Caso práctico de actualización de CNC

Contenido

Introducción

En este documento se describe un caso práctico de migración compleja a gran escala de una red inalámbrica fija de Cisco CNC 4.1 a 7.1 mediante ascensor y cambio.

Abstracto

En este documento se presenta un caso práctico detallado de la migración de una red inalámbrica fija a gran escala de Cisco Crosswork Network Controller (CNC) versión 4.1 a la versión 7.1. Debido a la ausencia de un mecanismo de actualización in situ, la transición requirió una implementación completa de "lift-and-shift", lo que introdujo una importante complejidad arquitectónica, operativa y de integración en más de 2000 dispositivos de red y varios sistemas interdependientes. El estudio examina los desafíos encontrados en múltiples áreas.

Un resultado clave destaca el papel esencial de la automatización a la hora de garantizar la escalabilidad, la precisión y el determinismo operativo, especialmente para flujos de trabajo de gran volumen. Los resultados también demuestran que los entornos de producción difieren considerablemente de las condiciones de laboratorio controladas, lo que requiere una resolución de problemas adaptativa, validación iterativa y un compromiso sostenido con los equipos de ingeniería del TAC y de la Unidad de Negocio. Este trabajo aporta información práctica, metodologías validadas y prácticas recomendadas que sirven como modelo de referencia para futuras actualizaciones de CNC y transiciones de plataformas de orquestación a gran escala.

Background

La proliferación de las redes 5G, la rápida adopción de dispositivos conectados y la digitalización de los entornos empresariales y de consumo han dado lugar a un aumento significativo del volumen de tráfico y a la diversidad de servicios que deben prestarse de forma segura y fiable a escala. Los proveedores de servicios de comunicaciones (CSP) utilizan ahora redes muy dinámicas en las que las herramientas operativas tradicionales, organizadas en silos, a menudo crean complejidad, degradan la experiencia del usuario y generan mayores gastos operativos (OpEx).

Para seguir siendo competitivos, los operadores están adoptando cada vez más modelos operativos modernizados basados en la automatización, la virtualización, los principios de SDN y las redes de optimización automática basadas en análisis.

Cisco Crosswork Network Controller (CNC) se ha diseñado para respaldar esta transformación

mediante la simplificación de los flujos de trabajo operativos, la reducción del coste total de propiedad (TCO) y la habilitación de la automatización basada en objetivos en redes de transporte de varios proveedores. CNC proporciona una plataforma unificada para el aprovisionamiento de servicios, la supervisión del estado de la red y la optimización en tiempo real, lo que ofrece a los operadores un único panel de acceso para gestionar redes IP de gran escala de forma más proactiva y eficiente.

La infraestructura de Crosswork subyacente ofrece un marco de clúster flexible y escalable en el que se ejecutan todas las aplicaciones CNC. Para CNC 7.1, esto incluye módulos como Optimization Engine, Active Topology, Change Automation, Health Insights, Element Management Functions (EMF), Service Health y Crosswork Workflow Manager (CWM), cada uno de los cuales contribuye a la orquestación y garantía de extremo a extremo.

Sin embargo, actualizar el CNC presenta desafíos únicos. CNC no admite actualizaciones in situ, por lo que se requiere una implementación completa en la que el nuevo entorno se crea en paralelo con el existente y todos los datos y servicios se migran a la nueva versión. En este caso práctico se examina una actualización a gran escala de CNC 4.1 a CNC 7.1 para un importante agregador de servicios australiano que presta servicios de red troncal a todos los demás proveedores de servicios.

La migración fue especialmente compleja debido a los diversos cuadernos de campaña personalizados de automatización de cambios, los KPI de Health Insight personalizados, los requisitos de reconciliación de servicios de VPN L2/L3 y la necesidad de un ZTP seguro.

El gran salto de versión introdujo una incertidumbre adicional, dados los cambios internos en la arquitectura y el comportamiento que dificultaban la predicción del comportamiento de los casos prácticos existentes en la nueva versión. Esto requería una validación y una alineación completas en todos los casos prácticos.

Se invirtió una planificación significativa en la determinación de la asignación óptima de recursos, incluidos los recuentos de nodos híbridos/de trabajo, la distribución CDG y el dimensionamiento de PCE, así como en la determinación de si se podía conservar el espacio de recursos existente.

La implementación y validación iniciales de CNC 7.1 se llevaron a cabo en un laboratorio CALO interno, proporcionando un entorno seguro para experimentar, refinar las configuraciones y generar confianza. A esto le siguió la implementación en el entorno de prueba interno, que refleja estrechamente la producción. La fase final implicó la implementación de CNC 7.1 en producción, la aplicación de cambios en la configuración de los dispositivos y la ejecución de una migración por fases de todos los dispositivos y servicios asociados al nuevo controlador.

Red de producción

La red de producción con brechas de aire se extiende por amplias partes de Australia. Con la presencia de más de 2000 dispositivos, desde NCS a ASR9K, CNC gestionó todos estos dispositivos proporcionando una vista topológica en directo. Aproximadamente 2000 dispositivos eran NCS540 conocidos localmente como SWR (Small Wireless Router) con IOS-XR 24.3.2 y 30 eran ASR-9K (Version 7.5.2) conocidos localmente como LWR (Large Wireless Router).

La configuración de Crosswork constaba de 3 nodos híbridos y 2 nodos de trabajo. Hubo un total de 5 CDG para los dispositivos, 4 de los cuales estaban activos y 1 era el nodo en espera. Esto ofrecía una protección limitada, ya que el grupo solo tenía 1 CDG en espera. Pero teniendo en cuenta sus requisitos, esto se le dio el visto bueno. El hecho de que todas las VM se encontraran en un único Data Center también facilitó la decisión de continuar con solo 1 servidor en espera.

El CDG es el componente que maneja la recolección de datos de los dispositivos a través de diversos protocolos como SNMP, CLI y GNMI. Los datos recogidos por CDG se exponen a Crosswork a través de la kafka interna. Un dispositivo incorporado a Crosswork debe estar conectado a un CDG, que permite que el gateway de datos se conecte al dispositivo y obtenga los datos del dispositivo.

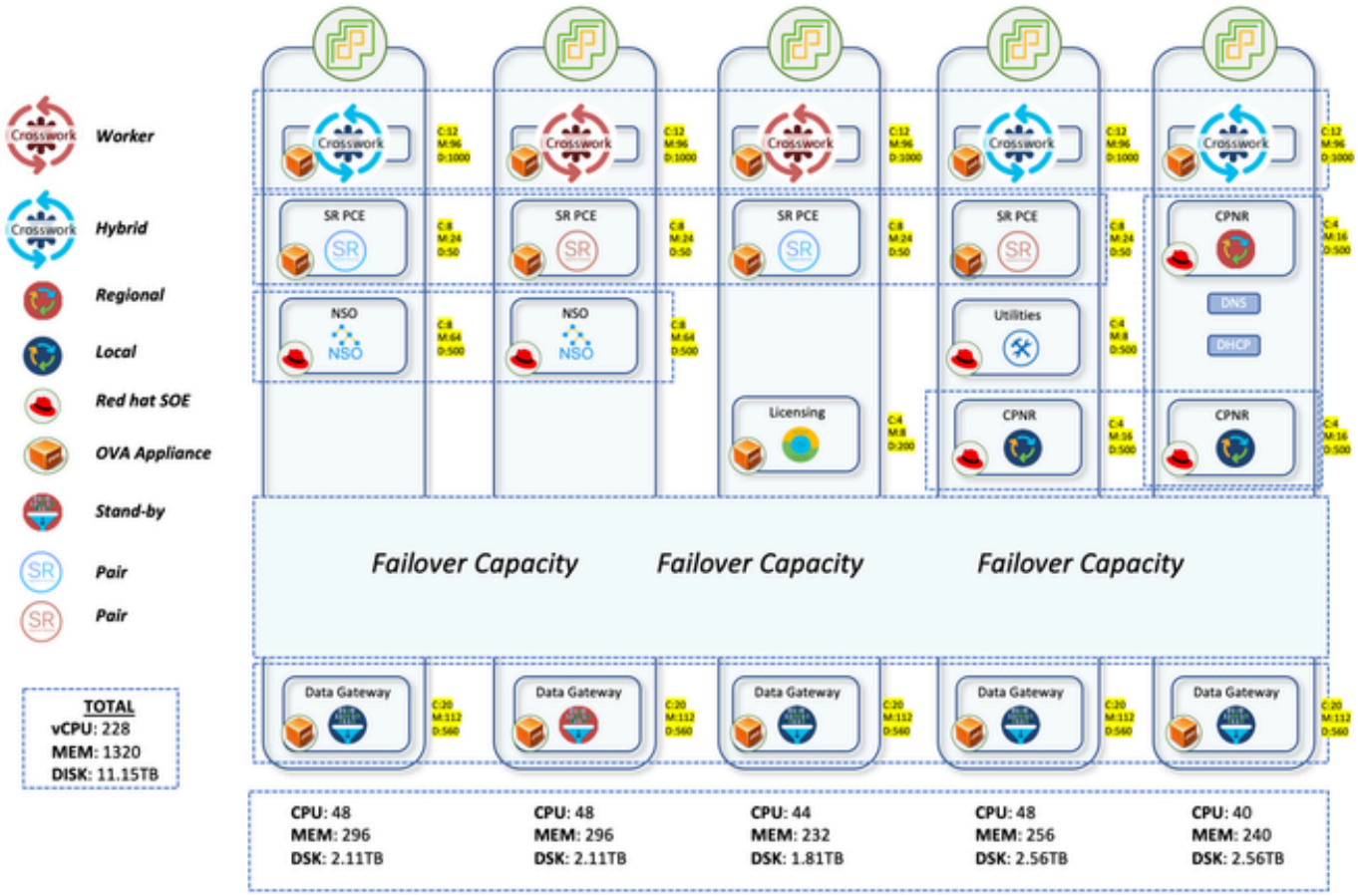
La distribución de dispositivos para los CDG también fue objeto de mucha reflexión. La implementación anterior había distribuido aleatoriamente los dispositivos entre los CDG. Esto dio lugar a una distribución muy sesgada con algunos CDG que transportaban más dispositivos, mientras que había 1-2 CDG con muy menos dispositivos. Esto dio lugar a un consumo excesivo y a una carga excesiva para algunos CDG, mientras que otros estaban subaprovisionados.

El proceso de pensamiento aquí en la actualización fue distribuir 700 SWR cada uno a los 4 CDG activos. Esto representó 2100 cables de acero alojados en los tres primeros CDG. Los LWRs que eran muy pesados en la interfaz frontal estaban reservados para el cuarto CDG. Aunque eran un número muy pequeño con un conteo de 30, esta asignación aseguraba que incluso si se realizaban más recolecciones desde estos dispositivos, no habría una carga pesada en el CDG. Cualquier incorporación posterior de los cables de acero también iría al 4° CDG. Esto garantizó una distribución uniforme en los tres primeros CDG con más espacio disponible en el 4° para incorporar nuevos dispositivos.

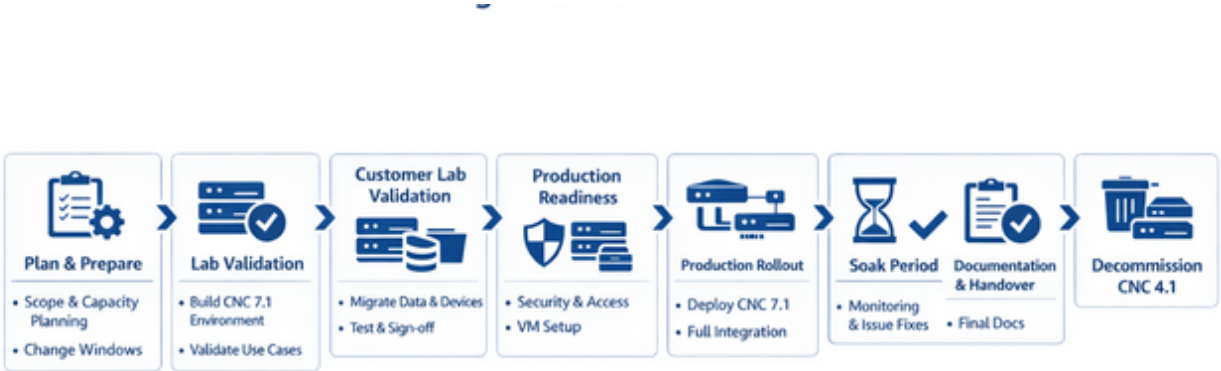
SR-PCE se implementó en 2 pares, es decir, 4 VM distribuidas en diferentes máquinas host. Un par gestiona 7 sitios POI y el otro gestiona los 8 sitios POI restantes. Las actualizaciones de topología en la GUI de CNC se realizan mediante el uso de SR-PCE. Aprende la topología de la red a través del peering BGP-LS con otros routers LWR. Este componente también se utiliza para todos los casos prácticos de ingeniería de tráfico en los que desempeña la función del controlador para dirigir el tráfico a diferentes rutas.

Para gestionar todos los casos prácticos de aprovisionamiento de servicios y configuración de dispositivos, NSO debe utilizarse junto con el CNC. Para la red de producción, se implementaron dos NSO con la versión 6.4.1.1 para trabajar en tándem en modo de alta disponibilidad. SR-PCE

(elemento de cálculo de ruta de routing de segmentos) es el componente necesario para proporcionar las actualizaciones de topología al CNC y también para gestionar los casos prácticos de ingeniería de tráfico en tiempo real. Aquí se implementaron cuatro SR-PCE con la versión 25.2.1 y cada PCE se vinculó a dos LWR diferentes.



Flujo de trabajo de migración de CNC 4.1 a CNC 7.1



Para la implementación de CNC, la opción preferida era seguir adelante con la basada en docker.

Sin embargo, como el cliente no aprobó la instalación de docker en sus instalaciones, no había otra opción que continuar con la implementación manual mediante vCenter. La implementación tarda más tiempo que la basada en scripts, ya que nos obliga a proporcionar entradas varias veces en la GUI del vCenter.

Una vez que se realizó la implementación CNC, todas las aplicaciones requeridas se implementaron con el archivo de instalación de acción automática proporcionado por la BU que carga y activa las aplicaciones todas a la vez, reduciendo así el tiempo que se tarda en hacerlo manualmente. Se implementó el nivel principal que incluye Crosswork Optimization Engine, Active Topology, Service Health, Element Management Functions, Crosswork Workflow Manager. Junto con esto, también se configuraron los paquetes complementarios, que incluyen Change Automation y Health Insight.

CWM y SH no tenían ningún caso práctico. Sin embargo, se implementaron porque estaban interesados en algunos de los casos prácticos que ofrecían estas aplicaciones en la siguiente versión.

Una vez configuradas las aplicaciones, el siguiente paso consistió en migrar los datos de la versión anterior de CNC. Se compone principalmente de perfiles de credenciales, proveedores, etiquetas, cuadernos personalizados, KPI personalizados, roles, vales sZTP y cualquier otro dato. CNC proporciona la opción de exportación para todos estos que se pueden aprovechar y luego importar al nuevo CNC.

Una vez configurados, es aconsejable iniciar la migración de dispositivos. En caso de actualizaciones, si el nuevo CNC se implementa en una nueva subred en comparación con la anterior, existe el requisito de realizar cambios de ACL en los dispositivos para proporcionar accesibilidad con el nuevo CNC. Este es un proceso que consume mucho tiempo, ya que requiere iniciar sesión manualmente en cada dispositivo y cambiar la configuración.

Una vez realizados estos cambios de ACL, el siguiente paso es importar los dispositivos al nuevo CNC y conectarlos a los CDG. Si el alcance es correcto y las credenciales SSH y SNMP son correctas, los dispositivos se muestran como accesibles en CNC y también se incorporan a NSO (Network Services Orchestrator).

En la parte frontal de NSO, todos los paquetes necesarios deben estar en su lugar y operativos para garantizar que CNC pueda hablar con NSO y viceversa. Por ejemplo, para incorporar automáticamente los dispositivos a NSO desde CNC, el paquete de funciones DLM es obligatorio. De manera similar, si existe algún requisito para que NSO configure las trayectorias del sensor MDT en el dispositivo, el paquete TM-TC debe implementarse en NSO. La esencia es que, en función del caso práctico, el paquete relevante debe implementarse en NSO.

En lugar de adoptar el enfoque manual para implementar estos paquetes necesarios,

especialmente los de SDN de transporte, se desarrolló un script automatizado para el aprovisionamiento. Con la actualización de CNC 7.1, se han introducido actualizaciones en los paquetes TSDN. Estos paquetes actualizados están pensados para su implementación en el servidor NSO con el fin de garantizar un soporte continuo para el aprovisionamiento de L2/L3 en el entorno actualizado. La secuencia de comandos automatiza la instalación de los paquetes TSDN actualizados y carga los metadatos necesarios en NSO, lo que le permite aprovisionar servicios según sea necesario.

Una instancia del servidor de licencias Cisco Smart Software Manager (SSM) y tres instancias de Cisco Prime Network Registrar (CPNR) también se implementarán en hosts diferentes.

Arquitectura CNC e integración con otros componentes

CNC proporciona una única plataforma para el aprovisionamiento, la optimización y la visualización de los servicios implementados a través de una interfaz de usuario unificada. A continuación se presenta un breve resumen de los componentes internos del CNC que residen en el conjunto de plataformas del CNC y los casos prácticos.

- Topología activa de trabajo cruzado (CAT):
    - Aplicación de componentes internos distribuida entre nodos de VM CNC
    - Proporciona visibilidad integral en tiempo real del inventario reconciliado
    - Integra la información de inventario de varias fuentes de datos en una sola pantalla
    - Cálculo de ruta de red de transporte
    - Descubrimiento de topología

- Motor de optimización de la interconexión (COE):
    - Aplicación de componentes internos distribuida entre nodos de VM CNC
    - Optimización de la red en tiempo real
    - Visualización de topología en tiempo real
    - Visualizaciones y aprovisionamiento de SR-TE
    - Visualización y aprovisionamiento de RSVP-TE
    - Ancho de banda a demanda
- Crosswork health insight (CHI):
    - Aplicación de componentes internos distribuida entre nodos de VM CNC
    - supervisión KPI
    - Tablero de alertas
- Automatización de cambios cruzados (CCA):
    - Aplicación de componentes internos distribuida entre nodos de VM CNC
    - Herramienta de operaciones de desarrollo con cuadernos listos para usar
    - Capacidad de programación para ejecutar reproducciones en el momento deseado
    - HI KPIs alerta de costura a juegos sugeridos como solución

Diagrama de arquitectura

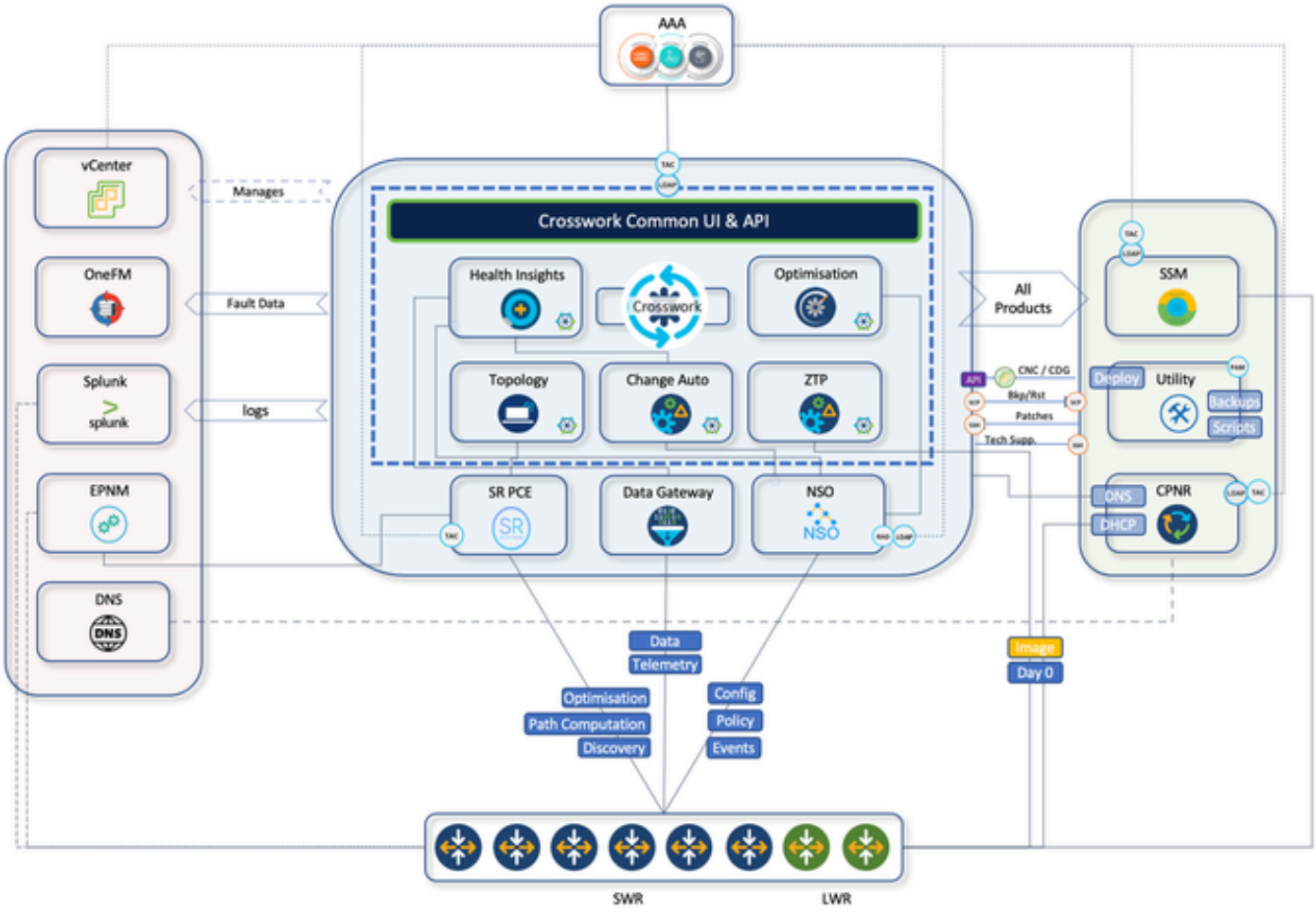
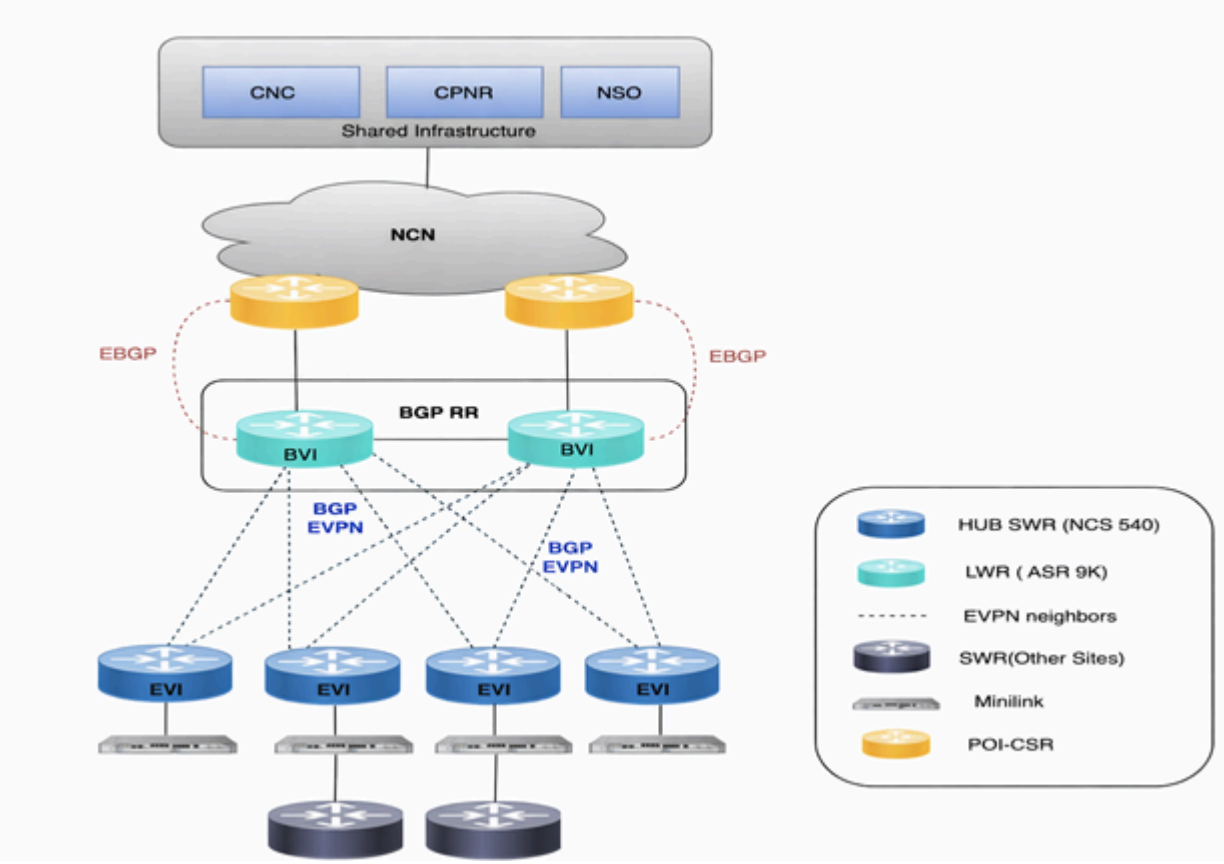


Diagrama de la red



Flujo de trabajo de migración detallado de CNC 4.1 → 7.1

Migración por fases de extremo a extremo de CNC 4.1 heredado a CNC 7.1 (el mismo flujo se puede seguir para cualquier actualización de CNC independientemente de las versiones)

Planear	›	Laboratorio	›	Laboratorio del cliente	›	Preparado para producción	›	Lanzamiento de producción	›	Período de remojo	›	Entrega	›	Retirada

FASE 1

1 Planificación y preparación

ÁMBITO Y PLANIFICACIÓN	PLANIFICACIÓN
· Definición del alcance	· Cambiar identificación de ventana
•Planificación de capacidad	· Alineación de partes interesadas

▼

FASE 2

2 Validación de laboratorio interna

INFRAESTRUCTURA · Build CNC 7.1 (híbrido/trabajadores) · Instalar aplicaciones · Implementación de NSO con HA · Implementación de pares SR-PCE	VALIDACIÓN · Validar todos los casos prácticos · Firma funcional

▼

FASE 3

3 Validación de laboratorio del cliente

CONSTRUCCIÓN DE INFRAESTRUCTURA · Build CNC 7.1 (híbrido/trabajadores) · Instalar aplicaciones · Implementación de NSO con HA · Implementación de pares SR-PCE	MIGRACIÓN DE DATOS · Exportación de artefactos CNC 4.1 · Recrear grupos de dispositivos · Importación en CNC 7.1 · Implementación de paquetes NSO	DISPONIBILIDAD DEL DISPOSITIVO · Actualizaciones de ACL · Importación de dispositivos y conexión CDG	SERVICIOS Y OBSERVABILIDAD · Sincronización y conciliación de servicios · Trabajos de recopilación y habilitación de KPI · Habilitación de scripts de cuaderno BNM · Observabilidad de HI/Grafana · Integración con Radius · Integración de Splunk · Integración con OneFM

			· Habilitación de copias de seguridad CNC

✓ Realizar ATP en Lab y obtener la aprobación

▾

FASE 4

4 Preparación para la producción

SEGURIDAD Y ACCESO · Revisión de la seguridad · Configuración de controles de acceso	INFRAESTRUCTURA · Configuración y dimensionamiento de VM de producción · Validación de red

▾

FASE 5

5 Transición de producción

↻ Repite todos los pasos de la Fase 3 en el entorno de producción

CONSTRUCCIÓN DE INFRAESTRUCTURA · Build CNC 7.1 (híbrido/trabajadores) · Instalar aplicaciones · Implementación de NSO con HA · Implementación de pares SR-PCE	MIGRACIÓN DE DATOS · Exportación de artefactos CNC 4.1 (Proveedores, perfiles de credencial, cuadernos, etiquetas) · Recrear grupos de dispositivos · Importación en CNC 7.1	DISPONIBILIDAD DEL DISPOSITIVO · Actualizaciones de ACL · Importación de dispositivos y conexión CDG	SERVICIOS Y OBSERVABILIDAD · Sincronización y conciliación de servicios · Trabajos de recopilación y habilitación de KPI · Habilitación del cuaderno de BNM · HI/Grafana, Splunk, OneFM

	· Implementación de paquetes NSO		· Habilitación de copias de seguridad CNC

✓ Lanzamiento de producción

▼

FASE 6

6 Período de estabilización

CONTROL · Supervisión de la estabilidad · Base de rendimiento	GESTIÓN DE PROBLEMAS · Seguimiento y resolución de problemas · Proceso de escalado

▼

FASE 7

7 Documentación y entrega

DOCUMENTACIÓN · MOP, documentos de diseño y documentos operativos · Diagramas de arquitectura	ENTREGA · Sesiones de transferencia de conocimientos · Firma de entrega

▼

FASE 8

8 CNC heredado 4.1

LIMPIEZA · Separe todos los dispositivos de CDG	ARCHIVAR · Archivar todas las exportaciones de

	· Elimine las entradas MDT que apuntan a las VM CDG 4.1 · Eliminar VM de producción	CNC 4.1 · Auditoría final y cierre de sesión

Casos de uso

L2VPN (basado en EVPN) Service Provisioning

El servicio L2VPN proporciona conectividad Ethernet de capa 2 a través de varios SWR, con algunos servicios anclados en LWR. La topología activa de CNC se utiliza para el aprovisionamiento de servicios, mientras que toda la lógica específica del entorno se implementa a través de plantillas personalizadas de NSO.

El aprovisionamiento de L2VPN se trata como una actividad de configuración de día 2 y requiere atributos de servicio proporcionados por el operador.

Plantillas de NSO personalizadas

Se han creado varias plantillas personalizadas para alinear las convenciones de nomenclatura y los comportamientos de interfaz específicos del entorno:

- CT-l2vpn-swr-hub-and-lwr
  Maneja las diferencias de denominación del lado del hub f-o bridge -group y bridge -domain en los hubs SWR y LWRs.
- CT-l2vpn-swr-nonhub-100 / 101 / 102 / 105
  Elimina la interfaz de enlace ascendente ZTP del grupo de puentes EVPN predeterminado y del dominio de puente para cada EVI específico de VLAN.

Estas plantillas garantizan una configuración EVPN uniforme en toda la red y abstraen las diferencias de nivel de hardware de ausencia.

L3VPN (VRF-Based) Service Provisioning

El caso práctico de L3VPN permite la prestación de servicios de capa 3 a través de varios SWR como terminal. El aprovisionamiento se realiza a través de la topología activa CNC, con requisitos específicos del entorno implementados mediante una plantilla NSO personalizada.

Al igual que con L2VPN, esta es una acción de configuración de día 2, que requiere entradas de operador.

Plantilla NSO personalizada

- CT-l3vpn-swr
  Recopila los parámetros específicos de VRF (número AS, nombre VRF, conjunto de prefijos, nombre de política de rutas y discriminador de rutas) y crea la política de importación/exportación de BGP necesaria, incluida la redistribución de rutas conectadas con una política de rutas definida por el usuario.

Ingeniería de tráfico

La aplicación Crosswork Optimization Engine (COE) del conjunto de aplicaciones CNC ayuda a controlar los flujos de tráfico en la red según la intención deseada.

Existen dos tipos de tráfico que requieren diferentes intentos (métricas de SLA):

- Tráfico TC1: SLA sensible a la latencia para garantizar que el tráfico se encuentre en la ruta de latencia más baja.
- Tráfico TC4: SLA de ancho de banda mínimo para garantizar que el ancho de banda dedicado esté siempre disponible para el tráfico TC4

Tráfico TC1 (latencia más baja)

Para garantizar que el tráfico TC1 siempre se lleva a cabo en la trayectoria de latencia más baja, se debe tener una política de Segment Routing (SR) creada en el SWR de cabecera con criterios de cálculo de trayectoria como latencia.

Esto se logra definiendo la configuración de Next Hop (ODN) a demanda en cada SWR de cabecera para colores específicos 1001 utilizando CNC para facilitar la creación de políticas de SR.

Tráfico TC4 (ancho de banda comprometido)

Para garantizar que el tráfico TC4 siempre se toma en el trayecto con ancho de banda dedicado, se debe tener una política de SR creada en el SWR de cabecera con criterios de cálculo de trayecto como ancho de banda.

Esto se logra mediante:

- Paquete de funciones Bandwidth on Demand (BoD) en CNC
- Definición de la configuración de Next Hop (ODN) a demanda en cada SWR de cabecera para el color específico 1004 mediante la creación de políticas CNC SR con estas configuraciones

El paquete de funciones de BoD se utiliza para calcular la ruta de las políticas de SR que tienen el ancho de banda como criterio para calcular la ruta. Realiza un seguimiento del ancho de banda comprometido con una política y mantiene la supervisión de la ruta actual de la política durante su ciclo de vida.

En cualquier momento, si el parche actual de la política BWOD no tiene suficiente capacidad disponible para satisfacer el ancho de banda comprometido, vuelve a calcular la trayectoria de la política BWOD y redirige la política a la nueva trayectoria. Esta política de redireccionamiento de BWOD es un proceso continuo y no necesita intervención manual.

En cierto modo, BWOD lleva a cabo la optimización sobre la marcha para el ancho de banda de la misma manera que SR-PCE para la latencia.

Activación del dispositivo mediante sZTP

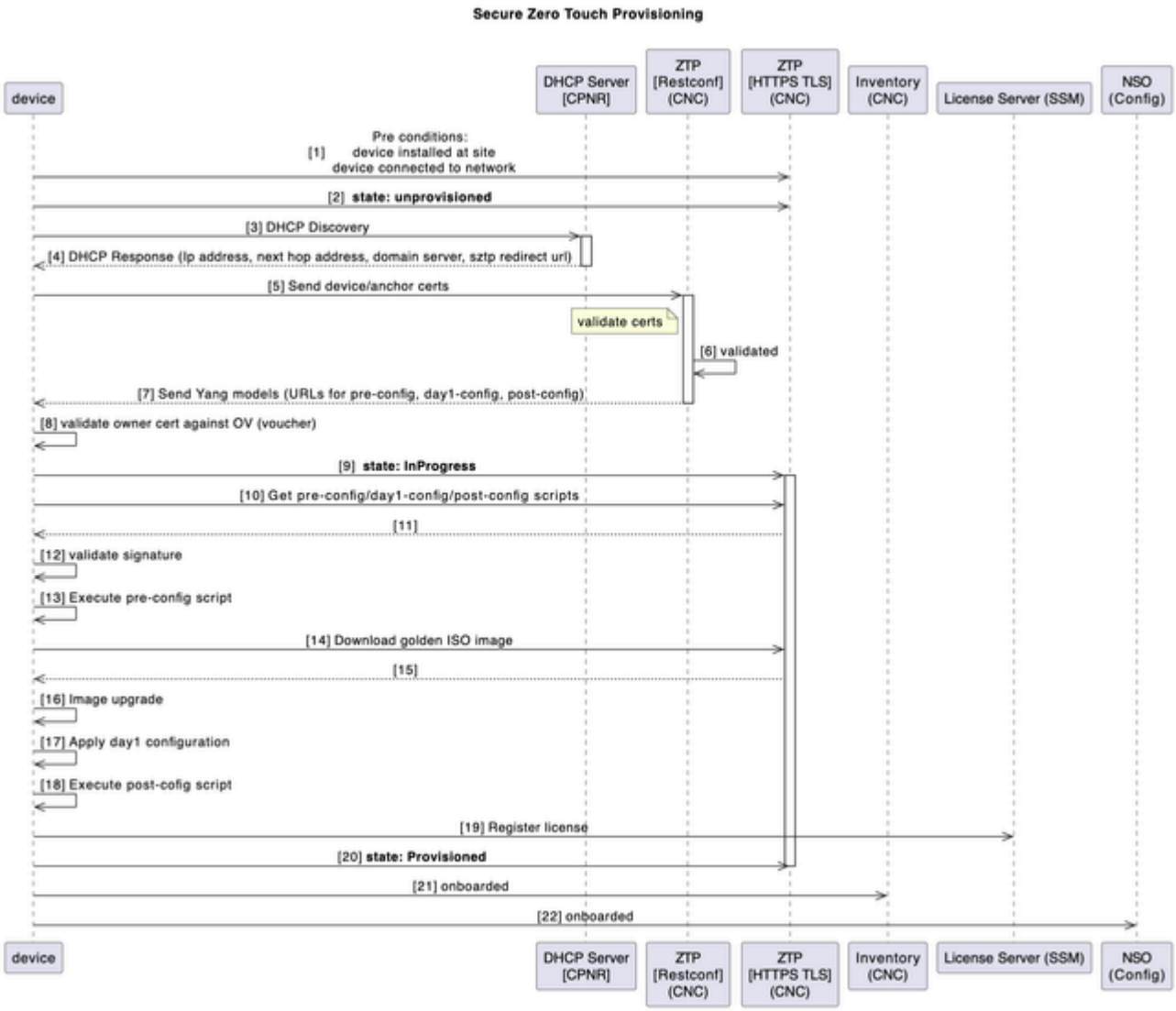
En el pasado modelo tradicional de instalación y soporte, el proceso de traer un nuevo dispositivo requería un cierto nivel de experiencia por parte del instalador para instalar, configurar y resolver problemas de la implementación de un nuevo componente. También es posible que se deba realizar un largo proceso de preparación del equipo en una ubicación externa, con el apoyo de muchas personas que trabajan en diferentes partes de la solución.

En el caso de los nuevos dispositivos SWR que se vayan a implementar en su entorno, este proceso de activación de dispositivos se automatiza con la aplicación ZTP (aprovisionamiento sin intervención) segura de CNC.

El flujo de trabajo de ZTP se activa al arrancar el dispositivo por primera vez y descargaría la imagen de plataforma planificada y la configuración inicial que debe aplicarse sin ninguna intervención manual.

El dispositivo también se incorpora automáticamente en CNC para una mayor orquestación.

Este diagrama muestra el flujo de trabajo del proceso ZTP seguro al encender el dispositivo:



Orquestación posterior a ZTP (impulsada por la automatización)

Una automatización de Python en el host de la utilidad organiza y audita el proceso de extremo a extremo mediante una entrada de Excel estructurada (por cadena):

- Genera y carga artefactos de día 1 y posteriores a la configuración en CNC.
- Crea reservas CPNR (entradas DHCP vinculadas a la serie SWR).
- Agrega el dispositivo a EPNM (para obtener visibilidad/garantía).
- Limpieza posterior a ZTP en CNC:
    - Asigna SWR a CDG (destino de telemetría)
    - Adjunta grupos de dispositivos y etiquetas
    - Actualiza la latitud/longitud para la visualización de la topología
    - Adjunta el perfil KPI de BNM para habilitar la transmisión de telemetría

Procesamiento del mensaje de notificación de ancho de banda (BNM) en CNC

El SWR puede recibir BNM desde el switch MiniLink co-ubicado, que corresponde al ancho de banda de los puertos WAN. Estos mensajes de notificación son mensajes CFM basados en estándares que incluirían el ancho de banda actual registrado en ejecución (RBW) y el ancho de banda máximo configurado, también conocido como ancho de banda nominal (NBW).

El ancho de banda actual es el ancho de banda en ejecución real del enlace WAN de microondas, según los anchos de banda agregados de los enlaces de microondas individuales y sus niveles de QAM en ejecución. El ancho de banda nominal es el ancho de banda WAN máximo posible configurado, según los anchos de banda agregados del QAM máximo configurado en cada uno de los enlaces de microondas individuales.

La optimización del ancho de banda se lleva a cabo en función de esta situación:

Cambio temporal (eventos fugaces)

- Cuando hay una degradación o interrupción pasajera en la red/link que se localiza en SWR (por ejemplo, debido a un evento meteorológico adverso que causa el desvanecimiento de la trayectoria de radio de microondas y la reducción del ancho de banda disponible debido a los cambios en los esquemas de modulación), entonces la corrección del modelado del tráfico ocurre en el SWR local en la interfaz de red afectada.
- Esto garantiza que se produzca una pérdida mínima de paquetes en la ruta de transmisión afectada.

Cuando se habilita un SWR con BNM KPI en CNC como parte de las actividades post-sZTP, CNC inserta las configuraciones de telemetría en SWR.

BNM MDT

basado en modelos de telemetría

destination-group <DGName>

vrf VRF-OMSWR-<AreaCode>1

address-family ipv4 <CDG IPv4Address> port 9010

codificación autodescriptiva-gpb

protocolo tcp

!

!

sensor-group <GroupName>

sensor-path Cisco-IOS-XR-ethernet-cfm-oper:cfm/nodes/node/bandwidth-notifications/bandwidth-notification

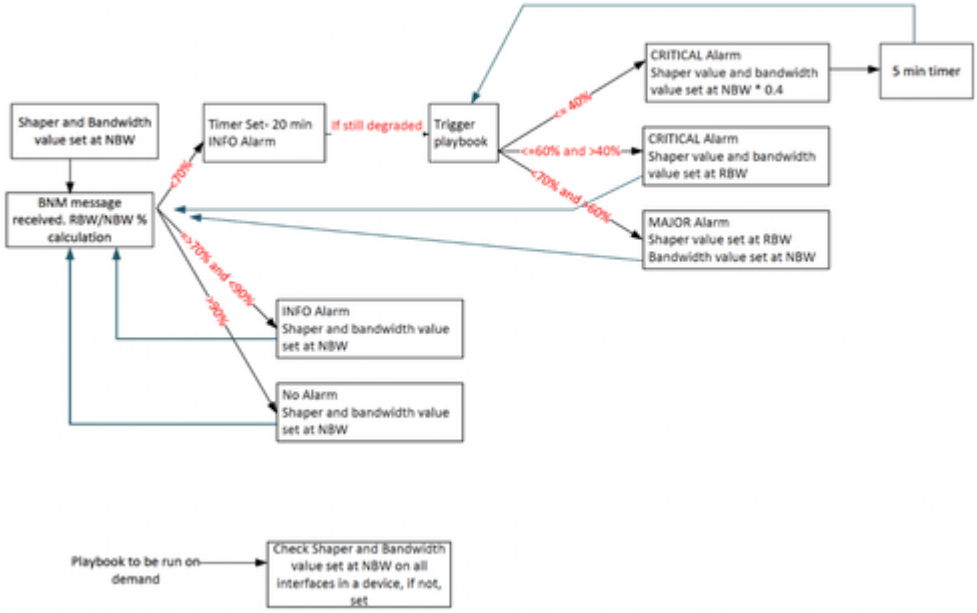
!

El CNC procesa estos mensajes BNM recibidos a través de la telemetría y toma medidas correctivas si es necesario. Aquí están los 2 componentes involucrados en el CNC:

- Health Insight (HI): la aplicación CNC se utiliza para ingerir la notificación BNM por KPI personalizado que supervisa la ruta específica del sensor para los mensajes BNM. Health Insight puede emitir alertas en caso de que los cambios en el ancho de banda sean significativos y deban tenerse en cuenta.
- Automatización de cambios (CA): la aplicación CNC se utiliza para actuar en la transmisión de mensajes BNM que causaron alertas HI. Se ha implementado 2 cuadernos personalizados para realizar estos cambios en la interfaz afectada:
    - Configuración del modelador de QoS en el nuevo RBW
    - Estableciendo la capacidad de la interfaz en el nuevo valor RBW.

Se desarrolla un script Python personalizado para ejecutar una lógica personalizada y ejecutar los cuadernos de CA automáticamente cuando se infringen los KPI de HI.

La secuencia de comandos de desencadenado de cuaderno funciona según este algoritmo:



Esta tabla explica los niveles de alerta personalizados que se han establecido en los grados de degradación del ancho de banda:

Ancho de banda notificado = RBW

Ancho de banda nominal = NBW

Valor de intervalos de alerta	Nivel de notificación
(RBW/NBW)*100 >=70	INFO
(RBW/NBW)*100 <70 y >60	Advertencia
(RBW/NBW)*100 <=60	Crítico

Este trayecto del sensor es monitoreado por CNC:

Cisco-IOS-XR-ethernet-cfm-oper:cfm/nodes/node/bandwidth-notifications/bandwidth-notification

Se crea un KPI personalizado en CNC para supervisar la ruta del sensor BNM. Este KPI se agrega a un perfil de KPI configurado con una cadencia de 120 segundos y umbrales de alerta. Al adjuntar cables de acero a este perfil, se transfiere automáticamente la configuración de

telemetría necesaria a los dispositivos a través de NSO.

Una vez habilitada, los dispositivos transmiten datos RBW/NBW a los CDG asignados en el intervalo configurado. Health Insight (HI) calcula la proporción RBW÷NBW y genera alertas cuando se superan los umbrales; los operadores pueden supervisar estos eventos en HI y a través de los paneles de Grafana.

Un proveedor de alertas en CNC reenvía estas alertas al nodo híbrido que aloja la automatización de Python. La secuencia de comandos analiza los detalles del dispositivo/interfaz/RBW/NBW y activa los cuadernos de campaña de automatización de cambios adecuados: ajuste del modelador, actualización del ancho de banda o ambos en función de la lógica de decisión definida.

Estos son los dos cuadernos de campaña que se utilizan en el flujo de trabajo:

1. Cuaderno de campaña para cambiar el valor del modelador

2. Cuaderno para cambiar el ancho de banda de la interfaz

Como ya se mencionó, el script hace girar un servidor web para actuar como proveedor para comunicarse con el CNC mediante la API REST. Cualquier respuesta que obtengamos para una solicitud POST se captura aquí. Las alertas se capturan en el formulario en JSON y luego se convierten en diccionario para extraer los parámetros necesarios.

Estandarización de las operaciones de red de día 2 mediante estrategias de automatización personalizadas

Se desarrollaron campañas personalizadas de automatización de cambios (CA) para optimizar y estandarizar las operaciones críticas de día 2 en todo el ciclo de vida de la red. Entre estas se incluyen el aprovisionamiento de Bundle-Ether, las actualizaciones de la descripción de la interfaz de gestión, la orquestación de la cadena de margarita CFM, la expansión de la capacidad de enlace sin problemas, la retirada del servicio de eNodeB y la incorporación eficiente de Mini-Link. Al integrar las mejores prácticas operativas en flujos de trabajo reutilizables, estas estrategias mejoran significativamente la coherencia de la ejecución, minimizan el riesgo de errores humanos y reducen la dependencia de las intervenciones manuales. En el contexto de una actualización de Cisco CNC, este marco de automatización desempeña un papel fundamental a la hora de acelerar el retorno de la actividad operativa, garantizar la continuidad del servicio y permitir procesos escalables y repetibles alineados con los objetivos modernos de transformación de la red.

Continuidad de la integración de TACACS+ en la actualización de Cisco CNC 7.1

Como parte de la actualización de Cisco CNC 4.1 a 7.1, la integración TACACS+ existente se conservó cuidadosamente para garantizar la continuidad de la autenticación y autorización centralizadas. El proceso de actualización validó y replicó la configuración de TACACS+ en Cisco CNC 7.1, manteniendo la alineación con las políticas de seguridad empresariales establecidas y los mecanismos de control de acceso basado en roles (RBAC).

Reenvío de CNC y CDG Syslog a Splunk

Se configura un reenvío de syslog para reenviar las alarmas/eventos/syslogs a un servidor Splunk. Para ello, se utilizó la capacidad de configuración inmediata del CNC para configurar el servidor syslog.

Desvío de alarmas a OneFM

Las alarmas CNC también se reenvían a un sistema ascendente como OneFM utilizando la API orientada a la conexión CNC restconf:

```
curl -L --request GET \

--url https://{server_ip}:30603/crosswork/notification/restconf/streams/v2/alarm.json \

--header 'Accept: application/txt'). This API must be used over a websocket connection config.
```

Automatización de copias de seguridad CNC diarias

Una secuencia de comandos automatizada hace uso de la API de copia de seguridad CNC para realizar la copia de seguridad completa de CNC y almacena el archivo de copia de seguridad en el host de la utilidad. Esta operación se realiza diariamente.

Desafíos

Gran salto en la versión Crosswork

La actualización del trabajo cruzado 4.4 a 7.1 representó un salto de versión significativo en lugar

de una actualización incremental rutinaria. Este salto de gran tamaño introdujo numerosas funciones nuevas en varias aplicaciones, junto con mejoras sustanciales y cambios arquitectónicos. Debido a esto, la actualización de CNC no era solo una sustitución de versión sencilla, sino que requería una validación exhaustiva para garantizar la compatibilidad, la estabilidad y la funcionalidad adecuada de todos los componentes integrados. El conjunto ampliado de funciones y las mejoras subyacentes implicaban que los flujos de trabajo, las configuraciones y las integraciones existentes requerían una verificación minuciosa, lo que hacía que las pruebas y la validación exhaustivas fueran fundamentales para el éxito de la actualización.

No hay actualización in situ

CNC no admite un modelo de actualización in situ. En lugar de ello, las actualizaciones deben seguir un enfoque integral, en el que se conserve la implementación existente y se cree un entorno completamente nuevo desde el principio con la versión final. Una vez instalado el nuevo sistema, las configuraciones, los datos y las integraciones deben migrarse y validarse cuidadosamente antes de que se pueda retirar el entorno anterior.

Este enfoque presenta varios retos operativos:

- Entornos paralelos: Tanto el entorno CNC antiguo como el nuevo deben ejecutarse simultáneamente hasta que la migración y la validación se completen por completo.
- Presión de recursos de hardware: La ejecución de dos entornos completos en paralelo aumenta considerablemente la demanda de recursos informáticos, de almacenamiento y de red, lo que puede sobrecargar la infraestructura disponible.
- Mayor esfuerzo de validación: Todos los datos, las configuraciones, las políticas y las integraciones migradas deben verificarse en la nueva versión para garantizar que funcionan exactamente como se esperaba.
- Complejidad de la migración de datos: La transferencia de datos históricos, configuraciones de aplicaciones y configuraciones operativas requiere una planificación cuidadosa para evitar incoherencias o pérdida de datos.
- Retraso en la clausura: El sistema antiguo y sus VM no se pueden eliminar hasta que se demuestre que la nueva implementación es estable, lo que prolonga el uso de recursos y la sobrecarga operativa.
- Coordinación operativa: Los equipos deben administrar la sincronización entre ambos entornos durante el período de transición para evitar alteraciones en la configuración o en el funcionamiento.
- Conflictos de automatización de bucle cerrado: CNC admite casos prácticos de automatización de bucle cerrado que activan acciones de forma dinámica en función de las condiciones de la red en tiempo real. Cuando tanto los controladores antiguos como los nuevos están activos durante la transición, existe el riesgo de que se pueda ejecutar la misma lógica de automatización desde ambos controladores, lo que podría dar lugar a cambios de configuración duplicados o acciones en conflicto en la red. Esto requiere un control cuidadoso de las políticas de automatización durante la ventana de migración.

- Los datos operativos heredados, incluidas las alarmas históricas, los eventos, los registros de errores y la información de auditoría, no se migran al nuevo entorno debido a la ausencia de capacidades de exportación nativas. Como resultado, estos datos históricos no están disponibles en el sistema actualizado y deben tratarse como no recuperables después de la migración.

Debido a estos factores, el modelo de elevación y desplazamiento hace que las actualizaciones de CNC requieran más recursos y sean más complejas desde el punto de vista operativo que una actualización in situ estándar.

Problemas de implementación sin opciones de reversión

Ciertos errores de configuración de implementación y posteriores a la implementación en CNC no tienen ninguna ruta de solución y requieren un desmontaje y una reimplementación completos del clúster. Por ejemplo, un FQDN incorrecto configurado para el VIP de datos de Crosswork , obligatorio para el caso de uso de sZTP, hizo que sZTP no funcionara. Dado que este valor no puede corregirse después de la implementación, se requería una reimplementación completa.

Del mismo modo, la configuración incorrecta de las credenciales de invalidación de dispositivos en la automatización de cambios no se pudo rectificar después de la implementación, lo que provocó otra reconstrucción del clúster. Otros errores, como direcciones IP de gateway mal configuradas o definiciones de subred, también se identifican como no recuperables.

Estos escenarios resaltan la importancia crítica de validar todos los parámetros inmutables durante la implementación inicial. La planificación meticulosa y la verificación de los insumos son esenciales para evitar las costosas modificaciones y el impacto de los programas.

Limitaciones de la validación de diagnóstico posterior a la implementación

CNC proporciona una utilidad de diagnóstico para evaluar los parámetros de estado en el nivel de VM, como la latencia de lectura/escritura del disco, IOPS, la latencia de sincronización, la velocidad de la interfaz de red y la frecuencia del reloj de la CPU. La utilidad informa de los valores medidos con respecto a los umbrales esperados y marca cada comprobación como superada o errónea. Sin embargo, estos diagnósticos sólo se pueden ejecutar después de que se haya implementado el clúster, por lo que no queda ningún mecanismo para validar la preparación de la infraestructura antes de la implementación.

Durante la instalación, el indicador "Ignorar comprobaciones de diagnóstico" se establece en false de forma predeterminada. En la práctica, si se produce un error en una única comprobación, el

instalador se detiene, lo que impide que continúe la implementación. Como resultado, los ingenieros de campo a menudo se ven obligados a habilitar este indicador y a omitir los diagnósticos por completo, ya que incluso los entornos de nivel de producción a menudo no superan una o más comprobaciones. Esto crea un dilema operativo: los equipos deben elegir entre aplicar una validación estricta que bloquee la implementación o continuar sin la garantía de que la infraestructura subyacente cumple los parámetros de rendimiento recomendados.

Cambio del procedimiento de creación de KPI personalizado de HI

En Health Insight 4.1, la creación de KPI personalizados se basaba en la lógica de secuencia de comandos Tick, donde las definiciones de KPI y la lógica de procesamiento se implementaban mediante secuencias de comandos dentro del marco Tick. Sin embargo, en la versión 7.1, este enfoque se sustituyó por un marco basado en archivos de seguimiento para definir y administrar KPI.

Debido a este cambio en la arquitectura, los KPI personalizados existentes no se pudieron reutilizar directamente y fue necesario volver a trabajar para alinearlos con el nuevo formato de archivo de seguimiento. Esto requirió una cantidad sustancial de tiempo y esfuerzo para:

- Comprenda el nuevo marco: El equipo tuvo que estudiar la estructura, la sintaxis y el comportamiento operativo del modelo de definición de KPI basado en archivos de seguimiento introducido en 7.1.
- Rediseñar la lógica existente: La lógica previamente implementada en los scripts Tick tuvo que ser traducida y adaptada al formato de archivo tracker.
- Volver a crear KPI de BNM: El KPI de BNM personalizado tenía que volver a crearse utilizando el nuevo marco para garantizar que produjeran los mismos resultados y perspectivas que antes.
- Validar precisión KPI: Se requería una validación exhaustiva para confirmar que las nuevas implementaciones generaban métricas coherentes y correctas en comparación con la versión anterior.
- Prueba y ajuste: El nuevo modelo también requería pruebas de rendimiento y comportamiento en condiciones reales de la red, seguidas de ajustes cuando fuera necesario.
- Falta de asistencia: Algunas funciones que funcionaban anteriormente con la secuencia de comandos tick ya no se admitían con la implementación del nuevo archivo de seguimiento. Por lo tanto, hubo que hacer algunos compromisos.

Este cambio en el mecanismo de creación de KPI aumentó significativamente el esfuerzo necesario durante la actualización, ya que implicaba tanto el aprendizaje de un nuevo sistema como la reimplementación de la lógica de supervisión personalizada existente para garantizar la continuidad de las perspectivas operativas.

Límite de tiempo API en cuadernos BNM Trigger Script

Los cuadernos BNM se activan a través de un script personalizado que interactúa con las API CNC. Durante el proceso de actualización y validación, se identificaron y abordaron varios problemas relacionados con la autenticación de API y la gestión de respuestas.

El token de la API CNC tiene una validez de 8 horas, pero el script original no incluía la lógica adecuada para actualizar el token una vez que caducó. Como resultado, aunque las alertas KPI en CNC 4.4 funcionaban correctamente, el script de activación del cuaderno dejó de ejecutarse después de que caducara el token. Este problema pasó desapercibido durante un largo período, lo que significa que el script de automatización no se había ejecutado de forma fiable durante más de un año. El problema solo se hizo visible durante las actividades de migración y validación en CNC 7.1.

Por consiguiente, se necesitaban varias mejoras y mejoras:

- Lógica de actualización de token: Se implementó la lógica adecuada para detectar el vencimiento del token y actualizar automáticamente el token de la API, lo que garantiza la ejecución ininterrumpida del script.
- Cambios en la respuesta de API: Las diferencias entre las versiones de CNC causaron problemas adicionales. En CNC 4.1, una respuesta de token caducada normalmente contenía el mensaje "caducado", mientras que en CNC 7.1, la respuesta devuelve "Clave no autorizada". La lógica del script tuvo que actualizarse para interpretar correctamente los nuevos patrones de respuesta en 7.1.
- Gestión global de token: Anteriormente, los tokens se almacenaban y utilizaban localmente dentro de las funciones. Esto creó escenarios donde el token era válido al ingresar a una función pero expiró antes de las llamadas de API subsiguientes. La implementación se modificó para utilizar la gestión global de tokens, lo que garantiza la coherencia y una actualización adecuada de todas las funciones.
- Gestión de errores mejorada: En algunos casos, la API "check sync" de NSO devolvió respuestas incompletas o diferentes de la estructura esperada. Esto provocó excepciones KeyError, que suspendieron la ejecución del script. Se introdujo una lógica de validación y gestión de excepciones adicional para que la secuencia de comandos pueda seguir ejecutándose incluso cuando se reciben respuestas de API inesperadas.
- Mejoras en la estabilidad de scripts: Se agregaron mecanismos de seguridad y comprobaciones adicionales para garantizar que los errores de API, los problemas de respuesta temporales o los eventos de actualización de token no provocan que el script finalice inesperadamente.

Estas mejoras no solo resolvieron los problemas descubiertos durante la actualización, sino que también mejoraron significativamente la fiabilidad, la resistencia y la capacidad de mantenimiento del marco de automatización del cuaderno de campaña de BNM.

Cambio de diseño del disparador de procesamiento y campaña BNM

La lógica de automatización de BNM está impulsada por eventos y se basa en alertas generadas por KPI en la aplicación Health Insight dentro de CNC. El flujo de trabajo general funciona de la siguiente manera:

1. El CNC lee los valores NB (ancho de banda nominal) y RBW (ancho de banda real) del dispositivo.
2. Calcula la proporción de ancho de banda (BW%) utilizando estos valores.
3. El KPI de Health Insight evalúa este ratio frente a umbrales de alerta predefinidos.
4. Cuando se genera una alerta, el script de activación del cuaderno BNM detecta la alerta y ejecuta los cuadernos correctivos correspondientes

Limitación en el diseño de alerta original

Los umbrales de alerta configurados fueron:

- BW% < 60 → Crítico
- 60 ≤ BW% ≤ 70 → Advertencia
- BW% > 90 → Información

Este diseño funcionó bien para identificar la degradación del ancho de banda, pero creó una brecha funcional durante los escenarios de recuperación del ancho de banda. En concreto, el intervalo del 70-90% no tenía definido ningún nivel de alerta.

Esto llevó a este comportamiento:

- Cuando el BW% cae por debajo del 70%, se genera una alerta crítica o de advertencia, que activa campañas que ajustan los valores de ancho de banda y modelador.
- Sin embargo, cuando se recuperó el ancho de banda y el BW% aumentó por encima del 70%, el KPI no generó ninguna alerta porque el valor cayó en la banda del 70-90% sin ningún nivel de alerta asociado.
- Dado que la secuencia de comandos de automatización BNM depende completamente de la generación de alertas para desencadenar acciones, no tuvo la oportunidad de leer los valores NBW/RBW actualizados ni de iniciar acciones de restauración.
- Como resultado, la restauración del ancho de banda no se realizaba automáticamente, aunque se disponía de suficiente ancho de banda. Tampoco había lógica de restauración en el diseño original.

Esta limitación se hizo visible en la red de producción, donde los links que previamente habían sufrido una reducción del ancho de banda permanecieron en un estado restringido incluso

después de que las condiciones mejoraran.

Impacto del cambio del marco de KPI

El problema se vio agravado por el cambio de marco introducido en CNC 7.1. En Health Insight 4.1, la implementación de KPI basada en marcas admitía hasta cinco niveles de alerta, lo que permitía un control más preciso de las bandas de umbral y facilitaba la implementación de la lógica de restauración.

Sin embargo, en CNC 7.1, el marco de KPI basado en archivos de seguimiento admite solo tres niveles de alerta, lo que reduce la flexibilidad a la hora de definir varios umbrales de recuperación y requiere el rediseño de la lógica de alerta para ajustarse a estas restricciones.

Desencadenado excesivo del cuaderno

Otro problema identificado en la implementación original fue la frecuencia extremadamente alta de las ejecuciones de los cuadernos de campaña. La lógica de automatización no incluía ningún tiempo de espera ni ventana de estabilización. Tan pronto como CNC lea un valor del dispositivo que cumplió la condición de alerta:

- La alerta fue levantada inmediatamente.
- El script de automatización activó inmediatamente los cuadernos de campaña correctivos.

Debido a que los valores de telemetría fluctúan con frecuencia en las redes activas, esto provocó que se activaran cientos de cuadernos de campaña cada hora, lo que no era ideal desde la perspectiva de la estabilidad de la red y del rendimiento de las aplicaciones.

Lógica de automatización rediseñada

Para hacer frente a estas limitaciones, el diseño de automatización de BNM se ha rediseñado con varias mejoras:

- Lógica de umbral de alerta revisada: Para garantizar que la banda de recuperación se capturara dentro de los tres niveles de alerta, se modificó la lógica para que cualquier BW% superior al 70% se tratara ahora como una alerta de nivel INFO, sustituyendo el enfoque anterior, en el que solo se clasificaban como INFO los valores superiores al 90%. Esto garantizó que la banda de recuperación del 70-90% se monitoree activamente, permitiendo que los cuadernos de recuperación se activen cuando mejoren las condiciones de ancho de banda.
- Introducción del tiempo de espera: Se introdujo un mecanismo de tiempo de espera de 20

minutos para garantizar que las condiciones de ancho de banda permanezcan estables durante un periodo definido antes de activar los cuadernos de campaña. Esto impide que la automatización reaccione a las fluctuaciones a corto plazo.
- Ejecución controlada de cuaderno: Con la lógica revisada y el tiempo de espera, la frecuencia de las ejecuciones de los cuadernos de campaña se redujo drásticamente, lo que evitó acciones de automatización innecesarias.
- Mecanismo de refuerzo para la degradación grave: Para los casos de degradación grave del ancho de banda, se introdujo un enfoque de refuerzo. En estos escenarios, la automatización ajusta proactivamente el modelador de tráfico y la asignación de ancho de banda al 40% del NBW, lo que permite una recuperación más rápida de la congestión.
- Estabilidad de automatización mejorada: El flujo de trabajo rediseñado garantiza que tanto los escenarios de reducción de ancho de banda como los de restauración de ancho de banda se gestionen de forma eficaz, incluso dentro de las limitaciones del marco de KPI basado en rastreador.

Resultado

Con estos cambios de diseño, combinados con las mejoras anteriores en el manejo de API, la administración de tokens y la robustez de scripts, el marco de automatización de BNM ahora funciona de una manera mucho más estable, eficiente y predecible. El sistema puede responder correctamente a las condiciones de congestión y recuperación, a la vez que evita ejecuciones excesivas del cuaderno de campaña y garantiza una optimización fiable del ancho de banda de la red.

Supresión de alarmas de dispositivos

En CNC 4.1, las alarmas fueron reenviadas a un sistema ascendente llamado OneFM a través de una API RESTCONF. Dado que la pila CNC 4.1 no incluía la funcionalidad EMF, la plataforma solo generaba alarmas a nivel del sistema. Estas alarmas se reenviaron en sentido ascendente sin ninguna complejidad relacionada con la categorización de alarmas.

Con la implementación de CNC 7.1, se introdujo la aplicación EMF, ampliando significativamente el modelo de alarma. Las alarmas se clasificaban ahora en tres tipos:

- Alarmas del sistema - relacionadas con la plataforma CNC y el estado de las aplicaciones
- Alarmas de red: relacionadas con las condiciones del servicio de red
- Alarmas de dispositivos: se generan directamente desde dispositivos de red y se reenvían a través de CNC.

Sin embargo, ya existía un EPNM responsable de recopilar y administrar las alarmas de nivel de dispositivo. Si CNC también envió estas alarmas a OneFM, se recibieron alarmas duplicadas de

ambos sistemas. Por lo tanto, el requisito era excluir las alarmas de dispositivos del CNC mientras se seguían reenviando las alarmas del sistema y de la red.

El principal desafío fue una limitación de la API ascendente RESTCONF utilizada para reenviar alarmas a OneFM. La API no admitía el filtrado de alarmas en función de la categoría de alarma. Si dicho filtrado hubiera estado disponible, la solución habría sido sencilla: simplemente excluya las alarmas de dispositivos en el nivel de API antes de reenviarlas al sistema ascendente.

Se evaluaron y discutieron varias posibles soluciones:

- Detención de desvíos de dispositivos en el origen: Impide que los dispositivos envíen trampas al CNC.
- Filtrado de alarmas en el sistema ascendente (OneFM): Permitir que el CNC envíe todas las alarmas pero filtre las alarmas de dispositivos dentro de OneFM.
- Filtrado dentro del CNC antes de enviar alarmas.

La detención de trampas en el nivel del dispositivo no se consideró viable porque el CNC confía en esas trampas para detectar eventos del dispositivo y mantener el reconocimiento operativo de las condiciones de la red. La desactivación de las trampas reduciría significativamente la capacidad del CNC para responder a los problemas de la red.

La solución implementada en última instancia aprovechó una función CNC integrada llamada Supresión de alarma de dispositivos. Esta función permite a los administradores suprimir tipos específicos de alarmas de dispositivos en función de los grupos de dispositivos, lo que evita que se procesen o se reenvíen más arriba.

Al configurar las políticas de supresión de alarmas de dispositivos, el sistema pudo:

- Suprime las alarmas generadas por dispositivos en el CNC.
- Continúe procesando y reenviando las alarmas del sistema y de la red.
- Evite que las alarmas de dispositivos duplicados lleguen al sistema OneFM.

Este enfoque proporcionaba una solución limpia y escalable sin interrumpir la capacidad del CNC para recibir trampas de los dispositivos. Como resultado, se agilizó el flujo de alarmas a OneFM, lo que garantiza que solo se reenvíen las alarmas relevantes del sistema y la red, a la vez que se evita la duplicación con la gestión de alarmas de dispositivos de EPNM.

Cambios fuera de banda

En la instalación existente, el equipo de operaciones recurría con frecuencia a scripts directos

basados en CLI para enviar las actualizaciones de configuración a los dispositivos de red, especialmente para tareas como modificaciones de ACL y actividades de depuración. Aunque este enfoque es eficaz a corto plazo, ha dado lugar a una variabilidad de la configuración, ya que los cambios realizados fuera de NSO no se han seguido dentro del sistema. Como resultado, los flujos de trabajo de aprovisionamiento de NSO se vieron afectados debido a las incoherencias entre el estado previsto (modelado) y las configuraciones de dispositivos reales, lo que provocó fallos e ineficiencias operativas.

Reconciliación de VPN L2/L3

Debido a cambios en la configuración fuera de banda: el equipo de redes había actualizado la configuración relacionada con VPN en dispositivos fuera de CNC/NSO y del flujo de trabajo de TSDN. Como resultado, el estado almacenado en NSO (desde la era CNC 4.1) no siempre coincidía con el estado de los dispositivos.

Estas discrepancias causaron varios errores e incoherencias en la reconciliación. En varios casos, NSO contenía datos del servicio VPN que ya no existían en los dispositivos (o que se habían modificado de un modo que NSO no reflejaba). Para alinear NSO con la red, era necesario eliminar las entradas de servicio VPN que existían solo en NSO y no en los dispositivos, y corregir otros desajustes causados por cambios fuera de banda.

Impacto de programación

Para resolver estas cuestiones se necesitaron aproximadamente dos semanas más después del plan de reconciliación original. El tiempo adicional se dedicó a identificar discrepancias, validar el estado del dispositivo y limpiar o corregir de forma segura los datos de NSO CDB.

‘Observaciones’

1. Autoridad de configuración: Los cambios fuera de banda en la configuración de VPN (o en cualquier configuración gestionada por TSDN) crean divergencias entre NSO y la red y complican la reconciliación.
2. Base previa a la migración: Una base clara de estado gestionado por NC/NSO frente al estado solo de dispositivos antes de la migración habría facilitado la detección y resolución de las discrepancias.
3. Automatización y conversión: Los scripts de conversión de carga útil y las personalizaciones específicas del usuario fueron esenciales para manejar las diferencias de formato y modelo entre 4.1 y 7.1 de manera uniforme.

Recomendaciones para actualizaciones similares

1. Aplicar una congelación de cambios para VPN (y otros servicios gestionados por TSDN) durante la ventana de reconciliación, con excepciones solo a través de un proceso controlado.
2. Ejecute una auditoría previa a la reconciliación en la que se compare CDB de NSO con la configuración del dispositivo para cuantificar y enumerar las discrepancias antes de iniciar la reconciliación.
3. Documentar y socializar que los cambios de VPN deben pasar por CNC/NSO TSDN después de la actualización para evitar la recurrencia de la deriva fuera de banda.
4. Conservar los scripts de conversión y reconciliación para reutilizarlos en futuras actualizaciones o para solucionar problemas.

Error de copia de seguridad CNC debido a dependencias del modo de mantenimiento

El mecanismo de copia de seguridad CNC exige que la plataforma se ponga en modo de mantenimiento antes de que se pueda iniciar una operación de copia de seguridad. Por diseño, la API de respaldo hace cumplir este requisito previo; si el CNC no puede pasar al modo de mantenimiento, el proceso de copia de seguridad se aborta automáticamente.

En la práctica, al entrar en el modo de mantenimiento se producen errores frecuentes debido a las actividades continuas del sistema, entre las que se incluyen:

- Ejecuciones del cuaderno de campaña de automatización de cambios activos (MOP)
- Flujos de trabajo sZTP continuos
- Operaciones de servicio DLM
- Actividades de adjuntar o desasociar perfiles de KPI
- Colecciones showtech a demanda
- Tareas de orquestación en segundo plano

La presencia de cualquier actividad de este tipo impide que CNC entre en modo de mantenimiento, haciendo que la operación de copia de seguridad falle antes de la ejecución.

Impacto operativo

Las copias de seguridad CNC diarias necesarias para garantizar el cumplimiento y el funcionamiento. Sin embargo, la actividad de automatización frecuente, en particular las campañas activadas por BNM, impedía que el sistema entrara en modo de mantenimiento. Como resultado, los fallos de copia de seguridad se produjeron de forma repetida, lo que generó un riesgo operativo significativo y requirió la intervención manual.

Estrategia de mitigación

1. Optimización de programación de respaldo: Se identificó una ventana de mantenimiento con actividad mínima del sistema. Según el análisis del tráfico y la automatización, el trabajo de copia de seguridad se programó para las 5:00 a.m. (AEST), cuando era menos probable que la orquestación y la ejecución del cuaderno estuvieran activas.

2. Validación de actividad previa a la copia de seguridad: se introdujo una comprobación previa automatizada antes de invocar la API de copia de seguridad:

- El script consulta las API CNC para detectar los trabajos MOP de automatización de cambios en ejecución.
- Si algún trabajo se informa como En ejecución, el script espera 5 segundos y vuelve a intentarlo.
- Este bucle continúa hasta que el sistema informa de que no hay trabajos activos.
- Sólo después de que el entorno se confirme inactivo, el script intenta habilitar el modo de mantenimiento y activar la copia de seguridad.

Esto evitó intentos de copia de seguridad innecesarios mientras el sistema se encontraba en un estado operativo ocupado.

3. Mecanismos de reintento y resiliencia: Para dar cabida a los estados transitorios del sistema, se añadieron salvaguardias adicionales:

- Hasta tres intentos de reintento si la API de copia de seguridad devuelve un error
- Intervalos de retraso cortos entre reintentos
- Gestión correcta de errores para evitar la terminación de scripts

Resultados y resultados

La mitigación combinada mejoró significativamente la fiabilidad de las copias de seguridad:

- Los fallos de copia de seguridad se redujeron drásticamente
- Después de la implementación, solo se observaron dos errores, ambos causados por un proceso sZTP bloqueado, que está fuera del control del script.
- La introducción de retrasos en la ejecución en la automatización del cuaderno de campaña BNM redujo aún más la contención con el modo de mantenimiento.

Reenvío de registros del sistema a Splunk

El destino de syslog se configuró en CNC para reenviar registros a Splunk sobre TLS. Sin embargo, una vez recibidos, los registros eran ilegibles en el lado Splunk. Debido a este problema que se origina en el entorno Splunk, se eligió la opción para volver al transporte UDP, después de lo cual los registros se procesaron correctamente.

Problema de migración de agrupación de dispositivos

El usuario creó previamente 18 grupos de dispositivos en CNC 4.1; sin embargo, esa versión no proporcionaba ningún mecanismo basado en la interfaz de usuario o en la API para exportar o importar grupos de dispositivos. Como resultado, la migración de estos grupos a CNC 7.1 requería un enfoque no estándar. Se identificaron dos API CNC internas: una que expone la jerarquía de grupos de dispositivos y otra que enumera los dispositivos asignados a cada nodo de jerarquía. Mediante estas API, todos los grupos de dispositivos y sus dispositivos asociados se extrajeron y almacenaron como salidas JSON. A continuación, se desarrolló un script personalizado para analizar las respuestas y extraer solo los nombres de host de los dispositivos de cada grupo.

CNC 7.1 introdujo capacidades nativas de importación/exportación para grupos de dispositivos, incluida una plantilla de importación basada en CSV. Después de extraer los nombres de host del sistema heredado, se creó un segundo script de automatización para rellenar las plantillas CSV en el formato requerido, asegurándose de que cada grupo de dispositivos se pudiera importar de forma precisa e independiente. Esta automatización era esencial; sin ella, la migración de los grupos de dispositivos a CNC 7.1 habría sido mucho más lenta y compleja desde el punto de vista operativo.

Aísle los dispositivos con deterioro grave del ancho de banda

A pesar de la implementación del caso práctico de BNM para remediar automáticamente las bajas ratios de RBW/NBW, un subconjunto de dispositivos continuó en estados severamente degradados durante periodos prolongados. Aunque las estrategias de modelado y ajuste del ancho de banda solían restaurar los dispositivos poco después de los eventos de degradación, varios dispositivos permanecieron en un estado Crítico durante más de una semana y necesitaron intervención manual. Sin embargo, la identificación de estos dispositivos presentaba un reto. Aunque la interfaz de usuario de CNC proporciona visualizaciones claras de alertas y métricas de ancho de banda, no revela fácilmente los dispositivos que han permanecido exclusivamente en estado crítico durante un intervalo prolongado.

Para abordar esta brecha operativa, se desarrolló una solución impulsada por API. CNC ofrece una API que recupera una lista de los principales dispositivos generadores de alertas en ventanas de tiempo configurables (por ejemplo, 7 días, un mes). Al obtener estos datos y filtrar por

dispositivos que solo generaban alertas críticas durante el período seleccionado, el equipo pudo aislar rápidamente los dispositivos que requerían una remediación manual. Este enfoque automatizado mejoró significativamente la eficacia de la resolución de problemas y redujo el tiempo necesario para identificar los casos de degradación persistentes.

Eliminación de configuración de telemetría del dispositivo

En CNC 4.1, las configuraciones de telemetría suministradas por NSO mediante el paquete them-tcfunction se aplicaban automáticamente cuando un dispositivo se asociaba a un perfil KPI de Health Insight (HI). Sin embargo, estas configuraciones (incluidas las referencias VIP de CDG) no se quitaron cuando se desasoció el perfil KPI. Como resultado, los dispositivos fueron acumulando entradas de telemetría obsoletas y redundantes a lo largo del tiempo.

Este problema se hizo más pronunciado durante la actualización a CNC 7.1. Los dispositivos a menudo conservaban configuraciones de telemetría CDG VIP heredadas de CNC 4.1 junto con las nuevas entradas generadas por CNC 7.1, lo que llevó a múltiples configuraciones de telemetría en conflicto en más de 2,000 dispositivos. Se plantearon preocupaciones sobre el impacto operativo y la higiene de la configuración, ya que solo la configuración VIP CNC 7.1 CDG debe haber permanecido activa.

Para solucionar este problema, se desarrolló un script automatizado para identificar y eliminar referencias CDG VIP obsoletas de la configuración de telemetría de cada dispositivo. Esta solución eliminó las incoherencias en la configuración, restableció la alineación con el modelo de telemetría 7.1 esperado e impidió lo que habrían sido varios días de esfuerzo manual de limpieza en toda la flota de dispositivos de gran tamaño.

Solucionar problemas de recopilación MDT

En CNC 7.1, la mayoría de las colecciones de KPI de Health Insight (HI) se basan en la telemetría basada en modelos (MDT). Cuando se habilita un perfil KPI en un dispositivo, NSO programa automáticamente las rutas de sensor necesarias y configura el CDG VIP como destino de telemetría. Una vez aplicada esta configuración, se crea un trabajo de recopilación CDG correspondiente para realizar un seguimiento del estado de telemetría del dispositivo.

Durante la validación, se informó de que a más de 100 dispositivos les faltaban configuraciones de telemetría. La identificación de estos dispositivos a través de la interfaz de usuario de CNC no resultó práctica, ya que la interfaz de usuario solo admite el filtrado por dispositivo y no se amplía de forma eficaz para una flota que supere los 2000 dispositivos. Esto requería un método automatizado para determinar qué dispositivos carecían de configuración de telemetría y necesitaban volver a habilitar los KPI.

Para solucionar este problema, utilizamos la etiqueta BNM asignada a los dispositivos cada vez que se activa un perfil KPI. En primer lugar, se generó una exportación de todos los dispositivos con la etiqueta BNM. A continuación, se desarrolló un script Python para interactuar con la API de recopilación CNC, incorporando la lógica de paginación para recuperar el conjunto completo de trabajos de recopilación (cada llamada de API devuelve un máximo de 100 entradas). El script extrajo los nombres de host de los datos del trabajo de recopilación y los comparó con la lista de dispositivos etiquetados BNM exportados.

Esta comparación dio como resultado la lista de dispositivos etiquetados pero que no aparecieron en el trabajo de recopilación BNM, lo que indica que la configuración de telemetría MDT no se había aplicado. El perfil KPI se volvió a habilitar en estos dispositivos y la validación confirmó que todos los trabajos de recopilación correspondientes se crearon correctamente.

Esta automatización simplificó significativamente el proceso de solución de problemas, lo que permitió al equipo identificar y remediar todos los dispositivos afectados en un solo día, un esfuerzo que no habría sido factible a través de la inspección manual.

Cambios de comportamiento de HA y ajuste del algoritmo de consenso en NSO 6.4.1.1

Durante la actualización de Cisco NSO 5.7.5.1 a 6.4.1.1 como parte de la transición a Cisco CNC 7.1, se observó un cambio notable en el comportamiento de alta disponibilidad (HA) debido a la habilitación implícita del algoritmo de consenso en la versión más reciente de NSO. Este no fue el comportamiento predeterminado en NSO 5.7.5.1, lo que llevó a un cambio en las características de failover después de la actualización. Específicamente, cuando el nodo principal se desactivó, el nodo secundario pasó a un estado de solo lectura, lo que le impidió gestionar las actividades de aprovisionamiento. De forma similar, cuando el nodo secundario se desactivó, el nodo principal pasó de un estado principal activo a un estado "ninguno", lo que afectó a la continuidad del servicio.

Para restaurar el comportamiento esperado de HA alineado con la implementación anterior, el algoritmo de consenso se deshabilitó explícitamente en NSO 6.4.1.1. Este ajuste garantizó que los nodos primarios y secundarios reanudaran sus funciones previstas durante los escenarios de conmutación por fallo, lo que permitió un aprovisionamiento ininterrumpido y mantuvo la estabilidad operativa coherente con la versión anterior de NSO.

Mejoras en la actualización de la versión de NSO y compatibilidad de paquetes

Como parte de la transición de Cisco CNC 4.1 a 7.1, la versión de Cisco NSO subyacente se actualizó de 5.7.5.1 a 6.4.1.1. Esta actualización de la versión introdujo cambios en las estructuras de plantillas XML dentro de los paquetes de NSO existentes, lo que provocó fallos en

algunos casos de pruebas de regresión que dependían del comportamiento de las plantillas heredadas.

Para subsanar estas lagunas de compatibilidad, se analizaron y actualizaron las plantillas de paquetes NSO afectadas para ajustarlas al esquema y los requisitos de procesamiento revisados de NSO 6.4.1.1. Estas mejoras garantizaron que todos los flujos de trabajo de automatización y los modelos de servicio siguieran funcionando según lo previsto, restableciendo la estabilidad de regresión y manteniendo la coherencia en el entorno CNC actualizado.

Problemas con la habilitación de KPI a escala

CNC proporciona un mecanismo de interfaz de usuario listo para usar para habilitar perfiles KPI en dispositivos. Si bien este enfoque funciona bien para las flotas pequeñas, se vuelve ineficiente y poco confiable a gran escala. En esta implementación, más de 2000 dispositivos SWR requerían la habilitación de KPI y la interfaz de usuario no ofrecía una forma eficaz de seleccionar o procesar dispositivos de forma masiva.

Inicialmente, se intentó un enfoque basado en etiquetas: a todos los dispositivos SWR se les asignó una etiqueta SWR y la habilitación de KPI se ejecutó mediante la selección de etiquetas en lugar de la selección manual de dispositivos. Sin embargo, el procesamiento de más de 2000 dispositivos en un único flujo de trabajo suponía importantes retos operativos. El trabajo duró más de tres horas y se completó con cientos de fracasos. Aunque todos los dispositivos se incluyeron en la intent, solo unos 750 recibieron correctamente la habilitación de KPI, y los intentos repetidos solo produjeron un progreso incremental. Este enfoque no resultó ni escalable ni repetible. Mostró problemas significativos con la carga.

Un segundo desafío surgió a raíz de los problemas de sincronización de dispositivos de NSO. Muchos errores indicaron que NSO no estaba sincronizado con los dispositivos correspondientes. Intentar realizar la sincronización manual desde las operaciones seguidas de la rehabilitación de KPI no era práctico y habría requerido un gran esfuerzo por parte del operador.

Para abordar estas limitaciones, se desarrolló un flujo de trabajo automatizado y dirigido por lotes:

1. Exporte el inventario CNC completo.
2. Procesar dispositivos en lotes de 50 (identificado como el tamaño óptimo mediante el ajuste).
3. Para cada lote, active una sincronización automática desde mediante UUID de dispositivo.
4. Ejecute la habilitación de KPI a través de la API CNC.
5. Supervisar el historial de trabajos de KPI y los errores de registro mediante programación.
6. Vuelva a procesar los dispositivos que hayan fallado repitiendo los pasos de sincronización y habilitación de KPI.
7. Una vez que el lote se complete correctamente, pase al siguiente conjunto de 50

dispositivos.

La automatización también incluía la capacidad de deshabilitar los perfiles de KPI, lo que permitía una gestión completa del ciclo de vida.

Esta solución ofrecía un proceso optimizado, predecible y altamente escalable para el aprovisionamiento de KPI. Eliminó la intervención manual, garantizó resultados uniformes y ahorró varios días de esfuerzo operativo. La misma automatización resultó inestimable cuando los perfiles KPI tuvieron que desactivarse y volver a activarse tras el cambio de diseño de BNM, lo que permitió una reconfiguración rápida y sin errores en toda la flota de 2000 dispositivos.

API ascendente RESTCONF restringida al acceso de administrador

La API ascendente basada en RESTCONF que se usa para reenviar alarmas y eventos desde CNC tiene una limitación por la cual se puede invocar solamente usando la cuenta admin. Los intentos de acceder a la API a través de cuentas de servicio no tuvieron éxito, a pesar de que estas cuentas tenían las funciones operativas necesarias. Como solución alternativa, se requería que el usuario usara las credenciales de administrador para el reenvío de alarmas al sistema ascendente, lo que introducía una restricción operativa y limitaba la adhesión a los principios de acceso con menos privilegios.

La automatización como facilitador estratégico

Dada la escala y complejidad del programa de migración y actualización del CNC, la ejecución manual de las tareas operativas demostró rápidamente ser insostenible. Actividades como la incorporación de dispositivos, el aprovisionamiento de KPI, la alineación de la configuración, la reconciliación y la validación de telemetría implican miles de elementos de red y flujos de trabajo repetidos que son muy propensos a errores humanos cuando se realizan manualmente. Por lo tanto, la automatización era esencial no solo para acelerar la ejecución, sino también para garantizar la coherencia, reducir el riesgo operativo y liberar a los equipos de entrega de tareas repetitivas y que requerían mucho tiempo.

Al sistematizar estos procesos a través de flujos de trabajo guiados y operaciones impulsadas por API, el programa de actualización logró importantes ganancias de eficiencia. La automatización permitió una finalización más rápida de las tareas, una mayor precisión y resultados predecibles en todas las secciones. Los ahorros resultantes no solo redujeron el plazo de implementación general, sino que también permitieron a los ingenieros centrarse en los esfuerzos de diseño y validación de mayor valor en lugar de en las tareas operativas rutinarias.

Algunas de las actividades de automatización se identificaron antes de que comenzara el

proyecto de actualización, mientras que otras evolucionaron cuando surgieron los retos. También hubo algunos que fueron necesarios por las cuestiones que se desarrollaron durante el curso del proyecto.

Esta tabla ilustra las áreas en las que la automatización tuvo un impacto sustancial en todo el programa.

Descripción de tarea	Esfuerzo manual (días)	Esfuerzo de automatización (días)	Ahorro estimado (días)
Actualizaciones de ACL (SWR/LWR)(más de 2000)	30.0	2.0	28.0
Migración de dispositivos y conexión a CDG(2K+)	5	1.0	4.0
Conexión KPI BNM a dispositivos (más de 2K)	4.0	1,5 (promedio)	2.5
Reconciliación de servicios	7	2.5	4.5
Migración de grupos de dispositivos	4	0,5	3.5
Aísle los dispositivos con degradación grave del ancho de banda	3	0,5	2.5
Troubleshooting de Colección MDT	3	0,5	2.5
Totales	56 días	8,5 días	47,5 días

Lecciones aprendidas

La actualización no es sencilla

CNC no admite actualizaciones in situ, y el modelo de elevación y desplazamiento introduce una complejidad operativa significativa. El proceso nunca debe ser asumido como simple, especialmente cuando el salto de versión es grande. Surgen problemas inesperados en las aplicaciones, las integraciones y los flujos de trabajo, y cada uno de ellos requiere tiempo, análisis y una mitigación cuidadosa. Un salto de versión importante amplía este desafío, por lo que resulta esencial llevar a cabo una planificación, validación y ejecución por fases exhaustivas. Tuvimos que pasar mucho tiempo extra en casos del TAC y en esfuerzos de resolución de problemas. Como no hemos mantenido el tiempo en el búfer para esto, se convirtió en un reto.

CX tiene que hacer el levantamiento pesado

Se espera un importante esfuerzo de CX en la implementación, las integraciones, la migración y la validación integral del caso práctico. No asuma que los flujos de trabajo probados en la versión anterior se comporta de manera idéntica en la nueva.- Mucho de la resolución de problemas y análisis sería necesario para hacer que las cosas funcionen.

Kit de herramientas de automatización es una necesidad

El proceso de actualización demostró que la automatización no es una comodidad opcional, sino un requisito básico para las implementaciones de CNC a gran escala. Planificamos la automatización de los candidatos necesarios desde el principio, pero nunca se puede suponer que vaya a ser suficiente. En mitad del proyecto, podrían identificarse problemas en casos prácticos en los que la automatización añadiría valor, como se ha demostrado en las secciones anteriores.

Evite los conflictos de controladores duales durante la migración

Durante la actualización, es fundamental asegurarse de que los entornos CNC antiguos y nuevos no estén activos simultáneamente. Aunque es necesario un breve período de estabilización para la validación, su ampliación significativa, como ocurrió en este proyecto durante más de 2 meses, crea riesgos operativos. Con ambos CNC activos durante más de 15-20 días, las funciones de automatización de bucle cerrado, como Bandwidth On Demand, generaban acciones incoherentes y conflictivas en toda la red, ya que la lógica de automatización se ejecutaba desde dos controladores a la vez.

Una lección clave es implementar barandillas claras durante la migración. Medidas como la desactivación administrativa de dispositivos en el antiguo CNC, la pausa de los flujos de trabajo

de automatización o la restricción de las suscripciones de telemetría habrían evitado estos conflictos. Las actualizaciones futuras deben planificar explícitamente el aislamiento estricto del controlador para evitar interferencias de dos controladores y garantizar un comportamiento de red predecible.

Las RdP no son sacrosantas

Aunque los documentos del método de procedimiento (MOP) se crean para cada implementación, integración y caso práctico, no es realista suponer que un MOP validado en condiciones de laboratorio se comporta de manera idéntica en producción. El entorno de producción reveló constantemente desviaciones, algunas leves, otras significativas, lo que puso de relieve lagunas que no eran visibles durante los ensayos controlados. Las redes reales, los comportamientos heredados, las dependencias externas y las condiciones de tráfico real introducen variables que las simulaciones de laboratorio no siempre pueden replicar.

El aprendizaje clave es que los equipos deben abordar la implementación de la producción con la expectativa de encontrar comportamientos inesperados, casos límite y nuevos descubrimientos. La flexibilidad, la capacidad de resolución de problemas rápida y la preparación para adaptar los procedimientos sobre la marcha son esenciales para una ejecución correcta a escala.

Eficacia de los casos TAC

Los problemas de postproducción son inevitables, y aunque la resolución de problemas inicial por parte del equipo de entrega es valiosa, confiar únicamente en el esfuerzo interno puede conducir a retrasos innecesarios. Es prudente abrir un caso TAC en paralelo como red de seguridad, especialmente para problemas relacionados con el producto o comportamientos complejos que no se pueden diagnosticar inmediatamente. Las investigaciones del TAC a menudo requieren tiempo, y el retraso de varios días en la creación de casos puede dar lugar a una pérdida significativa del impulso del proyecto. La participación temprana del TAC garantiza la disponibilidad de la asistencia de expertos cuando es necesario, acelera la identificación de las causas principales y evita el retraso evitable de la programación.

Involucre a la BU del CNC para obtener un apoyo efectivo al conocimiento

El fuerte apoyo de la unidad de negocio CNC es muy valioso durante cualquier proyecto CNC. Los usuarios a menudo requieren información detallada sobre los productos y aclaraciones que no están disponibles con el equipo de entrega solo. Disponer de un contacto de la unidad de negocio accesible durante todo el proceso de compromiso acelera la resolución de problemas, refuerza la precisión técnica y ayuda a crear una mayor confianza y un mejor entendimiento entre

los usuarios.

Prácticas recomendadas para la actualización de CNC

Planificación de una estrategia de actualización optimizada

CNC no admite actualizaciones in situ, por lo que la implementación en paralelo es inevitable. Considere el nuevo entorno como una instalación nueva y asigne suficiente capacidad informática, de almacenamiento y administrativa para ejecutar dos entornos simultáneamente. Planifique las fases de validación, la secuencia de la migración y las actividades de transición con mucha antelación.

La validación rigurosa previa a la implementación es esencial, especialmente para los parámetros inmutables

Muchas experiencias subrayan la importancia crítica de la diligencia durante la implementación inicial. La validación inicial de todas las entradas clave, especialmente los parámetros de configuración inmutables, es esencial para evitar las costosas reimplementaciones y el impacto de la programación. Por lo tanto, se recomienda encarecidamente el uso de listas de comprobación estructuradas previas a la implementación, revisiones inter pares y validaciones de simulación para minimizar el riesgo de errores de configuración irreversibles.

Utilizar un entorno de validación dedicado antes de tocar la producción

El establecimiento de un entorno interno de CALO/pruebas en las fases tempranas del proyecto permite a los equipos experimentar, validar flujos de trabajo, descubrir cambios específicos de la versión y generar confianza antes de tocar la producción. Esto reduce significativamente las incógnitas durante la implementación final.

Dimensionamiento basado en evidencia para componentes de entrecruzamiento distribuido

Al diseñar clústeres, distribuciones CDG y asignaciones PCE, las decisiones se basan en los tipos de dispositivos, la escala de la interfaz, la complejidad de la topología y la intensidad de la recopilación, en lugar de en simples recuentos de dispositivos. Las distribuciones equilibradas

evitan la sobrecarga y garantizan un rendimiento predecible en todo el clúster.

Automatización para trabajos repetitivos de gran volumen

Establecer una acumulación de automatización en las tareas iniciales que son repetitivas, de gran volumen o críticas desde el punto de vista operativo e invertir donde la automatización es obligatoria. Valide y perfeccione su automatización en el entorno SIT en primer lugar, asegurándose de que la producción no se base en correcciones de última hora. La escalabilidad aumenta el coste del trabajo manual; la automatización estandarizada mejora la calidad, velocidad y control. Resultados del paquete como recursos reutilizables (interfaces documentadas, trabajos parametrizados, bibliotecas compartidas) para que los equipos puedan aprovechar la misma automatización para futuras actualizaciones de Crosswork y proyectos adyacentes, reduciendo el tiempo de reprocesamiento e incorporación.

Evite el control de bucle cerrado dual durante la ejecución en paralelo

Durante la coexistencia, considere la automatización de bucle cerrado como una capacidad de un solo escritor: solo una ruta de orquestación puede impulsar de forma activa la remediación o la configuración basada en políticas. El CLA simultáneo en pilas antiguas y nuevas puede provocar disparadores duplicados e intentos divergentes, lo que puede desestabilizar el estado del dispositivo. Planifique la puesta en marcha de CLA como un hito de fase tardía, después de la validación funcional y la transición definitiva al nuevo controlador.

Realizar evaluación de impacto de actualización estructurada

Los saltos de las principales versiones introducen nuevas capacidades al tiempo que desaprueban o cambian las más antiguas. Es extremadamente importante tener en cuenta estos cambios. Muchas veces, el cambio no se documentará en las notas de la versión actualizada y aparecerá cuando lleguemos al campo. Realizar evaluaciones estructuradas de:

- API obsoletas
- Cambios del marco KPI
- Diferencias de comportamiento en el nivel de aplicación
- Desviaciones del modelo de configuración
- Alertas, procesamiento de la topología y cambios en la ejecución del cuaderno

Prueba de compatibilidad y comportamiento en la superficie de integración

CNC interactúa con varios sistemas externos como NSO, SSM, CPNR, EPNM, OneFM, Splunk y marcos de orquestación.
Antes de la migración:

- Validar compatibilidad de versiones
- Probar todas las integraciones ascendentes/descendentes
- Confirmar modelos de datos, trampas y flujos de telemetría
- Comprobar el comportamiento de autenticación SSL/RESTCONF

Los fallos de integración detectados tras la migración crean puntos ciegos operativos.

Establecer una estrategia sólida de exportación de datos antes de la migración

Exporte todo antes de comenzar la migración:

- Perfiles de credenciales
- Proveedores
- Etiquetas
- Cuadernos personalizados
- KPI personalizados
- Funciones y RBAC
- vales sZTP
- Grupos de dispositivos
- Metadatos de servicio históricos

Migración De Dispositivos Por Lotes Con Puertas De Validación Integradas

Al migrar miles de dispositivos, realice la migración en lotes controlados:

- Mover dispositivos en cohortes fijas (por ejemplo, por región, carga CDG o tipo de dispositivo)
- Validar la telemetría, el estado de sincronización de NSO y la disponibilidad antes de pasar al siguiente lote
- Revertir el lote si aparecen anomalías persistentes

Esto evita cargas altas en CDG y CNC en un corto intervalo de tiempo.

Gestión de cambios de configuración fuera de banda mediante la integración con NSO

Para hacer frente al desafío fuera de banda como parte de la actualización de CNC 4.1 a 7.1, se implementó un cambio estructurado hacia las operaciones impulsadas por NSO. Se proporcionó al equipo de operaciones acceso controlado y basado en usuarios a la CLI de NSO, mientras que se restringió el acceso administrativo directo a la CLI del dispositivo para evitar cambios fuera de banda. Además, las secuencias de comandos CLI heredadas se convirtieron sistemáticamente en automatización basada en RESTCONF integrada con NSO, lo que habilitó funciones como la validación a seco y la reversión transaccional. Este enfoque garantizó que todos los cambios de configuración se gestionaran de forma centralizada, fueran auditables y coherentes con los modelos de servicio de NSO, lo que eliminó de forma eficaz la variabilidad de la configuración y restableció la fiabilidad del aprovisionamiento.

Haga mucho hincapié en la congelación de cambios

Durante las ventanas de migración críticas:

- Congelar cambios de red iniciados por el usuario
- Restringir inserción de configuración
- Sincronizar con equipos de campo y NOC
- Planee una ventana para acomodar las actividades de emergencia como el reemplazo de dispositivos usando CNC/ZTP y así sucesivamente.

Esto reduce el ruido y garantiza que el estado de la red permanezca estable durante toda la actualización

Conclusión

La migración de CNC 4.1 a CNC 7.1 constituye un caso práctico significativo de las complejidades inherentes a las actualizaciones de las plataformas de orquestación de redes a gran escala. Este proyecto demuestra que estas transiciones no son solo avances de versiones, sino transformaciones completas en capas de arquitectura, flujos de trabajo operativos y ecosistemas de automatización. La ausencia de una ruta de actualización in situ requería una implementación completa de cambios y levantamientos, lo que introducía retos de entorno paralelos y requería una coordinación meticulosa entre CNC, NSO, SR-PCE, CDG e integraciones de sistemas externos. El panorama operativo resultante puso de relieve la importancia de contar con metodologías de migración sólidas, ciclos de validación exhaustivos y procesos de transición estrechamente controlados para mitigar los riesgos en los entornos de producción.

La actualización reveló además la importancia de la automatización como pilar indispensable para la escalabilidad y la precisión. Con más de 2.000 dispositivos, amplias configuraciones de telemetría, múltiples componentes dependientes y flujos de trabajo dinámicos de automatización de bucle cerrado, el proyecto destacó las limitaciones de los procedimientos manuales en entornos de esta magnitud. La automatización creada específicamente que abarca las actualizaciones de ACL, la incorporación de dispositivos, el aprovisionamiento de KPI, la limpieza de telemetría y el aislamiento de fallos resultó esencial para garantizar el determinismo, reducir los errores humanos y lograr unas ganancias de eficacia significativas. El marco de automatización no solo permitió la continuidad operativa durante la migración, sino que también estableció una base sostenible para la optimización continua de la red.

Igualmente importante fue el reconocimiento de que el comportamiento de la producción se desvía notablemente de las condiciones de laboratorio controladas. Los cambios en el marco de trabajo, como la transición de la lógica KPI basada en marcas a las definiciones basadas en rastreadores, introdujeron cambios de comportamiento imprevistos que requerían reingeniería, nuevas pruebas y perfeccionamiento iterativo. Del mismo modo, los retos operativos relacionados con la automatización de bucle cerrado, la fiabilidad de la telemetría y el comportamiento de la API pusieron de manifiesto la necesidad de una resolución de problemas adaptable, una evaluación proactiva de los riesgos y un compromiso continuo con los expertos en las materias del TAC y de la unidad de negocio. Estos factores ilustran colectivamente que las transiciones de las principales versiones exigen profundidad técnica y preparación organizativa. Quedan pocos problemas pendientes que se espera que se resuelvan en la próxima versión 7.2 del trabajo cruzado.

En general, esta actualización demuestra que las migraciones CNC a gran escala que se realizan con éxito se basan en cuatro pilares fundamentales: validación rigurosa previa a la implementación, automatización sistemática y resistente, sólida coordinación entre funciones y una postura operativa adaptable que anticipa las divergencias entre los entornos de laboratorio y de producción. La información obtenida de este compromiso no solo contribuyó a una implementación estable de CNC 7.1, sino que también ofrece un anteproyecto para futuras transiciones, que informa las mejores prácticas, refuerza las barreras arquitectónicas y fortalece el conocimiento institucional para la posterior evolución de su ecosistema de automatización de la red.

Glosario de términos

Término	Definición
BNM	Mensaje de notificación de ancho de banda.

GATO	Topología activa de Crosswork
CCA	Automatización del cambio de Crosswork
CDG	Gateway de datos de Crosswork
CHI	Crosswork Health Insight
CNC	Controlador de red Cisco Crosswork
COE	Motor de optimización de Crosswork
CPNR	Cisco Prime Network Registrar
CWM	Crosswork Workflow Manager
EMF	Funciones de administración de elementos
KPI	Indicador clave de rendimiento
LWR	Router inalámbrico grande
MDT	Telemetría basada en modelos
FREGAR	Método de procedimiento
NBW	Ancho de banda nominal
NSO	Network Services Orchestrator
RBW	Ancho de banda grabado
SR-PCE	Elemento de Cálculo de Ruta de Ruteo de Segmentos
SSM	Cisco Smart Software Manager

SWR	Router inalámbrico pequeño
TAC	Centro de asistencia técnica
TSDN	Transporte de redes definidas por software
ZTP	Aprovisionamiento sin intervención
RR	Reflector de ruta
RP	Perfil de ruta
POI	Punto De Interconexión
EVPN	Red privada virtual Ethernet.

Referencias

- Cisco Systems, Notas de la versión del controlador de red Cisco Crosswork, versión 7.1.0
- Guía de instalación de Cisco Systems, Cisco Crosswork Infrastructure 7.1
- Cisco Systems, Guía de administración de Cisco Crosswork Infrastructure 7.1 — Descripción general de los conceptos:
- Cisco Systems, Guía de Ingeniería y Optimización del Tráfico de Crosswork Network Controller, Versión 7.1
- Cisco Systems, Guía del usuario de Cisco Crosswork Health Insights, versión 7.1
- Guía de implementación de Cisco Systems, Crosswork Zero Touch Provisioning (ZTP)
- Cisco Systems, Guía de instalación del paquete Function Pack de Cisco NSO Transport SDN, versión 7.1.0
- Cisco Systems,Guía de configuración de Cisco SR-PCE

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).