

Notas de la versión del dispositivo virtual Cisco IQ v1.2.4

Introducción

Cisco IQTM proporciona a los clientes funciones diseñadas para mejorar la visibilidad de los recursos y ofrecer una perspectiva más inteligente de sus entornos. 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 agiliza los procesos para la participación y el éxito de los clientes.

Cisco IQ On-Prem Air-Gapped es el modo de implementación de Cisco IQ diseñado para entornos que no se pueden conectar a la nube. Se suministra como una máquina virtual (VM) independiente, denominada dispositivo virtual Cisco IQ (VA), que se ejecuta completamente en las instalaciones del cliente, sin depender en absoluto de las redes externas, con actualizaciones de software y paquetes de mantenimiento obtenidos de Cisco IQ SaaS y transferidos al VA a través de un proceso aprobado y manual.

Para las organizaciones que operan en entornos regulados, de alta seguridad y soberanos, el AV elimina el equilibrio entre la perspectiva y el control. Los clientes implementan las funciones de evaluación y activos de Cisco IQ dentro de su propia red y conservan la propiedad completa de sus datos, a la vez que obtienen la información y las recomendaciones que esperan de Cisco IQ. El modo de implementación Air-Gap amplía las funciones de Cisco IQ SaaS a entornos aislados, lo que permite a los equipos más importantes funcionar con la velocidad y la inteligencia de diagnóstico de las empresas conectadas a la nube.

Este documento describe las nuevas funciones, la compatibilidad de módulos y los problemas conocidos de Cisco IQ VA v1.2.4.

Puntos destacados clave

Módulo de recursos

El módulo Assets ofrece funciones de gestión y visibilidad completas para los recursos de Cisco y sirve de base para Cisco IQ, ya que proporciona una lista centralizada de todos los dispositivos de una organización. Al recopilar información de varias fuentes, actúa como una única fuente

fidedigna para el inventario de dispositivos. Está disponible como parte del instalador descargado y está disponible para su uso una vez instalado el dispositivo virtual. Los aspectos más destacados son:

Perspectivas sobre la importancia de activos

Asset Criticality Insights permite al módulo Assets predecir la función funcional y la importancia empresarial de los dispositivos de red. Al analizar las configuraciones de los dispositivos y las funciones habilitadas, Asset Criticality Insights le ayuda a identificar qué recursos tienen el mayor impacto en su red, lo que le permite priorizarlos para la remediación de la seguridad, las actualizaciones de software, la planificación del fin de vida útil/fin de soporte técnico y las decisiones sobre la cobertura.

Contratos de servicio

La página Service Contracts proporciona una supervisión centralizada de los contratos de asistencia. Entre las funciones principales se incluyen:

- Supervisión de contratos de servicio: Simplifique la planificación de renovaciones y las estrategias de cobertura con resúmenes de contratos completos y datos detallados.
- Información específica de los recursos: Identifique y mitigue las vulnerabilidades más rápidamente con datos claros y procesables vinculados directamente a sus recursos

Panel LDOS

El panel de fecha final de soporte técnico (LDOS) proporciona una vista centralizada de los hitos de LDOS y permite mejorar la planificación de recursos y la previsión de presupuestos antes de que el hardware o el software alcancen el fin de su vida útil, lo que le permite reducir significativamente el riesgo operativo.

Etiquetado de recursos

El etiquetado de activos proporciona una forma flexible de organizar, filtrar y actuar en su inventario mediante etiquetas personalizadas. Las etiquetas se pueden crear, modificar y asignar a recursos, con una gestión de etiquetas centralizada disponible para los administradores de cuentas. Puede asignar etiquetas a activos individuales o de forma masiva, así como filtrar el inventario por etiquetas para localizar rápidamente los activos deseados.

Módulo de evaluaciones

El módulo Evaluaciones proporciona visibilidad de su inventario mediante la evaluación de los recursos de su organización y ofrece un marco que le permite investigar y mitigar de forma proactiva los riesgos relacionados con la seguridad, la estabilidad, la capacidad, el cumplimiento y la antigüedad, lo que ayuda a mantener la seguridad de las redes. Los aspectos más destacados son:

Avisos de seguridad

Los consejos de seguridad integrados le permiten adelantarse a las amenazas potenciales. El sistema hace frente de forma proactiva a las vulnerabilidades relevantes, garantizando que se le informa de las actualizaciones críticas y que puede tomar medidas inmediatas para proteger su red.

Refuerzo de seguridad

La protección de la seguridad proporciona una visibilidad automatizada y en tiempo real de la condición en materia de seguridad de su infraestructura de red mediante la evaluación continua de sus recursos frente a las guías de protección de Cisco OS. Cada regla de refuerzo de la seguridad se evalúa en todos los recursos cubiertos para detectar desviaciones de la configuración, con conclusiones que se ordenan según la gravedad para ayudarle a abordar las brechas de seguridad, mejorar la resistencia y reducir el riesgo operativo

Configuración

Evalúe sus recursos frente a las prácticas recomendadas, basadas en la experiencia demostrada de Cisco, para detectar desviaciones de la configuración en toda su infraestructura que puedan afectar a la disponibilidad, la seguridad o el rendimiento. El sistema evalúa cada regla de prácticas recomendadas en los activos cubiertos, priorizando las conclusiones por gravedad para ayudarle a garantizar la coherencia de la configuración, mejorar la resistencia y reducir el riesgo operativo.

Field Notices

Los avisos de campo proporcionan notificaciones proactivas y oportunas sobre las actualizaciones de hardware y software. Al mostrar avisos de campo relevantes directamente en el panel Evaluaciones, esta función permite solucionar posibles problemas antes de que afecten a las operaciones.

Funciones alimentadas por IA

El VA de Cisco IQ ofrece funciones impulsadas por IA, que aportan información de IA de nivel SaaS directamente a su entorno con espacios abiertos. Aumenta el coeficiente intelectual de Cisco al transformar los datos sin procesar en información práctica, recomendaciones y acciones guiadas. Las funciones alimentadas por IA requieren un nodo equipado con una unidad de procesamiento de gráficos compatible. Estas funciones no se pueden habilitar en implementaciones solo de CPU. Las funciones incluyen:

- Ask AI Interface: Acceda a información interactiva basada en IA directamente dentro de los módulos Activos e Inventario.
- LDOS: Puede examinar una lista de avisos predefinidos para obtener resúmenes, identificar activos críticos o analizar familias de productos para activos LDOS
- Datos clave: Transforme los datos de activos y evaluaciones en información práctica y recomendaciones. Integrado en los flujos de trabajo para ofrecer información e informes en tiempo real

Gestión del ciclo de vida del software

Puede gestionar el ciclo de vida del software (instalación y configuración) de los módulos operativos, las reglas, los derechos y las funciones especializadas alimentadas por IA dentro del AV. Puede instalarlos descargando las versiones más recientes de Cisco IQ (SaaS) en System Settings (Configuración del sistema) > Package Catalog (Catálogo de paquetes).

Conector de Cisco IQ

Cisco IQ VA está equipado con un completo conector Cisco IQ, que permite una recopilación de datos de telemetría flexible desde conexiones directas a dispositivos y desde dispositivos gestionados a través de Cisco Catalyst Center para mejorar la gestión y la visibilidad de la red. Los aspectos más destacados son:

Definición de dispositivos

Cisco IQ VA proporciona opciones flexibles para definir el alcance del dispositivo. Puede especificar dispositivos cargando un archivo CSV, introduciendo manualmente una lista separada por comas, utilizando rangos de IP o aprovechando CDP (Cisco Discovery Protocol) o LLDP (Link Layer Discovery Protocol). Esta lista se puede actualizar en cualquier momento para agregar o quitar dispositivos, lo que garantiza que los grupos de dispositivos permanezcan actualizados.

Programación de descubrimiento y recopilación

Cisco IQ VA permite la programación independiente de los procesos de detección y recopilación,

lo que permite establecer fechas, horas y patrones de recurrencia específicos. Puede configurar estas tareas por separado para alinearlas con sus flujos de trabajo operativos. Además, puede realizar la redetección a demanda para dispositivos individuales en cualquier momento, lo que proporciona un mayor control sobre los ciclos de actualización de datos y tiempos de respuesta más rápidos para la resolución de problemas.

Hipervisores admitidos

Cisco IQ VA admite la implementación en las siguientes plataformas de hipervisor. Asegúrese de que su infraestructura cumple los requisitos de versión mínimos para su hipervisor específico antes de iniciar la implementación.

- VMware ESXi: compatible con entornos virtualizados estándar
- Microsoft Hyper-V Server: compatible con pilas de virtualización basadas en Windows
- VM basada en Red Hat Kernel: compatible con entornos de virtualización de código abierto

Compatibilidad con varios nodos sin HA

Cisco IQ VA admite una arquitectura de varios nodos que no sea de alta disponibilidad (HA), lo que permite una mayor escalabilidad y flexibilidad para sus entornos de implementación. El nodo múltiple ofrece una arquitectura distribuida que separa las funciones de gestión y de trabajo, lo que le permite adaptar y ampliar su infraestructura más allá de un único dispositivo virtual para satisfacer las demandas de cargas de trabajo más complejas y de mayor tamaño. El nodo de administración sirve como interfaz principal para el registro del clúster, la instalación de la plataforma y la supervisión posterior a la instalación.

Administración de Usuario

Las siguientes funciones tienen como objetivo simplificar los procesos de gestión de usuarios, lo que proporciona un mejor control y seguridad para los usuarios dentro del sistema.

Administración de usuarios local

Los usuarios pueden incorporar y administrar varios usuarios de forma segura con distintos privilegios de acceso. Los usuarios locales creados por un administrador pueden utilizar la opción Sign Up durante su primer inicio de sesión y establecer de forma segura sus propias contraseñas utilizando la dirección de correo electrónico configurada por el administrador.

Administración de seguridad de autoservicio

Ahora puede administrar la configuración de seguridad local de forma independiente, lo que proporciona control sobre el acceso a la cuenta y la recuperación. Las funciones de autoservicio incluyen la capacidad de restablecer contraseñas olvidadas y configurar preguntas de seguridad, lo que permite una experiencia de usuario más sencilla y segura sin necesidad de asistencia externa.

Configuración de SAML para Secure SSO

Cisco IQ VA admite funciones de inicio de sesión único (SSO) seguras mediante la integración de la autenticación de Lenguaje de marcado de aserción de seguridad (SAML) v2.0. Esta integración permite una federación de identidades perfecta con proveedores de identidad de terceros (IDP), lo que le permite autenticarse con sus credenciales empresariales existentes. Al aprovechar SAML v2.0, las organizaciones pueden mejorar la seguridad, agilizar el acceso de los usuarios y simplificar la gestión de identidades en sus entornos. Solo un (1) IDP puede estar activo en un momento dado. Los siguientes IDPs están soportados actualmente:

- Okta IDP
- IDP de ADFS
- Introducir IDP

Registros de actividad

Todos los registros operativos se almacenan localmente y los pueden ver los administradores de cuentas, lo que permite supervisar fácilmente las actividades de los usuarios y garantiza la transparencia.

Compatibilidad con NTP seguro y estándar

Cisco IQ VA admite el protocolo de tiempo de la red (NTP) seguro y estándar. El NTP seguro permite la sincronización de tiempo autenticado y cifrado entre el VA de Cisco IQ y los servidores NTP de confianza, mientras que el NTP estándar ofrece sincronización para entornos en los que la autenticación no es necesaria o no es compatible con intercambios NTP cifrados.

Compatibilidad con certificados SSL personalizados

Cisco IQ VA admite la instalación y la gestión de certificados SSL personalizados. Esta función permite a los administradores de cuentas sustituir los certificados predeterminados por los emitidos por la autoridad de certificación (CA) de su organización. Mediante el uso de certificados personalizados, puede garantizar una comunicación segura y de confianza y mantener el pleno cumplimiento de las políticas de seguridad internas de su organización. Actualmente, solo se

puede instalar y activar un (1) certificado SSL en un momento dado.

Compatibilidad con servidores Syslog externos

Cisco IQ VA admite la integración con servidores Syslog externos, lo que permite a los administradores de cuentas reenviar los registros del sistema a una plataforma de registro centralizada. Esta mejora simplifica la supervisión, la auditoría y la resolución de problemas al proporcionar una vista consolidada y persistente de los registros de seguridad y eventos del sistema en toda la infraestructura. Se pueden configurar hasta dos (2) servidores syslog en cualquier momento.

Inicio de sesión y banner personalizado

Cisco IQ VA ofrece ahora una función de banner configurable. Los administradores de cuentas pueden configurar y mostrar las notificaciones obligatorias del sistema y las advertencias de seguridad en la pantalla de inicio de sesión. Además, los administradores de cuentas pueden configurar y mostrar banners personalizados en Cisco IQ VA. Esta función permite la comunicación de información importante (por ejemplo, notificaciones, renuncias de responsabilidad o alertas) directamente a los usuarios del VA de Cisco IQ.

Administración del sistema

Puede ver e instalar las actualizaciones más recientes del VA de Cisco IQ a través de la pestaña Administración del sistema, que proporciona un acceso sencillo a las funciones, mejoras y mejoras más recientes. Cisco IQ VA admite actualizaciones de software automáticas enviadas desde Cisco IQ y actualizaciones de software manuales. Para las actualizaciones manuales, puede descargar los paquetes de software directamente desde Cisco IQ (SaaS) accediendo a System Settings > Package Catalog.

Problemas conocidos

Los siguientes problemas se están abordando de forma activa en el VA de Cisco IQ.

El Campo Programación Recurrente Muestra La Sintaxis Cron De UNIX

Actualmente, la entrada de programación recurrente para cargas de archivos de análisis de red requiere una expresión cron de UNIX con cinco (5) campos (por ejemplo, "0 2 * *"). Los usuarios que no estén familiarizados con la sintaxis cron pueden encontrar poco claro este formato de

entrada. Sin embargo, los usuarios pueden obtener información más detallada sobre la sintaxis cron y ejemplos en línea.

Fallo intermitente de recopilación de inventario para pocos dispositivos en implementaciones a gran escala

Actualmente, en implementaciones que superan los 10 000 dispositivos, es posible que un pequeño subconjunto de dispositivos no pueda realizar la recopilación de inventario a pesar de que el proceso de detección se haya realizado correctamente. Como solución alternativa, elimine los dispositivos que fallan del sistema y agréguelos de nuevo. Póngase en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC) para obtener ayuda adicional.

Estado de carga de derechos no visible durante la recopilación

Actualmente, después de cargar un archivo de derechos, no hay ninguna indicación clara en la interfaz de usuario de que el derecho se haya cargado y procesado correctamente. Iniciar una recopilación antes de que se procese completamente un derecho puede dar lugar a errores de cobertura. Como solución temporal, espere al menos una (1) hora después de la carga antes de ejecutar una recopilación.

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).