



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”.

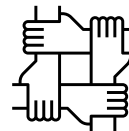
Aceptar como solución

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 ofreciéndonos la oportunidad de ganar premios además de ser una muestra valiosa de ¡nuestro reconocimiento!

o Útil



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](#)



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 Cardaña



Technical Consulting Engineer

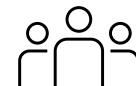
Eduardo es egresado de la Universidad Veracruzana con título en Instrumentación Electrónica, con seis años de experiencia en tecnología Cisco (R&S, Wireless, Collaboration y DNA Center).

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**

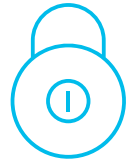


Agenda



1. Tipos de Incidentes

2. Alertas



3. Herramientas de Troubleshooting

4. Automation para Troubleshooting

5. Demostración



Tipos de Incidentes

Tipos de Incidentes

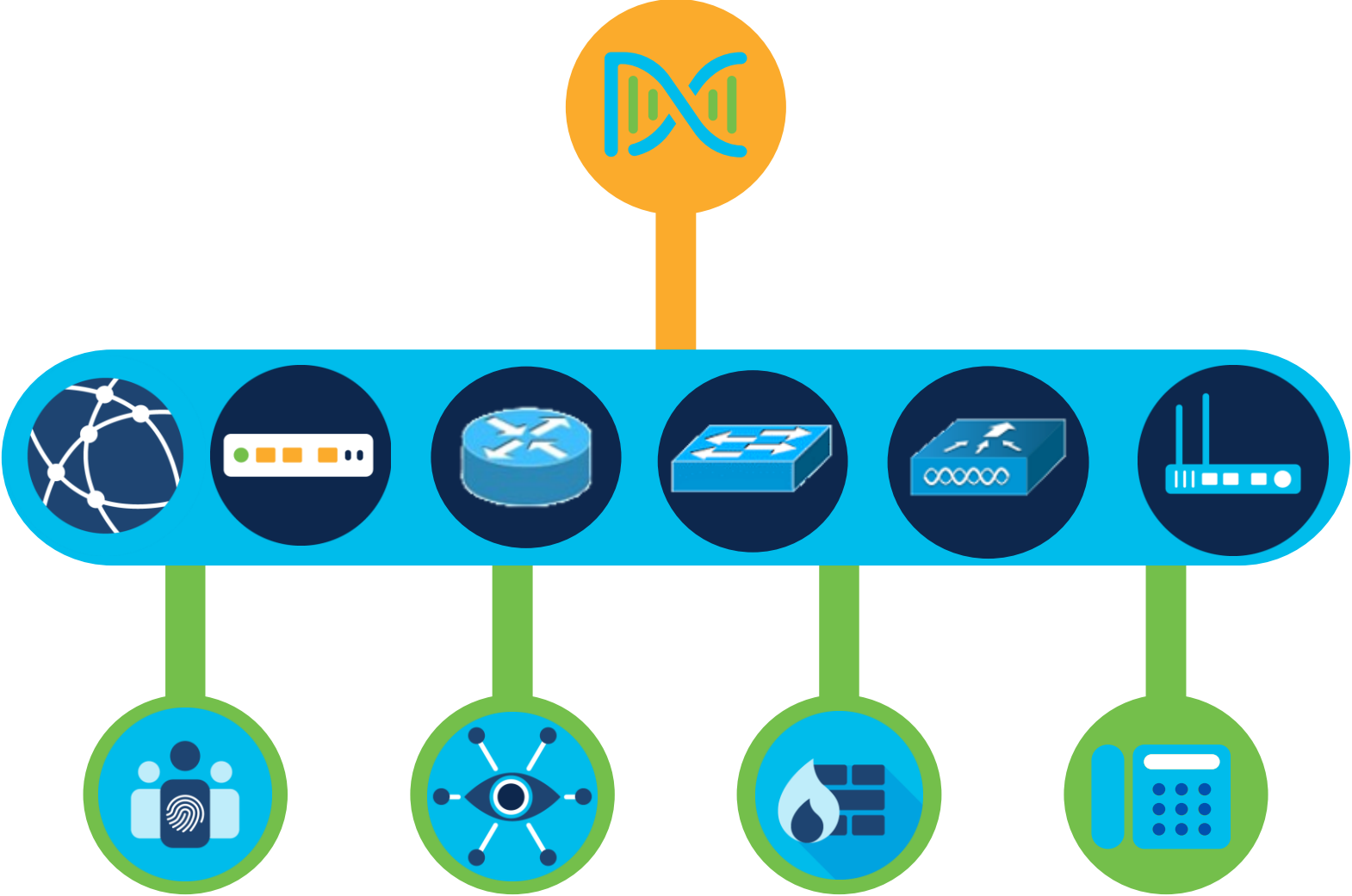
Alertas

Herramientas de
Troubleshooting

Automation para
Troubleshooting

Demostración

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 

Edit Device


 Two (2) Information Alerts on this page. [Expand](#) to see detail. 

Credentials Management IP Resync Interval Role

Type* 

Network Device 

Credentials [Validate](#)

 CLI and SNMP credentials are mandatory. Please ensure authenticity of credentials. In case of invalid credentials, device will go into a collection failure state.

 CLI* 

Select global credential Edit device specific credential

Username*

dnac

Password*

Enable Password

WARNING: Do not use 'admin' as the username for your device CLI credentials, if you are using ISE as your AAA server. If you do, this can result in you not being able to login to your devices.

 SNMP* 

 SNMP RETRIES AND TIMEOUT

 HTTP(S)

 NETCONF 

Protocol

Specify the protocol to use for this device.

SSH2 Telnet

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

- Tipos de Incidentes
- Alertas
- Herramientas de Troubleshooting
- Automation para Troubleshooting
- Demostración

Configuración de Eventos

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

Configurations

Set global settings or across multiple bundles for a custom platform experience.

Event Settings

Event Settings

These event settings are only applicable for the ITSM integration use case. For webhook/other destinations, please click [here](#).

Filter 0 Selected Find

<input type="checkbox"/>	Event Name	Domain	Type	Category	Severity	Workflow	Actions
<input type="checkbox"/>	Access Contract (SGACL) access policy installation failed on the device	Know Your Network	NETWORK	ERROR	2	Incident	Edit
<input type="checkbox"/>	Add device failed	Site Management	NETWORK	TASK_FAILURE	3	Incident	Edit
<input type="checkbox"/>	Add device successful	Site Management	NETWORK	TASK_COMPLETE	4	Incident	Edit
<input type="checkbox"/>	AP Coverage Hole	Know Your Network	NETWORK	WARN	3	Incident	Edit
<input type="checkbox"/>	AP CPU High Utilization	Know Your Network	NETWORK	WARN	3	Incident	Edit
<input type="checkbox"/>	AP disconnected from WLC	Know Your Network	NETWORK	ERROR	2	Incident	Edit
<input type="checkbox"/>	AP Flap	Know Your Network	NETWORK	WARN	3	Incident	Edit
<input type="checkbox"/>	AP License Exhausted on WLC	Know Your Network	NETWORK	WARN	3	Incident	Edit

Configuración de Eventos



<input type="checkbox"/>	Event Name [▲]	Domain	Type	Category	Severity	Workflow	Actions
<input type="checkbox"/>	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

Event Settings



These event settings are only applicable for the ITSM integration use case. For webhook/other destinations, please click [here](#).

 Filter 0 Selected  Find

<input type="checkbox"/>	Event Name ▲	Domain	Type	Category	Severity	Workflow	Actions
<input type="checkbox"/>	AP Reboot Crash	Know Your Network	NETWORK	WARN	3	Incident	Edit

Event Settings

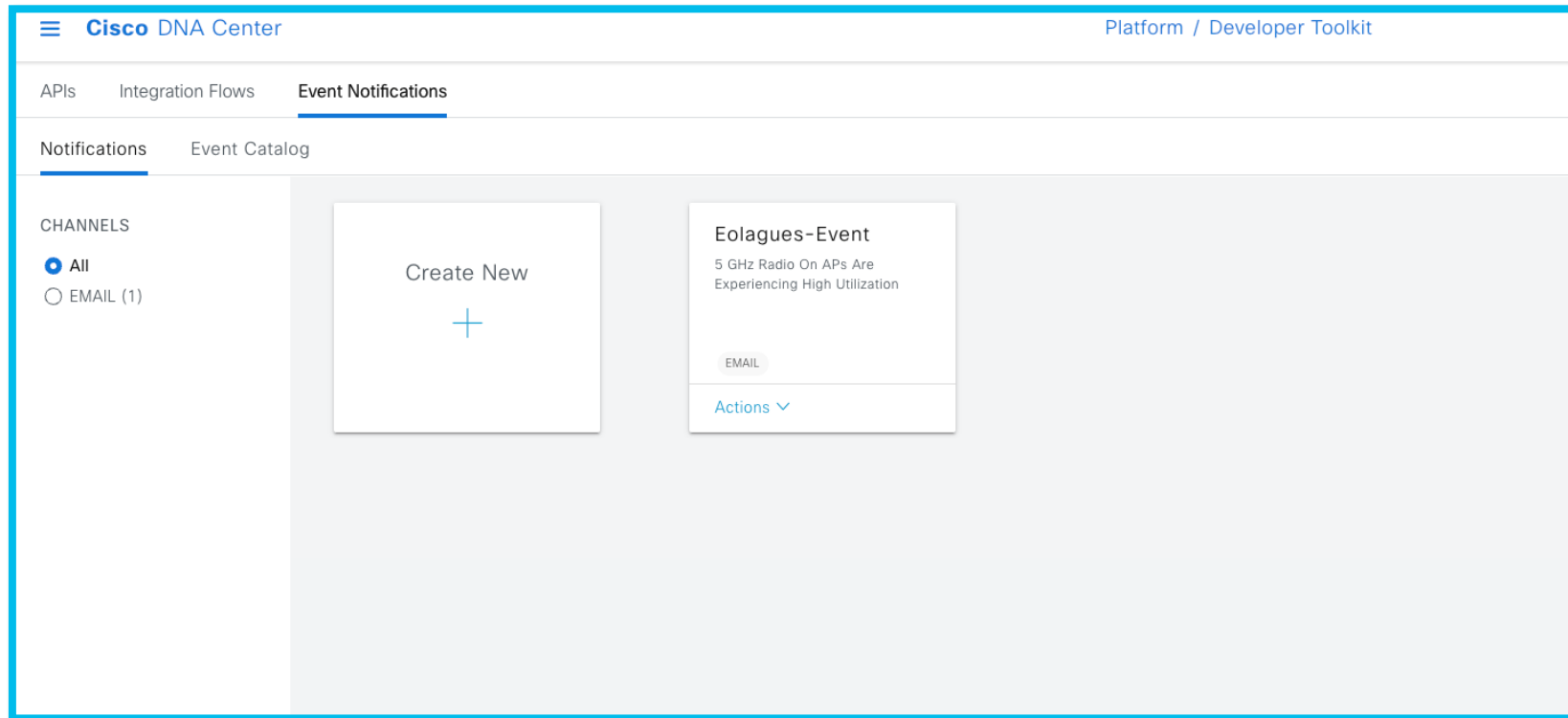
These event settings are only applicable for the ITSM integration use case. For webhook/other destinations, please click [here](#).

 Filter 0 Selected  Find

<input type="checkbox"/>	Event Name ▲	Domain	Type	Category	Severity	Workflow	Actions
<input type="checkbox"/>	AP Reboot Crash	Know Your Network	NETWORK ▼	WARN ▼	3 ▼	Incident ▼	

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.

The screenshot displays the Cisco DNA Center Developer Toolkit interface. On the left, a sidebar shows the 'Events' section with a list of event types, each with a checkbox and a 'Subscribe' link. The 'WLC Reboot Crash' event is selected. The main panel shows the details for this event, including a description, general information, tags, and a model schema. The 'Subscribe' button is highlighted in blue.

Developer Toolkit

APIs Integration Flows Data and Reports Multivendor Support

Events

Subscribe

Event ID	Name
<input type="checkbox"/> NETWORK-DEVICES-2-152	WLC Reboot Crash
<input type="checkbox"/> NETWORK-DEVICES-2-153	WLC Power Supply Failure
<input type="checkbox"/> NETWORK-DEVICES-2-201	Switch Power Failure
<input type="checkbox"/> NETWORK-DEVICES-2-202	Device Reboot Crash
<input type="checkbox"/> NETWORK-DEVICES-2-204	Stack Member Running Incompatib
<input type="checkbox"/> NETWORK-DEVICES-2-205	Switch Fan Failure
<input type="checkbox"/> NETWORK-DEVICES-3-103	AP CPU High Utilization
<input type="checkbox"/> NETWORK-DEVICES-3-104	AP Memory High Utilization

WLC Reboot Crash

Event Details Active Subscriptions

GENERAL INFORMATION

Description: WLC has rebooted due to a hardware or software crash

Event Id	NETWORK-DEVICES-2-152	Version	1.0.0
Namespace	ASSURANCE	Domain	Know Your Network
Sub Domain	Devices	Type	NETWORK
Category	ERROR	Severity	2
Cisco DNA Event link	dna/assurance/issueDetails?issueId=\$instanceId\$		
Note	To programmatically get more info see here - <a href="https://<ip-address>/dna/platform/app/consumer-portal/developer-toolkit/apis?apilid=8684-39bb-4e89-a6e4">https://<ip-address>/dna/platform/app/consumer-portal/developer-toolkit/apis?apilid=8684-39bb-4e89-a6e4		

TAGS

ASSURANCE wlc_reboot_crash_trigger

MODEL SCHEMA

Details REST Schema

```
1 1
2 2
3 3
4 4
```

"Type": "EventSource\$",
"Assurance Issue Priority": "\$priority\$",

Cancel Subscribe

Events - Syslog

Subscribe ×

1 Event selected

SUBSCRIPTION DETAILS

Name*

Subscription Type
SYSLOG

Select an existing instance. Or Click [here](#) to create a new instance.

Subscription Endpoint

SYSLOG CONFIGURATION

Hostname/IP

Port

Protocol

Events – REST API (Webhook)

Subscribe ×

1 Event selected

SUBSCRIPTION DETAILS

Name*

Subscription Type
REST

Select an existing instance. Or Click [here](#) to create a new instance.

Subscription Endpoint

URL

Trust Certificate
 Yes No

HTTP Method

Authentication
 Basic Token No Auth

Events - Email

Subscribe

1 Event selected

SUBSCRIPTION DETAILS

Name*

Subscription Type
EMAIL

Select an existing endpoint Create a new endpoint

Subscription Endpoint

> SMTP Configuration

∨ Email Recipients

From*

To*

Cancel **Subscribe**

Events

The screenshot displays the Cisco DNA Center interface for Event Notifications. The main area shows a 'Create New' button and a notification card for 'Eolagues-Event' with a description '5 GHz Radio On APs Are Experiencing High Utilization'. The card includes an 'EMAIL' channel and an 'Actions' dropdown. A 'Notification Details' modal is open on the right, showing the notification's name, description, sites (Global), and a list of events including 'Radio High Utilization (5GHz)'. The modal also displays the email configuration: From: dnac6@cisco.com, To: eolagues@cisco.com, and Subject: Radio High Utilization (5GHz). The notification is currently enabled.

Cisco DNA Center Platform / Developer Toolkit

APIs Integration Flows **Event Notifications**

Notifications Event Catalog

CHANNELS

- All
- EMAIL (1)

Create New

Eolagues-Event
5 GHz Radio On APs Are Experiencing High Utilization

EMAIL

Actions

Notification Details

Enabled

Name
eolagues-event

Description
5 GHz radio on APs are experiencing high utilization

Sites
Global x

Events (1)
Radio High Utilization (5GHz)

EMAIL

From
dnac6@cisco.com

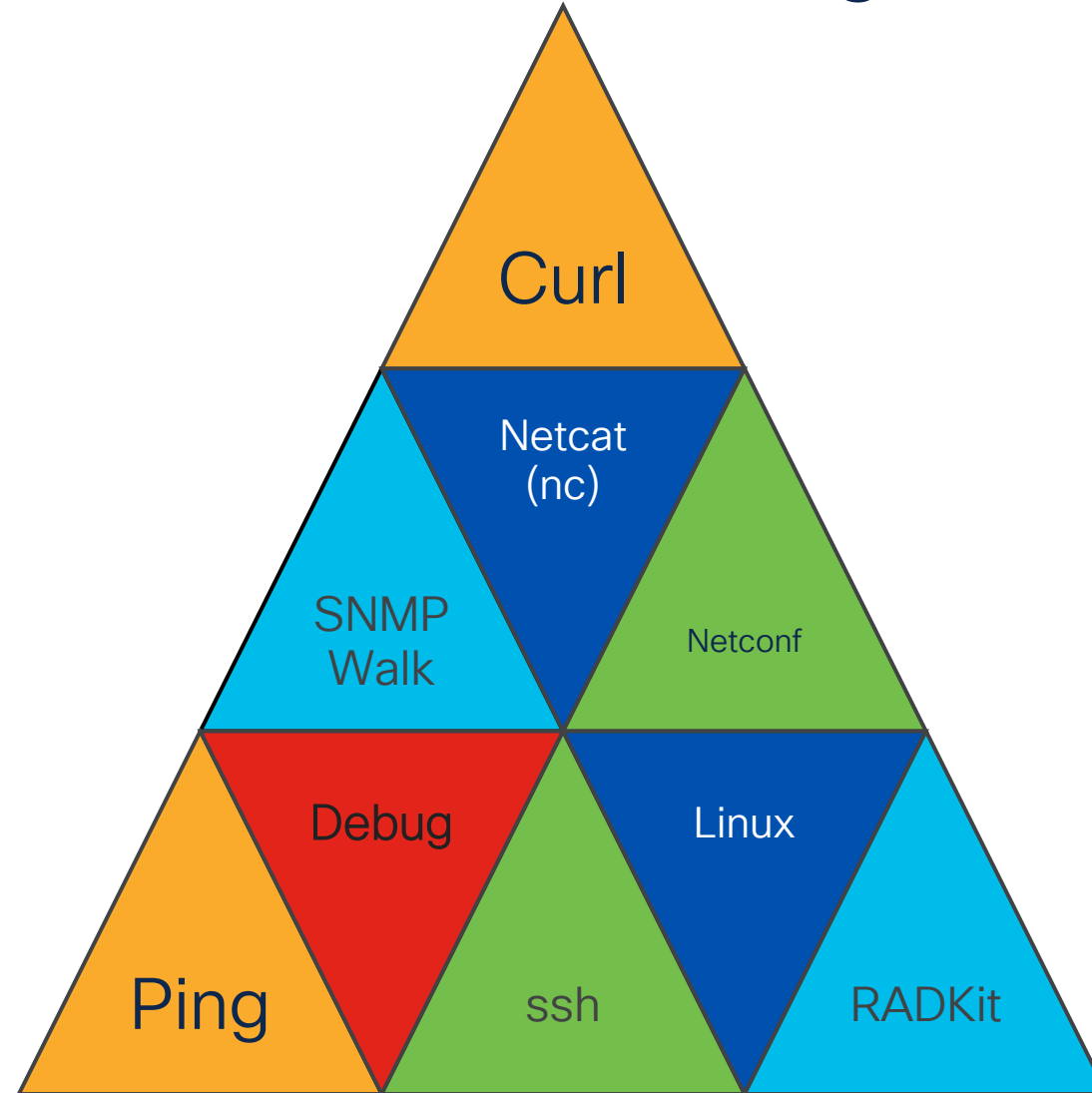
To
eolagues@cisco.com

Subject
Radio High Utilization (5GHz)

- Tipos de Incidentes
- Alertas
- Herramientas de Troubleshooting
- Automation para Troubleshooting
- Demostración

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.

IP Address	Device Family	Reachability ⓘ	Manageability ⓘ
iac-mxc.com ⓘ 10.62.149.155	Switches and Hubs (WLC Capable)	▲ Ping Reachable	▲ Managed SNMP Authenti...

Reason and Suggested Actions ×

SNMP Authentication Failure : NCIM12001: Device was not successfully authenticated via SNMP credentials. However, device is ping reachable. Either the mandatory protocol credentials are not correctly provided to Cisco DNA Center or the device is responding slow and exceeding the set timeout value. User can also run discovery again only for this device with correct credentials using the discovery feature.

Impacted Applications

ALL

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: Unknown 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)



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

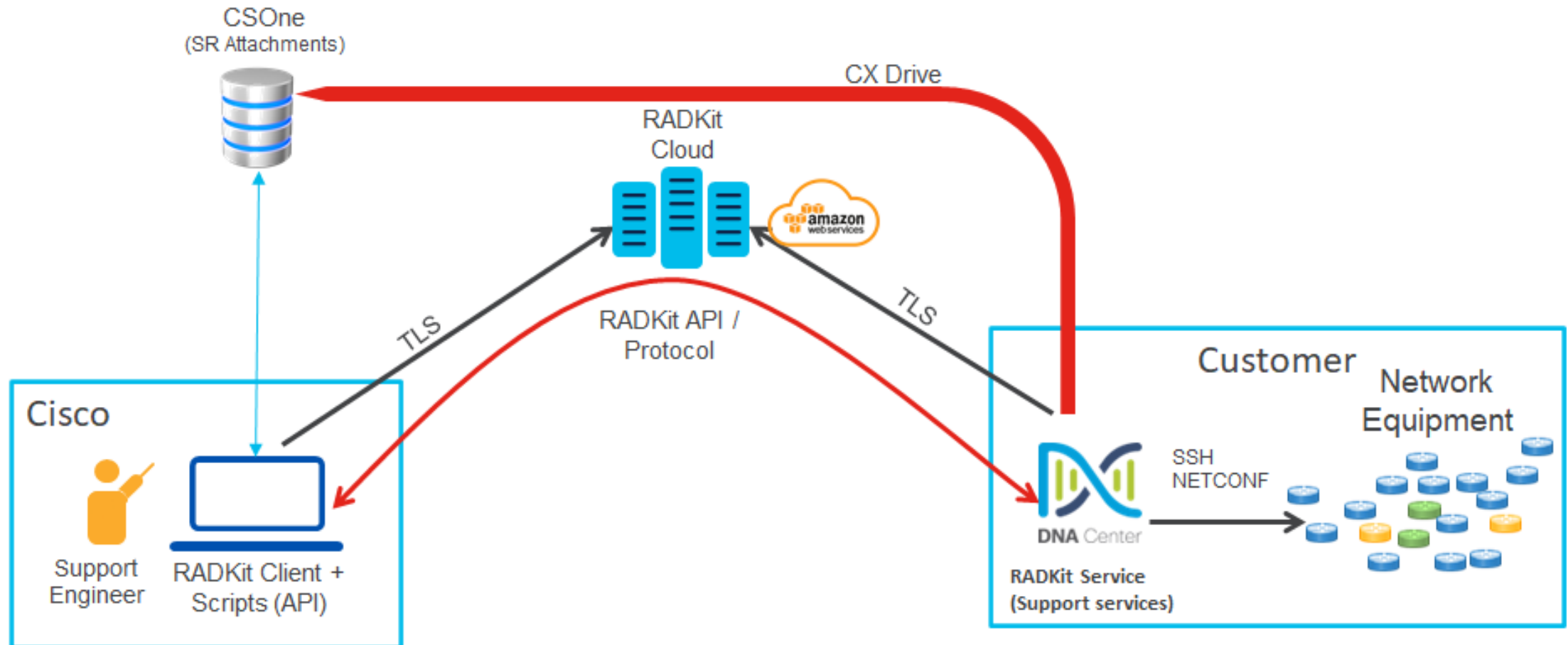


RADKit en Cisco DNA Center

- 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 Architecture – Service in 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

- Tipos de Incidentes
- Alertas
- Herramientas de Troubleshooting
- Automation para Troubleshooting
- Demostración

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.



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%

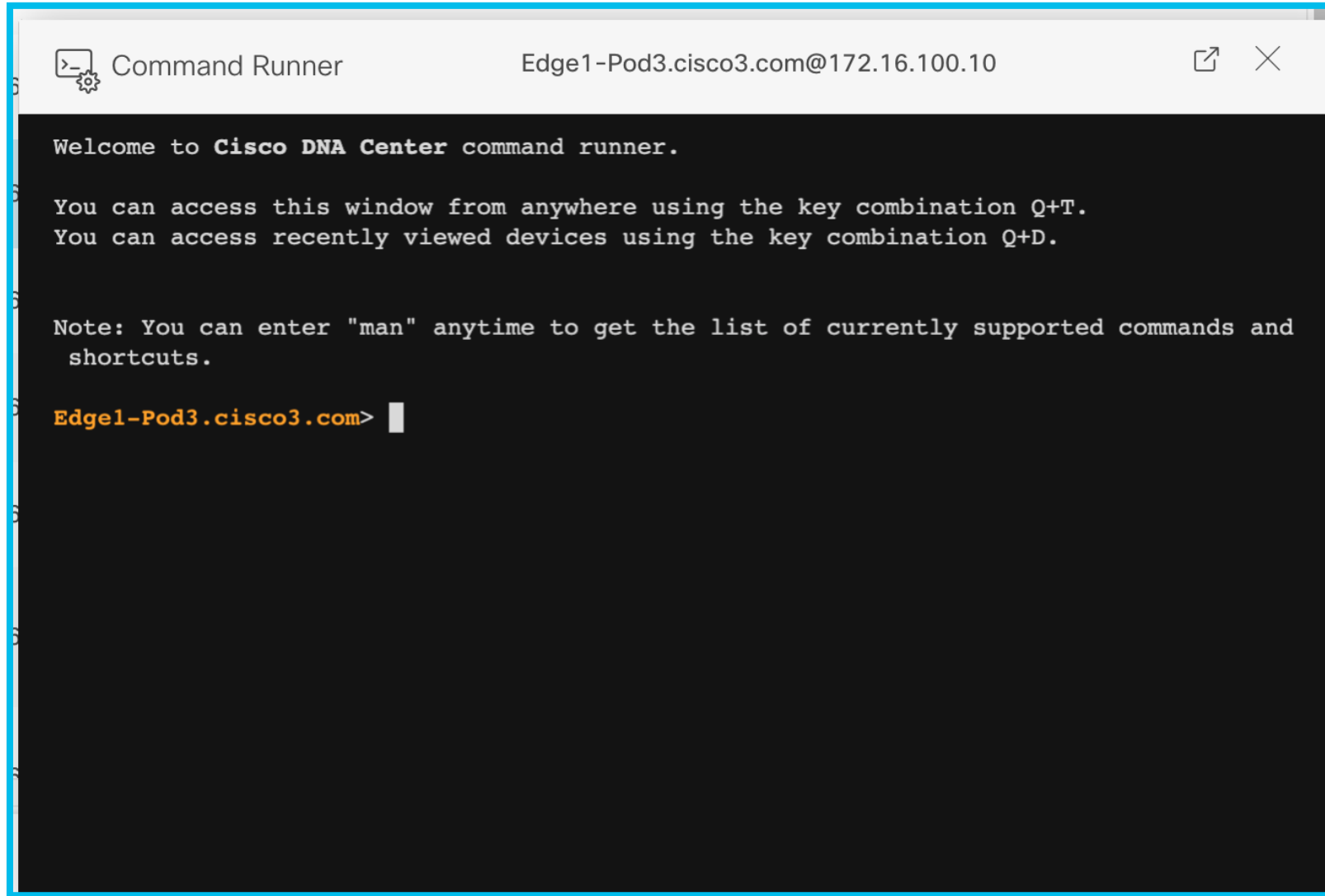
Command Runner

Command Runner

The screenshot displays the Cisco DNA Center interface for the Inventory section. The 'Inventory' tab is selected in the top navigation bar. A search bar is present at the top left. The main content area shows a list of devices with columns for Device Name, IP Address, and various status indicators. A red box highlights the 'Inventory' tab. Another red box highlights the 'Actions' menu, which is open and shows options like 'Inventory', 'Software Image', 'Provision', 'Telemetry', 'Device Replacement', 'Others', and 'Compliance'. The 'Others' option is selected, and a sub-menu is open showing 'Run Commands' and 'Command Runner', both highlighted with red boxes. A red arrow points from the 'Inventory' tab to the 'Command Runner' option. The table below shows a list of devices with their respective status and roles.

Device Name	IP Address	Device Role	Reachability	Manageability	Compliance	Health Score	Site
4500SW.Pod2.com	172.1	DISTRIBUTION	Unreachable	Managed Device Unreac...	Compliant	NA	.../Mexico/San Angel
AP5CE1.7629.0928	10.31	ACCESS	Unreachable	Managed Could Not Syn...	N/A	NA	Assign
AP6C71.0DF4.2910	172.1	ACCESS	Unreachable	Managed Not Syn...	N/A	NA	Assign
AP7872.5d60.67a4	172.1	ACCESS	Unreachable	Managed Could Not Syn...	N/A	NA	Assign
AP7872.5d60.92e0	172.16.110.1	ACCESS	Unreachable	Managed Could Not Syn...	N/A	NA	.../Insurgentes/Floor17
AP7872.5df3.9038	172.16.110.2	ACCESS	Unreachable	Managed Could Not Syn...	N/A	NA	.../Insurgentes/Floor17
AP-San-Angel1	172.19.5.3	ACCESS	Reachable	Managed	N/A	NA	.../San Angel/Floor A
AP-San-Angel2	172.19.5.6	ACCESS	Reachable	Managed	N/A	NA	.../San Angel/Floor A
AP-San-Angel3	172.19.5.5	ACCESS	Reachable	Managed	N/A	NA	.../San Angel/Floor A
Border1_MXC10	172.17.250.3	ACCESS	Reachable	Managed CLI Authentica...	Compliant	10	.../Mexico/Reforma
Border1-CN.Pod8.com	172.30.1.65	DISTRIBUTION	Reachable	Managed	Error	8	.../Oeiras - 3/Floor1
Border1-Pod3.cisco.com	172.16.100.1	DISTRIBUTION	Unreachable	Managed Device Unreac...	Non-Compliant	NA	.../Mexico/Insurgentes

Command Runner



```
Command Runner Edge1-Pod3.cisco3.com@172.16.100.10
```

Welcome to **Cisco DNA Center** command runner.

You can access this window from anywhere using the key combination Q+T.
You can access recently viewed devices using the key combination Q+D.

Note: You can enter "man" anytime to get the list of currently supported commands and shortcuts.

Edge1-Pod3.cisco3.com> █

Command Runner

```
Command Runner Edge1-Pod3.cisco3.com@172.16.100.1

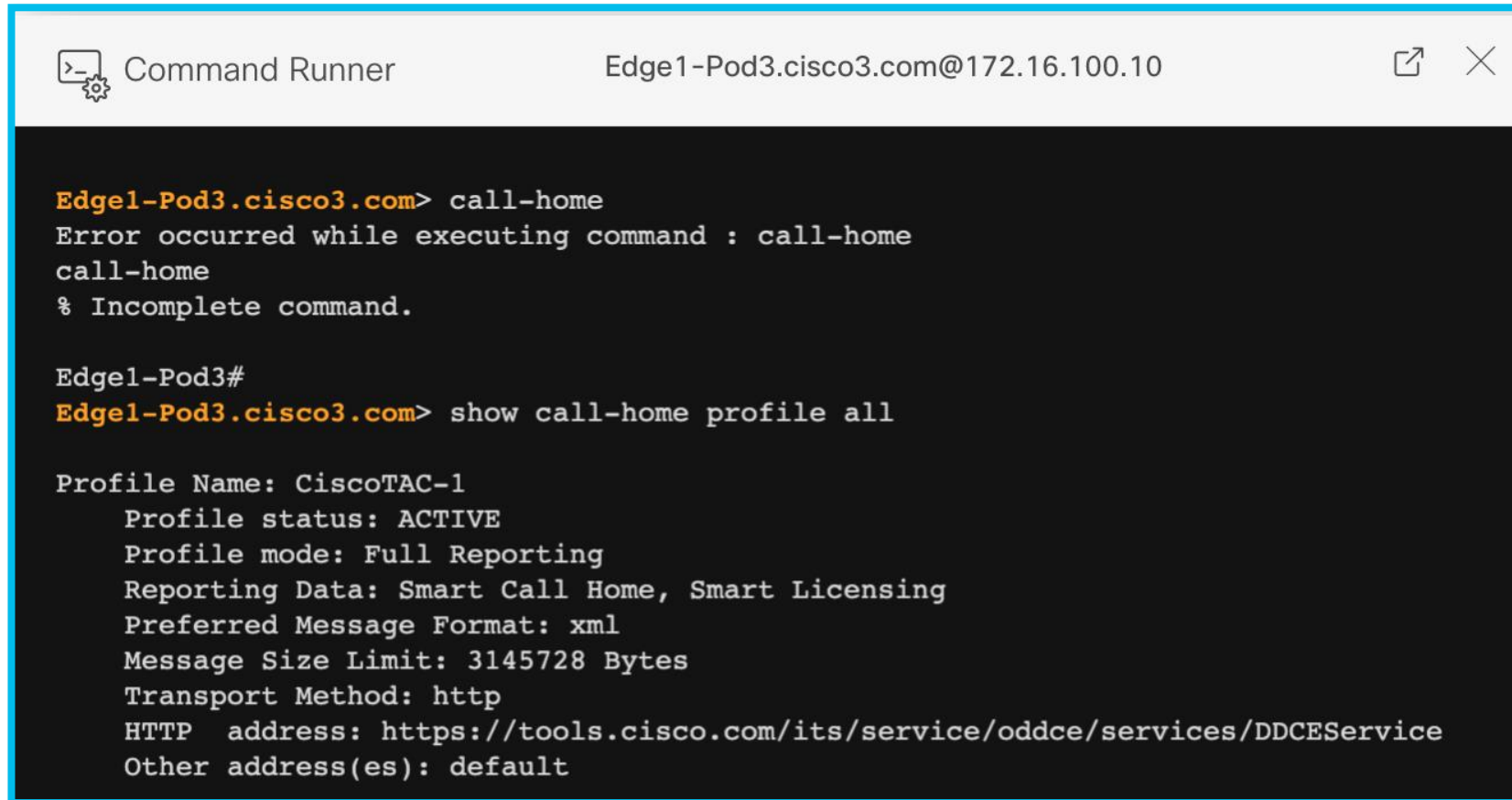
Edge1-Pod3.cisco3.com> man
This lists the commands currently supported by command runner:
man ---- Get the list of currently supported commands

quit ---- Exit from the device mode of terminal

call-home
cd
cping
crypto
dir
eping
grep
help
mediatrace
monitor
more
mping
mstat
ping
pwd
sdlc
show
sh
```

```
standby
start-chat
systat
tarp
test
traceroute
ucse
verify
where
which-route
```

Command Runner



```
Command Runner Edge1-Pod3.cisco3.com@172.16.100.10
```

```
Edge1-Pod3.cisco3.com> call-home
Error occurred while executing command : call-home
call-home
% Incomplete command.

Edge1-Pod3#
Edge1-Pod3.cisco3.com> show call-home profile all

Profile Name: CiscoTAC-1
  Profile status: ACTIVE
  Profile mode: Full Reporting
  Reporting Data: Smart Call Home, Smart Licensing
  Preferred Message Format: xml
  Message Size Limit: 3145728 Bytes
  Transport Method: http
  HTTP address: https://tools.cisco.com/its/service/oddce/services/DDCEService
  Other address(es): default
```

Command Runner

Cisco DNA Center Tools · Command Runner

Search by Device IP

Select/Enter commands*
Maximum of 5 commands can be added to a device.

Selected Device (1)

Search Table

Device

Edge1-Pod3.cisco3.com (172.16.100.10)	
---	--

Command Runner

Select/Enter commands*

Search or Add Value

- show clock
- show config
- show interface
- show interfaces
- show ip route
- show logging

show clock

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

Select any of the command to see its output here.

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 sta.  
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  
Edgel-Pod3#
```

Command Runner

Cisco DNA Center Tools - Command Runner

Device List | Selected 2 | [Export all CLI output](#) | Search by Device Name / IP | CLI Output

✓ Command(s) executed successfully.

Edge1.Pod2.com (172.19.1.39) | show clock | [Export CLI Output](#)

Edge1-Pod3.cisco3.com(172.16.100.10)	✓ 2	✗ 0	⚠ 0	🚫 0	<code>show clock</code>	<code>show version</code>
Edge1.Pod2.com(172.19.1.39)	✓ 2	✗ 0	⚠ 0	🚫 0	<code>show clock</code>	<code>show version</code>

```
show clock
*04:14:51.894 UTC Wed Jul 6 2022
Edge1#
```

Demostración

- Tipos de Incidentes
- Alertas
- Herramientas de Troubleshooting
- Automation para Troubleshooting
- 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

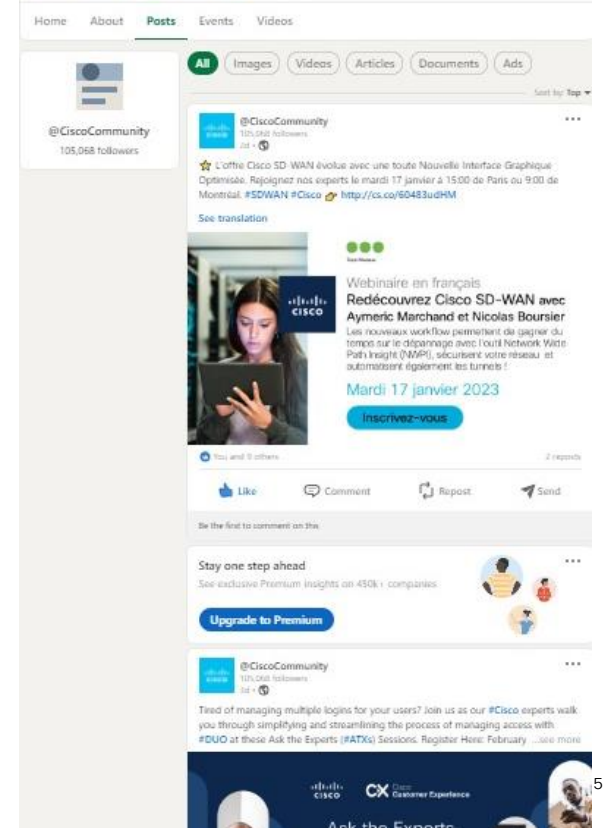
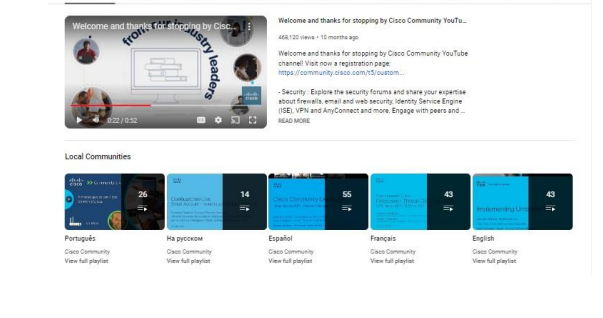
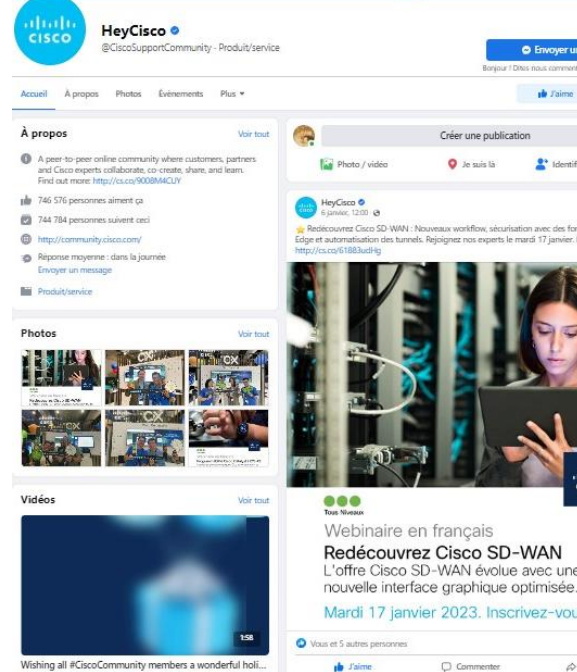
[@CiscoCommunity](#)

YouTube

[CiscoCommunity](#)

Facebook

[CiscoCommunity](#)





The bridge to possible