

Prácticas Líderes de Cisco: Cisco IOS Management Operations

Contenido

[Abstracto](#)

[Introducción](#)

[Overview](#)

[Objetivos](#)

[Destinatarios](#)

[Prerequisites](#)

[Creación de una Estrategia de Operaciones de Administración de Cisco IOS](#)

[Identificación de Entregables](#)

[Identificación de mediciones de dispositivos clave](#)

[Definición de Roles y Responsabilidades](#)

[Identificación de las áreas de especialización necesarias](#)

[Identificación de contribuyentes clave](#)

[Identificación de responsabilidades](#)

[Recursos presupuestarios](#)

[Siguiendo un Proceso de Operaciones de Administración de Prácticas Recomendadas de Cisco IOS](#)

[‘Control de versión de software’](#)

[Administración de fallas’](#)

[Administración de problemas](#)

[Estandarización de configuración](#)

[Gestión de disponibilidad](#)

[Lista de comprobación de operaciones de administración de Cisco IOS](#)

[Información Relacionada](#)

[Servicios y asistencia de Cisco](#)

Abstracto

Las prácticas principales de Cisco son un conjunto de documentos codificados que proporcionan una orientación relevante y fiable sobre las operaciones de red para los productos y soluciones de Cisco. Los galardonados ingenieros del Cisco TAC y de los servicios avanzados desarrollan y respaldan las prácticas líderes, que puede utilizar para crear su propio conjunto de prácticas líderes que emular. Los clientes de Cisco han aplicado estas prácticas líderes en su entorno de red para mejorar el rendimiento y la disponibilidad de la red.

Se recomienda encarecidamente complementar estas prácticas líderes con servicios de Cisco y sus partners. Para obtener más información sobre cómo optimizar el rendimiento y la disponibilidad de la red, póngase en contacto con el representante de ventas de servicios en la

Web de servicios avanzados de Cisco y obtenga más información sobre el Soporte de optimización de redes: soporte de ingeniería focalizado, soporte de mejora de la disponibilidad de la red (NAIS), evaluación de procesos de gestión de software (SMPA) e implementación de NAIS-SMPA.

Introducción

Overview

Los procesos operativos relacionados con la gestión del software pueden ayudar a reducir la complejidad de la red, disminuir los problemas de soporte reactivo y mejorar el tiempo de resolución de problemas. Este documento proporciona una estrategia, recomendaciones de herramientas y mejores prácticas para la administración general del software Cisco IOS® (Cisco IOS).

Las secciones [Creación de una Estrategia de Operaciones de Administración de Cisco IOS](#) y [Seguimiento de un Proceso de Operaciones de Administración de Cisco IOS de Prácticas Recomendadas](#) de este documento discuten la metodología recomendada para comenzar y enumera las mejores herramientas que se utilizarán para la fase de operaciones. La fase de operaciones incluye los procesos de prácticas recomendadas para lo siguiente:

Proceso	Descripción
'Control de versión de software'	Seguimiento, validación y mejora de la coherencia del software en las "opciones" de software identificadas.
Administración de fallas'	Monitoreo proactivo y actuación sobre los mensajes SNMP y Syslog de mayor prioridad generados por Cisco IOS.
Administración de problemas	Recolección rápida y eficiente de información crítica sobre problemas relacionados con el software para ayudar a prevenir futuros eventos.
Estandarización de configuración	"Estandarización" de configuraciones para reducir la posibilidad de que se utilice código no probado en producción y para estandarizar el protocolo de red y el comportamiento de las características.
Gestión de disponibilidad	Mejorar la disponibilidad en función de las métricas, los objetivos de mejora y los proyectos de mejora

Este documento asume que usted ha implementado los siguientes procesos recomendados para

la planificación, diseño e implementación de Cisco IOS:

- Se han identificado áreas de software gestionables (pistas de software) en su entorno en función de los requisitos de plataforma, módulo, función, protocolo y topología.
- Versiones de Cisco IOS seleccionadas, certificadas y comunicadas por pistas de software.
- Implementación coherente de las versiones estándar de Cisco IOS en cada una de las opciones de software.

Objetivos

Esta sección le ayuda a administrar y mantener las versiones estandarizadas de Cisco IOS dentro de las pistas definidas. Aprenderá a hacer lo siguiente:

- Desarrollar un proceso de control de versiones de software para garantizar la coherencia de las versiones de software en las opciones de software identificadas.
- Supervise, notifique y resuelva los procesos en función de los mensajes y alertas de administración de errores de dispositivos (SNMP/Syslog) para ayudar a resolver de forma proactiva posibles problemas de software y errores.
- Recopilación eficaz de información crítica sobre problemas de software para ayudar a reducir el tiempo de resolución de problemas relacionados con el software.
- Estandarice las configuraciones de los dispositivos para ayudar a garantizar la coherencia del protocolo, las funciones, el acceso y la seguridad del entorno.

Destinatarios

Este documento es apropiado para personas y administradores con una orientación técnica que son responsables del funcionamiento diario de la red. El documento describe cómo establecer procesos operativos para ayudarle a reducir la complejidad de la red, disminuir los problemas de soporte reactivo y mejorar el tiempo de resolución de problemas mediante la creación de consistencia en la red y la mejora de las capacidades para la administración proactiva de fallas.

Prerequisites

Quienes participan en las operaciones de gestión de Cisco IOS deben tener un conocimiento sólido del diseño y la administración de la infraestructura de la red, especialmente con los equipos de Cisco, y deben tener acceso a los detalles de la topología de la red de destino, la configuración del dispositivo, el perfil de actividad, el uso de la aplicación y la política de utilización de recursos. También es necesario tener acceso a las herramientas de información disponibles en [Cisco Connection Online](#) (CCO) y poder disfrutar de ellas. Si aún no se ha [registrado en CCO](#), le sugerimos que lo haga para acceder a las herramientas descritas en este documento.

Creación de una Estrategia de Operaciones de Administración de

Cisco IOS

Existen muchas estrategias y herramientas de calidad para ayudar a administrar los entornos de Cisco IOS. Este capítulo se centra en tres estrategias clave para administrar las operaciones de Cisco IOS en entornos de mayor disponibilidad e incluye una matriz de herramientas operativas clave que son específicamente útiles para administrar los problemas de Cisco IOS y Cisco IOS.

La primera estrategia clave consiste en mantener el entorno lo más simple posible, evitando en la medida de lo posible las variaciones en la configuración y las versiones de Cisco IOS. La certificación de Cisco IOS ya se ha analizado; sin embargo, la coherencia de la configuración es otra área clave. El grupo arquitectura/ingeniería debe encargarse de la creación de los estándares de configuración. El grupo de implementación y operaciones tiene entonces la responsabilidad de configurar los estándares y mantener los estándares a través del control de versiones de Cisco IOS y los estándares/control de configuración de Cisco IOS.

La segunda estrategia clave es la capacidad de identificar y resolver rápidamente los fallos de red. Por lo general, el grupo de operaciones debe identificar los problemas de red antes de que los usuarios los notifiquen, y los problemas deben resolverse lo más rápido posible sin que ello afecte o cambie el entorno. Dos prácticas recomendadas clave en esta área son la gestión de problemas y la gestión de errores (ambas se tratan más adelante en este documento).

Nota: La herramienta decodificadora de pilas de Cisco IOS se puede utilizar para ayudar a diagnosticar rápidamente las caídas del software Cisco IOS.

La tercera estrategia clave es "mejorar constantemente". El proceso principal consiste en mejorar un programa de mejora de la disponibilidad basado en la calidad. Al realizar un análisis de la causa principal de todos los problemas, incluidos los relacionados con Cisco IOS, una organización puede mejorar la cobertura de las pruebas, los tiempos de resolución de problemas y los procesos que eliminarán o reducirán el impacto de las interrupciones. La organización también puede analizar los problemas comunes y crear procesos para resolverlos más rápidamente.

Identificación de Entregables

Entre los elementos suministrados del proceso de operación de administración del software del IOS de Cisco se incluyen:

- Procesos y herramientas de control de versiones de software
- Supervisión y procesos de gestión de fallos
- Procesos de administración de problemas
- Estándares de configuración de dispositivos y procesos de auditoría
- Metodología de disponibilidad de la red, procesos de informes y revisión

Identificación de mediciones de dispositivos clave

Las métricas deben definirse como parte del plan de operaciones y utilizarse para determinar si las herramientas y los procesos están produciendo los resultados deseados. A continuación se muestran algunos ejemplos de métricas útiles de administración del software Cisco IOS:

- Disponibilidad de la red (debido a problemas de software)
- % de conformidad de la versión de Cisco IOS con el estándar (en función de las pistas)
- % de coherencia en la configuración del dispositivo (según los estándares)
- Métricas de gestión de problemas (MTTR, nº de tickets, códigos de cierre)

Definición de Roles y Responsabilidades

Identifique, califique y reúna un grupo multifuncional de gerentes y/o clientes potenciales de arquitectura de red, ingeniería de red y grupos de implementación/operaciones para ayudar a garantizar el éxito de las fases de planificación, diseño, implementación y operaciones de sus proyectos de actualización de IOS.

Identificación de las áreas de especialización necesarias

Reúna un grupo multifuncional de gerentes y/o clientes potenciales de los grupos de administración de redes, ingeniería de redes, implementación y operaciones para ayudar con la fase de operaciones de su proyecto de administración de Cisco IOS.

Identificación de contribuyentes clave

- Gestor(es) de red:

Nombre del gerente, departamento, información de contacto

Nombre de la copia de seguridad principal, departamento, información de contacto

Nombre de la copia de seguridad secundaria, departamento, información de contacto si es necesario

- Arquitecto(es) de red:

Nombre del arquitecto, departamento, información de contacto

Nombre de la copia de seguridad principal, departamento, información de contacto

Nombre de la copia de seguridad secundaria, departamento, información de contacto si es necesario

- Ingeniero(s) de red:

Nombre del ingeniero, departamento, información de contacto

Nombre de la copia de seguridad principal, departamento, información de contacto

Nombre de la copia de seguridad secundaria, departamento, información de contacto si es necesario

- Ingeniero(s) de operaciones de red (NOC):

Nombre del ingeniero, departamento, información de contacto

Nombre de la copia de seguridad principal, departamento, información de contacto

Nombre de la copia de seguridad secundaria, departamento, información de contacto si es necesario

Identificación de responsabilidades

- Los administradores de red son responsables de:
 - Mantenimiento del plan del proyecto
 - Asignación/reasignación de recursos
 - Administrar el control de cambios
 - Gestión del progreso
 - Administración de informes presupuestarios
- Los arquitectos de red son responsables de:
 - Análisis de estándares de red y advertencias de versiones
 - Mantenimiento de la matriz de actualización de software
 - Mantenimiento de la matriz de gestión de candidatos
 - Mantenimiento de la matriz de requisitos de memoria
- Los ingenieros de redes (NOC) son responsables de:
 - Implementar y garantizar el cumplimiento de los estándares de red
 - Identificación de problemas de software y causas principales
 - Recomendación de medidas correctoras
 - Supervisión de la red

Recursos presupuestarios

Las necesidades de recursos deben determinarse en la etapa de operaciones para apoyar la

estrategia de gestión de programas informáticos de la organización. Esto incluirá el tiempo de personal necesario y los gastos de capital necesarios para apoyar la estrategia de software.

En muchos casos, se puede generar un plan de rentabilidad de la inversión (ROI) o un plan presupuestario para las prácticas de gestión de software en función del coste del tiempo de inactividad y los requisitos de disponibilidad. Si la organización puede determinar el tiempo de inactividad debido a problemas de software, la mayor parte de este coste se puede compensar mediante las prácticas recomendadas de gestión de software identificadas. Si el coste no se puede compensar por completo, la organización debe considerar una estrategia de gestión de software más básica que ayude a mejorar la productividad evitando reelaboraciones adicionales como resultado de problemas de software.

Siguiendo un Proceso de Operaciones de Administración de Prácticas Recomendadas de Cisco IOS

Las prácticas recomendadas para seguir un proceso de operaciones de administración de Cisco IOS incluyen:

Prácticas recomendadas	Detalle
‘Control de versión de software’	Implementar solo versiones de software estandarizadas y supervisar la red para validar o, posiblemente, cambiar el software debido a que no se cumplen las versiones.
Administración de fallas’	La recopilación, supervisión y análisis de mensajes SNMP y Syslog son procesos de administración de fallas recomendados para resolver más problemas de red específicos de Cisco IOS que son difíciles o imposibles de identificar de otra manera.
Administración de problemas	Procesos detallados de gestión de problemas que definen la identificación de problemas, la recopilación de información y una ruta de solución bien analizada. Estos datos se utilizan para determinar la causa raíz.
Estandarización de configuración	Los estándares de configuración representan la práctica de crear y mantener parámetros de configuración "globales" estándar en

	dispositivos y servicios similares, lo que se traduce en una coherencia de la configuración global en toda la empresa.
Gestión de disponibilidad	Mejora de la calidad utilizando la disponibilidad de la red como métrica de mejora de la calidad.

‘Control de versión de software’

El control de versión de software es el proceso de implementación de sólo versiones de software estandarizadas y de supervisión de la red, con el fin de validar o, posiblemente, cambiar software debido a que la versión no es la adecuada. En general, el control de versiones de software se realiza mediante un proceso de certificación y un control de estándares. Muchas organizaciones publican estándares de versiones en un servidor Web central. Además, se forma al personal de implementación para que revise qué versión se está ejecutando y actualice la versión si no cumple con los estándares. Algunas organizaciones cuentan con un proceso de control de calidad en el que la validación secundaria se completa mediante auditorías para garantizar que se sigue el estándar durante la implementación.

Durante el funcionamiento de la red, también es frecuente ver versiones de software no estándar en la red, especialmente si la red es grande y cuenta con un gran personal de operaciones. Esto puede deberse a una de las causas siguientes:

- Personal nuevo sin formación
- Comandos de arranque mal configurados
- Implementaciones no comprobadas

Se recomienda validar periódicamente los estándares de versión de software mediante herramientas como CiscoWorks2000 Resource Manager Essentials (RME), que pueden ordenar todos los dispositivos por la versión de Cisco IOS. Cuando se identifica una versión no estándar, se debe marcar inmediatamente y se debe iniciar un ticket de problemas o un ticket de cambio para llevar la versión al estándar identificado.

Herramientas disponibles

CiscoWorks2000 RME Inventory Manager simplifica en gran medida la gestión de la versión de Cisco IOS de los routers y switches de Cisco a través de herramientas de generación de informes basadas en la Web que informan y clasifican los dispositivos en función de la versión de software, la plataforma del dispositivo y el nombre del dispositivo.

Administración de fallas’

La administración de fallas es el proceso de recolección, monitoreo y análisis de los mensajes SNMP y Syslog para resolver más problemas de red específicos de Cisco IOS que son difíciles o imposibles de identificar de otra manera.

Recopilación de trampas SNMP

La recolección y notificación de trampas SNMP es un proceso básico en la administración de fallas utilizado para identificar eventos de software o hardware y/o fallas sin sobrecarga de sondeo SNMP o demora incurrida en los intervalos de sondeo. Los mensajes de trampa se generan directamente desde el dispositivo de red a un sistema de administración de red que proporciona servicios de notificación. La recopilación y notificación de estas trampas es esencial para la rápida resolución de muchos eventos de red, incluidos los eventos que no afectan al usuario, como la pérdida de dispositivos primarios o enlaces en un entorno redundante.

Para recopilar y monitorear estas trampas, las trampas deben configurarse correctamente en el dispositivo, así como en los sistemas de administración de red. Los sistemas de administración de redes deben alertar al grupo de operaciones de red cuando se ha recibido una trampa. La notificación puede realizarse en forma de avisos, correos electrónicos o pantallas de eventos en un entorno de NOC.

Independientemente de cómo se presenten los datos, estos casos de error, o excepciones, deben ser analizados y revisados de forma regular (preferiblemente a diario) por el personal de operaciones de red o de soporte de red. Deben investigarse las causas de todas las excepciones encontradas. Es posible que algunas excepciones registradas no sean lo suficientemente importantes como para activar una alarma inmediatamente en el centro de operaciones de red. La revisión, la investigación y la resolución proactivas de excepciones menores pueden ayudar a los grupos de soporte de red a reducir o evitar las interrupciones de la red.

Recopilación de mensajes de Syslog

El dispositivo envía los mensajes de registro del sistema a un servidor de recopilación. Estos mensajes pueden ser errores de hardware o software o pueden ser informativos (como cuando alguien ha estado en la configuración de terminal en un dispositivo).

La supervisión de Syslog requiere compatibilidad con herramientas o scripts del sistema de administración de redes (NMS) para ayudar a analizar los datos de Syslog e informar sobre ellos. Esto incluye la capacidad de ordenar los mensajes de Syslog por fecha o período de tiempo, dispositivo, tipo de mensaje de Syslog o frecuencia de mensaje. En redes más grandes, se pueden implementar herramientas o scripts para analizar los datos de Syslog y enviar alertas o notificaciones a los sistemas de administración de eventos o al personal de operaciones e ingeniería. Si no se utilizan alertas para una amplia variedad de datos de Syslog, la organización debe revisar los datos de Syslog de mayor prioridad al menos una vez al día y crear informes de problemas para detectar posibles problemas. Con el fin de detectar de forma proactiva problemas de red que pueden no verse a través de la supervisión normal, se deben realizar revisiones y análisis periódicos de los datos históricos de Syslog para detectar situaciones que pueden no indicar un problema inmediato, pero que pueden proporcionar una indicación de un problema antes de que afecte al servicio.

Herramientas disponibles

Algunas de las herramientas más populares del receptor de trampas SNMP incluyen lo siguiente:

- HP OpenView Network Node Manager de Hewlett Packard en openview.hp.com
- Spectrum Integrity de Aprisma en www.aprisma.com
- NetView de IBM Tivoli en www.tivoli.com

La herramienta Syslog más popular para la administración de Cisco IOS es CiscoWorks2000 RME Syslog manager. Otras herramientas disponibles incluyen SL4NT, un programa de shareware de www.netal.com dejando cisco.com y Private I de OpenSystems en www.opensystems.com

Administración de problemas

La gestión de problemas, un aspecto de la gestión de fallos, es la disciplina de la gestión de problemas desde el momento en que se producen, mediante la identificación, la resolución de problemas y el cierre.

Muchos clientes experimentan tiempos de inactividad adicionales debido a la falta de procesos en la gestión de problemas. El tiempo de inactividad adicional puede producirse cuando los administradores de red intentan resolver el problema rápidamente mediante una combinación de comandos que afectan al servicio o cambios de configuración, en lugar de dedicar tiempo a la identificación del problema, la recopilación de información y una ruta de solución bien analizada. El comportamiento observado en esta área incluye recargar dispositivos o borrar tablas de IP Routing antes de investigar un problema y su causa raíz. En algunos casos, esto ocurre debido a los objetivos de resolución de problemas de soporte de primer nivel. El objetivo de todas las cuestiones relacionadas con software debería ser recolectar rápidamente la información necesaria para el análisis de las causas raíz antes de restaurar la conectividad o el servicio.

Se recomienda un proceso de administración de problemas, que debe incluir un cierto grado de descripciones predeterminadas de problemas y las colecciones de comandos "show" apropiadas antes de escalar el problema a un segundo nivel de soporte. El soporte de primer nivel nunca debe incluir borrar rutas o recargar dispositivos. Lo ideal sería que la organización de soporte de primer nivel recopilara información rápidamente y luego escalara el problema a soporte de segundo nivel. Al dedicar un poco más de tiempo a identificar y describir el problema en el nivel uno de soporte, es mucho más probable que se produzca un descubrimiento de la causa raíz, lo que permite una solución alternativa, la identificación del laboratorio y la generación de informes de errores. El soporte de segundo nivel debe estar bien versado en los tipos de información que Cisco puede necesitar para diagnosticar un problema o presentar un informe de errores, incluyendo:

- Volcados de memoria
- Salida de información de routing
- Resultado del comando show del dispositivo

Estandarización de configuración

Los estándares de configuración de dispositivos globales representan la práctica de mantener parámetros de configuración "globales" estándar en dispositivos y servicios similares, lo que se traduce en una coherencia de la configuración global de toda la empresa. Los comandos de configuración global son comandos que se aplican a todo el dispositivo y no a puertos, protocolos o interfaces individuales. Por lo general, afectan al acceso del dispositivo, al comportamiento general del dispositivo y a la seguridad del mismo. En Cisco IOS, esto incluye los siguientes comandos:

- Servicio
- IP
- VTY
- Puerto de consola
- Registro
- AAA/TACACS+
- SNMP (Protocolo de administración de red simple)
- Banner

También es importante en los estándares globales de configuración de dispositivos disponer de una convención de nomenclatura de dispositivos adecuada que permita a los administradores identificar el dispositivo, el tipo de dispositivo y la ubicación del dispositivo en función del nombre DNS del dispositivo. La coherencia global de la configuración es importante para la compatibilidad y fiabilidad globales de un entorno de red, ya que ayuda a reducir la complejidad de la red y a mejorar la compatibilidad de la red. Muchas veces se experimenta una dificultad de soporte sin la estandarización de configuración debido a un comportamiento incorrecto o incoherente del dispositivo, al acceso SNMP y a la seguridad general del dispositivo.

El mantenimiento de los estándares de configuración de dispositivos globales lo realiza normalmente un grupo de operaciones o ingeniería interna que crea y mantiene parámetros de configuración globales para dispositivos de red similares. También es una buena práctica proporcionar una copia del archivo de configuración global en los directorios TFTP para que puedan descargarse inicialmente a todos los dispositivos provisionados recientemente. También resulta útil un archivo accesible desde la Web que proporciona al archivo de configuración estándar una explicación de cada parámetro de configuración. Algunas organizaciones configuran todos los dispositivos similares de forma periódica para ayudar a garantizar la coherencia de la configuración global, o bien revisan periódicamente los dispositivos para comprobar que cumplen los estándares de configuración global correctos.

Los estándares de configuración de interfaz o protocolo representan la práctica de mantener estándares para la configuración de interfaz y protocolo, lo que mejora la disponibilidad de la red al reducir la complejidad de la misma, proporcionar el comportamiento esperado de dispositivos y protocolos, y mejorar la compatibilidad de la red. La incoherencia de la configuración de la interfaz o del protocolo puede dar lugar a un comportamiento inesperado del dispositivo, problemas de

routing del tráfico, problemas de conectividad aumentados y mayor tiempo de soporte reactivo.

Los estándares de configuración de interfaz pueden incluir:

- CDP (Cisco Discovery Protocol)
- Descriptores de interfaz
- Configuración de caché
- Otras normas específicas de protocolo

Los estándares de configuración específicos del protocolo pueden incluir:

- Configuración de IP Routing
- configuración DLSW
- Configuración de la lista de acceso
- configuración ATM
- configuración de Frame Relay
- Configuración de árbol de extensión
- Asignación y configuración de VLAN
- VTP (Virtual Trunking Protocol)
- HSRP (Hot Standby Routing Protocol)
- Otros dependiendo de lo que se configure dentro de la red

Un ejemplo de estándares IP puede incluir el tamaño de la subred, el espacio de la dirección IP utilizado, el protocolo de routing utilizado y la configuración del protocolo de routing.

El mantenimiento de los estándares de configuración de protocolos e interfaces es normalmente responsabilidad de los grupos de implementación e ingeniería de redes. El grupo de ingeniería debe ser responsable de identificar, probar, validar y documentar las normas. El grupo de implementación es responsable de utilizar los documentos de ingeniería o las plantillas de configuración para aprovisionar nuevos servicios. El grupo de ingeniería debería crear documentación sobre todos los aspectos de estándares requeridos para asegurar consistencia. También se deben crear plantillas de configuración para ayudar a aplicar los estándares de configuración. Los grupos de operaciones deberían capacitarse con respecto a las normas y deben ser capaces de identificar problemas de configuración no estándar. La coherencia de la configuración es de gran ayuda en la fase de prueba, validación y certificación. Sin plantillas de configuración estandarizadas, es casi imposible probar, validar o certificar adecuadamente una versión de Cisco IOS para una red moderadamente grande.

Gestión de disponibilidad

La gestión de la disponibilidad es el proceso de mejora de la calidad utilizando la disponibilidad de la red como métrica de mejora de la calidad. Muchas organizaciones están midiendo la disponibilidad y el tipo de interrupción. Los tipos de interrupción pueden incluir lo siguiente:

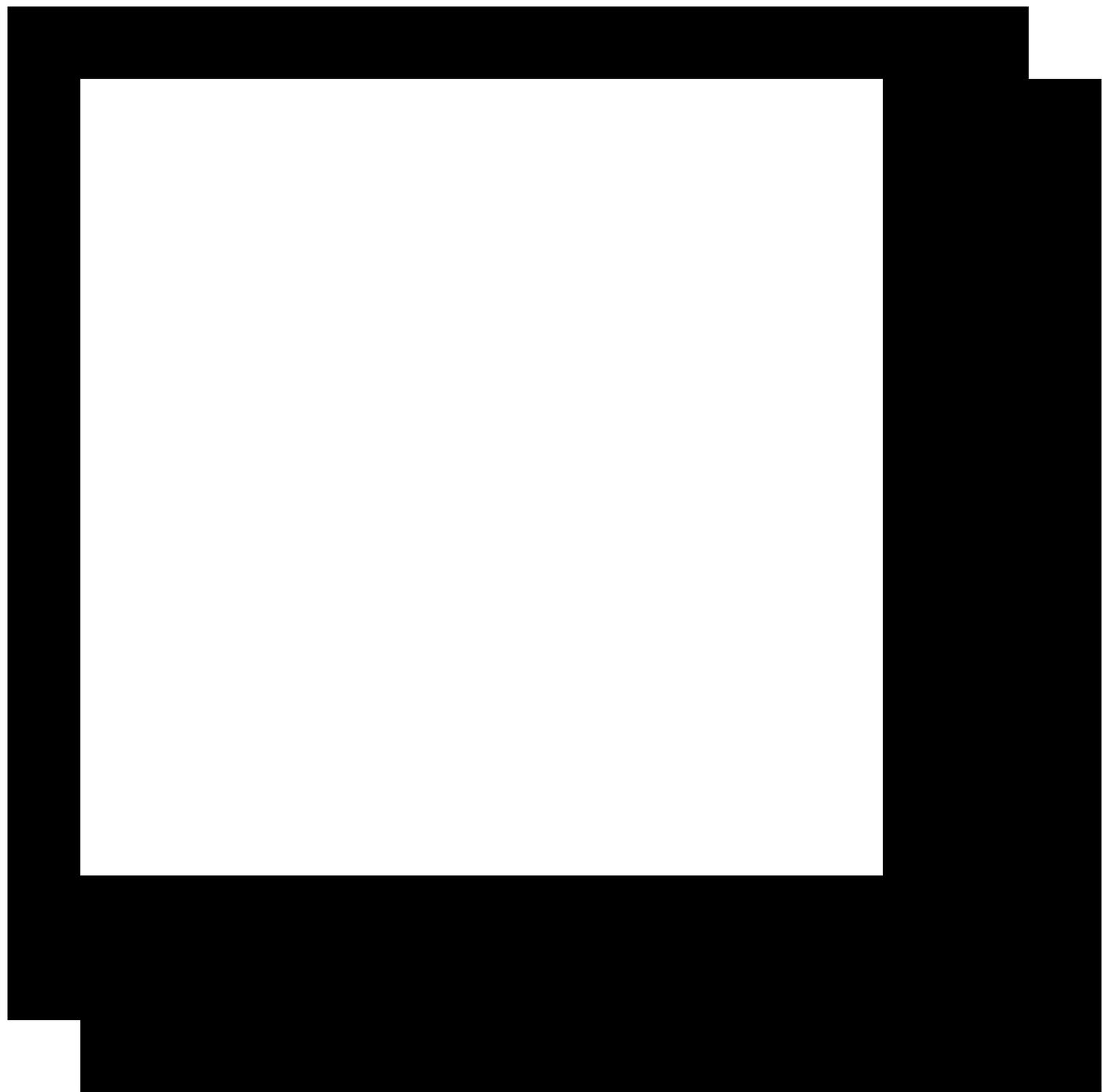
- Hardware
- Software
- Enlace/portadora
- Alimentación/entorno
- Diseño
- Error/proceso del usuario

Al identificar las interrupciones y realizar un análisis de las causas principales inmediatamente después de la recuperación, la organización puede identificar métodos para mejorar la disponibilidad. Casi todas las redes que han logrado una alta disponibilidad cuentan con algún tipo de proceso de mejora de la calidad.

Lista de comprobación de operaciones de administración de Cisco IOS

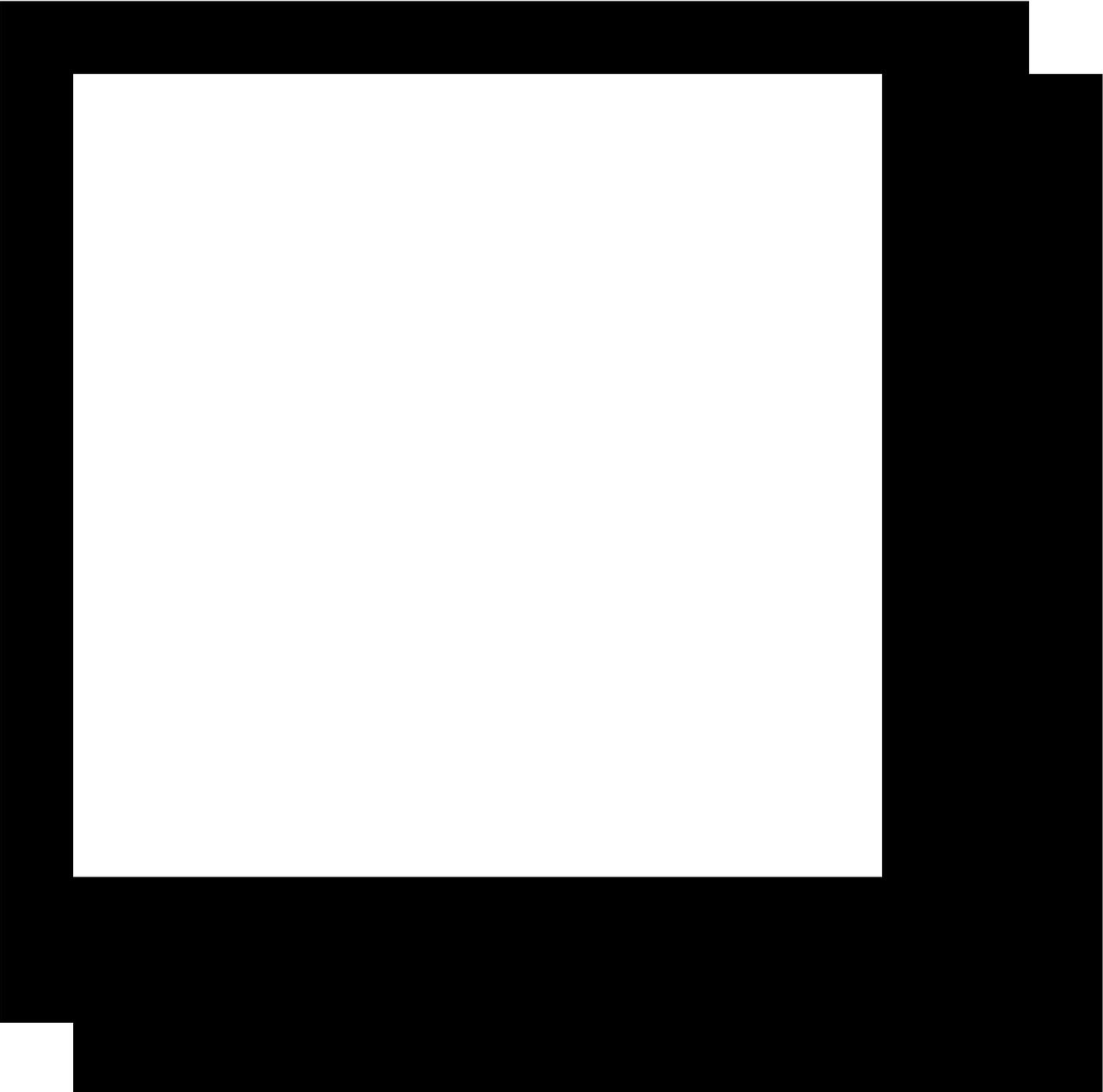
Paso 1: [Definir requisitos y objetivos empresariales](#) (sólo para clientes registrados)

Paso 2: [Evaluar el estado actual de las prácticas de administración del software Cisco IOS](#) (sólo para clientes [registrados](#))



Paso 3: [Definir funciones y responsabilidades](#) (sólo [para](#) clientes [registrados](#))

Paso 4: [Desarrollo de un plan de proyecto de gestión de software](#) (sólo para clientes [registrados](#))



Paso 5: [Desarrollo de una matriz de requisitos de software](#) (sólo [para](#) clientes [registrados](#))

Información Relacionada

Se ha creado un apéndice para ayudar al cliente a obtener otra información valiosa relacionada con Cisco IOS como: fundamentos de Cisco IOS, procesos internos de Cisco IOS Software, análisis de confiabilidad del software, programa interno de calidad de Cisco, metodologías de prueba internas de Cisco y un análisis de campo que muestra las prácticas actuales del sector y las experiencias generales del cliente con Cisco IOS Software

- Administración de Cisco IOS: se puede encontrar información adicional sobre la

administración de Cisco IOS y las prácticas recomendadas en el informe técnico "Administración de Cisco IOS para redes de alta disponibilidad" en el siguiente sitio:

http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800a998b.shtml

- Para obtener información específica sobre cómo ejecutar sondeos de red, qué comandos CLI utilizar, cómo analizar e interpretar los datos del tráfico de red y cómo establecer políticas de uso de aplicaciones, visite <http://www.cisco.com>. Este sitio proporciona una completa gama de soluciones de soporte, formación, referencia técnica y consultoría.
- Cisco IOS tiene convenciones de nombres específicas que se definen aquí: http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_tech_note09186a0080101cda.s
- La información sobre la disponibilidad de la versión de Cisco IOS se proporciona aquí: http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html
- Las versiones de Cisco IOS se eliminan de CCO y ya no se pueden solicitar. Asegúrese de establecer las expectativas del cliente en consecuencia.
- Los boletines de productos de Cisco IOS se utilizan para anunciar las versiones de Cisco IOS a los clientes. Contienen información breve sobre el contenido de la versión. Compruebe aquí la disponibilidad de las nuevas versiones de Cisco IOS http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html
- El equipo de respuesta ante incidentes de seguridad del producto se encarga de la seguridad de los productos de Cisco. Cualquier problema relacionado con la seguridad del IOS de Cisco debe remitirse a este equipo. Cisco publica públicamente sus vulnerabilidades de seguridad. <http://tools.cisco.com/security/center/publicationListing>
- Defectos de Cisco IOS: se recomienda aplazar los defectos graves de Cisco IOS. Cualquier empleado de Cisco puede hacer la recomendación.
- Los problemas de campo en Cisco IOS se comunican a los clientes a través de los asesores de Cisco IOS. http://www.cisco.com/en/US/products/products_security_advisory09186a0080b20ee1.shtml
- Funciones de Cisco IOS: la herramienta Feature Navigator permite a los clientes encontrar versiones compatibles con funciones específicas, y viceversa. <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>
- Cisco Software Advisor permite a los clientes encontrar asistencia para el software de funciones o asistencia para el software de hardware. <http://tools.cisco.com/Support/Fusion/FusionHome.do> (sólo para [clientes registrados](#))

Servicios y asistencia de Cisco

- [Servicios de asistencia técnica](#)
- [Servicios específicos para las tecnologías y soluciones de redes de Cisco](#)

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).

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).