

Guía de inicio de Cisco IQ Virtual Appliance

Introducción

Cisco IQTM proporciona a los clientes mejoras y funciones diseñadas para mejorar la visibilidad de los recursos, ofrecer una perspectiva más inteligente de sus entornos y simplificar la gestión de casos. Además, las funciones de inteligencia artificial, como el asistente de inteligencia artificial, optimizan los resultados operativos y la experiencia del usuario de Cisco IQ al proporcionar una comprensión contextual que permite a los usuarios tomar decisiones proactivas e informadas y agilizar los procesos para lograr el compromiso y el éxito de los clientes.

Cisco IQ On-Prem Air-Gapped es uno de los modos de implementación de Cisco IQ, diseñado para clientes de sectores altamente regulados con estrictos requisitos de cumplimiento, propiedad de datos y seguridad. En este modo, Cisco IQ se proporciona como una máquina virtual (VM) independiente denominada dispositivo virtual (VA) de Cisco IQ. El VA se ejecuta completamente en las instalaciones del cliente y funciona de forma totalmente aislada de las redes externas. Para mantener este aislamiento, las actualizaciones de software y los paquetes de mantenimiento se obtienen de Cisco IQ SaaS y se transfieren al VA mediante un proceso aprobado y manual.

Cisco IQ On-Prem Air-Gapped amplía las capacidades clave de Cisco IQ SaaS a entornos con espacios aislados, lo que permite a los equipos críticos funcionar con una velocidad e inteligencia de diagnóstico comparables a las empresas conectadas en la nube.

Esta guía proporciona instrucciones para configurar e implementar Cisco IQ VA for Air-Gap, incluido el proceso de configuración del entorno de red necesario.



Nota: El VA de Cisco IQ se limita actualmente a los clientes inscritos en el programa de versión controlada. El acceso a las descargas del VA y sus sistemas operativos (módulos, normas y derechos) está disponible exclusivamente para determinados clientes. Póngase en contacto con su representante de cuentas para obtener más información.

Opciones de implementación

Cisco IQ VA ofrece un modelo de implementación flexible diseñado para ofrecer valor con opciones que se adapten a las diferentes necesidades operativas. La implementación básica proporciona capacidades esenciales como la gestión de activos e inventarios, evaluaciones y otras operaciones.

Para los clientes que buscan automatización e información avanzada impulsada por IA, VA

también ofrece una opción de implementación basada en IA habilitada a través del hardware de la unidad de procesamiento de gráficos (GPU). Puedes desbloquear poderosas funciones de IA como el Asistente de IA, Key Insights y Full Insights con el complemento de AI.

Este enfoque le permite elegir el más adecuado para sus requisitos operativos y de seguridad, lo que convierte al AV en una solución escalable y preparada para el futuro.

Prerequisites

Asegúrese de que se cumplen los siguientes requisitos previos antes de configurar e instalar Cisco IQ VA.

Requisitos de recursos de hardware y VM

Cisco IQ VA se ha probado para capacidad de varias escalas y ofrece varios tamaños de implementación para satisfacer las necesidades de ampliación de su entorno. Consulte la tabla siguiente para seleccionar la configuración de recursos adecuada en función del recuento de detección de dispositivos planeado.

Tabla 1: Requisitos de recursos de hardware y VM

Recurso	Hasta 5000 dispositivos (no basados en GPU)	Hasta 20 000 dispositivos (sin GPU)	Hasta 20 000 dispositivos (basados en GPU)
vCPU	48	64	96
RAM	96 GB	128 GB	256 GB
Almacenamiento (SSD) (recomendado para un mejor rendimiento)	1,3 TB	1,3 TB	1,3 TB
Programación de recopilación	24 horas o más	24 horas o más	24 horas o más
Hipervisores	• VMware ESXi v8.0 o posterior con VMware vSphere Web Client v8.0 o		

admitidos	posterior • Hyper-V en Microsoft Server 2022 y 2025 • Hipervisor de máquinas virtuales basadas en kernel (KVM) en RHEL v9.7 o posterior
Servidor	• Unified Computing System M6 o modelos más recientes
Recomendación adicional	• Cisco recomienda utilizar el aprovisionamiento dinámico. Aunque es posible utilizar el aprovisionamiento dinámico, el aprovisionamiento excesivo puede provocar una falta de capacidad de almacenamiento, lo que puede provocar la degradación y la pérdida de servicio. • Se recomienda colocar discos de dispositivo en un volumen respaldado por SSD. • La velocidad de escritura en disco debe ser superior a 70 megabytes por segundo.

Requisitos de recursos de funciones AI

Cisco IQ VA se ha probado y es compatible con la GPU NVIDIA RTX Pro 6000 Blackwell Server Edition. Esta configuración de GPU cumple los requisitos de rendimiento y latencia a la escala de implementación planificada.

Tabla 2: Requisitos de recursos de las funciones AI

Recurso	Recomendado
GPU validada	NVIDIA RTX Pro 6000 Blackwell Server Edition
Opciones de GPU adicionales (no validadas)	• NVIDIA H200 (141 GB)
Opciones de GPU adicionales (no validadas, sugeridas con un (1) usuario simultáneo)	• NVIDIA H100 (80 GB) • NVIDIA H100 NVL (94 GB) • NVIDIA A100 (80 GB)



Nota: Las GPU que no sean NVIDIA RTX Pro 6000 Blackwell Server Edition no se han validado en los laboratorios de Cisco a la escala admitida. El rendimiento y la latencia no están garantizados para las GPU no validadas. Valide todo el hardware no compatible con la carga de trabajo prevista en un entorno de preproducción antes de la implementación de producción.

Requisitos de la red

VA admite una única interfaz de red.

Requisitos de dirección IP y nombre de host

Deben cumplirse los siguientes requisitos de dirección IP y nombre de host:

- Sistema de nombres de dominio (DNS): DNS simplifica la gestión del sistema al sustituir las direcciones IP numéricas por nombres de host coherentes y legibles. Este enfoque facilita un mantenimiento más sencillo, una integración de servicios perfecta y una validación de certificados fiable en entornos seguros. Asegúrese de que la dirección IPv4 está configurada en el DNS con lo siguiente:
- Un registro: Asigna el nombre de host a la dirección IPv4
- Registro de puntero asociado (PTR): Necesario para admitir búsquedas de DNS inversas; si una dirección IP se resuelve en varios nombres de host, el primer nombre de host resuelto se utiliza para acceder a la interfaz de usuario



Nota: Actualmente no se admite DHCP.

Requisitos de puerto

En la tabla siguiente se describen los puertos de red necesarios para la comunicación del VA de Cisco IQ.

Tabla 3: Requisitos de puerto

Puerto(s)	Protocolo	Descripción
22	TCP	Se utiliza para sesiones de depuración de la CLI del administrador y de soporte de Cisco

443	TCP	Se utiliza para la comunicación entre Cisco IQ On-Prem y los navegadores web, así como los destinos de terminales
53, 123, 161	UDP	Se utiliza para enviar y recibir tráfico DNS, NTP y SNMP

Navegadores admitidos

Debe utilizar la última versión estable de los navegadores siguientes para instalar e iniciar el dispositivo virtual:

- Google Chrome
- Microsoft Edge
- Safari de Apple
- Mozilla Firefox



Nota: La compatibilidad se limita a las versiones actuales del navegador, y es posible que las versiones anteriores no proporcionen funcionalidad completa o que no sean compatibles a medida que se lanzan nuevas actualizaciones.

Instalación de Virtual Appliance Setup

En esta sección se describen los procedimientos de instalación del AV. El ámbito actual incluye instrucciones para los siguientes hipervisores:

- VMware ESXi
- Servidor Microsoft Hyper-V
- KVM de Red Hat

Descargar dispositivo virtual

Los archivos del instalador de VA se pueden descargar desde Cisco IQ SaaS. Para descargar el AV:

1. Inicie sesión en [Cisco IQ](#) (SaaS).
2. Vaya a System Settings > Package Catalog.
3. En la tarjeta del VA de Cisco IQ, seleccione Opciones de descarga. Se abre la ventana Install Package.
4. Seleccione una de las siguientes opciones de hipervisor de la lista desplegable:

- ESXi: para VMware ESXi
 - Hyper-V: para Microsoft Hyper-V
 - KVM: para la máquina virtual basada en kernel de Linux (KVM)
5. Seleccione una versión en la lista desplegable.
 6. Haga clic en Descargar para guardar el archivo localmente.



Nota: Los archivos de instalación son grandes (20-25 GB); asegúrese de que dispone de suficiente espacio en disco antes de realizar la descarga.

Instalación del dispositivo virtual en VMware ESXi

El archivo de instalación de VA descargado está listo para instalarse. Para instalar el dispositivo virtual en VMware ESXi:



Nota: El OVA debe implementarse mediante VMware vCenter y no puede implementarse directamente en los servidores ESXi.

1. Inicie sesión en VMware vSphere Web Client con credenciales de administrador.
2. Haga clic con el botón derecho del ratón en el objeto vCenter correspondiente (Data Center, clúster o host ESXi) y seleccione Implementar plantilla OVF.
3. En el asistente Deploy OVF Template, elija la página de plantilla, especifique la ubicación de origen y haga clic en Next. Puede especificar una dirección URL o desplazarse a cualquier ubicación accesible.
4. En la página OVF Template Details, verifique los detalles de la plantilla OVF y haga clic en Next. No es necesaria ninguna entrada.
5. En la página Select a name and location, agregue o edite los campos Name y Location para el dispositivo virtual y haga clic en Next.
6. En la página Seleccione un recurso, elija el host (host de ESXi), el clúster o el grupo de recursos en el que desea realizar la implementación y haga clic en Siguiente.



Nota: Cada VM debe asignarse a un host específico en clústeres configurados con vSphere High Availability (HA) o con vSphere Distributed Resource Scheduler (DRS) en modo manual.

7. En la página Revisar detalles, verifique los detalles de la plantilla OVA y haga clic en Siguiente.
8. En la página Configuration, elija una configuración de implementación y haga clic en Next.
9. En la página Select storage, elija la ubicación de almacenamiento de destino para los archivos de VM en el host ESXi seleccionado y haga clic en Next.
10. Elija el Formato de disco para los discos virtuales de VM.



Nota: Se recomienda utilizar el aprovisionamiento grueso. Aunque es posible utilizar el aprovisionamiento dinámico, el compromiso excesivo de almacenamiento puede

provocar una falta de capacidad de almacenamiento, lo que se traduce en una degradación y una pérdida de servicio.

11. En la página Select networks, elija una red de origen y asígnela a una red de destino y haga clic en Next.
12. En la página Ready to Complete, seleccione Power On After Deployment y haga clic en Finish.
13. Asegúrese de que las VM estén configuradas con los siguientes parámetros adicionales. Para ello, haga clic con el botón derecho del ratón en la VM deseada en VMware ESXi y haga clic en Editar parámetros.
 - CPU: Seleccione Bajo en la primera lista desplegable Recursos compartidos.
 - Memoria: Marque la casilla de verificación Reserve all guest memory (All locked)
 - Configure la CPU y la RAM en función del tamaño de la escala; consulte [Requisitos de recursos de hardware y VM](#) para obtener más información
14. En VMware ESXi, seleccione la máquina virtual que desee.
15. Haga clic en la pestaña Summary.
16. Haga clic en la imagen mostrada o en el icono Iniciar consola para iniciar la consola.
17. Consulte [Configuración de red](#) para conocer los siguientes pasos.

Instalación del dispositivo virtual en Microsoft Hyper-V Server

Para instalar el dispositivo virtual en Hyper-V:

1. Inicie sesión en el Administrador del servidor de Hyper-V con credenciales de administrador.
2. Extraiga el paquete VA en la ubicación definida por el administrador de Hyper-V para almacenar todos los discos duros virtuales.
3. Verifique que todos los discos del Cisco IQ .tar.gz original estén en la carpeta Discos duros virtuales.
4. En el panel Acciones del Administrador de Hyper-V, elija Nuevo > Máquina virtual y haga clic en Siguiente.
5. Introduzca el nombre que desea asignar al dispositivo virtual y haga clic en Next.
6. Elija Generation 2 y haga clic en Next.
7. Introduzca el valor de memoria según el tamaño de memoria recomendado en [Hardware and VM Resource Requirements](#) y haga clic en Next.
8. Verifique que Use Dynamic Memory no esté marcado.
9. Elija el adaptador de red adecuado para su dispositivo virtual y haga clic en Next (Siguiente).
10. Agregue el disco duro virtual del dispositivo virtual proporcionado, asegurándose de que el disco uno (1) es el primer disco, y haga clic en Next (Siguiente).



Nota: Los otros dos (2) discos duros virtuales se agregan en un paso posterior.

11. Verifique las selecciones en el Resumen y haga clic en Finalizar. Hyper-V muestra la

máquina virtual recién creada.

12. Haga clic con el botón derecho del ratón en la VM y seleccione Settings.
13. En Seguridad, desmarque la casilla de verificación Habilitar arranque seguro.
14. Agregue los otros dos (2) discos duros virtuales a la máquina virtual repitiendo los mismos pasos utilizados para agregar el primer disco duro.
15. En Funciones avanzadas en el adaptador de red, compruebe que la opción Activar nombre de dispositivo está seleccionada.
16. Establezca el número de procesadores en las vCPU recomendadas, como se indica en [Requisitos de recursos de hardware y VM](#).
17. En el panel Acciones, seleccione Iniciar para encender la VM.
18. En el panel Acciones, seleccione Conectar para conectarse a la máquina virtual. Se muestra la consola de VM Connection.
19. Consulte [Configuración de red](#) para obtener más detalles.

Instalación de Virtual Appliance en Red Hat KVM

Asegúrese de que se cumplen los siguientes requisitos admitidos antes de instalar el dispositivo virtual en el KVM.

- SO host RHEL
- Acceso administrativo en el servidor Red Hat

Para instalar el dispositivo virtual en un hipervisor KVM, se necesita VM Manager.

1. Inicie sesión en el servidor del sistema operativo del host de Red Hat con credenciales de administrador.
2. Descargue y extraiga el paquete VA en el host.
3. Inicie el cliente Virtual Machine Manager (VMM).
4. Elija File > New Virtual Machine en el menú para instalar un nuevo dispositivo virtual.
5. Elija Importar imagen de disco existente y haga clic en Reenviar.
6. En Proporcionar la ruta de almacenamiento existente, haga clic en Examinar.
7. Cree un nuevo grupo de almacenamiento mediante la ruta de acceso en la que extrajo el paquete VA.
8. Elija el primer disco del dispositivo virtual del grupo de almacenamiento creado en el paso anterior y haga clic en Choose Volume.
9. En Elegir un tipo y versión del sistema operativo, elija AlmaLinux 9, y haga clic en Reenviar.
10. En Choose Memory and CPU settings, introduzca los detalles en función del tamaño de la escala y haga clic en Forward. Consulte [Requisitos de recursos de hardware y VM](#) para obtener más información.
11. En el cuadro de diálogo, complete la siguiente configuración:
 1. En Preparado para comenzar la instalación, introduzca un Nombre para la instancia de VA.
 2. Haga clic en la opción Customize configuration before install.

3. En Network selection, asegúrese de seleccionar la red virtual adecuada.
12. Haga clic en Finish para completar la adición del primer disco.
13. Agregue los dos (2) discos restantes:
 1. En la consola VMM, haga clic en Agregar hardware.
 2. En Almacenamiento, asegúrese de que la casilla de verificación Seleccionar o crear almacenamiento personalizado esté marcada y haga clic en Administrar.
 3. Busque y seleccione el segundo disco del archivo VA que ha extraído en el sistema.
 4. Haga clic en Elegir volumen.
14. Repita los mismos pasos (Agregar hardware) para agregar el tercer disco AV.
15. Asegúrese de que todos los tipos de bus de disco sean SCSI.
16. Haga clic en Finish (Finalizar).
17. En la sección Descripción general, elija UEFI para firmware.
18. Haga clic en Comenzar instalación.
19. Consulte [Configuración de red](#) para conocer los siguientes pasos.

Configuración de red

1. Inicie el dispositivo virtual desde la consola VM.



```
***** WARNING!!! *****  
***** READ THIS BEFORE ATTEMPTING TO LOGIN *****  
#  
# This System is for the use of authorized users only. Individuals  
# using this computer without authority, or in excess of their  
# authority, are subject to having all of their activities on this  
# system monitored and recorded by system personnel. In the course  
# of monitoring individuals improperly using this system, or in the  
# course of system maintenance, the activities of authorized users  
# may also be monitored. Anyone using this system expressly  
# consents to such monitoring and is advised that if such  
# monitoring reveals possible criminal activity, system personnel  
# may provide the evidence of such monitoring to law enforcement  
# officials. You cannot copy, disclose, display or otherwise  
# communicate the contents of this server except to other Cisco  
# employees who have been authorized to access this server.  
#  
***** Confidential Information *****  
cisc-infra login: admin  
Password:
```

Inicie sesión

2. Inicie sesión en la consola con las credenciales de red predeterminadas introduciendo "admin" tanto para el nombre de inicio de sesión como para la contraseña. Se muestra el menú principal.

 Nota: Las credenciales predeterminadas se proporcionan solo para la configuración inicial, ya que no hay datos que proteger en esta etapa de la instalación.



Menú principal

3. Introduzca "1" y pulse Intro para configurar los parámetros de red.
4. Proporcione los siguientes parámetros de red:

 Nota: Los usuarios pueden pulsar Intro para utilizar los valores detectados donde estén disponibles.

- Dirección IP
- IP de gateway
- Lista de IP de DNS
- Buscar dominio
- lista de servidores NTP

 Nota: Se admite la entrada de varios servidores NTP con un formato separado por comas.

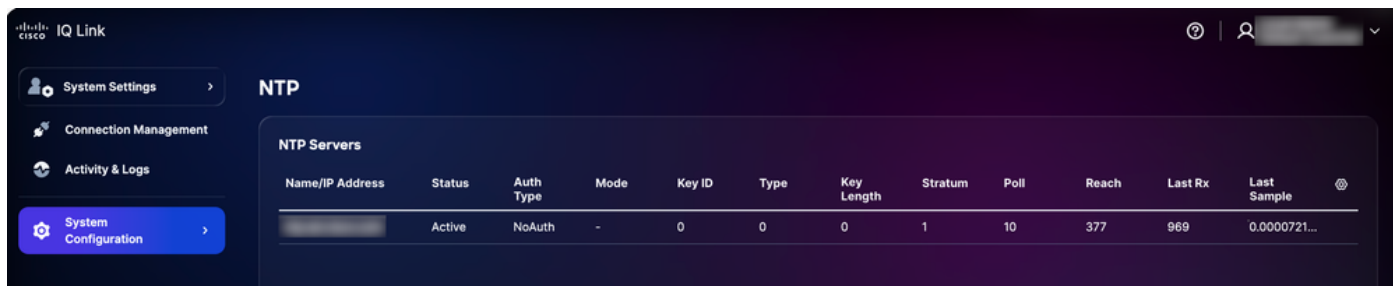
5. Configure la autenticación NTP presionando N para continuar sin un método de autenticación

O

Pulse Y e introduzca el número correspondiente de una de las opciones enumeradas a continuación:

- Autenticación tradicional basada en claves: Utiliza las credenciales proporcionadas para la sincronización horaria segura; después de seleccionar esta opción, introduzca un algoritmo válido y una clave hexadecimal
- Seguridad de tiempo de la red (NTS): Utiliza el protocolo NTS para proporcionar una comunicación NTP segura

 Nota: La información de NTP se puede validar en la interfaz de usuario después de la instalación. Para ello, vaya a Configuración del sistema.



Name/IP Address	Status	Auth Type	Mode	Key ID	Type	Key Length	Stratum	Poll	Reach	Last Rx	Last Sample	
[Redacted]	Active	NoAuth	-	0	0	0	1	10	377	969	0.0000721...	

Validación de NTP en UI

6. Introduzca y confirme una contraseña después de revisar los requisitos de contraseña en pantalla.
7. Revise el resumen y pulse Y para continuar. La configuración puede tardar varios minutos.
8. Una vez recibido el mensaje de confirmación, pulse Intro para volver al menú principal.



Menú de Cisco IQ

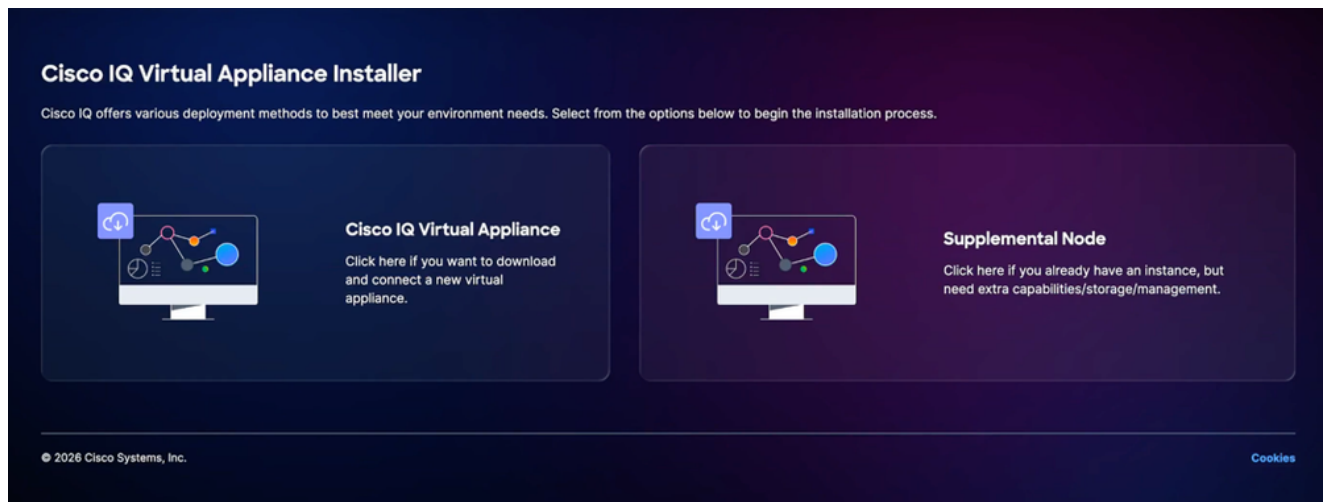
Los parámetros de red ya están configurados, pero el dispositivo virtual aún no se ha instalado. Se recomienda volver al hipervisor y tomar una instantánea de la nueva VM para futuras referencias. En este punto, también puede iniciar una conexión de Secure Shell utilizando la dirección IP y las credenciales recién configuradas.

Esto completa la configuración manual del AV.

Instalación del dispositivo virtual para el modo Air-Gap

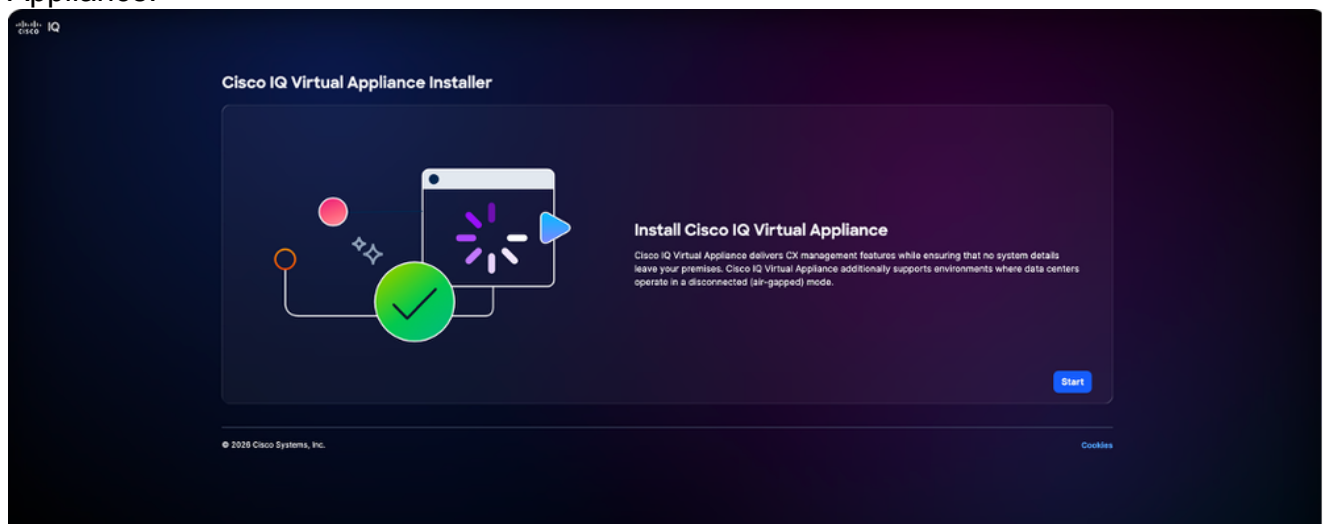
Para instalar VA:

1. Vaya a la interfaz web del instalador de VA (<https://<CIQ-HOST>/installer/welcome>) (se recibe después de configurar el VA en las VM). Se muestra la página Cisco IQ Virtual Appliance Installer.



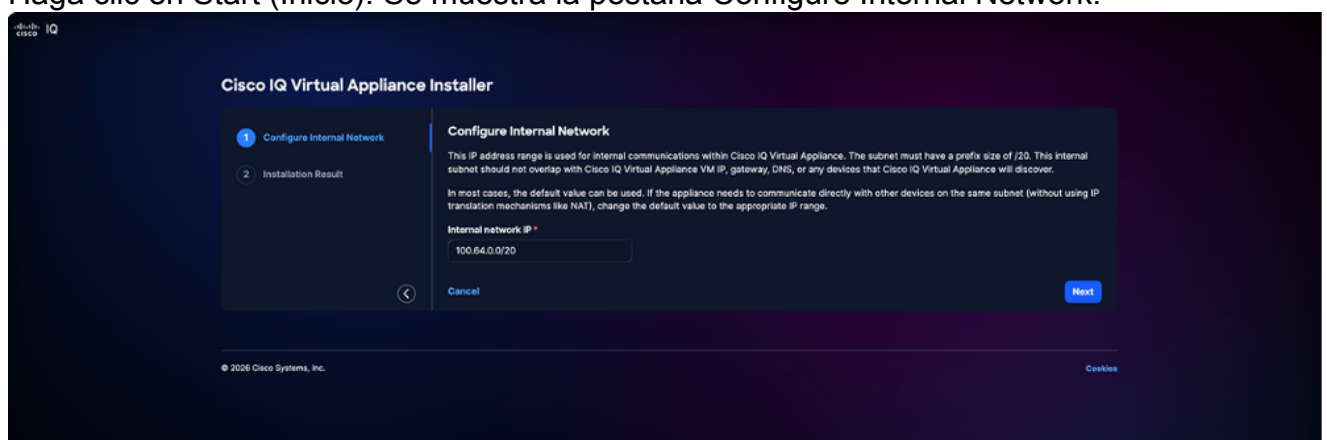
Página Instalador de dispositivo virtual

- Haga clic en Cisco IQ Virtual Appliance. Se muestra la página Install Cisco IQ Virtual Appliance.



Instalación del dispositivo virtual

- Haga clic en Start (Inicio). Se muestra la pestaña Configure Internal Network.

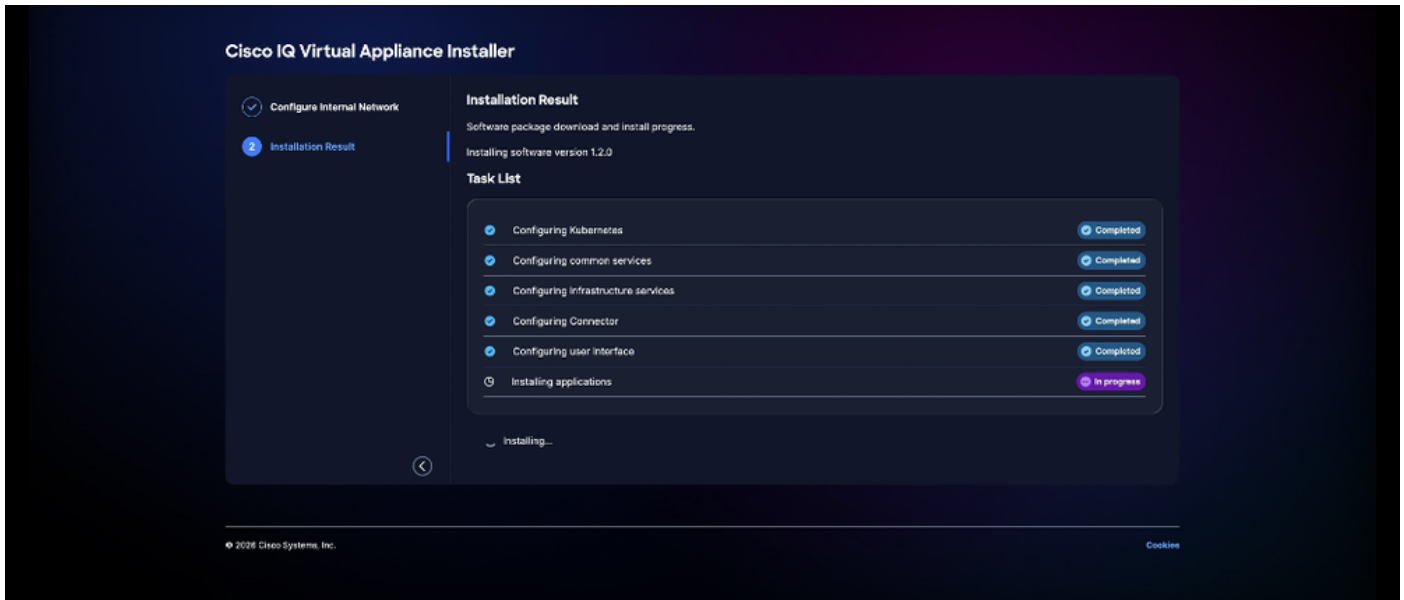


Configuración de la red interna

- Introduzca el intervalo IP interno.

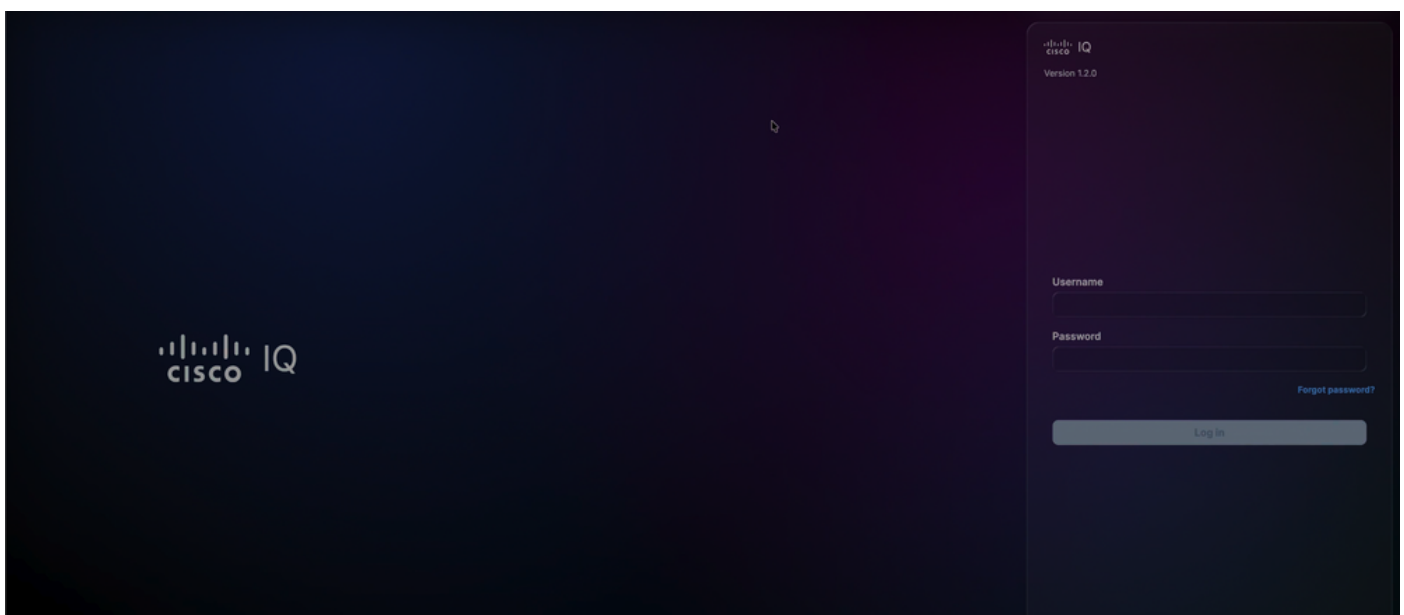
 Nota: Asegúrese de que la subred interna no se superpone con la IP de la máquina virtual, la puerta de enlace, el DNS o los rangos de red alcanzables.

5. Haga clic en Next. Se muestra la página Resultado del instalador.



Resultado de instalación

6. Espere hasta que se hayan completado todas las tareas mostradas. Una vez completada correctamente, el navegador se desplaza automáticamente a la página de inicio de sesión del dispositivo virtual de Cisco IQ. La finalización de la instalación puede tardar hasta dos (2) horas.



Inicio de sesión

Una vez que haya iniciado sesión correctamente, el sistema estará listo para detectar dispositivos

y admitirá la aplicación Assets sin compatibilidad con IA.

Instalación de módulos y reglas

Para ampliar las capacidades del sistema, puede descargar módulos y reglas adicionales directamente desde el portal SaaS de Cisco IQ y completar la instalación en VA. Consulte Instalación de paquetes en la [Guía de operaciones](#) para obtener más detalles.



Nota: El módulo Assets está preinstalado en el instalador de VA y está disponible para su uso inmediato. Puede actualizar el módulo de activo o la versión de regla de activo como cualquier otro módulo y regla, según sea necesario.

Funciones alimentadas por IA

Cisco IQ ofrece un modelo de implementación flexible que incluye una función complementaria alimentada por IA para mejorar la información de los clientes y las capacidades de automatización. Cisco IQ VA se puede instalar con o sin compatibilidad con GPU.

Implementación de appliances virtuales sin compatibilidad con GPU (funciones no relacionadas con la IA)

1. Inicie sesión en [Cisco IQ](#).
2. Vaya a System Settings > Package Catalog para descargar el instalador de VA de Cisco IQ y el instalador de los módulos de Cisco IQ que desee. Consulte Instalación de paquetes en la [Guía de operaciones](#) para obtener más detalles.
3. Asigne recursos de IP y VM e implemente la VM. Se requiere un mínimo de una (1) VM para la carga de trabajo de la CPU.
4. Instale el instalador del dispositivo virtual de Cisco IQ para preparar el sistema. Consulte [Instalación de Virtual Appliance Setup](#) para obtener más detalles.
5. Una vez instalado, inicie sesión en la interfaz de usuario de Cisco IQ VA.
6. Instale los módulos descargados navegando hasta System Settings > Package Management en VA. Consulte Instalación de paquetes en la [Guía de operaciones](#) para obtener más detalles.

El sistema ya está listo para su uso sin soporte de IA.

Implementación de appliances virtuales compatibles con GPU (funciones habilitadas para IA)

Para habilitar las funciones alimentadas por IA, el sistema debe configurarse como "AI Ready".

Prerequisites

- Asegúrese de que el nodo principal esté completamente configurado y en funcionamiento.
- Revise los requisitos de hardware de la GPU y seleccione un nodo complementario con capacidades de la GPU. Consulte [Requisitos de Recursos de Funciones AI](#) para obtener más información.
- Siga el procedimiento de implementación de varios nodos y designe el nodo suplementario como nodo de GPU. Para obtener más información, consulte [Adición de Soporte de Nodo y Nodo Múltiple](#).

Implementación compatible con GPU (funciones habilitadas por IA)

1. Inicie sesión en [Cisco IQ](#).
2. Vaya a System Settings > Package Catalog para descargar Cisco IQ VA Installer, los módulos de Cisco IQ deseados y Cisco IQ AI Inference Infrastructure. Consulte Instalación de paquetes y funciones alimentadas por IA en la [Guía de operaciones](#) para obtener más detalles.
3. Asigne IP y recursos de VM e implemente las VM. Se requieren un mínimo de dos (2) VM: una (1) para la carga de trabajo de la CPU y una (1) para la carga de trabajo de la GPU.
4. Instale el instalador del dispositivo virtual de Cisco IQ para preparar el sistema. Consulte [Instalación de Virtual Appliance Setup](#) para obtener más detalles.
5. Una vez instalado, inicie sesión en la interfaz de usuario de Cisco IQ VA.
6. Instale la infraestructura de inferencia de IA navegando hasta System Settings > Package Management. Consulte Funciones alimentadas por IA en la [Guía de operaciones](#) para obtener más detalles.
7. Instale cualquier módulo adicional descargado navegando hasta System Settings > Package Management. Consulte Agregar módulos en la [Guía de operaciones](#) para obtener más detalles.

El sistema ya está listo para su uso con funciones alimentadas por IA.

Para obtener más información sobre cómo habilitar las funciones alimentadas por IA, consulte la [Guía de operaciones](#).

Compatibilidad con varios nodos

La arquitectura de varios nodos permite ampliar un dispositivo virtual independiente en un clúster, lo que proporciona una mayor capacidad de recursos para el procesamiento y la implementación

de aplicaciones. Esta configuración permite agregar nodos complementarios a un nodo de gestión principal, lo que permite ampliar el sistema en función de los requisitos de carga de trabajo específicos.

Habilitar la capacidad de varios nodos es esencial para agregar un nodo de GPU. Esta integración permite que el entorno en las instalaciones aproveche los recursos de la GPU para la inferenciación de IA. Esta sección proporciona una guía detallada sobre la conexión de la GPU como un nodo complementario para el On-Prem, que es necesario para que los usuarios utilicen las capacidades de la GPU de manera eficaz.

Requisitos de la red

VA admite una única interfaz de red. Consulte [Requisitos de red](#) para obtener información detallada.

Requisitos de puerto

En la tabla siguiente se describen los puertos de red necesarios para la comunicación del VA de Cisco IQ en un entorno de varios nodos.

Tabla 4: Requisitos de puertos de varios nodos

Puerto(s)	Protocolo	Descripción	Tipo de nodo
22	TCP	Se utiliza para sesiones de depuración de la CLI del administrador y de soporte de Cisco	Nodos de gestión y suplementarios
443	TCP	Se utiliza para la comunicación entre Cisco IQ On-Prem y los navegadores web, así como los destinos de terminales	Nodos de gestión y suplementarios
53, 123, 161	UDP	Se utiliza para enviar y recibir tráfico DNS, NTP y SNMP	Nodos de gestión y suplementarios
10250, 10256	TCP	Se utiliza para la comunicación de Kubernetes entre el nodo	Nodos de gestión y suplementarios
179	TCP	Se utiliza para el plano de control VXLAN (BGP)	Nodos de gestión y

		entre nodos	suplementarios
4789	UDP	Se utiliza para el tráfico VXLAN entre nodos	Nodos de gestión y suplementarios
500, 4500	UDP	Se utiliza para el tráfico IKE IPsec entre nodos	Nodos de gestión y suplementarios
Todos	ESP (50)	Se utiliza para el tráfico IPsec ESP entre nodos	Nodos de gestión y suplementarios
6443	TCP	Utilizado para el servidor API de Kubernetes	Sólo nodo de administración



Nota: La agrupación en clústeres de varios nodos solo es compatible con implementaciones de AV estándar.



Nota: Un nodo suplementario debe tener exactamente la misma versión que el nodo de administración principal durante el proceso de unión inicial.



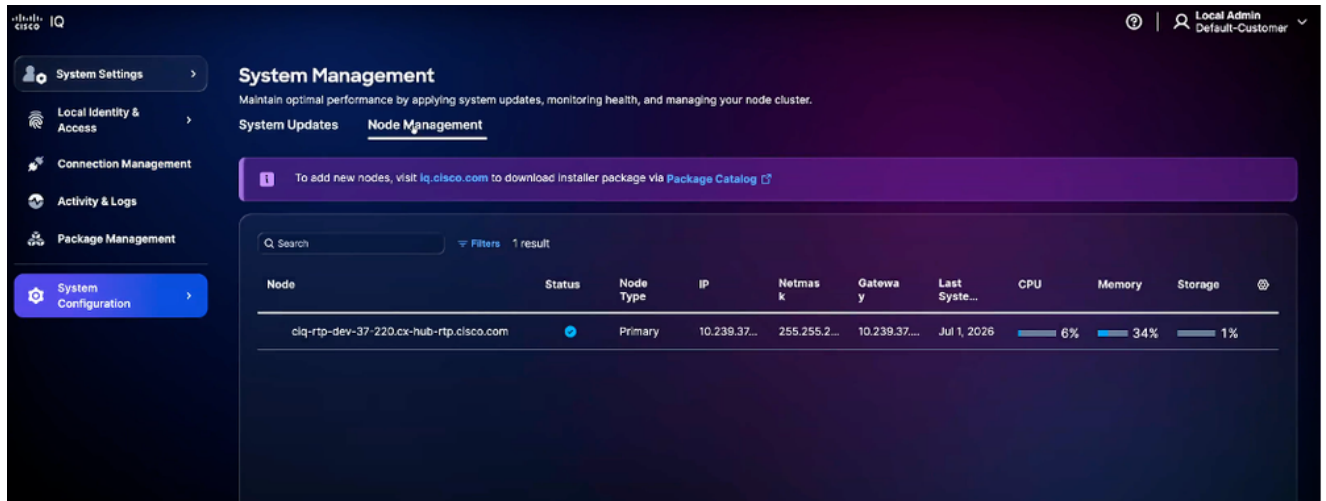
Nota: La implementación actual de varios nodos no proporciona alta disponibilidad (HA) para el plano de gestión. Si el nodo de administración principal deja de estar disponible, las operaciones del clúster se verán afectadas.

Adición de un nodo adicional

La adición de un nodo complementario requiere el mismo proceso que la instalación del dispositivo virtual. Una vez que haya descargado el instalador de AV del catálogo de paquetes de Cisco IQ (SaaS), instálelo en el hipervisor seleccionado. Consulte [Instalación de Virtual Appliance Setup](#) para obtener más detalles.

Antes de agregar un nodo suplementario, asegúrese de que el primer nodo esté completamente configurado como un dispositivo virtual estándar. Para agregar un nodo suplementario:

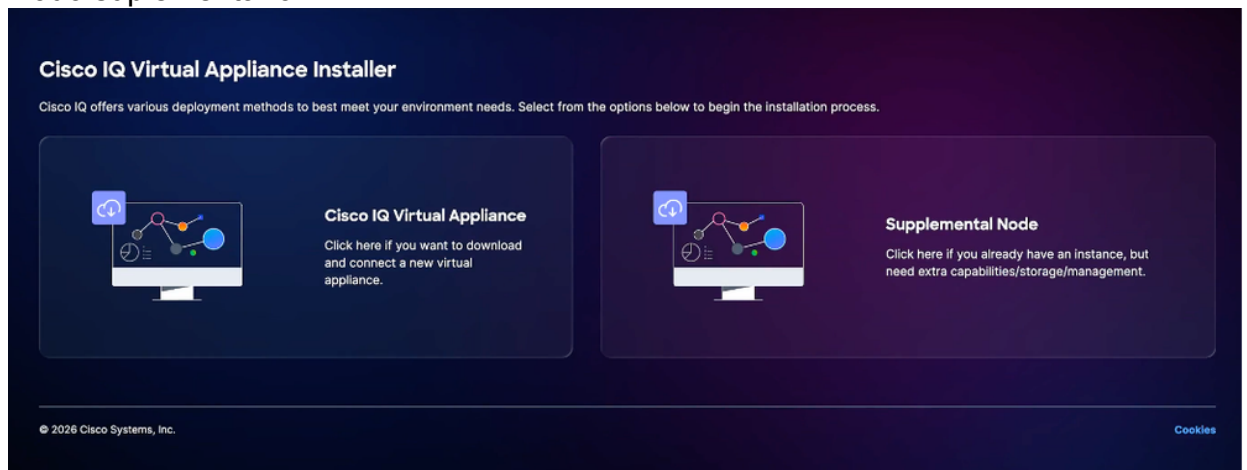
1. Vaya a System Configuration > Node Management.
2. Verifique que se muestre el nodo principal en la columna Nodo con el estado correcto.



Gestión de nodos

3. Vaya al instalador del dispositivo virtual. Se muestran las siguientes opciones:

- Dispositivo virtual Cisco IQ
- Nodo suplementario



Nodo suplementario

4. Haga clic en la opción Nodo suplementario. Se muestra la página Instalador de Nodo Suplementario.

Supplemental Node Installer

Connect to node

Select an action and provide your credentials to establish connection to your cluster.

Primary node FQDN

Local admin username

Password

 [Show](#)

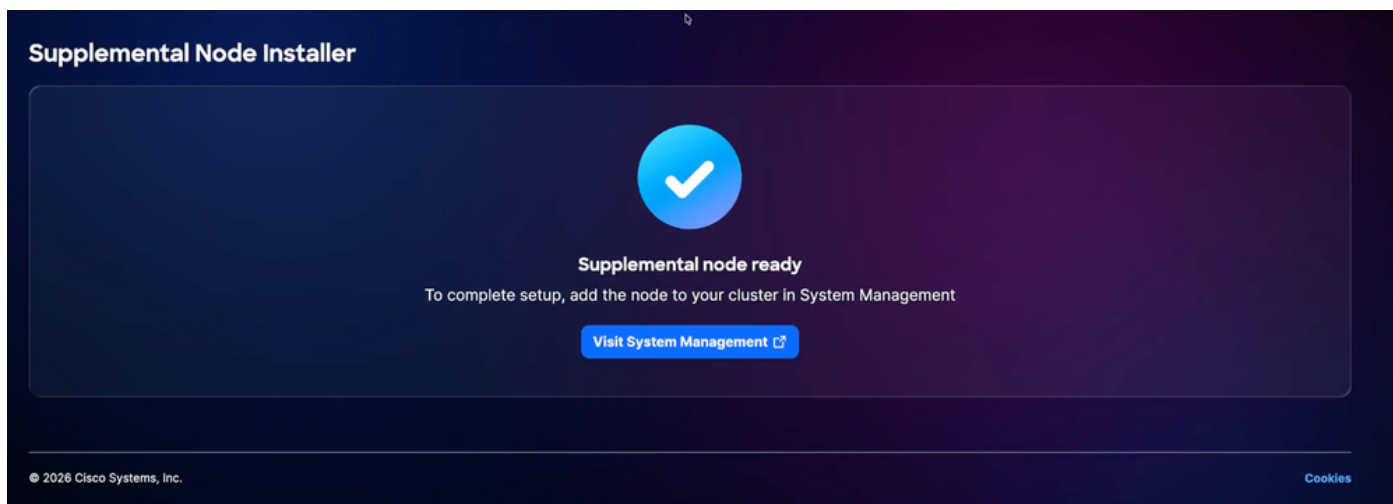
Node type

Página Nodo Complementario

5. Introduzca el FQDN del nodo principal.
6. Ingrese el nombre de usuario del administrador local.
7. Ingrese la contraseña.
8. Elija Tipo de nodo en la lista desplegable.

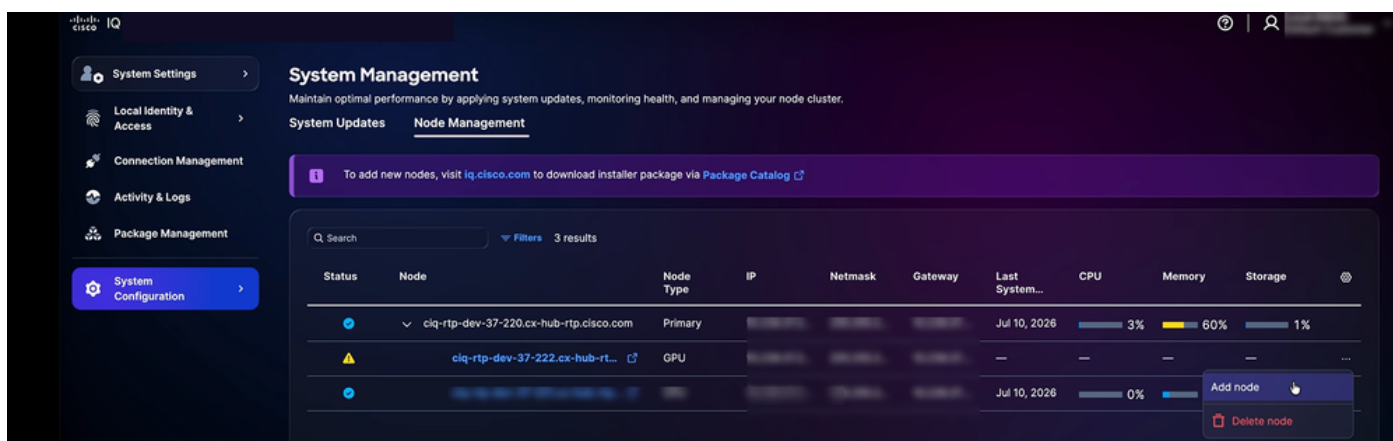
 Nota: Puede elegir el nodo de trabajo de GPU. Al elegir nodos de trabajo de GPU, asegúrese de que el entorno de hipervisor (por ejemplo, VMware o Hyper-V) esté configurado con el hardware necesario para admitir dispositivos de GPU, ya que son necesarios para la accesibilidad de los nodos de GPU. Consulte [Opciones de implementación](#) para obtener más información.

9. Haga clic en Agregar nodo. El mensaje "Nodo suplementario preparado" se muestra después de agregar correctamente el nodo.



Nodo suplementario preparado

10. Cuando aparezca "Nodo suplementario preparado", haga clic en el enlace Visitar administración del sistema o navegue hasta Administración del sistema > Administración de nodos para desencadenar la acción de agregar nodo y completar la integración.



Agregar nodo

11. Haga clic en el icono del menú Más > Agregar nodo. Se muestra la ventana Add GPU Node.

Add GPU node

Adding GPU node will initiate cluster expansion. This action typically takes 30 minutes, and the system will remain available during this process.

Note: Once added, this node's admin credentials will automatically synchronize with the primary node, overwriting any existing local credentials.

Cancel

Add GPU node 

Agregar nodo de GPU

12. Haga clic en Agregar nodo GPU. Una vez agregado correctamente el nodo, se muestra en el clúster.

Administración y sincronización de clústeres

Al agregar un nodo de trabajo, las credenciales administrativas del nodo de administración principal se sincronizan automáticamente con el nodo de trabajo. El acceso al nodo de trabajo debe realizarse con estas credenciales sincronizadas.



Nota: El clúster administra dinámicamente la distribución de aplicaciones. Cuando una aplicación requiere capacidades de procesamiento avanzadas, el sistema comprueba la disponibilidad de los nodos habilitados para GPU. Si hay un trabajador de GPU y se ha instalado el paquete de aplicación adecuado, el sistema habilita estas funciones avanzadas. Si el clúster carece de los recursos de hardware necesarios, el sistema funcionará en modo no acelerado para mantener la estabilidad.

Support

Puede crear casos de asistencia específicos de módulos y de dispositivos virtuales desde Cisco IQ SaaS. El módulo Support está disponible en Cisco IQ SaaS y ofrece una vista consolidada de sus casos de soporte. Permite filtrar, ordenar y personalizar la vista de lista de casos, lo que proporciona visibilidad tanto de los casos abiertos como de los cerrados a los que tiene derecho de acceso. Para obtener información más detallada sobre el módulo Support en Cisco IQ SaaS, consulte la [Guía de inicio de Cisco IQ SaaS](#).



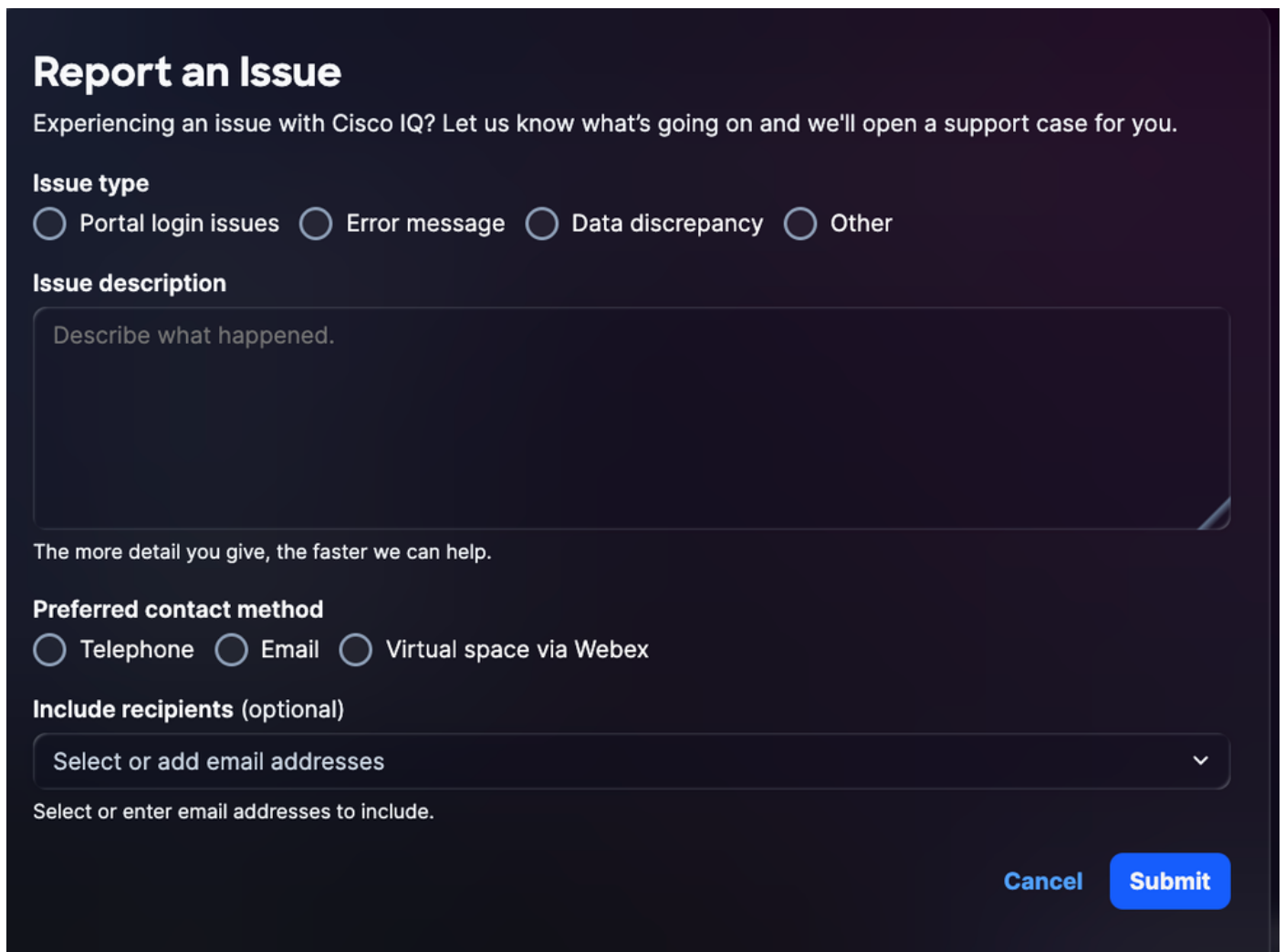
Nota: Los clientes de VA de Cisco IQ pueden acceder a la mayoría de las funciones del módulo de soporte SaaS de Cisco IQ, incluidos los casos de apertura del Technical

Assistance Center (TAC) relacionados con el VA de Cisco IQ y sus módulos, así como la creación y gestión de casos de productos.

Creación de un caso de soporte

Puede crear casos específicos de módulo y VA en Cisco IQ SaaS. Para crear un caso:

1. Inicie sesión en [Cisco IQ \(SaaS\)](#).
2. Haga clic en el icono Ayuda > Informar sobre un problema. Se abre la ventana Informar sobre un problema.



Report an Issue

Experiencing an issue with Cisco IQ? Let us know what's going on and we'll open a support case for you.

Issue type

☐ Portal login issues ☐ Error message ☐ Data discrepancy ☐ Other

Issue description

Describe what happened.

The more detail you give, the faster we can help.

Preferred contact method

☐ Telephone ☐ Email ☐ Virtual space via Webex

Include recipients (optional)

Select or add email addresses

Select or enter email addresses to include.

Cancel Submit

Informar sobre un problema

3. Proporcione los detalles necesarios.
4. Haga clic en Submit (Enviar).

Apéndice A

BOM de referencia para appliance virtual in situ con GPU

A continuación se muestra la lista de materiales de referencia (BOM) para el AV in situ que admite hasta 10 000 dispositivos:

Tabla 5: BOM de referencia

Número de Pieza	Descripción	Cantidad
UCS-M8-MLB	RACK UCS M8 MLB	1
UCSC-C240-M8SX	Rack UCS C240 M8 sin CPU, memoria, unidades, 2 U con placa base SFF	1
CON-L1NCO-UCSCCX4S	CX LEVEL 1 8X7XNCDOS UCS C240 M8 Rack con dos CPU, mem, unidades, 2	1
RHEL-2S2V-D3A	Red Hat Enterprise Linux (1-2 CPU, 1-2 VN); Solicitud de asistencia de 3 años	1
CON-ISV1-RHEL62S2	ISV 24X7 Red Hat Enterprise Linux 1-2 CPU, 1-2 VN	1
COMPUTE-AI	Caso práctico de informática de inteligencia artificial	1
GESTIONADO POR ISM	Modo de implementación para servidores de la serie C en modo independiente	1
UCSC-GPUAD-240M8	CONDUCTO DE AIRE GPU PARA C240M8	1
UCSC-M-V5Q50GV2-D	Cisco VIC 15427 4x 10/25/50G mLOM serie C con arranque	1

	seguro	
UCS-TPM-002D-D	TPM 2.0 TCG FIPS140-2 CC+ Cert M7 Compatible con Intel MSW2022	1
UCSC-RAIL-D	Kit de raíles de cojinete de bolas para servidores en rack C220 y C240 M7/M8	1
CIMC-LATEST-D	Versión más reciente de IMC SW (recomendado) para servidores C-Series	1
UCSC-HSLP-C220M8	Disipador térmico para C220M8, C240M8L y C240M8 con GPU	2
UCS-DDR5-BLK	DIMM en blanco UCS DDR5	24
UCSC-BBLKD-M7	Panel de obturación de la unidad UCS C-Series M7 SFF	20
CBL-RAID16-240M8	Cable MB C240M8 Y a RAID16/HBA	1
CBL-NVME-240M8-P4	Cable NVMe C240M8SFF para unidad 1-4 (P4)	1
CBL-NVME-240M8-P2	Cable NVMe C240M8SFF para unidad 21-24 (P2)	1
UCSC-SDBKT-24XM7	Soporte de controlador RAID SD UCS C-Series M7 2U	1
CBL-G5GPU-C240M7	Cable de alimentación de 12 VHPWR compatible con C240M7 PCIe CEM (hasta 450 W)	1

UCS-MRX64G2RE5	RDIMM 64 GB DDR5-6400, 2 Rx4 (16 Gb)	4
UCSC-RIS1A-240M8	Tarjeta vertical UCS C240 M8 1A PCIe Gen5 (x8, x16, x8)	1
UCSC-RIS2A-240M8	Tarjeta vertical UCS C240 M8 2A PCIe Gen5 (x8, x16, x8) (CPU2)	1
UCSC-RIS3C-240M8	Tarjeta vertical UCS C240 M8 3C PCIe Gen5 (x16) (CPU2)	1
UCSC-RAID-MP1L32	Controladora RAID MP1 trimodo 24G con 4 GB FBWC 32Drv con soporte 2U	1
UCSC-GPU-RTXP6000	NVIDIA RTX Pro 6000: GPU FHFL de 600 W, 96 GB y 2 ranuras	1
NV-GRID-OPT-OUT	EXCLUSIÓN DE NVIDIA GRID SW	1
UCS-M2-HWRAID2	Controlador Raid M.2 optimizado para arranque de Cisco para unidades SATA	1
UCS-M2-480G-D	SSD SATA M.2 de 480 GB	2
UCSC-M2I-240M8	Módulo M.2 interno UCS C240 M8	1
UCS-SDB1T9SA1VD	1,9 TB 2,5" SATA 6G 1X Samsung G1PM893A SSD	4
UCS-CPU-I6520P	Intel I6520P 2,4 GHz/210 W 24 núcleos/144 MB DDR5 6400 MT/s	2

UCSC-PSU1-2300W-D	Fuente de alimentación de CA de Cisco UCS 2300 W para servidores en rack Titanium	2
CAB-C19-CBN	Cable de alimentación del puente de armario, 250 V CA 16 A, conectores C20-C19	2
UCSC-RISAB-24XM7	Solo GPU de bloqueador de aire UCS C-Series M7 2U	2
DC-MGT-SAAS	Cisco Intersight SaaS	1
DC-MGT-ISSAAS-ES	Servicios de infraestructura SaaS/CVA: Essentials	1
SVS-DCM-SUPT-BAS	Cisco Support Basic para DCM	1
DC-MGT-UCSC1S	UCS Central por servidor: licencia de 1 servidor	1
DC-MGT-ADOPT-BAS	Entrevista: sesión de adopción virtual http://cs.co/requestCSS	1

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).