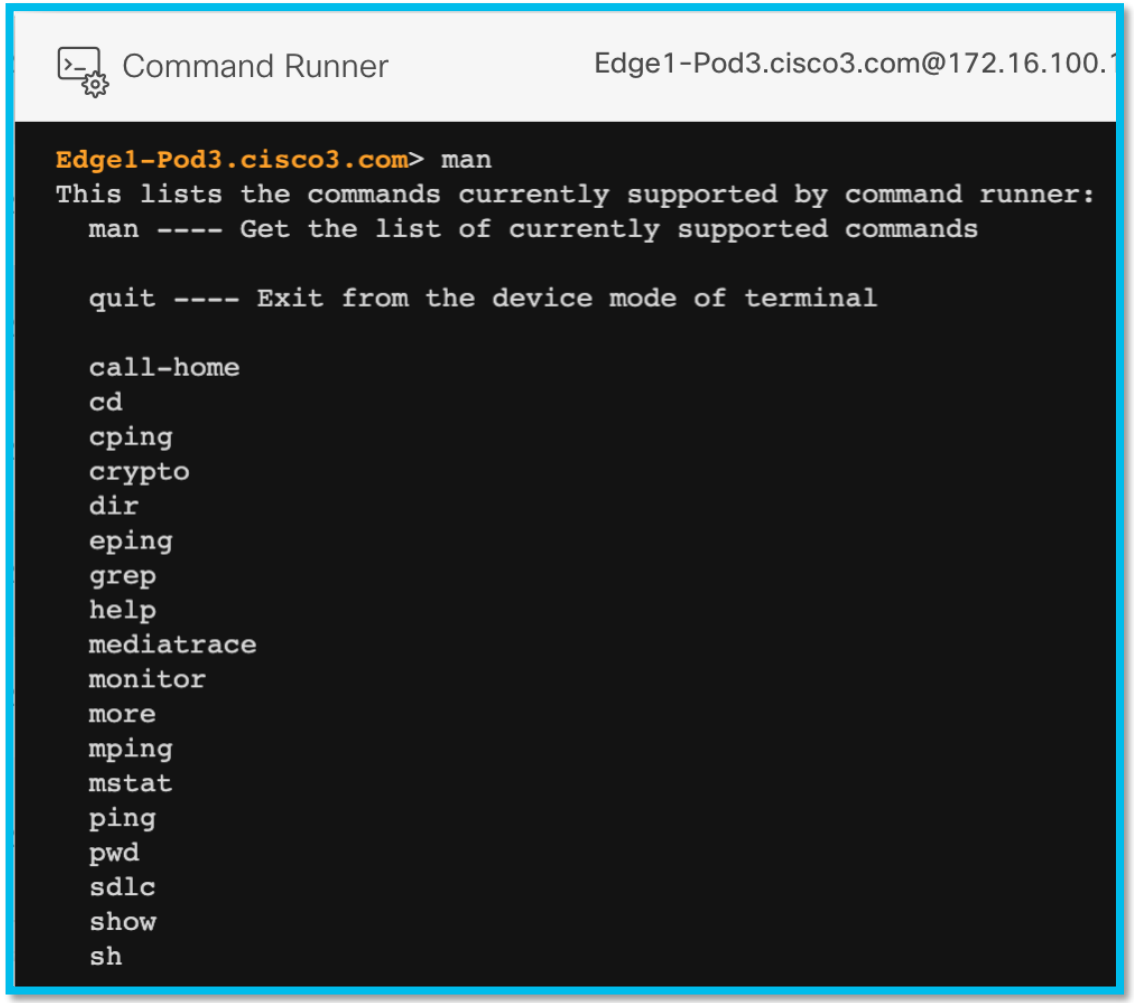
Command Runner

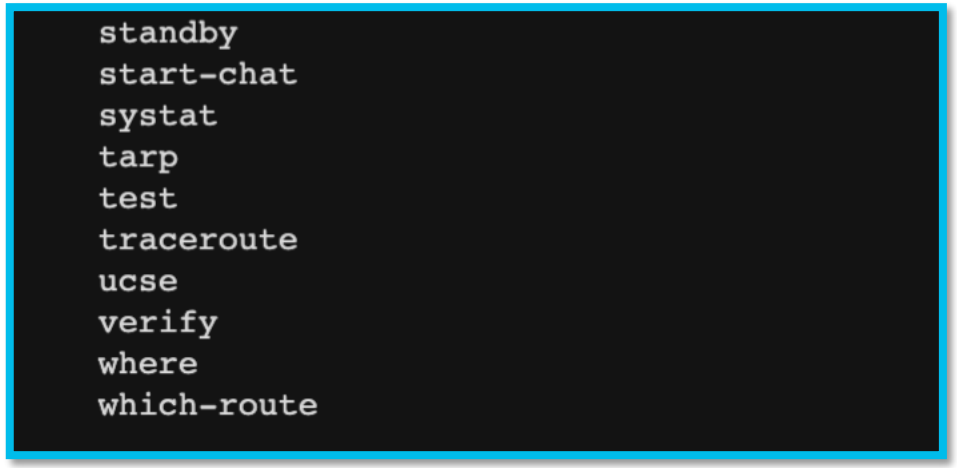


Command Runner

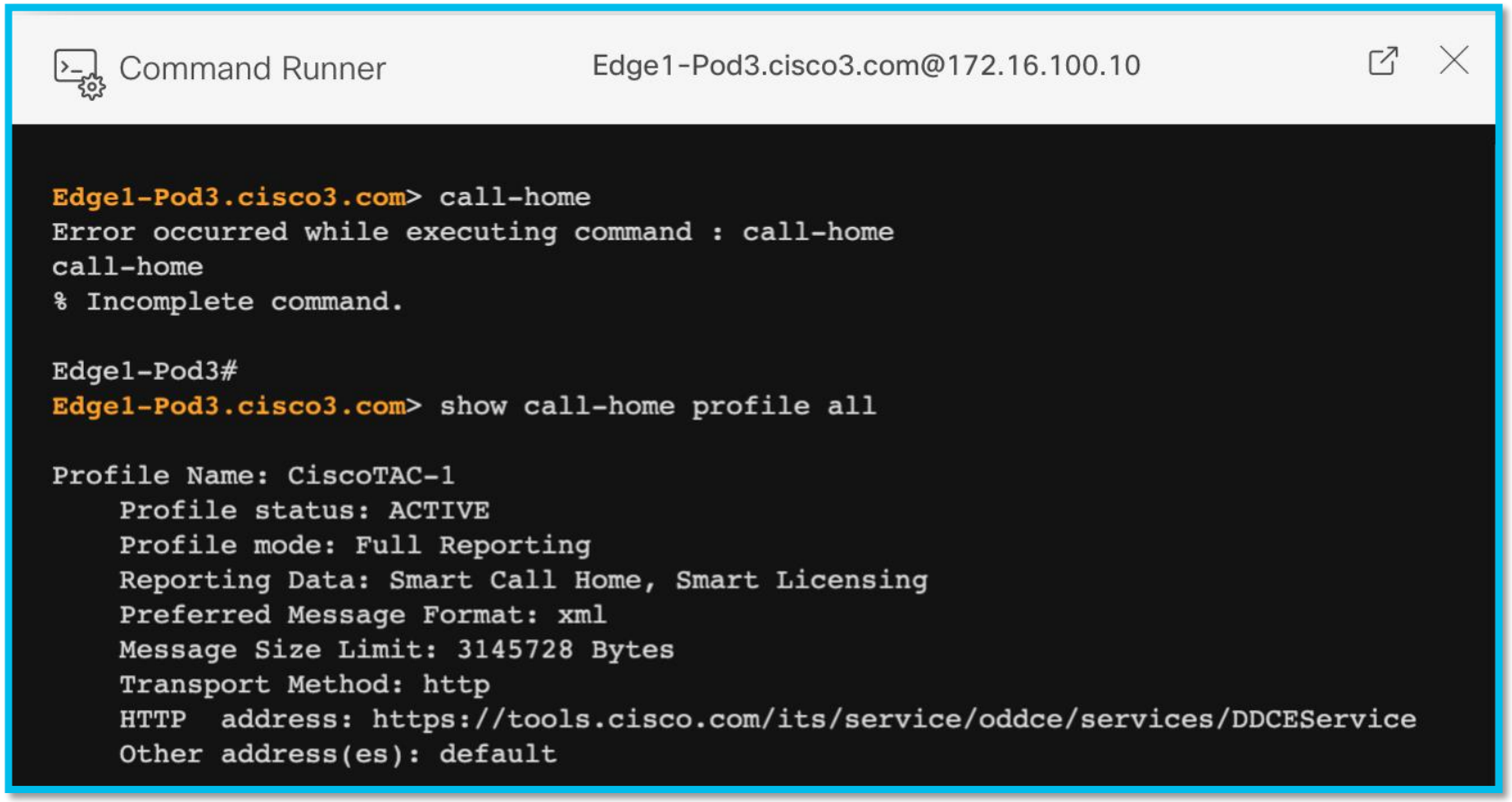


Command Runner

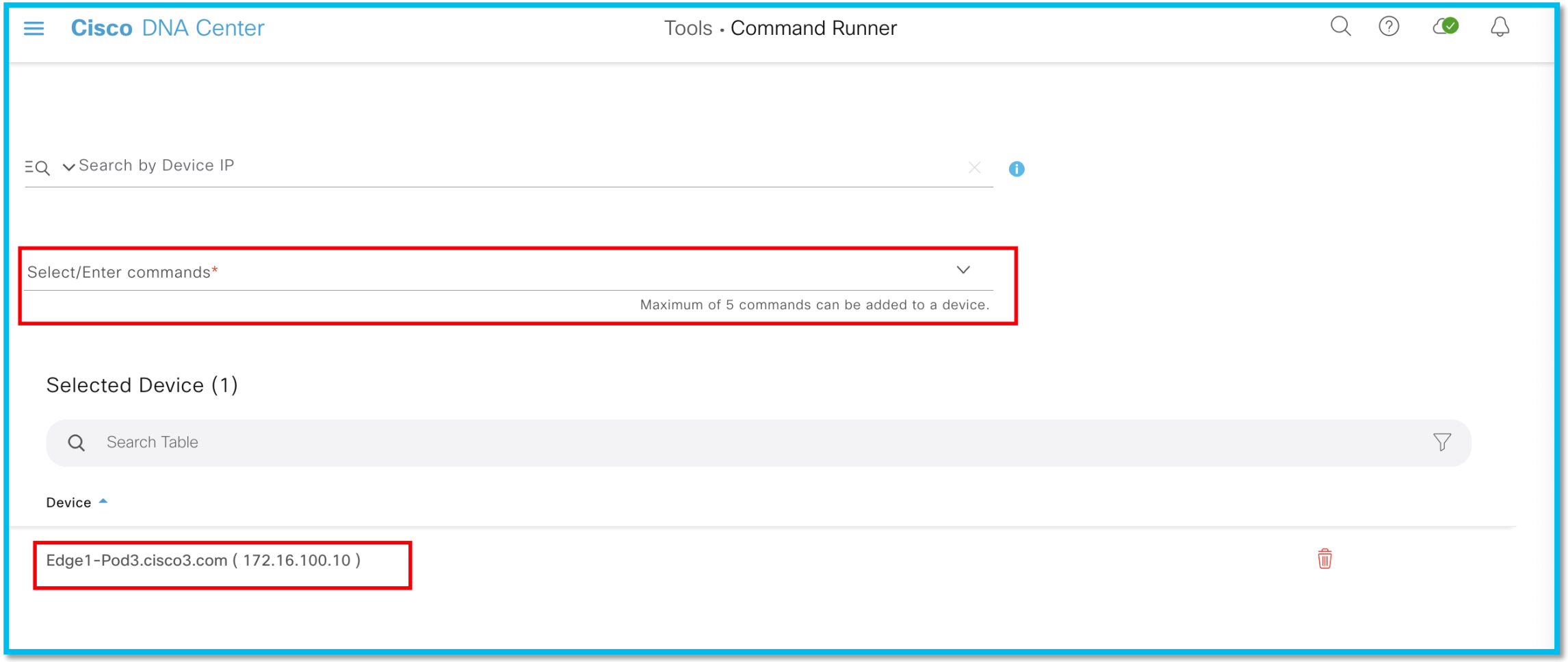




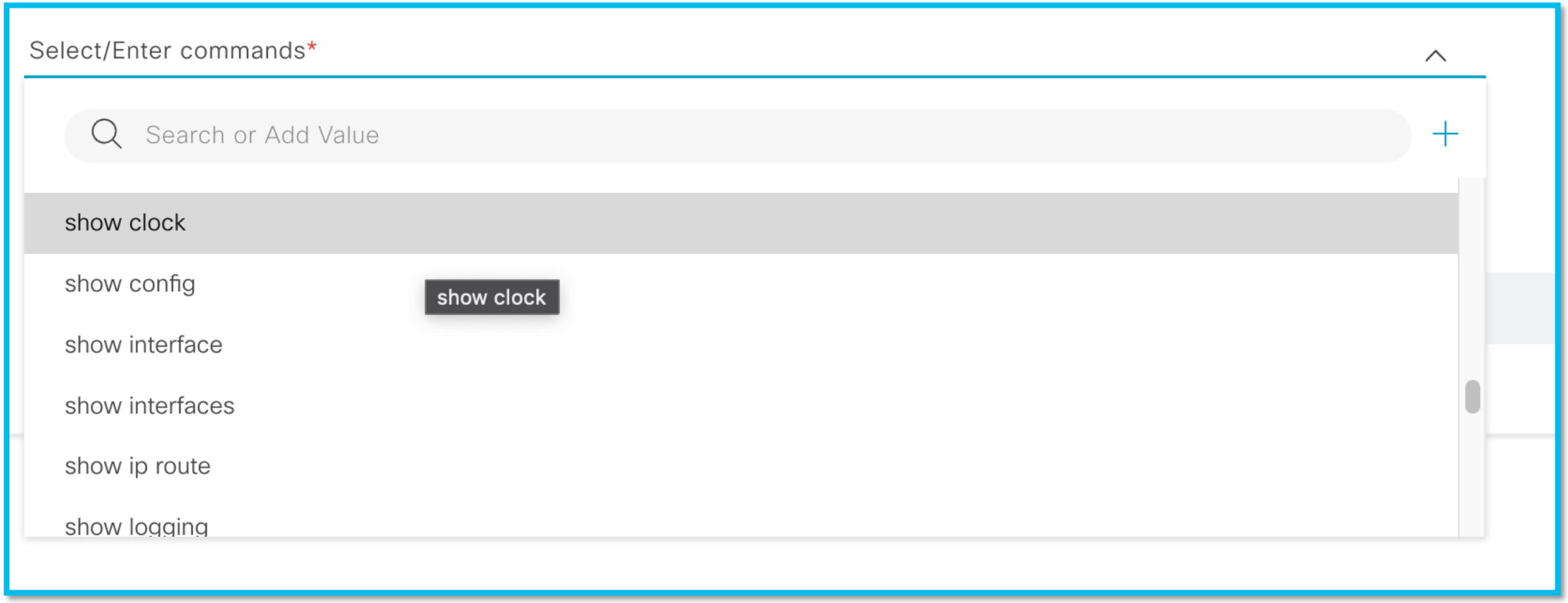
Command Runner



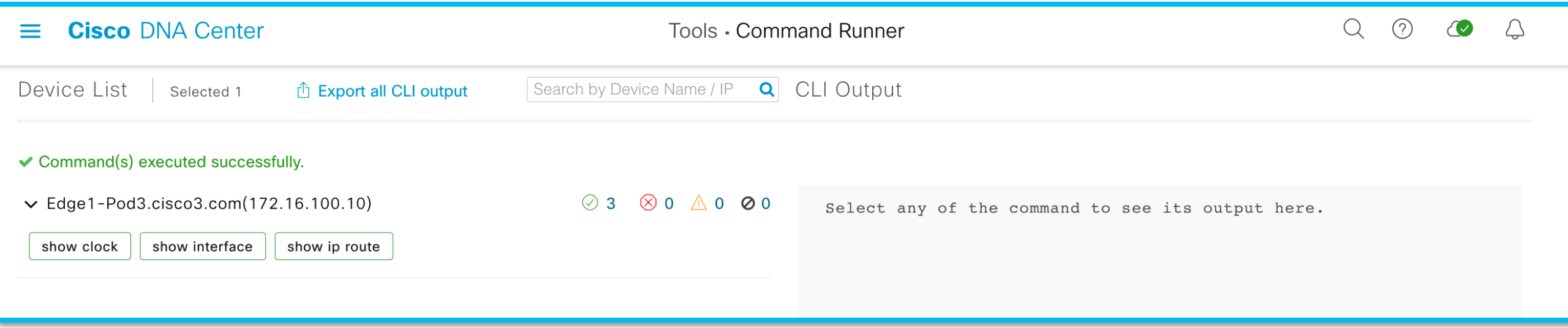
Command Runner

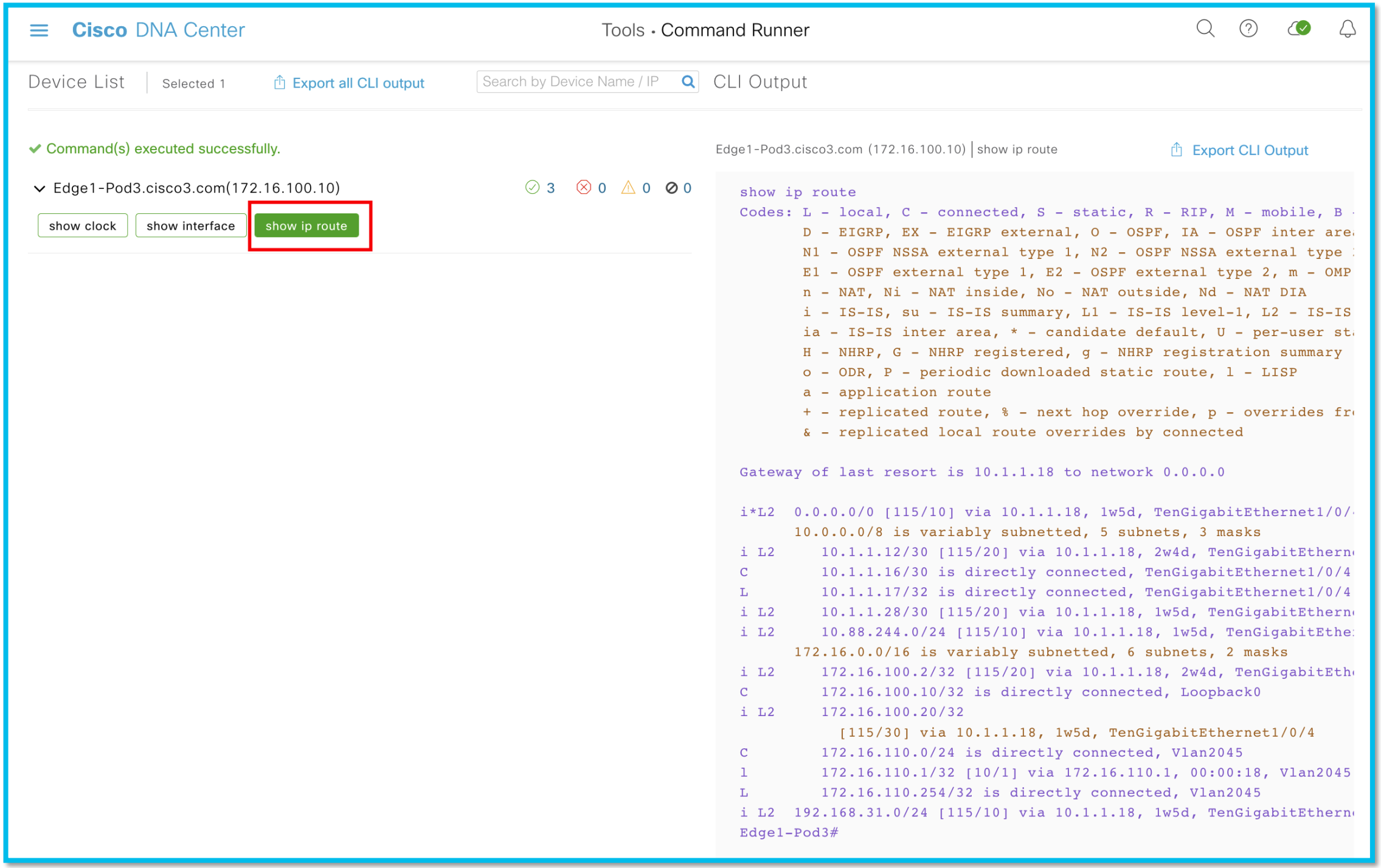


Command Runner

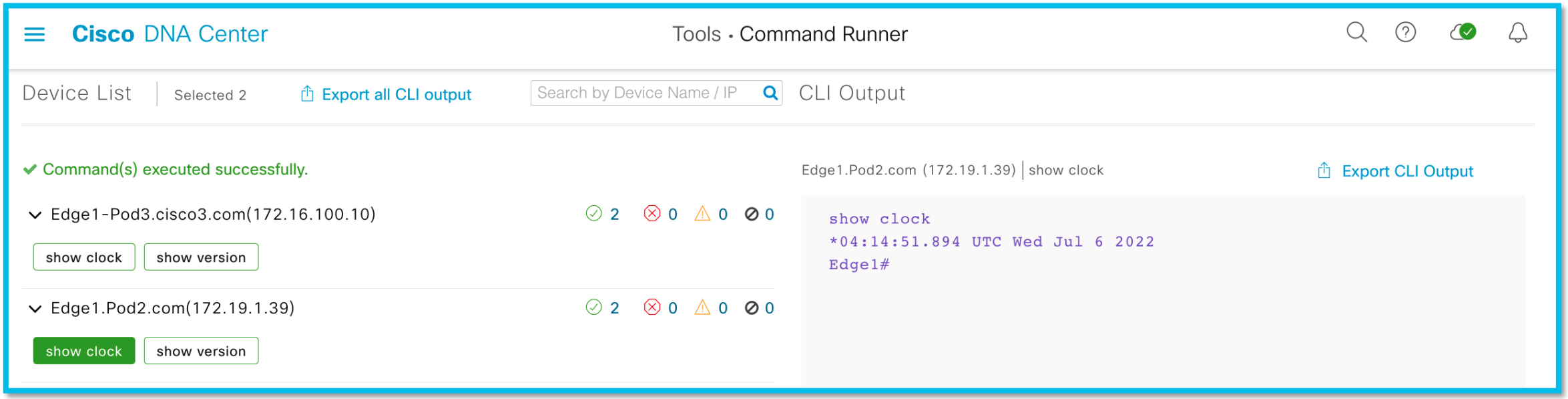


Command Runner




Cisco DNA Center
Tools • Command Runner
Device List
Selected 1
Export all CLI output
Search by Device Name / IP
CLI Output
Command(s) executed successfully.
Edge1-Pod3.cisco3.com(172.16.100.10)
3
0
0
0
show clock
show interface
show ip route
Edge1-Pod3.cisco3.com (172.16.100.10) | show ip route
Export CLI Output
show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter are
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
ia - IS-IS inter area, * - candidate default, U - per-user st
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides fr
& - replicated local route overrides by connected
Gateway of last resort is 10.1.1.18 to network 0.0.0.0
i*L2 0.0.0.0/0 [115/10] via 10.1.1.18, 1w5d, TenGigabitEthernet1/0/
10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
i L2 10.1.1.12/30 [115/20] via 10.1.1.18, 2w4d, TenGigabitEthern
C 10.1.1.16/30 is directly connected, TenGigabitEthernet1/0/4
L 10.1.1.17/32 is directly connected, TenGigabitEthernet1/0/4
i L2 10.1.1.28/30 [115/20] via 10.1.1.18, 1w5d, TenGigabitEthern
i L2 10.88.244.0/24 [115/10] via 10.1.1.18, 1w5d, TenGigabitEthe
172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
i L2 172.16.100.2/32 [115/20] via 10.1.1.18, 2w4d, TenGigabitEth
C 172.16.100.10/32 is directly connected, Loopback0
i L2 172.16.100.20/32
[115/30] via 10.1.1.18, 1w5d, TenGigabitEthernet1/0/4
C 172.16.110.0/24 is directly connected, Vlan2045
l 172.16.110.1/32 [10/1] via 172.16.110.1, 00:00:18, Vlan2045
L 172.16.110.254/32 is directly connected, Vlan2045
i L2 192.168.31.0/24 [115/10] via 10.1.1.18, 1w5d, TenGigabitEthern
Edge1-Pod3#

Command Runner



Demostración

Referencias

- Security Advisories

  Cisco DNA Center User Guide, Release 2.3.5 - Identify Network Security Advisories [Cisco Catalyst Center] - Cisco

- Inventory Insights

  Cisco DNA Center User Guide, Release 2.3.5 - Manage Your Inventory [Cisco Catalyst Center] - Cisco

- Network Reasoner

  Cisco DNA Center User Guide, Release 2.3.5 - Troubleshoot Network Devices Using Network Reasoner [Cisco Catalyst Center] - Cisco

- Issue Settings

  Cisco DNA Assurance User Guide, Release 2.3.5 - View and Manage Issues [Cisco Catalyst Center] - Cisco

- RADKit

Preguntas y respuestas

¿Aún tiene dudas?

Si hizo una pregunta en el panel de preguntas y respuestas o regresa a la comunidad en los días posteriores a nuestro webinar.

¡Nuestras expertas aún pueden ayudarlo!

Participe en el foro Ask Me Anything (AMA) antes del viernes 8 de diciembre de 2023

https://bit.ly/CL4ama-nov23

Haga valer su opinión

Responda a nuestra encuesta para...

- Sugerir nuevos temas
- Calificar a nuestros expertos y el contenido
- Enviar sus comentarios o sugerencias

¡Ayúdenos respondiendo a 5 preguntas de opción múltiple!

Al término de esta sesión, se abrirá una encuesta en su navegador.

Nuestras Redes Sociales

LinkedIn

Cisco Community

Twitter

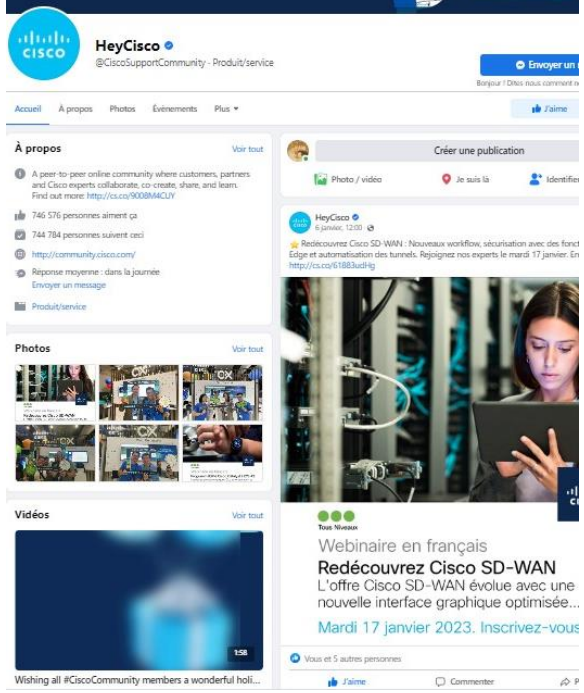
@CiscoCommunity

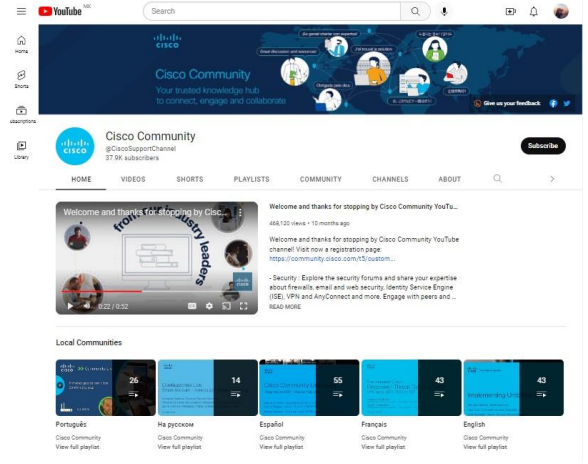
YouTube

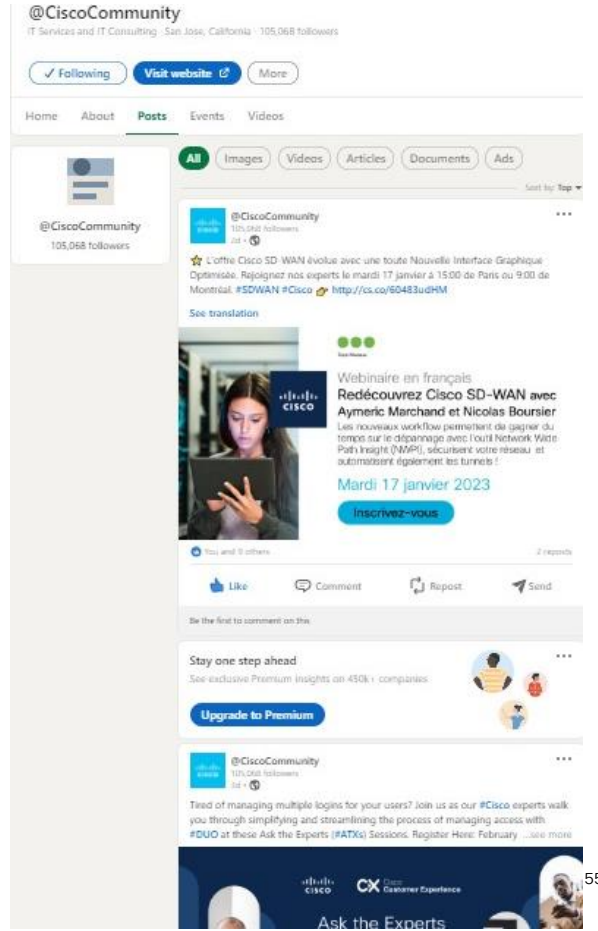
CiscoCommunity

Facebook

CiscoCommunity







The bridge to possible