Guía de preguntas frecuentes y resolución de problemas de CX Cloud Agent

Contenido

Introducción

Implementación

- P. ¿Es la redirección de URL tocloudfront.net un comportamiento esperadoal conectarse al dominio back-end de la nube de CX?
- P. Con la opción "Reinstalar", ¿puede el usuario implementar el nuevo agente en la nube CX con una nueva dirección IP?
- P. ¿Qué formatos de archivo están disponibles para la instalación?
- P. ¿En qué entorno se puede implementar el instalador?
- P. ¿Puede CX Cloud Agent detectar una dirección IP en un entorno DHCP?
- P. ¿Es el agente en la nube de CX compatible con la configuración de IPv4 e IPv6?
- P. Durante la configuración de IP, ¿se valida la dirección IP?
- P. ¿Cuánto tarda la implementación de OVA y la configuración IP?
- P. ¿Hay alguna limitación con respecto a cualquier tipo de hardware?
- P. ¿Se puede generar el código de emparejamiento en cualquier momento?
- P. ¿Cuáles son los requisitos de ancho de banda entre Cisco Catalyst Centers (para un máximo de 10 clústeres o 20 no clústeres) y CX Cloud Agent?
- P. ¿Cómo se puede acceder a los syslogs del agente para supervisar la máquina virtual (VM) del agente en la nube CX?

Versiones y parches

- P. ¿Cuáles son los diferentes tipos de versiones que aparecen en la lista para la actualización de CX Cloud Agent?
- P. ¿Dónde se encuentra la última versión de CX Cloud Agent y cómo actualizar la versión existente de CX Cloud Agent?

Autenticación y configuración de proxy

- P. ¿Cuál es el usuario predeterminado de la aplicación CX Cloud Agent?
- P. ¿Cómo se establece la contraseña para el usuario predeterminado?
- P. ¿Hay alguna opción disponible para restablecer la contraseña después del día 0?
- P. ¿Cuáles son las políticas de contraseñas para configurar CX Cloud Agent?
- P. ¿Cómo confirmo la disponibilidad de Secure Shell (SSH) para un dispositivo desde CX Cloud Agent?
- P. ¿Cómo confirmo la disponibilidad de SNMP a un dispositivo desde CX Cloud Agent?
- P. ¿Cómo configuro la contraseña de Grub?
- P. ¿Cuál es el período de caducidad de la contraseña de xcadminpassword?
- P. ¿Desactiva el sistema la cuenta después de intentos consecutivos de inicio de sesión fallidos?
- P. ¿Cómo se genera una frase de paso?
- P. ¿Admite el host proxy tanto el nombre de host como la IP?

SSH de Secure Shell

- Q. ¿Qué cifrados son soportados por el shell ssh?
- P. ¿Cómo inicio sesión en la consola?

P. ¿Están registrados los logins SSH?

P. ¿Cuál es el tiempo de espera de la sesión inactiva?

Puertos y servicios

P. ¿Qué puertos se mantienen abiertos en el agente en la nube de CX?

Conexión del agente en la nube CX con Cisco Catalyst Center y otros recursos

P. ¿Cuál es el propósito y la relación de Cisco Catalyst Center con CX Cloud Agent?

P. ¿Dónde pueden los usuarios proporcionar detalles de Cisco Catalyst Center sobre el agente en la nube CX?

P. ¿Cuántos Cisco Catalyst Centers se pueden agregar?

P. ¿Cómo elimino un Cisco Catalyst Center conectado de CX Cloud Agent?

P. ¿Qué función puede desempeñar el usuario de Cisco Catalyst Center?

P. ¿Cómo se reflejan las modificaciones en el agente en la nube de CX debido a los cambios en las credenciales conectadas de Cisco Catalyst Center?

P. ¿Cómo se almacenan los datos de Cisco Catalyst Center y los recursos de archivos simiente en CX Cloud Agent?

P. ¿Existe alguna limitación a la hora de introducir rangos de IP al añadir otros recursos?

P. ¿Se puede utilizar una subred pública para la implementación de CX Cloud Agent v2.4 para la subred personalizada de servicios y el clúster?

P. ¿Con qué frecuencia se puede iniciar la operación de redescubrimiento?

P. ¿Cuál es el flujo de trabajo para agregar "Otros activos como origen de datos" al cargar un archivo simiente?

P. ¿Qué tipo de cifrado se utiliza al acceder a la API de Cisco Catalyst Center desde el agente en la nube CX?

P. ¿Qué operaciones realiza CX Cloud Agent en el Cisco Catalyst Center Cloud Agent integrado?

P. ¿Qué datos predeterminados se recopilan de Cisco Catalyst Center y se cargan en el back-end?

P. ¿Qué datos adicionales se recopilan de Cisco Catalyst Center y se cargan en el back-end de Cisco?

P. ¿Cómo se cargan los datos de inventario en el backend?

P. ¿Cuál es la frecuencia de carga del inventario?

P. ¿Puede el usuario volver a programar el inventario?

P. ¿Cuándo se produce el tiempo de espera de conexión entre Cisco Catalyst Center y Cloud Agent?

Análisis de diagnóstico de CX Cloud Agent utilizado

P. ¿Qué comandos de escaneo se ejecutan en el dispositivo?

P. ¿Dónde se almacenan y se perfilan los resultados del análisis?

P. ¿Los duplicados (por nombre de host o IP) en Cisco Catalyst Center se agregan al Análisis de diagnóstico cuando el origen de Cisco Catalyst Center está conectado?

P. ¿Qué sucede cuando falla uno de los escaneos de comando?

P. ¿Qué sucede cuando se superponen varios escaneos?

Registros del sistema de agentes en la nube CX

P. ¿Qué información de estado se envía al portal de la nube de CX?

P. ¿Qué detalles del sistema y del hardware se recopilan?

P. ¿Cómo se envían los datos de salud al backend?

P. ¿Cuál es la política de retención de registros de datos de estado del agente en la nube de CX en el backend?

P. ¿Qué tipos de cargas están disponibles?

Resolución de problemas

Respuestas de fallos de recopilación

Respuestas de error de análisis de diagnóstico

Introducción

Este documento incluye preguntas frecuentes y situaciones de solución de problemas que los usuarios pueden encontrar mientras trabajan con el agente en la nube CX.

Implementación

P. ¿Es la redirección de URL a cloudfront.net un comportamiento esperado al conectarse al dominio back-end de la nube CX?

A. Sí, para algunos escenarios de implementación específicos, la redirección a cloudfront.net se espera. Ose debe permitir el acceso sin enlazar con la redirección habilitada en el puerto 443 para estos FQDN.

P. Con la opción "Reinstalar", ¿puede el usuario implementar el nuevo agente en la nube CX con una nueva dirección IP?

A. Sí

P. ¿Qué formatos de archivo están disponibles para la instalación?

A. OVA y VHD

P. ¿En qué entorno se puede implementar el instalador?

A. Para OVA

- VMWare ESXi versión 5.5 o posterior
- Oracle Virtual Box 5.2.30 o posterior

Para VHD

- Windows Hypervisor 2012 a 2016

P. ¿Puede CX Cloud Agent detectar una dirección IP en un entorno DHCP?

R. Sí, se detecta la asignación de dirección IP durante la configuración IP. Sin embargo, no se admite el cambio de dirección IP que se espera para el agente en la nube de CX en el futuro. Se recomienda que los clientes reserven la IP para el agente en la nube CX en su entorno DHCP.

P. ¿Es el agente en la nube de CX compatible con la configuración de IPv4 e IPv6?

R. No, sólo se admite IPV4.

P. Durante la configuración de IP, ¿se valida la dirección IP?

R. Sí, se validan la sintaxis de la dirección IP y la asignación de dirección IP duplicada.

P. ¿Cuánto tarda la implementación de OVA y la configuración IP?

R.La implementación de OVA depende de la velocidad de la red que copia los datos. La configuración IP tarda aproximadamente de 8 a 10 minutos, incluidas las creaciones de contenedores y Kubernetes.

P. ¿Hay alguna limitación con respecto a cualquier tipo de hardware?

R. La máquina host en la que se implementa OVA debe cumplir los requisitos proporcionados como parte de la configuración del portal CX. El agente en la nube CX se prueba con VMware/Virtual Box en un hardware con procesadores Intel Xeon E5 con una relación vCPU/CPU de 2:1. Si se utiliza una CPU de procesador menos potente o una proporción mayor, el rendimiento puede disminuir.

P. ¿Puede generarse el código de emparejamiento en cualquier momento?

R. No, el código de emparejamiento solo se puede generar cuando el agente en la nube CX no está registrado.

P. ¿Cuáles son los requisitos de ancho de banda entre Cisco Catalyst Centers (para un máximo de 10 clústeres o 20 no clústeres) y CX Cloud Agent?

R.El ancho de banda no supone una limitación cuando el agente en la nube CX y Cisco Catalyst Center se encuentran en la misma red LAN/WAN en el entorno del cliente. El ancho de banda de red mínimo requerido es de 2,7 Mbit/seg. para las colecciones de inventario de 5000 dispositivos +13000 Puntos de acceso para una conexión de agente a Cisco Catalyst Center. Si se recopilan registros del sistema para obtener información de nivel 2, el ancho de banda mínimo necesario es de 3,5 Mbits/seg. para cubrir 5000 dispositivos +13000 puntos de acceso para inventario, 5000 dispositivos registros del sistema y 2000 dispositivos para análisis; todos se ejecutan en paralelo desde CX Cloud Agent.

P. Cómo el Agente syslogs ¿Puede accederse a ella para supervisar la máquina virtual (VM) del agente en la nube de CX?

R. Se puede acceder a los registros del sistema para la VM del agente desde el inicio de sesión de la VM local mediante las dos rutas siguientes:

/var/log/syslog.1 (al que se accede a través de los inicios de sesión de cxcadmin y cxcroot)

/var/log/syslog (al que se accede mediante root)

Versiones y parches

P. ¿Cuáles son los diferentes tipos de versiones listadas para la actualización de CX Cloud Agent?

R. Aquí se muestra el conjunto de versiones lanzadas de CX Cloud Agent que se enumeran:

- A.x.0 (donde x es la última versión de la función principal de producción, por ejemplo:1.3.0)
- A.x.y (donde A.x.0 es obligatorio y debe iniciarse una actualización incremental, x es la última versión de la función principal de producción e y es la última revisión de actualización activa, por ejemplo: 1.3.1)
- A.x.y-z (donde A.x.0 es obligatorio y debe iniciarse una actualización incremental, x es la última versión de la función principal de producción, e y es la última revisión de actualización activa, y z es la corrección instantánea durante un período de tiempo muy corto, por ejemplo: 1.3.1-1)

donde A es una liberación a largo plazo distribuida en 3-5 años.

P. ¿Dónde se encuentra la última versión de CX Cloud Agent y cómo actualizar la versión existente de CX Cloud Agent?

R. Para localizar y actualizar al agente en la nube CX más reciente:

1. Inicie sesión en el portal de la nube de CX y navegue hasta el Centro de administración. Se abre la ventana Orígenes de datos.
2. Seleccione CX Cloud Agent para abrir la vista de detalles y haga clic en la pestaña Software.
3. Realice una selección en la lista desplegable Elegir una versión de software para actualizar a y haga clic en Instalar actualización.

Autenticación y configuración de proxy

P. ¿Cuál es el usuario predeterminado de la aplicación CX Cloud Agent?

A. cxcadmin.

P. ¿Cómo se establece la contraseña para el usuario predeterminado?

R. Las contraseñas se establecen durante la configuración de la red.

P. ¿Hay alguna opción disponible para restablecer la contraseña después del Día-0?

R. El agente en la nube de CX no proporciona ninguna opción específica para restablecer la contraseña, pero puede utilizar los comandos de Linux para restablecer la contraseña de cxcadmin.

P. ¿Cuáles son las políticas de contraseña para configurar CX Cloud Agent?

A. Las políticas de contraseña son:

- Edad máxima (duración) establecida en 90 días
- Edad mínima (duración) establecida en 8 días
- Longitud máxima 127 caracteres
- Se debe incluir al menos una mayúscula y una minúscula
- Debe contener al menos un carácter especial (por ejemplo, !$%^&*()_+|~-=\`{}[]:";'<>?,/)
- Los siguientes caracteres no están permitidos
  - Caracteres especiales de 8 bits (p. ej., \£, √Å √´, √¥, √ë,, √ü)
  - Espacios
- No deben ser las últimas 10 contraseñas utilizadas recientemente
- No debe contener una expresión regular
- No debe contener las siguientes palabras o derivados: cisco, sanjose y sanfran

P. ¿Cómo confirmo la disponibilidad de Secure Shell (SSH) para un dispositivo desde CX Cloud Agent?

A. Para confirmar la disponibilidad de SSH:

1. Inicie sesión como usuario cxcroot.
2. Ejecute el siguiente comando para habilitar el puerto SSH en Iptables:

   Iptables -A OUTPUT -p tcp -m tcp —dport 22 -j ACCEPT

3. Ejecute el siguiente comando para confirmar la disponibilidad de SSH:

   ssh user@ip-address:port

Para desactivar los puertos SSH activados anteriormente en el agente en la nube CX:

1. Ejecute el siguiente comando para obtener el número de línea del puerto SSH habilitado en iptables:

   iptables -L OUTPUT —line-number | grep dpt | grep ssh | awk '{print $1}'

2. Ejecute el siguiente comando para eliminar el número de línea obtenido:

   iptables -L OUTPUT <Line number>

P. ¿Cómo confirmo la disponibilidad de SNMP a un dispositivo desde CX Cloud Agent?

A. Para confirmar el alcance SNMP:

1. Inicie sesión como usuario cxcroot.
2. Ejecute el siguiente comando para habilitar los puertos SNMP en las tablas IP:

   iptables -A OUTPUT -p udp -m udp —dport 161 -j ACCEPT

iptables -A OUTPUT -p udp -m udp —dport 161 -j ACCEPT

3. Ejecute el siguiente comando snmpwalk/snmpget para confirmar el alcance SNMP:

snmpwalk -v2c -c cisco IPADDRESS

Para desactivar los puertos SNMP activados anteriormente en el agente en la nube CX:

1. Ejecute el siguiente comando para obtener los números de línea de los puertos SNMP habilitados (se generan dos números de línea como respuesta):

iptables -L OUTPUT —line-number | grep dpt | grep ssh | awk '{print $1}'

2. Ejecute el siguiente comando para eliminar los números de línea (en orden descendente):

iptables -L OUTPUT <Line number2 Número>

iptables -L OUTPUT <Line number1 Número>

P. ¿Cómo configuro la contraseña de Grub?

A. Para establecer la contraseña de Grub:

1. Ejecute .ssh como cxcroot y proporcione el token [póngase en contacto con el equipo de soporte técnico para obtener el token cxcroot].
2. Ejecute sudo su, para proporcionar el mismo token.
3. Ejecute el comando grub-mkpasswd-pbkdf2 y establezca la contraseña de Grub. Se imprimirá el hash de la contraseña proporcionada, copie el contenido.
4. vi al archivo /etc/grub.d/00_header.
5. Navegue hasta el final del archivo y reemplace la salida hash seguida por el content password_pbkdf2 root ***** con el hash obtenido para la contraseña obtenida en el paso 3.
6. Guarde el archivo con el comando :wq!.
7. Ejecute el comando update-grub.

P. ¿Cuál es el período de vencimiento de la contraseña de cxcadmin?

R. La contraseña caduca en 90 días.

P. ¿El sistema inhabilita la cuenta después de intentos consecutivos de inicio de sesión fallidos?

R. Sí, la cuenta se inhabilita después de cinco (5) intentos fallidos consecutivos. El periodo de bloqueo es de 30 minutos.

P. ¿Cómo genero una frase de contraseña?

A. Para generar una frase de contraseña:

1. Ejecute .ssh e inicie sesión como usuario cxcadmin.

2. Ejecute el comando remoteaccount cleanup -f.
3. Ejecute el comando remoteaccount create.

P. ¿El host proxy soporta el nombre de host y la IP?

R. Sí, pero para utilizar el nombre de host, el usuario debe proporcionar la dirección IP del servidor de nombres de dominio (DNS) durante la configuración de la red.

SSH de Secure Shell

P. ¿Qué cifrados son soportados por el shell ssh?

R. Se admiten los siguientes cifrados:

- chacha20-poly1305@openssh.com
- aes256-gcm@openssh.com
- aes128-gcm@openssh.com
- aes256-ctr
- aes192-ctr
- aes128-ctr

P. ¿Cómo inicio sesión en la consola?

A. Para iniciar sesión:

1. Inicie sesión como usuario cxcadmin
2. Proporcione la contraseña cxcadmin

P. ¿Están registrados los logins SSH?

R. Sí, se registran como parte del archivo "var/logs/audit/audit.log".

P. ¿Cuál es el tiempo de espera de la sesión inactiva?

R. El tiempo de espera de la sesión SSH se produce si el agente en la nube CX permanece inactivo durante cinco (5) minutos.

Puertos y servicios

P. ¿Qué puertos se mantienen abiertos en el agente en la nube CX?

R. Están disponibles los siguientes puertos:

- Puerto de salida: el agente en la nube CX implementado puede conectarse al backend de Cisco como se indica en la tabla del puerto HTTPS 443 o a través de un proxy para enviar datos a Cisco como se indica en la tabla siguiente. El agente en la nube CX implementado

puede conectarse a Cisco Catalyst Center en el puerto HTTPS 443.

AMÉRICA	EMEA	Asia Pacífico, Japón y China
cloudsso.cisco.com	cloudsso.cisco.com	cloudsso.cisco.com
api-cx.cisco.com	api-cx.cisco.com	api-cx.cisco.com
agent.us.csco.cloud	agent.emea.cisco.cloud	agent.apjc.cisco.cloud
ng.acs.agent.us.csco.cloud	ng.acs.agent.emea.cisco.cloud	ng.acs.agent.apjc.cisco.cloud

Nota: además de los dominios enumerados, cuando los clientes de EMEA o APJC reinstalen el agente en la nube CX, se debe permitir el dominio agent.us.csco.cloud en el firewall del cliente.
El dominio agent.us.csco.cloud ya no es necesario después de una reinstalación correcta.

Nota: Asegúrese de que se permita el tráfico de retorno en el puerto 443.

- Inbound port: para la gestión local de CX Cloud Agent, se debe poder acceder a 514 (Syslog) y 22 (ssh). Los clientes deben permitir que el puerto 443 de su firewall reciba datos de CX Cloud.

Conexión del agente en la nube CX con Cisco Catalyst Center y otros recursos

P. ¿Cuál es el propósito y la relación de Cisco Catalyst Center con CX Cloud Agent?

R. Cisco Catalyst Center es el agente en la nube que gestiona los dispositivos de red de las instalaciones del cliente. CX Cloud Agent recopila la información de inventario del dispositivo desde el Cisco Catalyst Center configurado y carga la información de inventario disponible en Asset View de CX Cloud.

P. ¿Dónde pueden los usuarios proporcionar detalles de Cisco Catalyst Center sobre el agente en la nube CX?

R. Durante el día 0 de la configuración del agente en la nube CX, los usuarios pueden agregar los detalles de Cisco Catalyst Center desde el portal de la nube CX. Durante las operaciones del día N, los usuarios pueden agregar Cisco Catalyst Centers adicionales desdeAdmin Settings > Data Source.

P. ¿Cuántos Cisco Catalyst Centers se pueden agregar?

R. Se pueden agregar diez (10) clústeres de Cisco Catalyst Center o 20 clústeres que no sean de Cisco Catalyst Center.

P. ¿Cómo elimino un Cisco Catalyst Center conectado de CX Cloud Agent?

R. Para quitar un Cisco Catalyst Center conectado de un agente en la nube de CX, póngase en contacto con el centro de asistencia técnica Technical Assistance Center (TAC) para abrir un caso de soporte desde el portal de la nube de CX.

P. ¿Qué función puede desempeñar el usuario de Cisco Catalyst Center?

R. El rol de usuario puede ser admin u Observer.

P. ¿Cómo se reflejan las modificaciones en el agente en la nube de CX debido a los cambios en las credenciales conectadas de Cisco Catalyst Center?

A. Ejecute el comando cxcli agent modifyController desde la consola de CX Cloud Agent:

Póngase en contacto con el servicio de asistencia para cualquier problema durante la actualización de credenciales de Cisco Catalyst Center.

P. ¿Cómo se almacenan los detalles de Cisco Catalyst Center y de los recursos de archivos simiente en CX Cloud Agent?

R. Todos los datos, incluidas las credenciales de los controladores conectados a CX Cloud Agent (por ejemplo, Cisco Catalyst Center) y los activos conectados directamente (por ejemplo, mediante un archivo simiente o un intervalo de IP), se cifran mediante AES-256 y se almacenan en la base de datos de CX Cloud Agent, que está protegida con una ID de usuario y una contraseña seguras.

P. ¿Existe alguna limitación a la hora de introducir rangos de IP al añadir otros activos?

R. Sí, el agente en la nube de CX no puede gestionar las operaciones de detección para rangos de IP de subred más grandes. Cisco recomienda utilizar rangos de subred minimizados limitados a 10 000 direcciones IP.

P. ¿Se puede utilizar una subred pública para la implementación de CX Cloud Agent v2.4 para la subred personalizada de servicios y el clúster?

R. Cisco no recomienda el uso de una subred de IP pública por los siguientes motivos:

- Riesgos de seguridad: las direcciones IP públicas exponen el clúster y los servicios a Internet, lo que aumenta el riesgo de acceso no autorizado, ataques y posibles violaciones

de datos.
- Conflictos de direcciones IP: el uso de subredes IP públicas puede provocar conflictos de IP, especialmente si se asignan las mismas direcciones IP en otro lugar de Internet, lo que provoca problemas de conectividad y comportamientos inesperados.
- Complejidad en la configuración de red: la gestión de políticas de red, reglas de firewall y routing se vuelve más compleja cuando se trata de direcciones IP públicas. Esto puede dar lugar a errores de configuración y aumentar los gastos de mantenimiento.

Una subred IP pública se puede utilizar si está asignada únicamente a una organización del cliente y configurada a través de la red del cliente.

P. ¿Con qué frecuencia se puede iniciar la operación de redescubrimiento?

R. La operación de redescubrimiento sólo se debe realizar si hay un cambio en la red del cliente (por ejemplo, después de agregar o eliminar dispositivos dentro de la red).

P. ¿Cuál es el flujo de trabajo para agregar "Otros activos como origen de datos" al cargar un archivo simiente?

R. El flujo de trabajo es el siguiente:

1. Cargue el archivo simiente en CX Cloud.
2. El archivo simiente se almacena temporalmente en la cubeta de Cisco Cloud AWS S3 (con la encriptación SSE habilitada).
3. El archivo simiente se envía al agente de nube CX y el archivo simiente se elimina de la cubeta S3
4. El agente en la nube de CX procesa las entradas del archivo simiente y cifra las credenciales mediante una clave AES 256 (esta clave es única para cada agente en la nube de CX). Estas credenciales cifradas se almacenan en la base de datos de agentes en la nube de CX.
5. El archivo simiente se elimina del agente de nube CX una vez que se procesan las entradas del archivo simiente.

P. ¿Qué tipo de cifrado se utiliza al acceder a la API de Cisco Catalyst Center desde el agente en la nube CX?

R. HTTPS sobre TLS 1.2 se utiliza para la comunicación entre Cisco Catalyst Center y CX Cloud Agent.

P. ¿Qué operaciones realiza CX Cloud Agent en el Cisco Catalyst Center Cloud Agent integrado?

R. El agente en la nube CX recopila datos de Cisco Catalyst Center sobre los dispositivos de red y utiliza la interfaz de ejecución de comandos de Cisco Catalyst Center para comunicarse con los dispositivos finales y ejecutar los comandos CLI (comando show). No se ejecutan comandos de cambio de configuración.

P. ¿Qué datos predeterminados se recopilan de Cisco Catalyst Center y se cargan en el back-end?

A.

- Entidad de red
- Módulos
- show version
- Config
- Información de imagen del dispositivo
- Etiquetas

P. ¿Qué datos adicionales se recopilan de Cisco Catalyst Center y se cargan en el back-end de Cisco?

R. Consulte este documento para obtener más información.

P. ¿Cómo se cargan los datos de inventario en el backend?

R. El agente de nube CX carga los datos de inventario a través del protocolo TLS 1.2 en el servidor backend de Cisco.

P. ¿Cuál es la frecuencia de carga del inventario?

R. La recopilación se activa según la programación definida por el usuario y se carga en el servidor de Cisco.

P. ¿Puede el usuario volver a programar el inventario?

R. Sí, hay una opción disponible en Centro de administración > Orígenes de datos para modificar la información de programación.

P. ¿Cuándo se produce el tiempo de espera de conexión entre Cisco Catalyst Center y Cloud Agent?

A. Los tiempos de espera se categorizan de la siguiente manera:

- Para la conexión inicial, el tiempo de espera máximo es de 300 segundos. Si no se establece la conexión entre Cisco Catalyst Center y Cloud Agent en un máximo de cinco (5) minutos, la conexión finaliza.
- Para actualizaciones recurrentes, típicas o periódicas: el tiempo de espera de respuesta es de 1800 segundos. Si no se recibe la respuesta o no se puede leer en 30 minutos, la conexión finaliza.

Análisis de diagnóstico de CX Cloud Agent utilizado

P. ¿Qué comandos de escaneo se ejecutan en el dispositivo?

R. Los comandos que deben ejecutarse en el dispositivo para el análisis se determinan dinámicamente durante el proceso de análisis. El conjunto de comandos puede cambiar con el tiempo, incluso para el mismo dispositivo (y que no esté bajo el control del Análisis de diagnóstico).

P. ¿Dónde se almacenan y se perfilan los resultados del análisis?

R. Los resultados escaneados se almacenan y perfilan en el backend de Cisco.

P. ¿Los duplicados (por nombre de host o IP) en Cisco Catalyst Center se agregan al Análisis de diagnóstico cuando el origen de Cisco Catalyst Center está conectado?

R. No, los duplicados se filtran de manera que solo se extraen los dispositivos únicos.

P. ¿Qué sucede cuando falla uno de los escaneos de comando?

R. El escaneo del dispositivo se detiene por completo y se marca como fallido.

P. ¿Qué sucede cuando los escaneos múltiples se superponen?

R. La ejecución simultánea de varias exploraciones de diagnóstico puede ralentizar el proceso de exploración y provocar posibles errores de exploración. Cisco recomienda programar análisis de diagnóstico o iniciar análisis bajo demanda con un intervalo de al menos 6-7 horas entre las programaciones de recopilación de inventario para que no se superpongan.

Registros del sistema de agentes en la nube CX

P. ¿Qué información de estado se envía al portal de la nube de CX?

R. Registros de aplicaciones, estado de Pod, detalles de Cisco Catalyst Center, registros de auditoría, detalles del sistema y detalles de hardware.

P. ¿Qué detalles del sistema y del hardware se recopilan?

A. Ejemplo de resultado:

detalles_del_sistema":{
"os_details":{
"containerRuntimeVersion":"docker://19.3.12",
"kernelVersion":"5.4.0-47-generic",
"kubeProxyVersion":"v1.15.12",
"kubeletVersion":"v1.15.12",
"machineID":"81edd7df1c1145e7bcc1ab4fe778615f",

"operatingSystem":"linux",
"osImage":"Ubuntu 20.04.1 LTS",
"systemUUID":"42002151-4131-2ad8-4443-8682911bdadb"
},
"hardware_details":{
"total_cpu":"8",
"cpu_utilization":"12.5%",
"total_memory":"16007MB",
"free_memory":"994 MB",
"hdd_size":"214G",
"free_hdd_size":"202G"
}
}
}

P. ¿Cómo se envían los datos de salud al backend?

R. Con CX Cloud Agent, el servicio de mantenimiento transfiere los datos al servidor de Cisco.

P. ¿Cuál es la política de retención de registros de datos de estado del agente en la nube de CX en el backend?

R. La política de retención de datos de estado del agente en la nube de CX en el backend es de 120 días.

P. ¿Qué tipos de cargas están disponibles?

A.

1. Carga del inventario
2. Carga de Syslog
3. Carga de estado del agente, incluida la carga de estado
    1. Estado de los servicios: cada cinco (5) minutos
    2. Podlog - Cada una (1) hora
    3. Registro de auditoría: cada una (1) hora

Resolución de problemas

Problema: no se puede acceder a la dirección IP configurada.

Solución: ejecute ssh utilizando la IP configurada. Si se agota el tiempo de espera de la conexión, la razón posible es una configuración incorrecta de IP. En este caso, reinstale configurando una dirección IP válida. Esto se puede hacer a través del portal con la opción de reinstalación proporcionada en laAdmin Centerpágina.

Problema: ¿cómo puedo comprobar que los servicios están en funcionamiento tras el registro?

Solución: siga estos pasos para confirmar que los grupos de dispositivos están en funcionamiento:

1. ssh a la IP configurada como cxcadmin
2. Proporcione la contraseña
3. Ejecute el comando kubectl get pods

Los grupos de dispositivos pueden estar en cualquier estado (En ejecución, Inicializando o Creando contenedor). Después de 20 minutos, las vainas deben estar en el estado En ejecución.

Si el estado es no se está ejecutando o Pod Inicializando, verifique la descripción del pod con el comando kubectl describe pod <podname> .

El resultado tendrá información sobre el estado del grupo de dispositivos.

Problema: ¿Cómo verificar si el interceptor SSL está inhabilitado en el proxy del cliente?
Solución: ejecute el comando curl que se muestra aquí para verificar la sección del certificado del servidor. La respuesta tiene los detalles del certificado del servidor web concsoweb.

curl -v —header 'Autorización: básica xxxxxx' https://concsoweb-prd.cisco.com/

* Certificado de servidor:

* subject: C=US; ST=California; L=San José; O=Cisco Systems, Inc.; CN=concsoweb-prd.cisco.com

* fecha de inicio: 16 de febrero 11:55:11 2021 GMT

* fecha de caducidad: 16 de febrero 12:05:00 2022 GMT

* subjectAltName: el host "concsoweb-prd.cisco.com" coincidió con "concsoweb-prd.cisco.com" de cert

* emisor: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID SSL, CA G3

* Certificado SSL verificado de acuerdo.

> GET / HTTP/1.1

Problema: los comandos kubectl fallaron y muestra el error como "La conexión al servidor X.X.X.X:6443 fue rechazada - ¿especificó el host o puerto correcto?"
Solución:

- Compruebe la disponibilidad de los recursos. [ejemplo: CPU, Memoria].
- Espere a que comience el servicio Kubernetes.

Problema: ¿Cómo obtener los detalles de la falla de recolección para un comando/dispositivo?

Solución:

- Ejecute kubectl get pods y obtenga el nombre del pod de recolección.
- Ejecute kubectl logs <collectionPodName> para obtener los detalles específicos del comando/dispositivo.

Problema: el comando kubectl no funciona con el error "[authentication.go:64] No se puede autenticar la solicitud debido a un error: [x509: el certificado ha caducado o aún no es válido, x509: el certificado ha caducado o aún no es válido]"

Solución:Ejecute los comandos que se muestran aquí como usuario cxcroot

rm /var/lib/rancher/k3s/server/tls/dynamic-cert.json
systemctl restart k3s
kubectl —insecure-skip-tls-verify=true delete secret -n kube-system k3s-serve
systemctl restart k3s

Respuestas de fallos de recopilación

La causa de la falla de recolección puede ser cualquier restricción o problema que se observe con el controlador o los dispositivos agregados presentes en el controlador.

La tabla que se muestra aquí tiene el fragmento de error para los casos prácticos vistos en el microservicio de recopilación durante el proceso de recopilación.

caso de uso	Fragmento de registro en microservicio de recopilación

Si el dispositivo solicitado no se encuentra en Cisco Catalyst Center	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": " No se ha encontrado ningún dispositivo con id 02eb08be-b13f-4d25-9d63-eaf4e882f71a "
	}

Si el dispositivo solicitado no es accesible desde Cisco Catalyst Center	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Error al ejecutar el comando: show version\nError al conectar con el dispositivo [Host: 172.21.137.221:22]Sin ruta al host: sin ruta al host "
	}

Si el dispositivo solicitado no es accesible desde Cisco Catalyst	{ "command": "show version",

caso de uso	Fragmento de registro en microservicio de recopilación
Center	"status": "Failed", "commandResponse": "", "errorMessage": "Error al ejecutar el comando: show version\nError al conectar con el dispositivo [Host: X.X.X.X.X]Tiempo de espera de conexión agotado: /X.X.X.X:22 : Tiempo de espera de conexión agotado: /X.X.X.X:22" }

Si el comando solicitado no está disponible en el dispositivo	{
	"command": "show run-config",
	"status": "Success",
	"commandResponse": " Error al ejecutar el comando: show run-config\n\nshow run-config\n ^\n% Se ha detectado una entrada no válida en el marcador \u0027^\u0027.\n\nXXCT5760#",
	"errorMessage": ""
	}

Si el dispositivo solicitado no tiene SSHv2 y Cisco Catalyst Center intenta conectar el dispositivo con SSHv2	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Error al ejecutar el comando: show version\nCanal SSH2 cerrado: el participante remoto utiliza un protocolo incompatible, no es compatible con SSH-2."
	}

Si el comando está deshabilitado en el microservicio de recopilación	{
	"comando": "config paging disable",
	"status": "Command_Disabled",
	"commandResponse": "La colección de comandos está deshabilitada",
	"errorMessage": ""
	}

Si se produce un error en la tarea Command Runner Task y Cisco Catalyst Center no devuelve la URL de la tarea	{ "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "Error en la tarea de ejecución del comando

caso de uso	Fragmento de registro en microservicio de recopilación
	para el dispositivo %s. La URL de la tarea está vacía." }

Si no se pudo crear la tarea Command Runner Task en Cisco Catalyst Center	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Error en la tarea de ejecución del comando para el dispositivo %s, RequestURL: %s. Sin detalles de la tarea".
	}

Si el microservicio de recopilación no recibe una respuesta para una solicitud de Command Runner de Cisco Catalyst Center	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Error en la tarea de ejecución del comando para el dispositivo %s, RequestURL: %s."
	}

Si Cisco Catalyst Center no está completando la tarea dentro del tiempo de espera configurado (5 minutos por comando en el microservicio de recopilación)	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Operation Timedout. Error en la tarea del ejecutor de comandos para el dispositivo %s, RequestURL: %s. Sin detalles de progreso".
	}

Si la tarea Command Runner Task falló y el ID de archivo está vacío para la tarea enviada por Cisco Catalyst Center	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Error en la tarea de ejecución del comando para el dispositivo %s, RequestURL: %s. La ID de archivo está vacía."
	}

Si la tarea Command Runner Task falló y Cisco Catalyst Center no	{ "command": "show version",

caso de uso	Fragmento de registro en microservicio de recopilación
devuelve la etiqueta de ID de archivo	"status": "Failed", "commandResponse": "", "errorMessage": "Error en la tarea de ejecución del comando para el dispositivo %s, RequestURL: %s. No hay detalles de ID de archivo." }

Si el dispositivo no es apto para la ejecución del ejecutor de comandos	{
	"comando": "config paging disable",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Los dispositivos solicitados no están en el inventario. Pruebe con otros dispositivos disponibles en el inventario"
	}

Si el ejecutor de comandos está deshabilitado para el usuario	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "{\"message\":\"El rol no tiene permisos válidos para acceder a la API\"}\n"
	}

Respuestas de error de análisis de diagnóstico

Los fallos de análisis y las causas pueden provenir de cualquiera de los componentes enumerados.

Cuando los usuarios inician un análisis desde el portal, ocasionalmente se muestra como "error: error interno del servidor".

La causa del problema es uno de los componentes enumerados

- Punto de control
- Gateway de datos de red
- Conector
- Análisis de diagnóstico
- CX Cloud Agent Microservice [administrador de dispositivos, recopilación]
- Cisco Catalyst Center
- APIX
- Mashería

- Ping Access
- BANCO DE HIERRO
- IRONBANK GW
- Big Data Broker (BDB)

Para ver los registros:

1. Inicie sesión en la consola de CX Cloud Agent.
2. Ejecute kubectl get pods.
3. Obtenga el nombre de la recopilación, el conector y la facilidad de mantenimiento del grupo de dispositivos.
4. Para comprobar los registros de microservicios de recopilación, conector y mantenimiento.

- Execute kubectl logs <collection podname>
- Ejecutar registros kubectl <connector>
- Ejecutar registros kubectl <servicability>

La tabla siguiente muestra el fragmento de error que se ve en los registros de microservicio de recopilación y microservicio de mantenimiento que se produce debido a problemas o restricciones con los componentes.

Caso de uso	Fragmento de registro en microservicio de recopilación

El dispositivo puede ser accesible y compatible, pero los comandos que se ejecutan en ese dispositivo se enumeran en bloques en el microservicio de recopilación	{
	"comando": "config paging disable",
	"status": "Command_Disabled",
	"commandResponse": "La colección de comandos está deshabilitada",
	}

Si el dispositivo para un análisis no está disponible. Se produce en un escenario, cuando hay un problema de sincronización entre los componentes, como el portal, el análisis de diagnóstico, el componente CX y Cisco Catalyst Center	No se ha encontrado ningún dispositivo con id 02eb08be-b13f-4d25-9d63-eaf4e882f71a
Si el dispositivo que se intenta escanear está ocupado, (en un escenario) en el que el mismo dispositivo ha sido parte de otro trabajo y no se manejan solicitudes	Todos los dispositivos solicitados ya están siendo consultados por el ejecutor de comandos en otra sesión. Pruebe con otros dispositivos

Caso de uso	Fragmento de registro en microservicio de recopilación
paralelas desde Cisco Catalyst Center para el dispositivo	
Si el dispositivo no es compatible con el análisis	Los dispositivos solicitados no están en el inventario. Pruebe con otros dispositivos disponibles en el inventario.
Si el dispositivo que se ha intentado escanear no está accesible	"Error al ejecutar el comando: show udi\nError al conectar con el dispositivo [Host: x.x.x.x:22] Sin ruta al host: sin ruta al host

Si no se puede acceder a Cisco Catalyst Center desde el microservicio Cloud Agent o Collection del Cloud Agent no está recibiendo respuesta para una solicitud de Command Runner de Cisco Catalyst Center	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Error en la tarea de ejecución del comando para el dispositivo %s, RequestURL: %s."
	}

caso de uso	Fragmento de registro en el microservicio del agente de punto de control
Si la solicitud de análisis tiene detalles de programación que faltan	Error al ejecutar la solicitud {"message":"23502: el valor nulo de la columna \"schedule\" infringe la restricción no nula"}
Si la solicitud de análisis tiene detalles del dispositivo que faltan	No se pudo crear la directiva de digitalización. No hay dispositivos válidos en la solicitud
Si la conexión entre el CPA y la conectividad está inactiva	Error al ejecutar la solicitud
Si el dispositivo para análisis solicitado no está disponible en Análisis de diagnóstico	No se pudo enviar la solicitud de análisis. Motivo = {\"mensaje\":\"No se encontró el dispositivo con nombre de host=x.x.x.x'\"}

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).