Cisco IOS Administración para la conexión en red de alta disponibilidad: Informe oficial de Mejores Prácticas

Contenido

Introducción

El software confiable de Cisco que despliega y que mantiene IOS® es una prioridad en el entorno de red crítica de hoy del negocio que requiere Cisco renovado y la concentración del cliente alcanzar la Disponibilidad directa. Mientras que Cisco debe concentrarse en su compromiso por la calidad del software, los grupos de diseño y soporte de red también deben concentrarse en las mejores prácticas para la administración de software del IOS de Cisco. La meta es más de gran disponibilidad y eficiencia de la administración del software. Este método es una sociedad combinada para compartir, aprender e implementar las mejores prácticas de administración de software.

Este documento proporciona un contexto de funcionamiento efectivo de las prácticas de administración del Cisco IOS para la empresa y los clientes del proveedor del servicio que ayudan a promover la confiabilidad de software mejorado, la complejidad de la red reducida, y la mayor disponibilidad de la red. Este marco también ayuda a mejorar la eficacia de la administración de software al identificar áreas de responsabilidad y superposiciones en las pruebas de la administración del software y la validación entre las operaciones de lanzamiento de Cisco y la base de clientes de Cisco.

Resumen de las mejores prácticas IOS de Cisco

Las siguientes tablas proporcionan una descripción general de las mejores prácticas de Cisco IOS. Se pueden utilizar estas tablas como una descripción general de la administración de las mejores prácticas definidas como una lista de control del análisis de problemas para revisar las prácticas de administración actuales del IOS de Cisco, o como un marco para crear procesos alrededor de la administración del IOS de Cisco.

Las tablas definen a los cuatro componentes del ciclo de vida útil de la Administración del Cisco IOS. Cada tabla comienza con una estrategia y las herramientas sumarias para el área identificada del ciclo vital. Después de la estrategia y de las herramientas el resumen es las mejores prácticas específicas que se aplican solamente al área definida del ciclo vital.

Planificación - Construyendo el Marco de administración del Cisco IOS — Las hojas de operación (planning) son la fase inicial de Administración del Cisco IOS necesaria para ayudar a una organización para determinar cuando Actualizar software, donde actualizar, y qué proceso será utilizado para probar y para validar las imágenes posibles.

Mejor práctica	Detalle
Estrategia y herramientas para la planificación del IOS de Cisco	La introducción con la planificación de la administración del Cisco IOS comienza con una evaluación honesta de las prácticas actuales, del desarrollo de objetivos alcanzables, y de la planificación de proyectos.
Definiciones de seguimiento de versione	Identifica donde el estado coherente del software puede ser mantenido. Un agrupamiento de versiones de software se puede definir como agrupamiento de versión de software único, distinguido de otras áreas

s de software	por la geografía única, las Plataformas, el módulo, o los requisitos de la función.
Ciclo de actualización y definiciones	Las definiciones del ciclo de actualización pueden ser establecidas como pasos de calidad básicos en la administración de software y modificaciones, usados para determinar en qué momento debe iniciarse un ciclo de actualización del software.
Proceso de certificación	Los pasos del proceso de certificación deben incluir la identificación de la pista, las definiciones del ciclo de actualización, la administración del candidato, la prueba/validación, y por lo menos un cierto uso de la producción piloto.

Diseño - Selección y validación de las versiones de IOS — Tener un proceso bien definido para seleccionar y validar las versiones deL Cisco IOS ayuda a una organización para reducir el tiempo de inactividad imprevisto debido a los intentos de actualización fracasados y a los defectos del software imprevistos.

Mejor práctica	Detalle
Estrategia y herramientas para la selección y validación de IOS de Cisco	Defina los procesos para seleccionar, probar, y validar las versiones del nuevo Cisco IOS. Esto incluye un laboratorio de prueba de la red que emula la red de producción.
Administración del candidato	La administración del candidato es la identificación de los requisitos de versión de software y de los riesgos potenciales para el hardware en particular y los conjuntos de características habilitados.
Prueba y validación	Prueba y validación son aspectos críticos para la administración de software y la red de gran disponibilidad. La prueba de laboratorio apropiada puede reducir perceptiblemente el tiempo de inactividad de la producción, ayudar a entrenar al equipo de soporte de red, y ayudar a aerodinamizar los procesos de la implementación de la red.

Implementación - Despliegue rápido y acertado del Cisco IOS — Los procesos de instrumentación bien definidos permiten una organización despliegan a rápidamente y con éxito las versiones del nuevo Cisco IOS.

Mejor	Detalle

práctica	
Estrategia y herramientas para la instalación del IOS de Cisco	La estrategia básica para las implementaciones del IOS de Cisco es realizar una certificación final vía un proceso piloto y una implementación rápida por medio de herramientas de actualización y un proceso de implementación bien definido.
Proceso piloto	Para minimizar la exposición potencial y más con seguridad a la captura se recomienda cualquier problema de producción restante, un piloto de software. El plan piloto individual debe considerar la selección experimental, la duración experimental, y la medida.
Instrumentación	Después de la realización de la fase piloto, la fase de implementación del Cisco IOS debe comenzar. La fase de implementación puede incluir diversos pasos para asegurar el éxito de la actualización del software y la eficacia de la implementación, incluyendo inicio lento, certificación final, preparación de la actualización, automatización de la actualización y validación final.

Operaciones - Manejando la implementación de gran disponibilidad del Cisco IOS — Las mejores prácticas para las operaciones del Cisco IOS incluyen el control de versión de software, el Cisco IOS Administración de Syslog, la administración de problemas, la estandarización de la configuración, y la Administración de la disponibilidad.

Mejor práctica	Detalle
Estrategias y herramientas para el funcionamiento del IOS de Cisco	La primera estrategia de las operaciones del Cisco IOS es mantener el entorno tan simple como sea posible, evitando la variación la configuración y las versiones deL Cisco IOS. La segunda estrategia es la capacidad de identificar y de resolver rápidamente a las fallas de la red.
'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.
Administración proactiva	La recolección, el monitoreo y el análisis de Syslog son los procesos de administración de fallas recomendados para resolver más

de Syslog	problemas de redes específicos de Cisco IOS que son difíciles o imposibles de identificar por otros medios.
Administración de problemas	Procesos de administración de problema detallados que definen la Identificación del problema, la recopilación de información, y un trayecto de solución bien analizado. Estos datos pueden utilizarse para determinar la causa raíz.
Estandarización de la configuración	Las normas de configuración representan la práctica de crear y de mantener los dispositivos y los servicios similares estándar de los Parámetros de configuración global a través dando por resultado la coherencia de configuración global a nivel empresarial.
Administración de la disponibilidad	La Administración de la disponibilidad es el proceso de la mejora de la calidad usando la disponibilidad de la red como la mejora de la calidad métrica.

Información general sobre el proceso de administración de la vida útil del software

La administración del ciclo vital del Cisco IOS Software se define como el conjunto de las hojas de operación (planning), de diseño, de implementación, y de los procesos operativos que se recomiendan para las implementaciones y la conexión de redes de alta disponibilidad del software confiable. Esto incluye procesos para seleccionar, validar o mantener las versiones del IOS de Cisco en la red.

La meta de la administración del ciclo vital del Cisco IOS Software es mejorar la disponibilidad de la red bajando los defectos del software identificados probabilidad de producción o el cambio/las fallas de la actualización relacionados software. Las mejoras prácticas que se definen en esta documentación han sido presentadas para reducir tales defectos y revertir las fallas en base a la experiencia en la práctica de muchos clientes de Cisco y del equipo de Servicios avanzados de Cisco. Es posible que la administración de la vida útil del software inicialmente aumente los gastos, sin embargo, pueden lograrse costos generales de propiedad debido a las interrupciones y los mecanismos de soporte y despliegue más racionalizados.

Planificación – Crear el marco de administración de Cisco IOS

La planificación es la fase inicial de la administración del IOS de Cisco que tiene por objeto ayudar a una organización a determinar cuándo actualizar el software, dónde actualizarlo y qué proceso se usará para probar y validar las posibles imágenes.

Las mejores prácticas incluyen las definiciones de pista de la versión de software, ciclo de actualización y las definiciones, y la creación de un proceso de certificación de la interna del software.

Estrategia y herramientas para la planificación del IOS de Cisco

Comience la planificación de la administración del Cisco IOS con una evaluación honesta de las prácticas actuales, del desarrollo de objetivos alcanzables, y de la planificación de proyectos. La evaluación propia debería hacerse mediante la comparación de las mejores prácticas que se describen en este documento y los procesos que se aplican en su empresa. Las preguntas básicas deben incluir el siguiente:

- ¿Mi organización tiene un proceso de certificación del software que ésa incluya la prueba/validación del software?
- ¿Mi organización tiene estándares del Cisco IOS Software con las cantidades limitadas de versiones deL Cisco IOS que se ejecutan en la red?
- ¿Mi organización tiene dificultad que determina cuando actualizar el Cisco IOS Software?
- ¿Mi organización tiene software ambos del nuevo Cisco IOS de la dificultad que despliega de manera eficaz y eficiente?
- ¿Mi organización tiene problemas de estabilidad del Cisco IOS después del despliegue que afecten seriamente el costo de tiempo de inactividad?

Después de la evaluación, su organización debe comenzar a definir las metas para la Administración del Cisco IOS Software. Comience haciendo posible un grupo de funcionalidad recíproca de administradores o terminales desde los grupos de planificación de arquitectura, ingeniería, implementación y operaciones para ayudar a definir los objetivos del IOS de Cisco y los proyectos de mejoras de proceso. El propósito de las reuniones iniciales debería ser la determinación de los objetivos, los roles y las responsabilidades generales, la asignación de ítems de acción y la definición de la programación inicial del proyecto. También, defina las medidas y factores de éxito importantes para determinar a los beneficios de administración del software. La medición potencial incluye:

- Disponibilidad (debido a los problemas de software)
- costo de mejoras del software
- tiempo requerido para las actualizaciones
- número de versiones de software actuales en producción
- éxito/tasas de fallas del cambio de actualización del software

Además del Marco de administración total del Cisco IOS que planea, algunas organizaciones también definen a las reuniones de planificación en curso del software para ocurrir mensualmente o trimestralmente. La meta de estas reuniones es revisar el despliegue de software actual y comenzar a planear cualquier nuevo requisito de software. La planificación puede incluir volver a analizar o modificar procesos de administración de software actuales, o sencillamente definir papeles y responsabilidades para las diferentes fases de la administración de software.

Las herramientas de la fase de planificación constan únicamente de herramientas de software para administración de inventario. El administrador de inventario del Resource Manager Essentials del CiscoWorks 2000 (RME) es la herramienta primaria usada en esta área. El Administrador de inventarios RME CiscoWorks2000 simplifica grandemente la administración de la versión de los routeres Cisco y del Switches a través de las herramientas de informe basadas en web que los dispositivos Cisco IOS del informe y de la clase basaron en la versión de software, la plataforma del dispositivo, el tamaño de la memoria, y el Nombre del dispositivo.

Definiciones de seguimiento de versiones de software

La primera mejor práctica de la planificación de la administración del Cisco IOS Software identifica

donde el estado coherente del software puede ser mantenido. Un agrupamiento de versiones de software se define como agrupamiento de versión de software único, distinguido de otras áreas por la geografía única, las Plataformas, el módulo, o los requisitos de la función. Lo óptimo es que una red deba ejecutar una sola versión de software. Esto baja grandemente los costes relacionados administración del software y proporciona un entorno constante y fácilmente manejado. Sin embargo, la realidad es que la mayoría de las organizaciones deben funcionar con varias versiones en la red debido a la característica, la plataforma, la migración, y los temas de disponibilidad dentro de las áreas específicas. En muchos casos, la misma versión no trabaja en las plataformas heterogéneas. En otros casos, la organización no puede esperar una versión para soportar todos sus requisitos. El objetivo es identificar la menor cantidad de seguimientos de software para la red considerando los requisitos de prueba/validación, certificación y actualización. En muchos casos, la organización puede tener levemente más pistas para bajar la prueba/validación, certificación, y costes de la actualización en conjunto.

El primer hecho diferenciador es el soporte de plataforma. En general, cada uno de los switches LAN, switches WAN, routers de núcleo y routers de borde tienen ramas de software individuales. Pueden necesitarse otros seguimientos de software para funciones o servicios específicos, como Data-Link Switching (DLSw), Calidad de Servicio (QoS) o IP Telephony, especialmente si este requisito puede localizarse dentro de la red.

Otros criterios son confiabilidad. Muchas organizaciones intentan funcionar con la mayoría del software confiable hacia el núcleo de la red y el centro de datos, mientras que ofrecen más nuevas funciones avanzadas, o el soporte del hardware, hacia el borde. Por otra parte, el scalability o las características del ancho de banda es a menudo las más necesarias de los entornos de la base o del centro de datos. SE pueden necesitar otras pistas para plataformas específicas, tales como sitios de distribución que tengan una plataforma de router WAN diferente. La siguiente tabla es un ejemplo de definición de seguimiento de software para una organización empresarial grande.

Seguimiento	Área	Plataformas de hardware	Funciones	Versión deL Cisco IOS	Estado de certificación
1	Transferencia de la base LAN	6500	QoS	12.1E(A8)	Prueba
2	Switch de acceso a LAN	2924XL 2948XL	Protocolo de detección de link unidireccional (UDLD), Protocolo de árbol transversal (STP).	12.0(5.2)XU	3/1/01 certificado
3	Distribución de LAN/acceso	5500 6509	Supervisor 3	5.4(4)	7/1/01 certificado

4	(RSM) del Route Switch Module del switch de distribución	RS	Ruteo Abrir el trayecto más corto primero (OSPF)	12.0(11)	3/4/02 certificado
5	Distribución WAN de cabecera	7505 7507 7204 7206	Frame Relay OSPF	12.0(11)	11/1/01 certificado
6	Acceso a WAN	2600	Frame Relay OSPF	12.1(8)	6/1/01 certificado
7	Conectividad de IBM	3600	Headend del Synchronous Data Link Control (SDLC)	11.3(8)T1	11/1/00 certificado

Las asignaciones de seguimiento también pueden modificarse con el transcurso del tiempo. En muchos casos, las características o el soporte del hardware pueden integrar en más versiones de software del mainline permitiendo que diversas pistas emigren eventual junto. Una vez establecidas las definiciones de rastreo, la organización puede usar otros procesos definidos para lograr la consistencia y validación de nuevas versiones. Las definiciones de seguimiento son también un esfuerzo en curso. En cualquier momento una nueva función, servicio, hardware, o se identifica el requerimiento del módulo, una nueva pista debe ser considerada.

Las organizaciones que desean iniciar un proceso de la pista deben comenzar con los requisitos nuevamente definidos de la pista, o en algunos casos, los proyectos de la estabilización para las redes existentes. Una organización puede también tener algunas normalidades identificables con las versiones de software existentes que pueden hacer la definición de pista actual posible. En la mayoría de los casos, la migración rápida a las versiones identificadas no se requiere si el cliente tiene suficiente estabilidad de la red. La arquitectura de red, o el grupo de ingeniería, posee normalmente el proceso de la definición de pista. En algunos casos, un individuo puede ser responsable de las definiciones de pista. En otros casos, los terminales de componente del proyecto son responsables de desarrollar los requisitos de software y las nuevas definiciones de pista basados en los proyectos individuales. Es también una buena idea revisar las definiciones de pista sobre una base trimestral para determinar si se requieren las nuevas pistas, o si las pistas viejas requieren la consolidación o la actualización.

Las organizaciones que identifican y mantienen el seguimiento de software con control estricto de versión han demostrado tener el éxito más alto con un número decreciente de versiones de software en la red de producción. Esto generalmente se traduce en una mayor estabilidad del software y en la confiabilidad general de la red.

Ciclo de actualización y definiciones

Las definiciones del ciclo de actualización se definen como pasos de calidad básicos en la administración del software y de las modificaciones, usados para determinar en qué momento debe iniciarse un ciclo de actualización del software. Las definiciones del ciclo de actualización permiten que una organización planee correctamente para un ciclo de la actualización del software y afecte un aparato a los recursos requeridos. Debido a los requisitos de la función en las versiones actuales estables, sin las definiciones de ciclos de actualización, una organización experimenta normalmente un aumento de problemas de confiabilidad del software. Otra exposición podría ser la organización que perdía la oportunidad de probar y de validar correctamente una nueva versión antes de que se requiera el uso para la producción.

Un aspecto importante de esta práctica está identificando cuando y en qué medida los procesos de planificación del software deben ser iniciados. Esto es debido al hecho de que una causa principal de los problemas del software está girando una característica, un servicio, o una capacidad del hardware en la producción sin la diligencia debida, o a actualizar al nuevo Cisco IOS una versión sin las consideraciones sobre administración del software. Otro problema no está actualizando. Ignorando los ciclos del software normales y los requisitos, muchos clientes hacen frente a la tarea difícil de la actualización de software a través de varias diversas versiones principales. La dificultad se debe al tamaño de las imágenes, cambios de comportamiento predeterminado, cambios en el Interpretador del nivel de comando (CLI) y cambios de protocolo.

Cisco recomienda un ciclo de actualización bien definido, sobre la base de las mejores prácticas según lo definido en este papel, para ser iniciado siempre que se requiera la nuevo característica importante, servicio, o soporte del hardware. El grado de certificación y comprobación/validación debe analizarse (en función del riesgo), para determinar los requisitos precisos de comprobación/validación. El análisis de riesgos pueden realizarse por la ubicación geográfica, la ubicación lógica (capas de acceso, núcleo y distribución) o la cantidad aproximada de gente/clientes afectados. Si la característica importante o la capacidad del hardware se contiene en la versión actual, algunos procesos de ciclo de actualización mejorado deben también ser iniciados. Si la característica es relativamente de menor importancia, considere el riesgo y después decida qué procesos deben ser iniciados. Además, el software se debe actualizar en dos años o menos para ayudar a asegurarse de que su organización permanece relativamente actual y de que el proceso de actualización no es demasiado incómodo.

Los clientes deben también considerar el hecho de que no se hará ningunos arreglos del bug a las secuencias de software que han pasado el estatus del fin de la vida útil (EOL). También deberían tenerse en cuenta los requisitos de la empresa, ya que muchos entornos pueden tolerar, o incluso aceptar, más adiciones de características con muy pocos procesos de prueba/validación, o sin necesidad de ellos, y un tiempo de inactividad reducido. Los clientes deben también considerar los más nuevos datos recopilados en las operaciones de la Versión de Cisco cuando en vista de sus requerimientos de prueba. Un análisis de los bug y de las causas raíz mostró que el amplia mayoría de las causas raíz del bug era el resultado de los desarrolladores que cifraban dentro de la área de software afectada. Esto significa que si una organización está agregando una función particular o un módulo a su red en una versión existente, allí es la probabilidad de experimentar un bug relacionado con esa característica o módulo, pero una probabilidad mucho más baja que la nueva función, el hardware, o el módulo afectarán otras áreas. Estos datos deben permitir que las organizaciones reduzcan los requisitos de comprobación cuando se agregan características o módulos nuevos compatibles con las versiones existentes, al comprobar sólo el nuevo servicio o característica junto con los servicios habilitados. Los datos también se deben considerar al realizar la actualización del software basada en unos pocos errores críticos encontrados en la red.

La siguiente tabla muestra los requisitos de actualización recomendados para una organización empresarial de alta disponibilidad:

Disparador del administrador de software	Requisitos de Ciclo vital del software
Nuevo servicio de red. Por ejemplo, una nueva estructura básica de ATM o un nuevo servicio VPN.	Validación completa del Ciclo vital del software incluyendo la prueba de la nueva función (conjuntamente con otra servicios habilitados), la prueba de topología colapsada, la Análisis del rendimiento del qué si, y la prueba del perfil de aplicación.
La nueva capacidad de la red no se soporta en la versión de software actual. Los ejemplos incluyen QoS y el Multiprotocol Label Switching (MPLS).	La validación completa del Ciclo vital del software incluyendo la prueba de la nueva función, conjuntamente con otra habilitó los servicios, la prueba de topología colapsada, la Análisis del rendimiento del qué si, y la prueba del perfil de aplicación.
Nueva característica importante o módulo de hardware que existen en la versión actual. Por ejemplo, agregando un nuevo módulo, soporte multidifusión, o DLSW del GigE.	Proceso de gestión de candidatos. Validación completa posible basada en los requisitos de versión. Posibilidad de validación o prueba limitada si la administración de candidatos identifica a la versión actual como potencialmente aceptable.
Adición menor de característica. Por ejemplo, un dispositivo TACACS para el control de acceso.	Considere la administración del candidato basada en el riesgo de la característica. Considere probar o pilotar la nueva función basada en el riesgo.
Software en la producción por dos años o un estudio trimestral del software.	Administración del candidato y decisiones comerciales en lo que respecta a la administración del ciclo vital completa de identificar la versión defendible actual.

Actualizaciones de emergencia

En algunos casos, las organizaciones hacen frente a la necesidad Actualizar software debido a los bug grave. Esto puede provocar problemas si la organización no posee una metodología de actualización de emergencia. Los problemas con el software pueden variar desde actualizaciones de software no administradas, donde el software se actualiza sin administración de la vida útil del software, hasta situaciones donde los dispositivos de red fallan continuamente, pero la organización no se actualiza ya que no se ha completado la certificación/prueba sobre la siguiente versión candidata. Cisco recomienda un proceso de actualización de emergencia para estas situaciones donde realizan la prueba limitada y a los pilotos en menos áreas críticas del negocio de la red.

Si los errores catastróficos ocurren sin la solución alternativa aparente y el problema es defecto del software relacionado, Cisco recomienda que el soporte de Cisco esté dedicado completamente para aislar el defecto y para determinarlo si o cuando un arreglo está disponible. Cuando la solución se encuentra disponible, Cisco recomienda realizar un ciclo de actualización de emergencia para determinar rápidamente si el problema puede separarse con un tiempo de inactividad limitado. En la mayoría de los casos, una organización está funcionando con una versión admitida del código y el arreglo del problema está disponible en una más nueva versión interina existente del software.

Las organizaciones también pueden prepararse para potenciales actualizaciones de emergencia. La preparación incluye la migración para soportar versiones de IOS de Cisco y la identificación/desarrollo de versiones de reemplazo de candidato dentro del mismo tren de IOS de Cisco como la versión certificada. El software compatible es importante, ya que significa que el desarrollo de Cisco está aún agregando arreglos de errores a la secuencia de software identificada. Manteniendo el software admitido en la red, la organización reduce el tiempo de validación a causa a la base más familiar y códigos estables. Generalmente, un candidato para reemplazo es una nueva imagen de software interina/temporal dentro del mismo tren del IOS de Cisco sin agregados de soporte de funciones o hardware. Una estrategia de reemplazo del candidato es especialmente importante si la organización es en los primeros que lo adquieran la fase de una secuencia de software determinada.

Proceso de certificación

Un proceso de certificación ayuda a asegurarse de que el software validado está desplegado constantemente en el entorno de producción de la organización. Los pasos del proceso de certificación deben incluir la identificación de la pista, las definiciones del ciclo de actualización, la administración del candidato, la prueba/validación, y un cierto uso de la producción piloto. Un proceso de certificación simple, sin embargo, todavía ayuda a asegurarse de que las versiones de software consistente están desplegadas dentro de las pistas identificadas.

Inicie un proceso de certificación identificando a las personas de la arquitectura, ingeniería/implementación y operaciones que elaborarán y administrarán el proceso de certificación. El grupo debe primero considerar las metas comerciales y las capacidades de recurso de asegurarse de que el proceso de certificación habrá continuado el éxito. Después, asigne los individuos o la responsabilidad total de los grupos de los pasos dominantes en el proceso de certificación incluyendo la Administración de la pista, las definiciones actualizadas del ciclo vital, la prueba/validación, y los pilotos. Cada uno de estas áreas se debe definir, aprobar, y comunicar formalmente dentro de la organización.

También incluya los guías para la calidad o la aprobación en cada fase del proceso de certificación. Esto a veces se llama un proceso de la puerta de la calidad porque cierto criterio de calidad debe ser cumplido antes de que el proceso pueda moverse al siguiente paso. Esto ayuda a garantizar que el proceso de certificación sea eficaz y que merezca los recursos asignados. Generalmente cuando los problemas se encuentran con la calidad en una área, el proceso aparta el esfuerzo un paso.

Los softwares candidato pueden no cumplir los criterios de certificación definidos debido a la calidad del software o la conducta inesperada. Cuando existen problemas que afectan el entorno, la empresa debe aplicar un proceso más efectivo a fin de certificar una próxima versión provisoria. Esto ayuda a reducir los requisitos de recursos y, en general, es eficaz si la organización puede entender qué cambió y qué defectos se resolvieron. No es inusual para que una organización experimente un problema con un candidato inicial y certifique un Cisco IOS Release interino

posterior. Las organizaciones pueden también hacer una certificación limitada o proporcionar las advertencias si algunos problemas existen y pueden actualizar a una versión completamente certificada posterior cuando se ha validado un nuevo interino. El siguiente organigrama a continuación es un proceso de certificación básica e incluye gates de calidad (una revisión siguiendo cada bloque):

Diseño - Selección y validación de las versiones deL Cisco IOS

Tener una metodología bien definida para seleccionar y validar las versiones deL Cisco IOS ayuda a una organización para reducir el tiempo de inactividad imprevisto debido a los intentos de actualización fracasados y a los defectos del software imprevistos.

La fase de diseño incluye la administración del candidato y la prueba/validación. La administración del candidato es el proceso usado para identificar las versiones específicas para los agrupamientos de versiones de software definidos. La prueba/validación es una parte del proceso de certificación y se asegura de que la versión de software identificada es acertada dentro de la pista requerida. La prueba/validación debe realizarse en un entorno de laboratorio con una topología colapsada y una configuración muy similar a la del entorno de producción.

Estrategia y herramientas para la selección y validación de IOS de Cisco

Cada organización debe tener un proceso para seleccionar y validar las versiones deL Cisco IOS estándar para la red que comienza con un proceso para seleccionar la versión deL Cisco IOS. Un equipo multidisciplinar de la arquitectura, de la ingeniería, y de las operaciones debe definir y documentar el proceso de gestión de candidatos. Una vez que está aprobado, el proceso se debe volcar al grupo apropiado de la salida. También se recomienda que una plantilla estándar de la administración del candidato esté creada que se puede poner al día con la información del candidato mientras que se identifica.

No todas las organizaciones tienen un ambiente de laboratorio sofisticado que pueda imitar fácilmente el entorno de producción. Algunas organizaciones saltan la prueba de laboratorio debido al costo y la capacidad de pilotar una nueva versión en la red sin el impacto comercial importante. Sin embargo, animan a las organizaciones con amplia disponibilidad a construir un laboratorio que imite la red de producción y a desarrollar una prueba/proceso de validación para asegurar la alta prueba-cobertura para las versiones del nuevo Cisco IOS. Una organización debe dar un plazo de cerca de seis meses para construir el laboratorio. Durante este tiempo, la organización debe trabajar para crear los planes de prueba y los procesos específicos de asegurarse de que el laboratorio será utilizado a su ventaja completa. Para el Cisco IOS, esto significa la creación de los planes de prueba específicos del Cisco IOS para cada pista del software requerido. Estos procesos son fundamentales en organizaciones más grandes porque muchos laboratorios dejan de utilizarse para introducir nuevos productos y software.

Las siguientes secciones describen brevemente las herramientas de administración y prueba/validación que se deben utilizar para la selección y validación de Cisco.

Herramientas de administración del candidato

Nota: Para utilizar la mayoría de las herramientas que se proporcionan a continuación, debe ser un usuario registrado y debe haber iniciado sesión.

- Release Note — Provee información con respecto el hardware, el módulo, y al soporte de

característica de una versión. Las notas de la versión deben revisarse durante la administración de candidato para asegurarse de que haya toda la compatibilidad de software y hardware requerida en la versión potencial, y para comprender cualquier problema de migración incluyendo diferentes comportamientos predeterminados o requisitos de actualización.

Herramientas de prueba y validación

Las herramientas de prueba y validación se utilizan para probar y validar las soluciones de red, incluido el nuevo hardware, el nuevo software y las nuevas aplicaciones.

- **Generadores de tráfico** — Genere los flujos de tráfico de protocolos múltiples y las velocidades de paquetes sin procesar usados para modelar la tarifa a través de cualquier link determinado que utiliza los protocolos específicos. Los usuarios pueden identificar los números de zócalo, MAC de destino y origen. Estos valores pueden incrementarse en pasos específicos o pueden configurarse como estáticos/fijos o en incrementos aleatorios. Los generadores de tráfico pueden generan paquetes para los siguientes protocolos:IPIntercambio de paquetes entre redes (IPX)DECNetAppleSistemas de red Xerox (XNS)Internet Control Message Protocol (ICMP)Internet Group Management Protocol (IGMP)Servicio de red sin conexión (CLNS)User Datagram Protocol (UDP)Servicio de red integrado virtual (VINES)Paquetes de links de datosLas herramientas son disponible desde Agilent y Comunicaciones Spirent .
- **Contador de paquetes/captura/decodificador (sniffer)** — permite que el cliente capture y decodifique selectivamente los paquetes en todo el paquete y capas del link de datos. La herramienta tiene la capacidad de permitirle al usuario especificar los filtros, lo que permite capturar sólo datos de protocolo específicos. Los filtros más futuros permiten que el usuario especifique la captura de los paquetes que corresponden con un IP Address particular, un número del puerto o una dirección MAC. Las herramientas están disponibles en Sniffer Technologies.
- **Simulador de red/emulador** — Permite que el cliente pueble las tablas de ruteo de Routers específico, sobre la base de los requisitos de la red de producción. Soporta la generación de routers de IP Routing Information Protocol (RIP), OSPF, Intermediate System-to-Intermediate System (IS-IS), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP) y Border Gateway Protocol (BGP). Las herramientas son disponible desde comunicaciones y Comunicaciones Spirent de PacketStorm.
- **Emuladores de sesión** — Los flujos de tráfico de protocolos múltiples de la ventana de desplazamiento Generate y son capaces de enviar los flujos de tráfico de protocolos múltiples a través de la red de prueba hacia el dispositivo receptor. El dispositivo receptor devuelve los paquetes con la función de eco hacia la fuente. El dispositivo de origen comprueba el número de paquetes enviados y recibidos, los paquetes sin secuencia y los paquetes con error. La herramienta también otorga flexibilidad para definir los parámetros de ventana en el Protocolo de control de transmisión (TCP), imitando de este modo las sesiones de tráfico cliente/servidor en la red de laboratorio. Las herramientas están disponibles desde Empirix.
- **Emuladores de la red a gran escala** — Ayude en la prueba del scalability de entornos más grandes. Estas herramientas pueden crear e inyectar tráfico del tipo control en una topología de laboratorio con facilidad, con el objetivo de reproducir con mayor detalle, un entorno de producción. Las capacidades incluyen los inyectores de la ruta, los vecinos de protocolo, y acodan a 2 vecinos de protocolo. Las herramientas son disponible desde Agilent y Comunicaciones Spirent .

- **Simuladores de WAN** — Ideal para el tráfico de prueba de la aplicación para empresas donde están potencialmente un problema el ancho de banda y el retardo. Estas herramientas permiten que las organizaciones localmente prueben una aplicación con el retardo y el ancho de banda estimados para ver cómo la aplicación funciona sobre WAN. A menudo se utilizan estas herramientas para el desarrollo de aplicaciones y para los tipos de pruebas para perfiles de aplicaciones dentro de las organizaciones empresariales. Adtech, a

Administración del candidato

La administración del candidato es el proceso de identificar los requisitos de versión de software y los riesgos potenciales para el hardware en particular y los conjuntos de características habilitados. Se recomienda que una organización pasa cuatro a ocho horas que investigan correctamente los requisitos de software, los Release Note, los defectos del software, y los riesgos potenciales antes de pilotar una versión. Lo que sigue delinea la base para la administración del candidato:

- Identifique a los softwares candidato vía las herramientas del Cisco Connection Online (CCO).
- Madurez del software de la análisis de riesgo, nueva función, o soporte del código.
- Identifique y siga los bug de software conocido, los problemas, y los requisitos en el ciclo vital.
- Identifique la conducta de configuración predeterminada de la imagen seleccionada.
- Maintain se retira y los candidatos de la restauración actualizada al candidato potencial cambian.
- Bug-friega.
- Soporte de Advanced Services de Cisco.

La identificación de los softwares candidato llegó a ser más compleja con el número creciente de producciones de Cisco y de secuencias de software. El CCO ahora tiene varias herramientas incluyendo el planificador de la actualización de Cisco IOS, la Herramienta de búsqueda de progración, la matriz de compatibilidad del software-hardware, y la Herramienta de actualización del producto que puede ayudar a las organizaciones para identificar a las revisiones candidata potencial. Estas herramientas se pueden encontrar en http://www.cisco.com/cisco/software/navigator.html.

Después, analice el riesgo del software del candidato potencial. Éste es el proceso de entender donde el software reside actualmente en la curva de la madurez y después el pesaje de los requisitos para despliegue con el riesgo potencial del candidato de la versión. Por ejemplo, si una organización está deseando poner el software del Early Deployment (ED) en un entorno de alta disponibilidad crítico, el riesgo y el requerimiento de recurso asociados para la certificación acertada deben ser considerados. Una organización debe por lo menos agregar a los recursos de administración del software para que las situaciones de más alto riesgo aseguren el éxito. Por otra parte, si una versión del general deployment (GD) está disponible que cubre las necesidades de una organización, después menos recursos de administración del software son necesarios.

Cuando se identifican posibles entregas y riesgos, realice una limpieza de errores para determinar si existe algún error catastrófico ya identificado que potencialmente pudiera impedir la certificación. El vigilante del bug de Cisco, el navegador del bug, y los agentes de vigilancia del bug pueden ayudar a identificar los problemas potenciales y deben ser utilizados en el Ciclo vital del software para identificar los problemas de la seguridad potencial o del defecto.

Un nuevo software candidato debe también ser revisado para la conducta de configuración predeterminada potencial. Esto puede lograrse mediante una revisión de las notas de actualización de la nueva imagen de software y de las diferencias de configuración con la imagen potencial cargada en las plataformas designadas. La administración del candidato puede también incluir la identificación de se retira las versiones o ir-a las versiones si la versión elegida no cumple los criterios de certificación en algún momento del proceso. Mirando los bug relacionados con las características para una pista especificada, una organización puede mantener a los candidatos potenciales para la certificación.

El Advanced Services de Cisco es también una herramienta excelente para la administración del candidato. Este grupo puede proporcionar la opinión más completa en el proceso de desarrollo y la Colaboración entre un gran número de expertos de la industria en muchos diversos entornos del mercado vertical. Generalmente, los mejores eliminadores de errores o las capacidades de administración de candidatos están contemplados por el soporte de Cisco debido al nivel de experiencia y visibilidad en las versiones de software de producción ejecutadas en otras organizaciones.

Prueba y validación

La prueba y la validación es mejores prácticas y conexión de redes de alta disponibilidad de un aspecto crítico de la administración, totales. Las pruebas en laboratorio correctas pueden reducir significativamente el tiempo de inactividad de la producción, ayudan a capacitar al personal del soporte técnico de redes y hacen que los procesos de instrumentación de red sean más eficientes. Sin embargo, para ser eficaz, la organización debe asignar los recursos necesarios para crear y mantener el entorno de laboratorio adecuado, aplicar los recursos necesarios a fin de realizar las pruebas correctas y utilizar una metodología de prueba recomendada que incluya la recopilación de mediciones. Sin ninguno de estos áreas, una prueba y un proceso de validación pueden no resolver las expectativas de una organización.

La mayoría de las organizaciones corporativas no tienen el ambiente de laboratorio recomendado de la prueba. Por este motivo, muchas organizaciones han desplegado las soluciones incorrectamente, han experimentado los errores de modificación de la red, o los problemas del software experimentados que se habrían podido aislar en un ambiente de laboratorio. En algunos entornos, esto es aceptable, pues el costo de tiempo de inactividad no compensa el coste de un ambiente de laboratorio sofisticado. En muchas organizaciones sin embargo, el tiempo muerto no puede ser tolerado. Se insta a estas organizaciones para que desarrollen los laboratorios recomendados, tipos y metodologías de pruebas para mejorar la calidad de la red de producción.

Laboratorio y entorno de prueba

El laboratorio debe ser una zona aislada con suficiente espacio para escritorios, bancos de trabajo, engranajes de prueba y gabinetes o bastidores de equipos. La mayoría de las organizaciones grandes necesitarán entre cuatro a diez estantes de equipo para imitar el entorno de producción. Se recomienda algún tipo de seguridad física para ayudar a mantener un entorno de prueba mientras las pruebas se están realizando. Esto ayuda a evitar que un prueba de laboratorio sea interrumpido debido a otras prioridades de laboratorio incluyendo el préstamo, el entrenamiento, o los ensayos de implementación del hardware. La seguridad lógica también se recomienda para evitar que las rutas falsas ingresen la red de producción o el tráfico indeseable de salir el laboratorio. Esto se puede llevar a cabo con la ayuda de filtros de ruteo y listas de acceso ampliado en un router de gateway de laboratorio. La Conectividad a la red de producción es útil para las descargas del software y el acceso a la red de laboratorio del entorno de producción.

La topología de laboratorio debe ser capaz de duplicar el entorno de producción para los planes de prueba específicos. Se recomienda el hardware de reproducción, la topología de red, y las configuraciones de la característica. Por supuesto, la reproducción de la topología real es casi imposible, pero qué puede ser hecha es reproducir la jerarquía de red y la interacción entre los dispositivos de producción. Esto es importante para la interacción del protocolo o de la función entre varios dispositivos. Algunas topologías de prueba serán diferentes según los requisitos de prueba del software. El Cisco IOS PÁLIDO del borde que prueba, por ejemplo, no debe requerir los dispositivos de tipo LAN o la prueba y puede requerir solamente los routeres de borde de WAN y a los routeres de distribución de WAN. La clave es imitar la funcionalidad del software sin la producción de duplicación. En algunos casos, las herramientas se pueden incluso utilizar para imitar el comportamiento en grande tal como cuentas y tablas de ruteo del vecino de protocolo.

También se necesitan herramientas para ayudar con algunos tipos de pruebas mediante la mejora de la capacidad para duplicar el entorno de producción y para reunir datos de pruebas. Las herramientas que ayudan a la producción mímica incluyen colectores de tráfico, generadores de tráfico y dispositivos de simulación WAN. Smartbits es un buen ejemplo de un dispositivo que puede recolectar y repetir el tráfico de red o generar volúmenes de tráfico grandes. Una organización puede también beneficiarse de los dispositivos que pueden ayudar a recoger los datos, tales como analizadores de protocolo.

El laboratorio también requiere una cierta Administración. Muchas organizaciones más grandes tienen un administrador de laboratorio a tiempo completo que tenga la responsabilidad de manejar la red de laboratorio. Otras organizaciones utilizan la arquitectura existente y los equipos de ingeniería para validación de lab. Las responsabilidades de administración del laboratorio incluyen el equipo y activo de laboratorio que ordenan administración del espacio que siguen, del cableado, físico, definiendo las reglas y dirección del laboratorio, laboratorio que programa, documentación de laboratorio, configurando las Topologías de laboratorio, escribiendo los planes de prueba, realizando los pruebas de laboratorio, y el manejo de los problemas identificados potencial.

Tipos de pruebas

En general, hay muchos tipos de pruebas diferentes que pueden realizarse. Antes de que construya un laboratorio y un plan de prueba completos de prueba que puedan probar todo en un conjunto de configuraciones, una organización deba entender los diversos tipos de prueba, el intento de la prueba, e independientemente de si deben el dirigir de Cisco, la comercialización técnica, o la Ayuda al cliente o podría ser responsable de algunas de las diversas pruebas. Los planes de prueba del cliente cubren generalmente los tipos expuestos de la prueba. La siguiente tabla ayuda a entender los diferentes tipos de prueba, cuándo deben realizarse las pruebas y las partes responsables.

De las pruebas abajo, la prueba apropiada del conjunto de características específico de una organización, la topología, y la combinación de aplicaciones es normalmente las más valiosas. Es importante saber que Cisco realiza la característica y la prueba de regresión completas, no obstante Cisco no puede probar el perfil de aplicación de su organización con su combinación de topología, hardware, y funciones configuradas específicos. De hecho, es infeasible probar el alcance total de las características, del hardware, de los módulos, y de las permutaciones de topología. Además, Cisco no puede probar la Interoperabilidad con el equipo de proveedor externo. Cisco recomienda que las organizaciones prueban la combinación exacta de hardware, de módulos, de características, y de topología encontrada en su entorno. Esta prueba se debe conducir en un laboratorio, con una topología derrumbada representando el entorno de producción de su organización con otros prueba-tipos que soportan tales como funcionamiento, Interoperabilidad, caída del sistema, y marcar a fuego.

Prueba	Información general sobre pruebas	Responsabilidad de prueba
Característica y funciones	Determina si los módulos básicos de las características deL Cisco IOS y de Cisco Hardware funcionan según lo hecho publicidad. Las opciones de configuración de la característica o de la funcionalidad del módulo así como de la característica deben ser probadas. La extracción de configuración y la adición deben ser probadas. La prueba básica de interrupción y el testeo programado es incluidos.	Prueba del dispositivo de Cisco
Regresión	Determina si la característi	Prueba de regresión de Cisco

	ca o el módulo funciona conjuntamente con otros módulos y características, y si la versión deL Cisco IOS funciona conjuntamente con otras versiones deL Cisco IOS en relación con las características definidas. Incluye cierto marcar a fuego y prueba de interrupción.	
Funcionamiento del dispositivo básico	Determina el rendimiento básico de la característica o del módulo para determinar si la característica deL Cisco IOS o los módulos de hardware cumple los requerimientos mínimos	Prueba del dispositivo de Cisco

	bajo carga.	
Topología/característica/combinación de hardware	Determina si las características y los módulos funcionan según lo esperado en una topología y un módulo/una característica/una combinación de hardware específicos. Esta prueba debería incluir la verificación de protocolos, funciones y de los comandos show, las pruebas programadas en fábrica y las pruebas de interrupción.	Cisco prueba las topologías des divulgación estándar en los laboratorios tales como Enterprise Solutions Engineering (ESE) e ingeniería de prueba de integridad de las soluciones en red (NSITE). Los clientes de gran disponibilidad deben probar la característica/el módulo/las combinaciones de topología como sea necesario, especialmente con los primeros que lo adquieran el software y las topologías no estándar.
Interrupción (Qué pasa si)	Incluye los tipos o los comportamientos comunes de la caída del sistema que pueden ocurrir en un impacto específico de las	Cisco es responsable de la prueba básica de interrupción. Los clientes son en última instancia responsables por problemas de rendimiento de la caída del sistema relacionados con el scalability de su entorno individual. La prueba de interrupción debe ser hecha, si es

	funciones de la característica/del módulo/del entorno de topología y del potencial. Las pruebas de interrupción incluyen el intercambio de tarjeta, oscilación de link, fallas de link y fallas de tarjeta.	posible, en el entorno del laboratorio del cliente.
NetworkPerformance (qué si)	Investiga la carga del dispositivo en relación con una característica/un hardware/una combinación de topología específicos. El centro de atención es el desempeño y la capacidad del dispositivo como por ejemplo la utilización de la CPU, la memoria y el búfer y el uso del link con relación al	Los clientes son en última instancia responsables de la carga del dispositivo y del scalability. La carga y las dudas acerca de la escalabilidad son despertadas a menudo por las ofertas de Cisco o el Advanced Services y probadas a menudo con los laboratorios de Cisco tales como el Customer Proof-of-Concept Labs (CPOC).

	tipo de tráfico y a los requerimientos de los recursos en cuanto a protocolos, vecinos, número de rutas y otras características del conjunto. Esta prueba ayuda a asegurar la escalabilidad en entornos más grandes.	
Arreglo del bug	Se asegura de que los arreglos del bug reparen el defecto identificado.	Cisco prueba los arreglos del bug para asegurarse de que el bug está reparado. Los clientes deben también probar para asegurarse de que el bug que han experimentado está reparado y de que el bug no rompe ningún otro aspecto del módulo o de la característica. Las versiones de mantenimiento son regresión probada pero las versiones interinas no están generalmente.
Administración de la red	Investiga las capacidades de administración del Simple Network Management Protocol	Cisco es responsable de probar las características SNMP, las funciones, y la exactitud básicas de la variable MIB. Los clientes deben validar los resultados de administración de red y son en última instancia

	(SNMP), la precisión variable del SNMP MIB, el soporte de trampa, y el soporte de Syslog.	responsables de la estrategia de administración y de la metodología para las implementaciones de la tecnología nueva.
Emulación de la red a gran escala	La emulación de la red a gran escala utiliza las herramientas tales como simulador del router de Agilent y conjunto de herramientas de evaluación de Spirent para simular entornos más grandes. Esto podría incluir los vecinos protocolos, los conteos de circuito virtual permanente de retransmisión de tramas (PVC), los tamaños de las tablas de ruteo, las entradas de memoria	Los clientes de Cisco son generalmente responsables de los aspectos de la prueba de la simulación de red que reproduce su entorno de red, que puede incluir el número de vecinos del Routing Protocol/las adyacencias y los tamaños de la tabla de ruteo asociados y otros recursos que estén en la producción.

	caché y otros recursos normalmente necesarios en la producción que no están disponibles en laboratorio de forma predeterminada.	
Interoperabilidad	Prueba todos los aspectos en cuanto a conectividad al equipo de red de tercera persona, especialmente si se requiere la Interoperabilidad del protocolo o de la señalización.	Los clientes de Cisco son generalmente responsables de todos los aspectos de la prueba de Interoperabilidad.
Marcar a fuego	Investiga a los recursos del router en un cierto plazo. Las pruebas del marcar a fuego requieren típicamente un dispositivo estar bajo cierta carga con	Cisco realiza el testeo programado básico. La Prueba de cliente se recomienda en relación con la topología única, el dispositivo y las combinaciones de características.

	la investigación en la utilización de recursos incluyendo la memoria, el CPU, y los buffers en un cierto plazo.	

Metodología de prueba

Una vez que una organización conoce lo que él está probando, una metodología se debe desarrollar para el proceso de prueba. El objetivo de una mejor práctica es probar la metodología para ayudar a comprobar que lo acordado sobre las pruebas es completo, bien documentado, fácil de reproducir y valioso en términos de encontrar los problemas potenciales de producción. La documentación y los escenarios de laboratorio de la reconstrucción es especialmente importantes para las versiones posteriores de prueba o para los arreglos del bug de prueba encontró en el ambiente de laboratorio. Los pasos de una metodología de prueba se muestran abajo. También pueden realizarse algunos pasos de prueba simultáneamente.

1. Cree una Topología de prueba que simule el entorno de producción bajo prueba. Un entorno de prueba PÁLIDO del borde puede incluir algunos routeres del núcleo y a un router de borde solamente, mientras que una prueba LAN puede incluir más dispositivos que puedan representar mejor el entorno.
2. Características de la configuración que simulan el entorno de producción. La configuración de los dispositivos del laboratorio debe hacer juego de cerca la configuración del hardware y del software prevista del dispositivo de producción.
3. Escriba un plan de prueba, definiendo las pruebas y las metas, documentando la topología, y definiendo las pruebas funcionales. Las pruebas incluyen la validación básica del protocolo, la validación del comando show, interrupción de la prueba y prueba de impresión a fuego. Un ejemplo de una prueba específica dentro de un plan de prueba se encuentra en la tabla siguiente.
4. Valide la encaminamiento y la funcionalidad del protocolo. Documento o resultados previstos línea de fondo del **comando show**. Los protocolos deberían incluir tanto protocolos de Capa 2 (por ejemplo ATM, Frame Relay, Protocolo de detección de Cisco (CDP), Ethernet y Árbol de expansión) como protocolos de Capa 3 (por ejemplo IP, IPX y multidifusión).
5. Valide la funcionalidad de la característica. Documento o resultados previstos línea de fondo del **comando show**. Las características pueden incluir los comandos global configuration y cualquier función crítica tal como Authentication, Authorization, and Accounting (AAA).
6. Simule carga, que es lo esperado en el entorno de producción. La simulación de la carga se puede hacer con los colectores/los generadores del tráfico. Validar las variables de uso del dispositivo de redes esperadas incluidas la CPU, memoria, uso del búfer y estadísticas de interfaz con una investigación de pérdida de paquetes. El documento o la línea de fondo contaba con los resultados del **comando show**.

7. Realice la prueba de interrupción del donde se esperaba que el dispositivo y el software trataran o previnieran bajo carga. Por ejemplo, "cómo retirar la placa", link inestable, inestabilidad de ruta, y tormentas de broadcast. Asegúrese de que el SNMP traps correcto se esté generando sobre la base de las características que son utilizadas dentro de la red.
8. Documente los resultados de la prueba y las mediciones del dispositivo como las pruebas deben ser repetibles.

Pruebe el nombre	**Conmutación por falla del Hot Standby Router Protocol (HSRP)**
Pruebe los requisitos para la configuración	Aplique la carga a la interfaz del gateway principal. El tráfico debe ser aproximadamente 20% hacia la gateway desde la perspectiva de la estación del usuario y 60% entrante hacia la perspectiva de la estación del usuario. También, aumente el tráfico a una carga más alta.
Pasos de prueba	Monitor STP y HSRP vía los **comandos show**. Falle la conexión de interfaz del gateway principal y después recupere la conexión después de que se recoja la información.
Medidas esperadas	CPU durante la Conmutación por falla. Muestra la interfaz antes, durante y después del gateway principal y secundaria. Mostrar la interfaz HSRP antes, durante, y después.
'Resultados esperados'	La gateway primaria conmuta por error hacia la otra gateway del router en dos segundos. **los comandos show** reflejan correctamente el cambio. La Conmutación por falla al gateway principal ocurre cuando se restablece la Conectividad.
Resultados reales	
Éxito o error	
Modificaciones requeridas para alcanzar el paso	

Mediciones del dispositivo

Durante la fase de prueba, realice y documente las medidas siguientes para asegurarse de que el dispositivo se está realizando correctamente:

- Uso de la memoria

- Cargas CPU
- Uso de búfer
- Estadísticas de la interfaz
- Tablas de rutas
- Debugging específico

La información para las mediciones varía de acuerdo a la prueba implementada. Puede haber información adicional para la medición. Esto depende de los problemas específicos que se están tratando.

Para cada aplicación se esté probando que, los parámetros de la medida a asegurar allí no son ningún impacto del rendimiento adverso en la aplicación dada. Esto es completada utilizando una línea de base de rendimiento que se pueda utilizar para comparar el funcionamiento pre y el despliegue del poste. Los ejemplos para las pruebas de la medida de la aplicación incluyen:

- El tiempo promedio que lleva registrarse en una red.
- El tiempo promedio que requiere el Sistema de archivos de red (NFS) para copiar un grupo de archivos.
- El tiempo promedio que toma para poner en marcha una aplicación y para conseguir indicada con la primera pantalla.
- Otros parámetros específicos de la aplicación.

Implementación - Despliegue rápido y acertado del Cisco IOS

Un proceso de instrumentación bien definido permite que una organización despliegue eficientemente las versiones del nuevo Cisco IOS.

La fase de implementación incluye el proceso piloto y el proceso de instrumentación. El proceso piloto se asegura de que la versión deL Cisco IOS sea acertada en el entorno y el proceso de instrumentación permite las implementaciones rápidas y acertadas del Cisco IOS de una escala más grande.

Estrategia y herramientas para la instalación del IOS de Cisco

La estrategia para las implementaciones del Cisco IOS es realizar una certificación final vía un proceso piloto y una implementación rápida por medio de herramientas de actualización y un proceso de implementación bien definido.

Antes de iniciar un proceso piloto de la red, muchas organizaciones construyen las guías de consulta experimentales generales. Las pautas piloto deberían incluir las expectativas de todos los pilotos, como criterios, ubicaciones aceptables de pilotos, documentación piloto, expectativas de propietarios de pilotos, requisitos de notificación de usuarios y tiempos piloto previstos. Un equipo multidisciplinar de la ingeniería, de la implementación, y de las operaciones está implicado normalmente en la construcción de las guías de consulta experimentales totales y de un proceso piloto. Una vez creado el proceso piloto, los grupos individuales de implementación pueden llevar a cabo pilotos exitosos mediante los mejores métodos de práctica conocidos.

Una vez que se haya aprobado una nueva versión de software para la implementación y la certificación final, la organización necesita iniciar la planeación de la actualización de IOS de Cisco. La planificación comienza con la identificación de los requerimientos de una nueva imagen, que incluyen la plataforma, la memoria, flash y la configuración. La arquitectura y los grupos de

ingeniería definen normalmente los nuevos requisitos de la imagen del software en la fase de la administración del candidato del ciclo de vida de la administración del Cisco IOS. Una vez que se identificaron los requerimientos, el grupo de implementación debe validar cada dispositivo y, si es posible, actualizarlo. El módulo CiscoWorks2000 Software Image Manager (SWIM) también puede ejecutar el paso de validación mediante la validación de los requerimientos de Cisco IOS en relación con el inventario de dispositivos. Cuando todos los dispositivos fueron validados y/o actualizados con los nuevos estándares de imagen correctos, el grupo de implementación puede iniciar un proceso de implementación de comienzo lento que utiliza el módulo SWIM de CiscoWorks2000 como herramienta de despliegue de software.

Una vez que la nueva imagen se ha implementado exitosamente varias veces, la organización puede comenzar a ponerse en funcionamiento al usar SWIM CiscoWorks.

Administración de inventario del Cisco IOS

El administrador de inventario CiscoWorks2000 Resource Manager Essentials (RME) simplifica mucho la administración de versiones de los routers y switches de Cisco a través de herramientas de informes basados en la Web que informan y ordenan los dispositivos Cisco IOS según la versión del software, la plataforma del dispositivo y el nombre de éste.

SWIM del Cisco IOS

El SWIM CiscoWorks2000 puede ayudar a reducir las complejidades falibles del proceso de actualización. Los links incorporados al CCO correlacionan información en línea de Cisco sobre las parches de software con el Cisco IOS y el software Catalyst desplegado en la red, resaltando las notas técnicas relacionadas. Las nuevas herramientas de las hojas de operación (planning) encuentran los requisitos del sistema y envían las notificaciones cuando las actualizaciones de hardware (ROM del inicio, RAM de destello) son necesarias soportar las actualizaciones propuestas de la imagen del software.

Antes de que se inicie una actualización, los requisitos previos de una nueva imagen se validan contra los datos del inventario del Switch o del router de la blanco para ayudar a asegurar una actualización satisfactoria. Cuando se actualizan múltiples sistemas, SWIM sincroniza las tareas de descarga y permite al usuario monitorear el progreso del trabajo. Los trabajos programados son controlados a través de un proceso de cierre de datos, permitiendo que los gerentes autoricen las actividades de un técnico antes de iniciar cada actividad de actualización. RME 3.3 incluye la capacidad para analizar las actualizaciones del software para Cisco IGX, BPX, y las plataformas de MGX, que en gran medida simplifican y reducen el tiempo requerido para determinar el impacto de una actualización de software.

Proceso piloto

Para minimizar la exposición potencial y más con seguridad a la captura se recomienda cualquier problema de producción restante, un piloto de software. En general, los pilotos son más importantes para los nuevos despliegues tecnológicos, sin embargo, muchos despliegues nuevos de software serán enlazados con los servicios, las funciones o hardware nuevos, donde un piloto es más crítico. El plan piloto individual debe tener en cuenta la selección piloto, la duración piloto y la medición. La selección de piloto es el proceso para identificar cuándo y dónde debe realizarse un piloto. La medición piloto es el proceso de recopilación de los datos necesarios para identificar el éxito y el fracaso o los problemas potenciales.

La selección experimental identifica donde y cómo completarán a un piloto. Un piloto puede

comenzar con un dispositivo en un área de bajo impacto y extender a los dispositivos múltiples en un área más de alto impacto. Algunas consideraciones para la selección piloto donde se puede reducir el impacto son las siguientes:

- Instalado en un área de la red resistente a un impacto del único dispositivo debido a la Redundancia.
- En un área de la red con un número mínimo de usuarios detrás del dispositivo seleccionado que puede ocuparse de un cierto impacto posible de la producción.
- Consider que separa al piloto a lo largo de las líneas de la arquitectura. Por ejemplo, pilótela en el acceso, la distribución, y/o las capas del núcleo de la red.

La duración de este piloto deberá basarse en el tiempo que requiere para probar y evaluar suficientemente todas las funciones de los dispositivos. Esto debe incluir el marcar a fuego y la red bajo cargas de tráfico normales. La duración también depende del paso en la actualización de código y del área de la red donde el Cisco IOS se está ejecutando. Si el Cisco IOS es una nueva versión principal, se prefiere un período piloto más largo. Mientras que si la actualización es una versión de mantenimiento con funciones nuevas mínimas, un período piloto más corto será suficiente.

Durante la fase piloto es importante monitorear y documentar los resultados de la misma manera como pruebas iniciales. Puede incluir encuestas, recolección de datos piloto, recolección de problemas y criterios de falla/éxito. Los individuos deben ser directamente responsables del seguir y el progreso experimental que monitorea para asegurar todos los problemas se identifica y que satisfacen a los usuarios y a los servicios implicados en el piloto con los resultados experimentales. La mayoría de las organizaciones certificarán una versión si es acertada en un piloto o un entorno de producción. En algunos entornos, este paso es un fracaso crítico debido a un éxito percibido cuando no se identifican o documentan criterios de medición o éxito.

Instrumentación

Después de la fase piloto se ha completado dentro de la red de producción, comienzan la fase de implementación del Cisco IOS. La fase de implementación incluye diversos pasos para asegurar el éxito de la actualización del software y la eficacia de la implementación, incluyendo inicio lento de la implementación, certificación final, preparación de la actualización, automatización de la actualización y validación final.

El lento-principio de la implementación es el proceso lentamente de implementar una versión nuevamente probada para asegurarse de que la imagen tiene exposición completa al entorno de producción antes de la certificación final y de la conversión completa. Algunas organizaciones pueden comenzar con un dispositivo y un día de exposición antes de pasar a las actualizaciones de dos dispositivos al día siguiente y quizás algunos más al otro día. Cuando aproximadamente diez dispositivos se han puesto en la producción, la organización puede esperar hasta una a dos semanas antes de la certificación final de la versión deL Cisco IOS determinada. En la certificación final, la organización puede desplegar más rápidamente la versión identificada con un nivel de confianza mucho más alto.

Después de que el proceso lento del comienzo, todos los dispositivos identificados para la actualización se deba revisar y validar usando el inventario de dispositivos y una matriz de los estándares del Cisco IOS mínimo para que la carga inicial, el DRAM, y el flash se aseguren de que los requisitos están cumplidos. Los datos pueden adquirirse a través de herramientas internas, herramientas SNMP de terceros o a través del uso de CiscoWorks2000 RME. El CiscoWorks2000 SWIM no revisa o inspecciona estas variables antes de instrumentarlas. Sin embargo, es siempre una buena idea conocer cuál esperar durante la implementación intenta.

Si más de cientos dispositivos similares se programan para las actualizaciones, se recomienda fuertemente que un método automatizado esté utilizado. La automatización se ha mostrado para mejorar la eficacia de la actualización y para mejorar el porcentaje de los éxitos de la actualización de dispositivo durante las implementaciones grandes, sobre la base de una actualización interna de 1000 dispositivos con y sin el SWIM. Cisco recomienda que el SWIM del CiscoWorks 2000 esté utilizado para los despliegues debido grandes al grado de verificación que se realiza durante la actualización. El SWIM incluso se retirará de una versión deL Cisco IOS si se detecta un problema. NADE las funciones creando y programando las tareas de actualización, donde un trabajo se configura con los dispositivos, las imágenes de actualización deseadas, y el tiempo de ejecución del trabajo. Cada trabajo debe contener doce o menos actualizaciones de dispositivo, y hasta doce trabajos pueden ejecutarse en paralelo. SWIM también verifica que la versión de actualización de Cisco IOS programada se ejecute satisfactoriamente luego de la actualización. Se recomienda para dar un plazo de aproximadamente veinte minutos para cada actualización de dispositivo (verificación incluyendo). Usando esta fórmula, una organización puede actualizar treinta y seis dispositivos por hora. Cisco también recomienda que un máximo de cientos dispositivos esté actualizado por la tarde para reducir la exposición del problema potencial.

Después de una actualización automática a una nueva versión, una cierta validación se debe hacer para asegurar el éxito. La herramienta SWIM de CiscoWorks2000 puede ejecutar secuencias de comandos personalizadas luego de la actualización a fin de realizar más comprobaciones de éxito. La verificación incluye la validación de que el router tiene el número de rutas apropiado, la garantía de que las interfaces físicas/lógicas están funcionando y activas o la validación de que el dispositivo es accesible. La lista de verificación siguiente de la muestra puede validar completamente el éxito de un despliegue del Cisco IOS:

- ¿El dispositivo recargó correctamente?
- ¿Están dispositivo al que se le puede hacer ping y accesible vía el sistema de administración de la red (NMS) las Plataformas?
- ¿Están las interfaces previstas en el dispositivo para arriba y el active?
- ¿El dispositivo tiene las adyacencias correctas del Routing Protocol?
- ¿Se puebla la tabla de ruteo?
- ¿El dispositivo está pasando el tráfico correctamente?

Funciones: gestionar la implementación de Cisco IOS de alta disponibilidad

Las operaciones de gran disponibilidad de la mejor práctica del entorno del Cisco IOS ayudan a reducir la complejidad de la red, a mejorar el tiempo de solución de problemas, y a mejorar la disponibilidad de la red. La sección de operaciones de la administración de Cisco IOS incluye estrategia, herramientas y metodologías de mejores prácticas recomendadas para administrar Cisco IOS.

Las mejores prácticas para las operaciones del Cisco IOS incluyen el control de versión de software, el Cisco IOS Administración de Syslog, la administración de problemas, la estandarización de la configuración, y la Administración de la disponibilidad. El control de versión de software es el proceso de seguir, de validar, y de mejorar el estado coherente del software dentro de los agrupamientos de versiones de software identificados. La Administración de Syslog del Cisco IOS es el proceso dinámico de monitorear y de la actuación sobre mensajes de Syslog más prioritarios generados por el Cisco IOS. La administración de problemas es la práctica de recolectar información sobre problemas críticos de manera rápida y eficiente para cuestiones de

software, con el fin de prevenir que se repitan en el futuro. La estandarización de la configuración es el proceso de estandardizar las configuraciones para reducir el potencial para que el código no comprobado sea ejercitado en la producción y para estandardizar el Network Protocol y el comportamiento de la característica. La Administración de la disponibilidad es el proceso de mejorar la Disponibilidad basado en la métrica, los objetivos de mejora, y los proyectos de la mejora.

Estrategias y herramientas para el funcionamiento del IOS de Cisco

Muchas estrategias de calidad y herramientas existen para ayudar a manejar los entornos del Cisco IOS. La primera estrategia clave para las operaciones de Cisco IOS es mantener el entorno sencillo, al evitar la variación en la configuración y en las versiones de Cisco IOS tanto como sea posible. La certificación del Cisco IOS se ha discutido ya, no obstante 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 de operaciones tenía a su cargo la configuración y el mantenimiento de los estándares por medio del control y los estándares de configuración y control de la versión ISO de Cisco.

La segunda estrategia para las operaciones del Cisco IOS es la capacidad de identificar y de resolver rápidamente a las fallas de la red. Los problemas de red se deben identificar generalmente por el grupo de operaciones antes de que los usuarios los llamen adentro. Deberían resolverse los problemas tan pronto como sea posible antes de que afecten aún más el entorno o provoquen cambios mayores en él. Algunas las prácticas recomendadas dominantes en esta área son administración de problemas y Administración de Syslog del Cisco IOS. Una herramienta a ayudar rápidamente a diagnosticar las caídas del Cisco IOS Software es el Output Interpreter de Cisco.

La tercera estrategia es mejora constante. El proceso primario es mejorar una Disponibilidad calidad-basada del programa de mejora. Realizando la análisis de la causa raíz en todos los problemas, incluyendo los asuntos relacionados del Cisco IOS, una organización puede mejorar la cobertura de la prueba, mejorar los tiempos de solución de problemas, y mejorar los procesos que eliminan o reducen el impacto de la caída del sistema. La organización también puede analizar los problemas comunes y crear procesos para resolverlos más rápidamente.

Las herramientas para operaciones de IOS de Cisco incluyen administración del inventario para el control de la versión de software (CiscoWorks2000 RME), administración de Syslog para mensajes Syslog y administradores de configuración de dispositivos para administrar la uniformidad en la configuración de dispositivos.

Administración de Syslog

Los mensajes syslog son mensajes enviados por el dispositivo a un servidor de recolección. Estos mensajes pueden ser errores (por ejemplo, un link bajando), o pueden ser informativos, tales como cuando alguien ha ingresado a configurar una terminal en un dispositivo.

Las herramientas de Administración de Syslog registran y los mensajes de Syslog de la pista recibidos por el Routers y el Switches. Algunas herramientas poseen filtros para permitir la eliminación de mensajes no deseados que pueden opacar a otros verdaderamente importantes. Las herramientas de Syslog también permiten la creación de informes basados en los mensajes recibidos. Los informes pueden ordenarse por período de tiempo, dispositivo, tipo de mensaje o prioridad de mensaje.

La herramienta más popular del Syslog para la Administración del Cisco IOS es CiscoWorks2000 administrador de RME Syslog. Otras herramientas están disponibles incluyendo el SL4NT, un programa del shareware de Netal y el soldado I de OpenSystems.

Administrador de la configuración del dispositivo de los CiscoWorks

El administrador de la configuración del dispositivo CiscoWorks2000 mantiene un archivo activo y proporciona una forma sencilla de poner al día los cambios de configuración a través de los routeres Cisco y del Switches múltiples. El administrador de configuración monitorea la red para los cambios de configuración, pone al día el archivo cuando se detecta un cambio, y registra el cambio en la información al servicio de la auditoría de cambio. Una interfaz de usuario en Internet permite que usted busque el archivo para los atributos de la configuración específicos y que compare el contenido de dos archivos de configuración para la identificación fácil de las diferencias.

Output Interpreter de Cisco

El Cisco Output Interpreter es una herramienta utilizada para diagnosticar caídas del sistema forzadas por software. La herramienta puede ayudar a identificar defectos de software sin llamar al Centro de asistencia técnica de Cisco (TAC), o puede ser usada como información primaria para el TAC luego de producirse una caída del sistema forzada por software. Esta información ayudará generalmente a apresurar una resolución al problema, por lo menos en términos de colección de la Información requerida.

'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. El control de versión de software es generalmente realizado usando un proceso de certificación y un control de los estándares. Muchas organizaciones publican los estándares de versión en un servidor Web central. Además, entrenan al personal de la implementación para revisar qué versión se está ejecutando y poner al día la versión si no es cumple con las normas. Algunas organizaciones tienen un proceso de la puerta de la calidad donde la validación secundaria se completa con las auditorías para asegurarse de que el estándar está seguido durante la implementación.

Durante la operación, no es infrecuente ver las versiones no estándar en la red, especialmente si la red y el personal de las operaciones son grandes. Esto podría deberse al personal más reciente sin entrenamiento, a los comandos de inicio mal configurados o a las implementaciones sin verificar. Es siempre una buena idea validar periódicamente los estándares de versión de software usando las herramientas tales como CiscoWorks 2000 RME que pueda clasificar todos los dispositivos por la versión deL Cisco IOS. Cuando se identifican versiones de software no estándar, deben marcarse inmediatamente y debe iniciarse un ticket de problema o uno de cambio para hacer que la versión corresponda al estándar identificado.

Administración proactiva de Syslog

La recolección, el monitoreo y el análisis de Syslog son los procesos de administración de fallas recomendados para resolver más problemas de redes específicos de Cisco IOS que son difíciles o imposibles de identificar por otros medios. La colección de syslog, la supervisión, y la ayuda del análisis para mejorar el tiempo de solución de problemas identificando y resolviendo muchos incidentes dinámico antes de que se experimenten más problemas de red grave, o son señaladas

por los usuarios. El Syslog también proporciona un método más eficiente de recoger una amplia variedad de problemas cuando está comparado a la Consulta SNMP constante para un gran número de variables MIB. La colección de syslog, la supervisión, y el análisis es lograda utilizando la configuración del Cisco IOS correcta, las herramientas de la correlación del Syslog, tales como Administración CiscoWorks2000 RME, y/o del evento de syslog. Remitiendo hace a la Administración del evento de syslog analizando los datos Syslog recogidos para los mensajes críticos identificados y después una alerta o el desvío a un administrador del evento para la notificación y la resolución en tiempo real.

La supervisión del sistema de registro requiere de la ayuda de la herramienta NMS o de secuencias para el análisis y la generación de informes en los datos del sistema de registro. Incluye la capacidad para ordenar los mensajes de Syslog por período de tiempo y fecha, dispositivo, tipo de mensaje o frecuencia de mensaje. En redes más grandes, las herramientas o los scripts se pueden implementar para analizar los datos Syslog y para enviar las alertas o las notificaciones a los sistemas de administración de eventos o las operaciones y personal de ingeniería. Si las alertas para una amplia variedad de datos Syslog no se utilizan, la organización debe revisar un diario más prioritario de los datos Syslog por lo menos y crear los ticketes de problemas por problemas potenciales. Para dinámico detectar los problemas de red que no se pueden considerar con la supervisión normal, revisión periódica y análisis de los datos Syslog históricos se deben realizar para detectar las situaciones que pueden no indicar un problema inmediato, pero puede proporcionar una indicación de un problema antes de que se convierta en afectación del servicio.

Administración de problemas

Muchos clientes experimentan el tiempo de inactividad debido adicional a una falta de procesos en administración de problemas. El tiempo muerto adicional puede ocurrir cuando los administradores de la red intentan resolver el problema que usa rápidamente una combinación de comandos o de cambios de configuración de servicio-afectación bastante que pasando el tiempo en la Identificación del problema, la recopilación de información, y un trayecto de solución bien-analizado. La conducta observada en esta área incluye recargar los dispositivos, o borrar las tablas de IP Routing antes de investigar un problema y su causa raíz. En algunos casos, esto ocurre debido a los objetivos de la solución de problemas del 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.

Un proceso de administración de problema se recomienda en entornos más grandes. Este proceso debe incluir una cierta cantidad de descripciones de problemas predeterminados y de grupos de comandos show adecuados antes de subir al segundo nivel. El primer soporte de nivel debe nunca borrar las rutas o recargar los dispositivos. Óptimamente, la organización de primer nivel debe recolectar información rápidamente y ascender a un segundo nivel. Pasando apenas algunos más minutos inicialmente en la Identificación del problema o la descripción de problemas, una detección de la causa raíz es mucho más probable, así permitiendo una solución alternativa, una Identificación de laboratorio, y una información del bug. El soporte del segundo nivel se debe versificar bien en los tipos de información que Cisco puede necesitar para diagnosticar un problema o clasifiar un informe de bug. Esto incluye vaciados de memoria, resultado de información de ruteo y resultado del comando show del dispositivo.

Estandarización de la configuración

Las normas de configuración del dispositivo globales representan la práctica de mantener los

dispositivos y los servicios similares estándar de los Parámetros de configuración global a través dando por resultado la coherencia de configuración global a nivel empresarial. Los comandos global configuration son los comandos que se aplican al dispositivo entero y no a los puertos individuales, a los protocolos, o a las interfaces. Los comandos global configuration afectan generalmente el acceso del dispositivo, el comportamiento general del dispositivo, y la seguridad del dispositivo. En el Cisco IOS esto incluye los comandos service, los comandos ip, los comandos vty, los comandos del puerto de la consola, los comandos logging, los comandos AAA/TACACS+, los comandos SNMP, y los comandos del banner. También importante en las normas de configuración del dispositivo globales es una convención para nombres apropiada del dispositivo que permite que los administradores identifiquen el dispositivo, el tipo de dispositivo, y la ubicación del dispositivo basada en el nombre del Sistema de nombres de dominio (DNS) del dispositivo. La coherencia de configuración global es importante para la compatibilidad total y la confiabilidad de un entorno de red porque ayuda a reducir la complejidad de la red y a aumentar la compatibilidad de 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.

Mantener las normas de configuración del dispositivo globales es lograda normalmente por un grupo interno de la ingeniería o de operaciones que cree y mantenga los Parámetros de configuración global para los dispositivos de red similares. Es también una práctica adecuada proporcionar una copia del archivo de configuración global en los directorios TFTP para poderlos descargar inicialmente a todos nuevamente los dispositivos del aprovisionado. También útil es un archivo accesible de la red que proporciona el archivo de configuración estándar con una explicación de cada parámetro de la configuración. Incluso, algunas organizaciones configuran periódicamente dispositivos similares de manera global para garantizar la coherencia de tal configuración o para revisar los dispositivos con regularidad en función de las normas de configuración global adecuadas. Los estándares de configuración de interfaz y protocolo representan la práctica de estándares de mantenimiento para la configuración de interfaz y protocolo.

La consistencia entre la configuración del protocolo y la de la interfaz aumenta la disponibilidad de la red al reducir la complejidad de ésta, brindar el funcionamiento esperado del dispositivo y el protocolo e incrementar la capacidad de soporte de la red. La irregularidad en la configuración de un protocolo o de una interfaz puede resultar en un comportamiento inesperado del dispositivo, problemas de ruteo de tráfico, crecientes problemas de conectividad y creciente tiempo de soporte reactivo. Los estándares de la configuración de la interfaz deben incluir los descriptores de interfaz CDP, la configuración de guardado en memoria caché, y otros estándares del específico del protocolo. Las normas de configuración específicas del protocolo pueden incluir:

- Configuración de IP Routing
- Configuración de DLSw
- Configuración de la lista de acceso
- Configuración de ATM
- Configuración de Frame Relay
- Configuración del árbol de expansión
- Asignación VLAN y configuración
- Protocolo virtual trunking (VTP)
- HSRP

Nota: Es posible tener otras normas de configuración específicas del protocolo dependiendo de qué se configura dentro de la red.

Un ejemplo de los estándares IP puede incluir:

- Tamaño de subred
- Espacio de IP Address usado
- Protocolo de ruteo utilizado
- Configuración de protocolo de ruteo

Mantener los estándares del protocolo y de la configuración de la interfaz es normalmente la responsabilidad de los grupos de la ingeniería y de la implementación de la red. El personal de ingeniería debe encargarse de identificar, probar, validar y documentar los estándares. El grupo de la implementación es entonces responsable de usar los documentos de ingeniería o las plantillas de configuración para provision los nuevos servicios. El grupo de ingeniería debería crear documentación sobre todos los aspectos de estándares requeridos para asegurar consistencia. Las plantillas de configuración se deben también crear para ayudar a aplicar las normas 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 seve de gran asistencia en la prueba, la validación, y la fase de la certificación. De hecho, sin las plantillas de configuración estandardizadas, es casi imposible probar, validar, o certificar adecuadamente una versión deL Cisco IOS para moderado una Red grande.

Administración de la disponibilidad

La Administración de la disponibilidad es el proceso de la mejora de la calidad usando la disponibilidad de la red como la mejora de la calidad métrica. Muchas organizaciones ahora están midiendo el tipo de la Disponibilidad y de la caída del sistema. Los tipos de interrupción incluyen hardware, software, link/portadora, energía/entorno, diseño o error de usuario/proceso. Identificando las caídas del sistema y realizando la análisis de la causa raíz inmediatamente después de la recuperación, la organización puede identificar los métodos para mejorar la Disponibilidad. Casi todas las redes que han alcanzado la Alta disponibilidad tienen cierto proceso de la mejora de la calidad.

Apéndice A - Versiones de la visión general del Cisco IOS

La estrategia de publicación del software del IOS de Cisco se construye alrededor del desarrollo de software seguro, control de calidad y tiempos rápidos de comercialización, factores fundamentales para el éxito de las redes de los clientes de Cisco.

El proceso se define alrededor de cuatro categorías de versiones que se explican a continuación:

- Versión de despliegue temprana (ED)
- Versión principal
- Versión de despliegue limitada (LD)
- Versión del despliegue general (GD)

Cisco crea y mantiene un mapa de ruta IOS que tenga información sobre las versiones individuales, los mercados objetivos, los trayectos de migración, las descripciones de las nuevas funciones, y así sucesivamente.

La figura siguiente ilustra el ciclo de vida de la versión de software del IOS de Cisco:

Versiones ED

Las versiones del Cisco IOS ED son los vehículos que traen la novedad al mercado. Cada

revisión de mantenimiento del versión ED incluye no sólo los arreglos del bug, pero también un conjunto de las nuevas funciones, el nuevo Soporte de la plataforma, y las mejoras generales a los protocolos y a la infraestructura del Cisco IOS. Todos a dos años, las características y las Plataformas de las versiones ED se viran hacia el lado de babor al Cisco IOS Release siguiente del mainline.

Existen cuatro tipos de versiones de ED, cada una con características de modelo de versión y ciclo de vida ligeramente distintas. Las versiones ED se pueden clasificar como:

- **Versiones del Consolidated Technology Early Deployment (CTED)** — El modelo de la versión del nuevo Cisco IOS utiliza el tren de ED release consolidado, también conocido como el tren “T”, para introducir las nuevas funciones, las nuevas plataformas de hardware, y otras mejoras al Cisco IOS. Él se llama tecnología consolidada porque él supera las definiciones internas de las unidades comerciales (BU) y de la línea de negocios (PELOTA ALTA). Los ejemplos de las versiones de tecnología consolidada son Cisco IOS 11.3t, 12.0T, y 12.1T.
- **Versiones del Specific Technology Early Deployment (STED)** — Las versiones STED tienen características similares de la consolidación de la característica como versiones CTED salvo que apuntan un teatro específico de la tecnología o del mercado. Siempre se presentan en plataformas específicas y están solamente bajo la supervisión de una Cisco BU. Las versiones STED se identifican agregando dos letras a la versión principal. Los ejemplos de las versiones STED son el Cisco IOS 11.3NA, 11.3MA, 11.3WA, y 12.0DA.
- **Versiones del Specific Market Early Deployment (S ED)** — El Cisco IOS S ED es distinguido de los STED por el hecho de que él apunta un segmento de mercado vertical específico (ISP, las empresas, las instituciones financieras, las compañías telefónicas, y así sucesivamente). Los S ED incluyen los requisitos de la función específicos de la tecnología solamente para las plataformas de relevancia específicas utilizadas por el mercado vertical previsto. Pueden ser distinguidos de los CTED por el hecho de que están construidos solamente para las plataformas de relevancia específicas al mercado vertical, mientras que los CTED serían construidos para más Plataformas basadas en un requerimiento de tecnología más amplio. Las versiones del Cisco IOS S ED son identificadas por un carácter alfabético añadido al final del fichero al versión principal, edición (apenas como el CTED). Los ejemplos de los S ED son Cisco IOS 12.0S y 12.1E.
- **Las versiones de despliegue tempranas efímeras, también conocidas como versiones X (XED)** — las versiones del Cisco IOS XED introducen el nuevo hardware y las Tecnologías al mercado. No proporcionan revisiones de mantenimiento de software ni proporcionan revisiones interinas de software normal. Si un defecto se encuentra en el XED antes de su convergencia con el CTED, se inicia una recopilación del software y un número se añade al final del fichero al nombre. Por ejemplo, los Cisco IOS Releases 12.0(2)XB1 y 12.0(2)XB2 son ejemplos de las reconstrucciones 12.0(2)XB.

Versiones principales

Las versiones principales son los vehículos de implementación primaria para los Productos del Cisco IOS Software. Son administrados por la División Tecnología del IOS de Cisco y consolida las funciones, plataformas, funcionalidad, tecnología y la proliferación del host de versiones ED anteriores. Las versiones principales de Cisco IOS buscan la mayores estabilidad y calidad. Por esa razón, las versiones principales no validan la incorporación de características o las Plataformas. Cada revisión de mantenimiento proporciona los arreglos del bug solamente. Por ejemplo, los Cisco IOS Software Releases 12.1 y 12.2 son versiones principales.

Las versiones principales tienen actualizaciones de mantenimiento planificado llamadas las versiones de mantenimiento que son completamente regresión probada, incorporan los arreglos del bug más recientes, y no soportan ningunas nuevas Plataformas o característica. El número de versión de una versión importante identifica la importancia de la versión y el nivel de mantenimiento. En el Cisco IOS Software Release 12.0(7), 12.0 es el número de la versión principal, y 7 es su nivel del mantenimiento. El número de versión completo es 12.0(7). De modo similar, 12.1 es una versión principal y 12.1(3) es la tercera versión de mantenimiento de la versión principal 12.1 del IOS de Cisco.

Versiones de la instrumentación limitada (LD)

El LD es la fase de madurez del Cisco IOS entre el FCS y el General Deployment para las versiones principales. Las versiones del Cisco IOS ED viven solamente en la fase de instrumentación limitada porque nunca logran la certificación GD.

Versiones del general deployment (GD)

En algún momento durante la vida útil de la versión, Cisco declarará una versión principal para estar lista para la certificación GD. Sólo una versión principal puede alcanzar el estado GD. Cumple con el objetivo de la certificación GD cuando Cisco se satisface de que la versión ha sido:

- Probada a través de exposición prolongada en el mercado en diversas redes.
- Calificado según mediciones analizadas en función de tendencias de estabilidad y errores.
- Calificado mediante las encuestas de satisfacción de los clientes.
- Una reducción en la tendencia normalizada del cliente encontró los defectos en la versión sobre las cuatro versiones de mantenimiento anteriores.

Forman a un equipo multidisciplinar de la certificación de la Ayuda al cliente GD integrado por los ingenieros de TAC, los ingenieros del Advanced Engineering Services (AES), la ingeniería de prueba del sistema, y dirigir del Cisco IOS para evaluar cada defecto extraordinario de la versión. Este equipo otorga la aprobación final para la certificación GD. Cuando una versión alcance el estado GD, todas las revisiones subsecuentes de la versión también serán GD. Por lo tanto, una versión es una vez GD declarado; ingresa automáticamente la fase de mantenimiento restringido. Mientras está en esta fase, la modificación de ingeniería del código, incluidas las correcciones de errores con rediseño del código principal, está estrictamente limitada y controlada por un administrador de programas. Esto asegura que no se introduzcan errores adversos en una versión de software del IOS de Cisco con certificación GD. GD se logra por medio de una versión de mantenimiento particular. Las actualizaciones del mantenimiento subsiguiente para esa versión son también versiones GD. Por ejemplo, el Cisco IOS Software Release 12.0 consiguió la certificación GD en 12.0(8). Así, los Cisco IOS Software Release 12.0(9), 12.0(10), y así sucesivamente son versiones GD.

Experimental o imágenes de diagnóstico

Experimental o las imágenes de diagnóstico se refieren a veces como especiales de ingeniería y se crean solamente cuando se han identificado los problemas de software críticos. Estas imágenes no son parte del proceso de lanzamiento normal. Las imágenes en esta categoría son estructuras específicas del cliente diseñadas para ayudar a diagnosticar un problema, para probar un arreglo del bug, o para proporcionar un arreglo inmediato. Un arreglo inmediato puede ser proporcionado cuando no es una opción para esperar el interino o la versión de mantenimiento siguiente. Experimental o las imágenes de diagnóstico puede ser empleado cualquier base del software admitido incluyendo el mantenimiento o las versiones interinas de cualquier tipo de versión. Ningunas convenciones para la asignación de nombres oficial existen, pero en muchos

casos el promotor agregará las iniciales, el exp (para experimental), o los dígitos adicionales al nombre de la imagen base. Estas imágenes son soportadas solamente de manera temporal junto con el desarrollo de Cisco debido a que las operaciones de Cisco TAC y de la versión Cisco IOS no conservan documentación complementaria como tablas de símbolos o historia de imagen base. Estas imágenes no experimentan ninguna prueba interna de Cisco.

Puntos destacados de la vida útil de la versión

En algún momento, las versiones GD son substituidas por más nuevas versiones por las últimas tecnologías de interconexión de redes. Por lo tanto, un proceso de eliminación de versión fue establecido con los siguientes tres ejes principales:

- **Final de las ventas (EOS)** — Para las versiones principales, la fecha EOS es tres años después de la fecha del First Commercial Shipment (FCS). Esto fija una última fecha para la cual la versión se pueda comprar para los nuevos sistemas. La versión de EOS aún puede descargarse desde Conexión en línea de Cisco (CCO) para realizar actualizaciones de mantenimiento.
- **Final de la ingeniería (EOE)** — La versión EOE es la versión de mantenimiento más reciente para la versión GD, y sigue típicamente cerca de tres meses después de que la versión EOS. Los clientes pueden continuar recibiendo el Soporte técnico del TAC de Cisco, así como descargan la versión EOE del CCO. Se publica el boletín del producto que anuncia las fechas y versiones de EOS y EOE un año antes de la fecha estipulada de EOS. Ahora, los clientes deben comenzar a investigar actualizar su Cisco IOS Software para aprovecharse de las últimas tecnologías de interconexión de redes.
- **Fin de la vida útil (EOL)** — En el extremo de la vida útil de la versión, todo el soporte para la versión de Cisco IOS Software se termina y no más disponible para descargar la fecha EOL. La fecha EOL es generalmente cinco años después de la fecha EOE. Un boletín de productos EOL se publica aproximadamente un año antes de la fecha real EOL.

Convención para nombres de la versión deL Cisco IOS

La convención para nombres de imágenes del IOS de Cisco proporciona un perfil completo de todas las imágenes lanzadas. El nombre incluye siempre el identificador de la versión principal y el identificador de la versión de mantenimiento. El nombre también podría incluir un designador de tren, un designador de reconstrucción (para la versión de mantenimiento), designadores de características específicas de una unidad de negocios (BU) e identificadores de reconstrucción de designador de característica específica de una BU. El formato puede ser analizado como sigue:

Sección de la convención para nombres	Explicación
x.y	Una combinación de dos (uno o dos) identificadores de dígito separados separados por “.” eso identifica el valor de la versión principal.

	Este valor es determinado comercializando del Cisco IOS. Ejemplo: 12.1
z	Un a tres dígitos que identifica la versión de mantenimiento de x.y. Esto ocurre cada ocho semanas. Los valores son 0 en beta, 1 en FCS y 2 para la primera versión de mantenimiento. Ejemplo: 12.1(2)
p	Un carácter alfa que identifica una reconstrucción de x.y (z). El valor comienza con una "a" minúscula para la primer reconstrucción, sigue con una "b" y así sucesivamente. Ejemplo: 12.1(2a)

A	Una a tres cartas alfa son el diseñador del tren de versión y son obligatorias para las versiones CTED, STED, y X. También identifica una familia de productos o las Plataformas. Las versiones ED de tecnología utilizan dos letras. La primera letra representa la tecnología y la segunda letra se utiliza para diferenciación. Por ejemplo: `A = Access Server/Dial technology (example:11.3AA)`
	`B = Broadband (example:12.2B)`
	`D = xDSL technology (example:12.2DA)`
	`E = Enterprise feature set (example:12.1E)`
	`H = SDH/SONET technology (example:11.3HA)`
	`N = Voice, Multimedia, Conference (example:11.3NA)`
	`M = Mobile (example:12.2MB)`
	`S = Service Provider (example:12.0S)`
	`T = Consolidated Technology (example:12.0T)`
	`W = ATM/LAN Switching/Layer 3 (example:12.0W5)`"X" en la primera posición del nombre de la versión identifica una versión única basada en el tren CTED “T”. Por ejemplo, XA, XB, XC, y así sucesivamente. Un “x” o “Y” en la segunda posición del nombre de la versión identifica una versión de ED de poca duración basada encendido, o afiliada a, una versión STED. Por ejemplo, 11.3NX (basado en 11.3NA), 11.3WX (basado en 11.3WA), y así sucesivamente.

o	Designador numérico opcional de uno o dos dígitos que identifica una reconstrucción de un valor de versión en particular. Deje el espacio en blanco si no que representa una reconstrucción. Comienzo con 1, entonces 2, y así sucesivamente. Ejemplo: 12.1(2)T1, 12.1(2)XE2
u	Designador numérico de uno o dos dígitos que identifica la funcionalidad de la versión específica de la BU. El valor está determinado por el equipo de marketing de BU. Ejemplo: 11.3(6)WA4, 12.0(1)W5
v	Designador numérico de uno a dos dígitos que identifica la versión de mantenimiento del código específico de la BU. Los valores son 0 en beta, 1

	en FCS y 2 para la primera versión de mantenimiento. Ejemplo: 11.3(6)WA4(9), 12.0(1)W5(6)
p	Un indicador de carácter alfa que identifica una nueva compilación de una versión tecnológica específica. El valor comienza con una "a" minúscula para la primera recopilación; luego, "b" y así sucesivamente. Ejemplo: 11.3(6)WA4(9a) sería una recopilación de 11.3(6)WA4(9).

El siguiente gráfico rotula las distintas secciones de la convención de nombres de IOS de Cisco:

Apéndice B - Confiabilidad del Cisco IOS

La confiabilidad del Cisco IOS es un área donde Cisco se esfuerza continuamente mejorar. Antes de discutir las mejores prácticas orientadas al cliente, una cierta comprensión de la calidad de Cisco IOS interno y esfuerzos de confiabilidad es necesarios. Estas secciones principalmente tienen el propósito de proporcionar una descripción general de los esfuerzos más recientes de Cisco en la calidad del software del IOS de Cisco y qué suposiciones de los clientes deberían realizarse teniendo en cuenta la confiabilidad del software.

Programa de calidad del Cisco IOS

Cisco tiene un proceso de desarrollo bien definido IOS llamado gran metodología de la ingeniería de GEM (GEMA). Este proceso tiene un ciclo vital trifásico:

- Estrategia y planificación
- Ejecución
- Despliegue

Las áreas generales dentro del ciclo vital incluyen el priorización de la introducción de la característica, el desarrollo, el proceso de prueba, las fases de la introducción al software, el primer cliente enviado (FCS), el GD, y la ingeniería de mantenimiento. Cisco también sigue varias mejores pautas prácticas de la calidad del software de las organizaciones tales como Organización Internacional de Normalización (ISO), Telcordia (antes Bellcore), IEEE y el instituto del Software Engineering del Carnegie Mellon. Estas guías de consulta se incorporan en los procesos de la GEMA de Cisco. Los procesos de desarrollo del software de Cisco son ISO 9001 (1994) certificado.

El proceso principal para el mejoramiento de la calidad del software IOS de Cisco es un proceso orientado al cliente mediante el cual Cisco escucha al cliente, define las metas y las métricas, implementa las mejores prácticas y monitorea los resultados. Un equipo cruz-de organización que está confiado a mejorar la calidad del software conduce este proceso. Un diagrama del proceso de la mejora de la calidad del Cisco IOS se muestra abajo:

El proceso de la mejora de la calidad tiene Objetivos medibles particulares para el FY2002 y más allá. El enfoque principal de estos objetivos es el de reducir los defectos al identificar los problemas de software en una etapa temprana del ciclo de prueba, reducir el registro de defectos, mejorar la consistencia de características y la claridad de la versiones de software, y brindar programas de versiones predecibles y calidad de software de manera constante. Las iniciativas para dirigir estas áreas incluyen las nuevas herramientas de la cobertura de la prueba (que

identifican las áreas de una cobertura más débil de la prueba), la mejora del proceso de la acción correctiva de la prueba, y las mejoras de la prueba de regresión del sistema del Cisco IOS. Han aplicado a los recursos adicionales para abordar estos problemas y hay consolidación ejecutiva y multidisciplinar para todas las versiones de Cisco IOS Software primarias.

Prueba del Cisco IOS Release

Una parte integrante del esfuerzo de calidad de la confiabilidad del software dentro de Cisco es la calidad, el alcance, y la cobertura de la prueba. Total, Cisco tiene los objetivos de calidad siguientes IOS:

- Reducir los defectos de regresión interna de Cisco encontrados. Esto incluye más de alta calidad en el desarrollo y la identificación de más problemas en los parásitos atmosféricos/la análisis dinámico.
- Reduzca los defectos encontrados cliente
- Reducción de los defectos extraordinarios totales.
- Aumente la claridad de la versión de software y el estado coherente de la característica
- Proporcione la característica y las versiones de mantenimiento con los horario y la calidad

La prueba interna de Cisco se puede pensar en como proceso donde diversos defectos se identifican en diversas etapas de la prueba. El objetivo general es encontrar las clases correctas de defectos en el laboratorio derecho. Esto es importante por varios motivos. La primera y más importante es que posiblemente no exista una cobertura de prueba adecuada en las etapas de prueba posteriores. Los costos de las pruebas también aumentan significativamente de etapa a etapa debido a la posibilidad de automatizar en etapas anteriores y a la creciente complejidad y experiencia requeridas posteriormente. El siguiente diagrama describe el espectro de prueba de Cisco IOS.

El primer paso es el desarrollo del software. Cisco tiene varios esfuerzos en esta área para ayudar a mejorar la calidad del software inicial. Los grupos del desarrollo también realizan las revisiones de código o aún las revisiones de código múltiples para asegurarse de que otros promotores aprueban los Cambios de software o el código de la nueva función.

La próxima etapa es la prueba de unidad. La prueba unitaria utiliza las herramientas que examinan la interacción de software sin el uso de un laboratorio. DevTest es los pruebas de laboratorio que incluyen la Prueba de característica/funcionalidad y la prueba de regresión. La Prueba de característica/funcionalidad se diseña para examinar las funciones de una característica dada. Esto incluye la configuración, la desconfiguración y la prueba de todas las combinaciones de características, tal como está definido en la especificación de las características. La prueba de regresión se realiza en un recurso para pruebas automatizado diseñado para validar la funcionalidad y el comportamiento de funciones de manera continua. Las pruebas se centran principalmente en el ruteo, la conmutación y la funcionalidad de las características en diferentes topologías de red mediante el uso de pings y la generación limitada de tráfico. La prueba de regresión se hace solamente en una combinación limitada de características, de Plataformas, de versiones de software, y de topologías debido al número extremo de permutaciones posibles, no obstante sobre 4000 Pruebas de regresión los scripts se utilizan hoy. La prueba de integración se diseña para ampliarse en las capacidades de testeo en laboratorio para un más conjunto completo de Productos y de Interoperabilidad. La prueba de integración también aumenta la cobertura de código de la prueba ampliando la prueba para incluir las pruebas de interoperabilidad, tensión y las pruebas de rendimiento, las pruebas del sistema, y prueba negativa (Eventos inesperados de la prueba).

La próxima fase de laboratorio ofrece una prueba de extremo a extremo para los entornos comunes de cliente. Éstos se muestran en el diagrama arriba como el laboratorio de pruebas financieras (FTL) y NSITE, prueba del escenario del cliente. El FTL fue construido para proporcionar la prueba para la comunidad de la misión en situación financiera crítica. El NSITE es un grupo que proporciona más testeo en profundidad para diversas Tecnologías Cisco IOS. Los laboratorios NSITE y FTL se concentran en áreas como la comprobación de escalabilidad y rendimiento, capacidad de actualización, disponibilidad y resiliencia, interoperabilidad y capacidad de servicio. La utilidad se centra en los problemas, la administración de eventos/la correlación y el troubleshooting a granel del aprovisionamiento bajo carga. Otros laboratorios existen dentro de Cisco para que diversos mercados verticales ayuden a probar estas áreas.

El último laboratorio que se muestra en el diagrama de arriba está identificado como el laboratorio del cliente. La Prueba de cliente es una extensión del esfuerzo de calidad y recomendada para que los entornos de gran disponibilidad se aseguren de que la combinación exacta de características, la configuración, las Plataformas, los módulos, y la topología se han probado completamente. Una cobertura de evaluación adecuada debería incluir el rendimiento y la escalabilidad de la red en la topología identificada, pruebas de aplicaciones específicas, pruebas negativa en la configuración identificada, pruebas de interoperabilidad para dispositivos que no son de Cisco y pruebas automatizadas, completas y continuas.

Software MTBF

Una de la mayoría de las métricas comunes de confiabilidad general es el Mean Time Between Failure (MTBF). El MTBF para la confiabilidad del software es útil debido a las capacidades de análisis que se han desarrollado para la confiabilidad de hardware usando el MTBF. La confiabilidad de hardware se puede determinar más exactamente usando algunos estándares existentes. Cisco utiliza el método de la cuenta de las piezas basado en las informaciones estándars de MTBF de Telcordia Technologies. El software de MTBF, sin embargo, no tiene ninguna metodología de análisis correspondiente y debe confiar en la medición de campo para la análisis MTBF.

Por los últimos tres años, Cisco ha realizado las mediciones de campo de la confiabilidad del software para la red interna de Cisco las TIC y este trabajo se documenta dentro de Cisco. El trabajo se basa en las caídas del sistema forzadas por software en los dispositivos con IOS de Cisco, que pueden ser medidas utilizando la información de trampas de SNMP de administración de red y la información de tiempo de actividad. El estudio identifica la confiabilidad del software usando un modelo logarítmico normal estadístico de la distribución para las versiones de software identificadas. El tiempo intermedio hasta la reparación (MTTR) de la falla de software es por término medio reinicio y tiempos de recuperación basados del router. Seis tiempos de recuperación minuciosos se utilizan para los entornos para empresas y quince minutos se utilizan para Proveedores de servicios de Internet más grandes (ISP). El resultado de este estudio en curso es que el software resuelve generalmente la Disponibilidad fina de los nines cuando está liberado, o después de algunas versiones de mantenimiento, y es incluso más alto en un cierto plazo, como medido usando el software forzado causa un crash como la única fuente de inactividad. El estudio identificó los valores MTBF potenciales como un intervalo entre 5,000 horas para el software de liberación temprana y 50,000 horas para el software de liberación general.

La refutación más común de este trabajo es que las caídas forzadas por el software no incluyen todas las instancias de interrupciones que tienen lugar debido a problemas de confiabilidad del software. Si este métrico se utiliza en esfuerzos de la mejora de la calidad, puede ayudar a mejorar el índice de caídas forzadas software pero puede ignorar otras áreas críticas de confiabilidad del software. Este comentario permanece sin respuesta debido a la dificultad de

predecir con exactitud la confiabilidad del software utilizando una metodología de estadística. Los profesionales de estadísticas de calidad del software de Cisco han concluido que un conjunto más grande de la muestra de las precisas de datos sería necesario predecir confiablemente el MTBF del software usando una gama más amplia de los tipos de la caída del sistema. Además, la análisis estadístico teórica sería difícil debido a las variables tales como complejidad de la red, experiencia del personal para resolver los asuntos relacionados del software, diseño de red, características habilitadas, y procesos de administración del software.

Ahora, no se ha completado ningún trabajo de la industria a predice más exactamente la confiabilidad del software con las mediciones de campo debido a la dificultad exactamente de recoger este tipo de datos vulnerables. ¿También, la mayoría de los clientes ponen? t quiere la información de disponibilidad de recolección de Cisco directamente de su red debido a las naturalezas de los datos de disponibilidad propietarias. Algunas organizaciones sin embargo recogen los datos sobre la confiabilidad del software y Cisco anima a las organizaciones que recojan la métrica en la disponibilidad debido a las caídas del sistema del software, y realicen la análisis de la causa raíz en esas caídas del sistema. Algunas organizaciones con mayor confiabilidad de software han usado esta actitud proactiva para mejorar la confiabilidad del software mediante una cantidad de prácticas que pueden controlar.

Suposiciones acerca de la confiabilidad del software

Como resultado del comentario del cliente, los estudios dinámicos realizados por el grupo de Tecnologías Cisco IOS y la Análisis de la causa de raíz realizada por el Advanced Services de Cisco combinan, algunas más nuevas suposiciones y se han formado las mejores prácticas que ayudan a mejorar la confiabilidad del software. Estas suposiciones se centran en las responsabilidades de prueba, la madurez o edad del software, las características habilitadas, y la cantidad de versiones del software desplegadas.

Responsabilidad de las pruebas

La primera nueva suposición se refiere a la responsabilidad de pruebas. Cisco es siempre responsable de la probar/que valida las nuevas funciones y las funciones para asegurarse de que trabajan en productos nuevos. Cisco es también responsable de la prueba de regresión asegurarse de que las nuevas versiones de software son compatibles con versiones anteriores. Sin embargo, Cisco no puede validar cada característica, topología, y plataforma contra cada advertencia potencial que un entorno del cliente pueda aplicar (las idiosincrasias, carga, y los perfiles del tráfico del diseño). Las mejores prácticas de gran disponibilidad para los clientes incluyen la prueba en una Topología de laboratorio derrumbada que imite la red de producción usando las características, el diseño, los servicios, y el tráfico de aplicación definidos cliente.

Confiabilidad vs. Madurez del software

La confiabilidad del software es principalmente un factor de la madurez del software. El software madura a medida que se expone (con el uso) y se corrigen los errores de funcionamiento identificados. Las operaciones de la Versión de Cisco han ido a una arquitectura de la versión del tren a asegurarse de que el software se madura sin las nuevas funciones que son agregadas. Los clientes que requieren la Alta disponibilidad están buscando un software más maduro con las características que ahora necesitan. Un equilibrio entonces existe entre la madurez del software, los requerimientos de disponibilidad, y los driveres comerciales para las nuevas funciones o las funciones. Muchas organizaciones tienen los estándares o el guía para una madurez aceptable. Algunas sólo aceptan la quinta versión provisoria de un tren determinado. Para otros, puede ser el noveno o certificación GD. En última instancia, la organización debe decidir sus niveles

aceptables de riesgo en términos de madurez de software.

Confiabilidad vs. cantidad de características y estándares

La confiabilidad del software es también un factor de cuánto del código se prueba y se ejercita en un entorno de producción. Mientras que la cantidad de diversos plataformas de hardware y módulos aumenta, la cantidad de código ejercitada también aumenta, que aumenta generalmente la exposición a los defectos del software. Se puede decir lo mismo sobre la cantidad de protocolos configurados, la variedad de configuraciones e incluso la variedad de topologías o diseños implementados. El diseño, la configuración, los protocolos, y los factores del módulo de hardware pueden contribuir a la cantidad de código que se ejercite y al riesgo o a la exposición creciente a los defectos del software.

Las operaciones de versión de software ahora tienen un software específico que generalmente limita el código disponible en un área en particular. Las unidades comerciales han recomendado los diseños y las configuraciones que se prueban más a conciencia dentro de Cisco y son utilizados más extensamente por los clientes. Los clientes también han comenzado a adoptar las mejores prácticas para que las topologías y las configuraciones estándars modulares estandardizadas bajen la cantidad de exposición no comprobada del código y mejoren la confiabilidad del software total. Algunas redes de disponibilidad alta tienen pautas de configuración estándar estrictas, estándares de topología modular y control de versión de software que ayudan a reducir el riesgo de exposición al código no probado.

Confiabilidad vs. Cantidad de versiones desplegadas

Otro factor de confiabilidad del software es Interoperabilidad entre las versiones y la cantidad escarpada de código que consiga ejercitado con las versiones múltiples. Mientras que la cantidad de versiones de software aumenta, la cantidad de código ejercitada también aumenta, que entonces aumenta la exposición a los defectos del software. El riesgo para la confiabilidad se incrementa casi exponencialmente debido al código adicional que se utiliza con versiones múltiples. Ahora se reconoce que las organizaciones necesitan funcionar con por lo menos las varias versiones en la red para cubrir la característica y los requisitos de la plataforma específicos. Sin embargo, la ejecución de alrededor de cincuenta versiones en un ambiente de red mayormente homogéneo, es normalmente una indicación de que existen problemas de software debido a la incapacidad de analizar o validar correctamente tantas versiones.

Para mejorar la confiabilidad del software, el desarrollo Cisco realiza la prueba de regresión del software para asegurarse de que diversas versiones de software son compatibles. Además, el código del software es más modular y los módulos del núcleo son menos probables cambiar perceptiblemente entre las versiones en un cierto plazo. Las operaciones de la Versión de Cisco también han cambiado la cantidad de software disponible a los clientes mientras que las versiones con los defectos conocidos o los problemas de interoperabilidad se quitan rápidamente del CCO mientras que se encuentran los defectos.

Información Relacionada

- Sistemas operativos de interconexión de redes (IOS) de Cisco
- Soporte Técnico y Documentación - Cisco Systems