Étude de cas Mise à niveau CNC

Table des matières

Introduction

Ce document décrit une étude de cas d'une migration complexe et à grande échelle d'un réseau sans fil fixe de Cisco CNC 4.1 vers la version 7.1 via la technologie « lift-and-shift ».

Résumé

Ce document présente une étude de cas détaillée de la migration d'un réseau fixe sans fil à grande échelle de Cisco Crosswork Network Controller (CNC) version 4.1 vers la version 7.1. En raison de l'absence d'un mécanisme de mise à niveau en place, la transition a nécessité un déploiement complet avec levage et décalage, introduisant une complexité architecturale, opérationnelle et d'intégration significative sur plus de 2 000 périphériques réseau et plusieurs systèmes interdépendants. L'étude examine les difficultés rencontrées dans de nombreux domaines.

Un résultat clé met en évidence le rôle essentiel de l'automatisation pour garantir l'évolutivité, la précision et le déterminisme opérationnel, en particulier pour les flux de travail à volume élevé. Les résultats montrent en outre que les environnements de production diffèrent considérablement des conditions de laboratoire contrôlées, ce qui nécessite un dépannage adaptatif, une validation itérative et un engagement soutenu avec les équipes d'ingénierie du TAC et de l'unité commerciale. Ces travaux fournissent des informations pratiques, des méthodologies validées et des meilleures pratiques recommandées qui servent de plan de référence pour les futures mises à niveau de la commande numérique et les transitions à grande échelle de la plate-forme d'orchestration.

Fond

La prolifération des réseaux 5G, l'adoption rapide des périphériques connectés et la numérisation des environnements des entreprises et des particuliers ont entraîné une augmentation significative du volume de trafic et de la diversité des services qui doivent être fournis de manière sécurisée et fiable à grande échelle. Les fournisseurs de services de communication (CSP) exploitent désormais des réseaux hautement dynamiques où les outils opérationnels traditionnels en silos créent souvent de la complexité, dégradent l'expérience utilisateur et augmentent les dépenses d'exploitation.

Pour rester compétitifs, les opérateurs adoptent de plus en plus des modèles opérationnels modernisés basés sur l'automatisation, la virtualisation, les principes SDN et les réseaux basés sur l'analytique et l'auto-optimisation.

Cisco Crosswork Network Controller (CNC) est conçu pour prendre en charge cette transformation en simplifiant les workflows opérationnels, en réduisant le coût total d'acquisition (TCO) et en permettant une automatisation basée sur les intentions sur les réseaux de transport multifournisseurs. CNC fournit une plate-forme unifiée pour le provisionnement des services, la surveillance de l'état du réseau et l'optimisation en temps réel, offrant aux opérateurs une interface unique pour gérer les réseaux IP à grande échelle de manière plus proactive et efficace.

L'infrastructure Crosswork sous-jacente fournit une structure de cluster résiliente et évolutive sur laquelle toutes les applications CNC s'exécutent. Pour CNC 7.1, cela inclut des modules tels que Optimization Engine, Active Topology, Change Automation, Health Insights, Element Management Functions (EMF), Service Health et Crosswork Workflow Manager (CWM), chacun contribuant à l'orchestration et à l'assurance de bout en bout.

La mise à niveau du CNC présente toutefois des défis uniques. CNC ne prend pas en charge les mises à niveau sur place, ce qui nécessite un déploiement complet avec changement d'opérateur, où le nouvel environnement est construit en parallèle avec l'environnement existant et où toutes les données et tous les services sont migrés vers la nouvelle version. Cette étude de cas examine une mise à niveau à grande échelle de CNC 4.1 à CNC 7.1 pour un agrégateur de services australien majeur prenant en charge la fourniture de services de réseau fédérateur pour tous les autres fournisseurs de services.

La migration a été particulièrement complexe en raison de plusieurs guides personnalisés d'automatisation des modifications, des indicateurs de performance clés personnalisés de Health Insight, des exigences de rapprochement des services VPN L2/L3 et de la nécessité d'un protocole ZTP sécurisé.

Le saut de version important a introduit une incertitude supplémentaire, étant donné les changements architecturaux et comportementaux internes qui ont rendu difficile la prédiction du comportement des cas d'utilisation existants dans la nouvelle version. Cela a nécessité une validation et une harmonisation complètes dans tous les cas d'utilisation.

Une planification importante a été mise en oeuvre pour déterminer l'allocation optimale des ressources, y compris le nombre de noeuds hybrides/travailleurs, la distribution CDG et le dimensionnement PCE, et pour déterminer si votre empreinte de ressources existante pouvait être conservée.

Le déploiement et la validation initiaux de CNC 7.1 ont été effectués dans un laboratoire CALO interne, offrant un environnement sécurisé pour expérimenter, affiner les configurations et renforcer la confiance. Ensuite, le déploiement dans l'environnement de test interne, qui reflète étroitement la production, a été effectué. La phase finale a consisté à déployer CNC 7.1 en production, à appliquer les modifications de configuration au niveau des périphériques et à effectuer une migration progressive de tous les périphériques et services associés vers le nouveau contrôleur.

Réseau De Production

Le réseau de production à l'air libre est réparti sur de grandes parties de l'Australie. Avec la présence de plus de 2 000 périphériques, allant de NCS à ASR9K, CNC a géré tous ces périphériques en fournissant une vue topologique en direct. Environ 2 000 périphériques étaient des NCS540 localement connus sous le nom de SWR (Small Wireless Router) exécutant IOS-XR 24.3.2 et 30 étaient des ASR-9K (Version 7.5.2) localement connus sous le nom de LWR (Large Wireless Router).

La configuration Crosswork comprenait 3 noeuds hybrides et 2 noeuds de travail. Il y avait un total de 5 CDG pour les périphériques, 4 étant actifs et 1 étant le noeud de secours. Cela offrait une protection limitée puisque le pool n'avait qu'un seul CDG en veille. Mais compte tenu de vos exigences, cela a été donné le feu vert. Le fait que toutes les machines virtuelles se trouvent sur un seul data center a également facilité la décision de passer à une seule machine en veille.

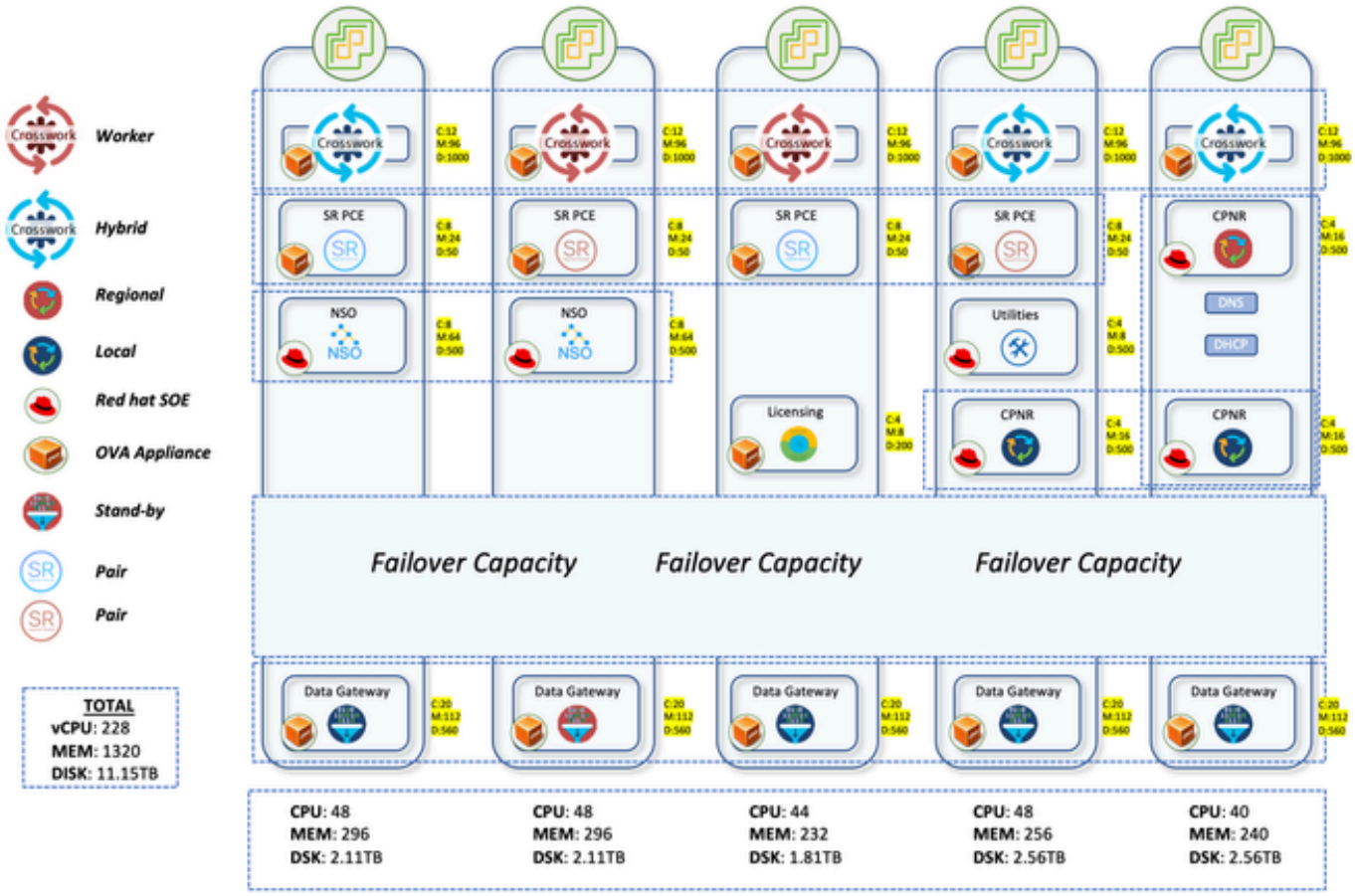
Le CDG est le composant qui gère la collecte de données à partir des périphériques via divers protocoles tels que SNMP, CLI et GNMI. Les données recueillies par CDG sont exposées à Crosswork par le biais de la kafka interne. Un périphérique intégré à Crosswork doit être connecté à un CDG, ce qui permet à la passerelle de données de se connecter au périphérique et d'obtenir les données du périphérique.

La distribution des appareils pour les CDG a également fait l'objet de beaucoup de réflexion. Le déploiement précédent avait distribué au hasard les appareils parmi les CDG. Cela a donné lieu à une distribution très asymétrique avec certains CDG transportant plus d'appareils alors qu'il y avait 1-2 CDG avec beaucoup moins d'appareils. Cela a conduit à une surconsommation et à une surcharge de certains CDG, tandis que d'autres étaient sous-approvisionnés.

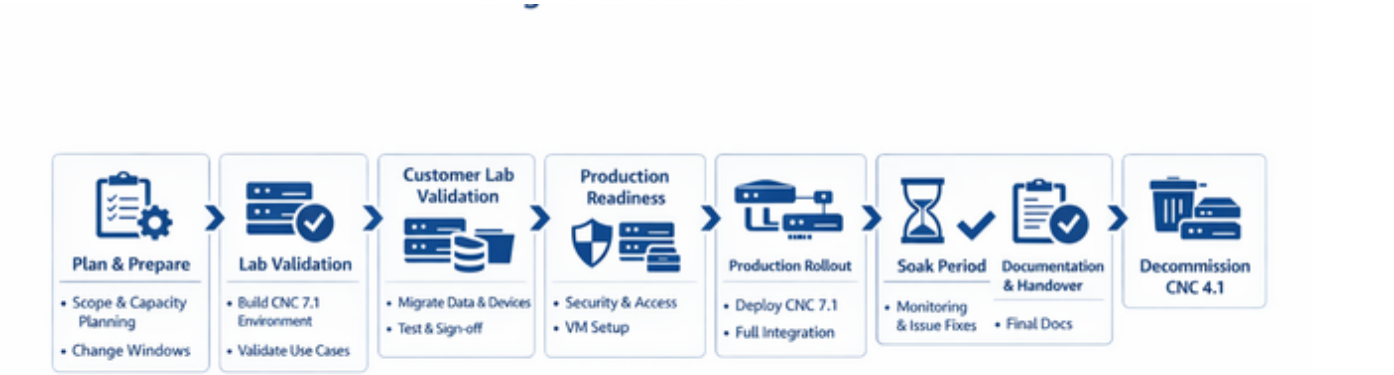
Le processus de réflexion ici dans la mise à niveau a consisté à distribuer 700 SWR chacun aux 4 CDG actifs. Cela représente 2 100 DTS qui ont été accueillis dans les trois premiers CDG. Les LWR très lourds sur le front de l'interface étaient tous réservés au quatrième CDG. Bien qu'il s'agisse d'un très petit nombre, avec un nombre de 30, cette attribution a permis de s'assurer que même si plus de collectes étaient effectuées à partir de ces appareils, il n'y aurait pas de charge lourde sur le CDG. Toute intégration ultérieure des câbles en acier irait également au 4^{e} CDG. Cela a assuré une distribution uniforme dans les trois premiers CDG avec plus d'espace disponible dans le 4^{e} pour accueillir de nouveaux appareils.

SR-PCE a été déployé en 2 paires, ce qui signifie 4 machines virtuelles distribuées sur différents ordinateurs hôtes. Une paire gère 7 sites POI et l'autre les 8 autres sites POI. Les mises à jour de topologie sur l'interface graphique utilisateur CNC sont effectuées à l'aide de SR-PCE. Il apprend la topologie du réseau par l'appairage BGP-LS avec d'autres routeurs LWR. Ce composant est également utilisé pour tous les cas d'utilisation d'ingénierie de trafic où il joue le rôle du contrôleur pour diriger le trafic vers différents chemins.

Pour gérer tous les cas d'utilisation de configuration de périphérique et de mise en service de services, NSO doit être utilisé en association avec le CNC. Pour le réseau de production, deux NSO avec la version 6.4.1.1 ont été déployés pour fonctionner en tandem en mode haute disponibilité. SR-PCE (Segment Routing Path Computation Element) est le composant requis pour fournir les mises à jour topologiques à CNC et pour gérer les cas d'utilisation d'ingénierie de trafic en temps réel. Quatre SR-PCE avec la version 25.2.1 ont été déployés ici, chaque PCE étant appairé à deux LWR différents.



Workflow de migration de CNC 4.1 vers CNC 7.1



Pour le déploiement CNC, le choix préféré était d'aller de l'avant avec le docker basé. Mais comme le client n'a pas approuvé la configuration de docker dans ses locaux, il n'y avait pas d'autre option que de procéder à un déploiement manuel à l'aide de vCenter. Cela prend plus de temps à déployer que le déploiement basé sur un script, car cela nous oblige à fournir des entrées plusieurs fois dans l'interface graphique utilisateur de vCenter.

Une fois le déploiement CNC terminé, toutes les applications requises ont été déployées avec le fichier d'installation d'action automatique fourni par l'unité commerciale, qui télécharge et active les applications en une seule fois, réduisant ainsi le temps nécessaire pour le faire manuellement. Le premier niveau a été déployé, qui inclut le moteur d'optimisation du travail croisé, la topologie active, l'intégrité du service, les fonctions de gestion des éléments et le gestionnaire de flux de travail croisé. En plus de cela, les packages complémentaires ont également été configurés qui incluent Change Automation et Health Insight.

CWM et SH n'avaient aucun cas d'utilisation. Mais ils ont néanmoins été déployés car ils étaient intéressés par certains des cas d'utilisation offerts par ces applications dans la version suivante.

Une fois les applications configurées, l'étape suivante consistait à migrer les données de l'ancienne version de CNC. Il s'agit principalement des profils d'informations d'identification, des fournisseurs, des balises, des guides personnalisés, des indicateurs de performance clés personnalisés, des rôles, des bons sZTP et de toute autre donnée. CNC fournit l'option d'exportation pour tous ces éléments qui peuvent être exploités puis importés dans le nouveau CNC.

Une fois ces paramètres configurés, il est prudent de commencer la migration du périphérique. En cas de mises à niveau, si le nouveau CNC est déployé dans un nouveau sous-réseau par rapport à l'ancien, il est nécessaire d'effectuer des modifications de liste de contrôle d'accès sur les périphériques pour assurer l'accessibilité avec le nouveau CNC. Ce processus est long, car il nécessite une connexion manuelle à chaque périphérique et une modification de la configuration.

Une fois ces modifications apportées à la liste de contrôle d’accès, l’étape suivante consiste à importer les périphériques dans le nouveau CNC et à les connecter aux CDG. Si l'accessibilité est correcte et que les informations d'identification SSH et SNMP sont correctes, les périphériques s'affichent comme accessibles sur CNC et sont également intégrés au NSO (Network Services Orchestrator).

Sur le plan des ONS, tous les ensembles requis doivent être en place et opérationnels pour que le CNC puisse communiquer avec les ONS et vice versa. Par exemple, pour intégrer automatiquement les périphériques à NSO depuis CNC, le pack de fonctions DLM est obligatoire. De même, si le NSO doit configurer des chemins de capteur MDT sur l'appareil, le package TM-TC doit être déployé sur le NSO. L'essentiel est que, selon le cas d'utilisation, le package approprié doit être déployé sur NSO.

Au lieu d'adopter l'approche manuelle pour déployer ces packages requis, en particulier les packages Transport-SDN, un script automatisé a été développé pour le provisionnement. Avec la mise à niveau de CNC 7.1, des mises à jour ont été introduites dans les packages TSDN. Ces packages mis à jour sont destinés à être déployés sur le serveur NSO afin d'assurer la prise en charge continue du provisionnement L2/L3 dans l'environnement mis à niveau. Le script automatise l'installation des packages TSDN mis à jour et charge les métadonnées nécessaires dans NSO, ce qui lui permet de fournir les services requis.

Une instance du serveur de licences Cisco Smart Software Manager (SSM) et 3 instances de Cisco Prime Network Registrar (CPNR) peuvent également être déployées sur différents hôtes.

Architecture CNC et intégration avec d'autres composants

CNC fournit une plate-forme unique pour le provisionnement, l'optimisation et la visualisation des services déployés via une interface utilisateur unifiée. Voici un bref résumé des composants internes CNC qui résident dans la suite de plates-formes CNC et les exemples d'utilisation.

- Topologie active croisée (CAT) :
    - Application de composant interne distribuée sur les noeuds de machine virtuelle CNC
    - Fournit une visibilité de bout en bout en temps réel de l'inventaire rapproché
    - Intègre les informations d'inventaire provenant de plusieurs sources de données dans un seul affichage
    - Calcul du chemin du réseau de transport
    - Découverte de topologie

- Moteur d'optimisation du travail croisé (COE) :
    - Application de composant interne distribuée sur les noeuds de machine virtuelle CNC
    - Optimisation du réseau en temps réel
    - Visualisation de la topologie en temps réel
    - Visualisations et provisionnement SR-TE
    - Visualisation et mise en service RSVP-TE
    - Bande passante à la demande
- Crosswork health insight (CHI) :
    - Application de composant interne distribuée sur les noeuds de machine virtuelle CNC
    - Surveillance KPI
    - Tableau de bord des alertes
- L'automatisation des modifications transversales (CCA)
    - Application de composant interne distribuée sur les noeuds de machine virtuelle CNC
    - Outil Dev-ops avec guides de lecture prêts à l'emploi
    - Possibilité de programmer des lectures à l'heure souhaitée
    - Les indicateurs de performance clés HI signalent les piquages aux jeux suggérés en guise de correction

Diagramme D'Architecture

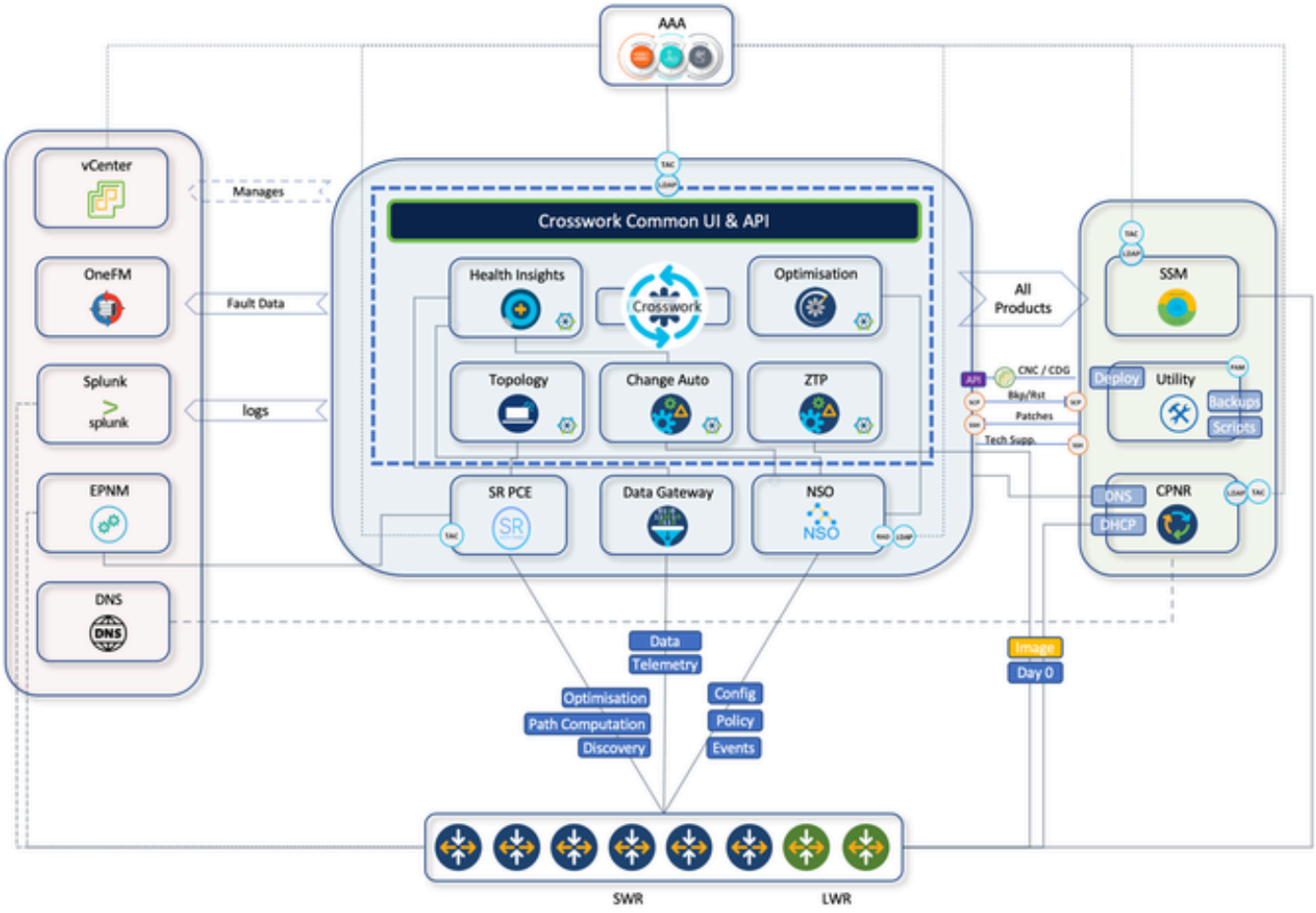
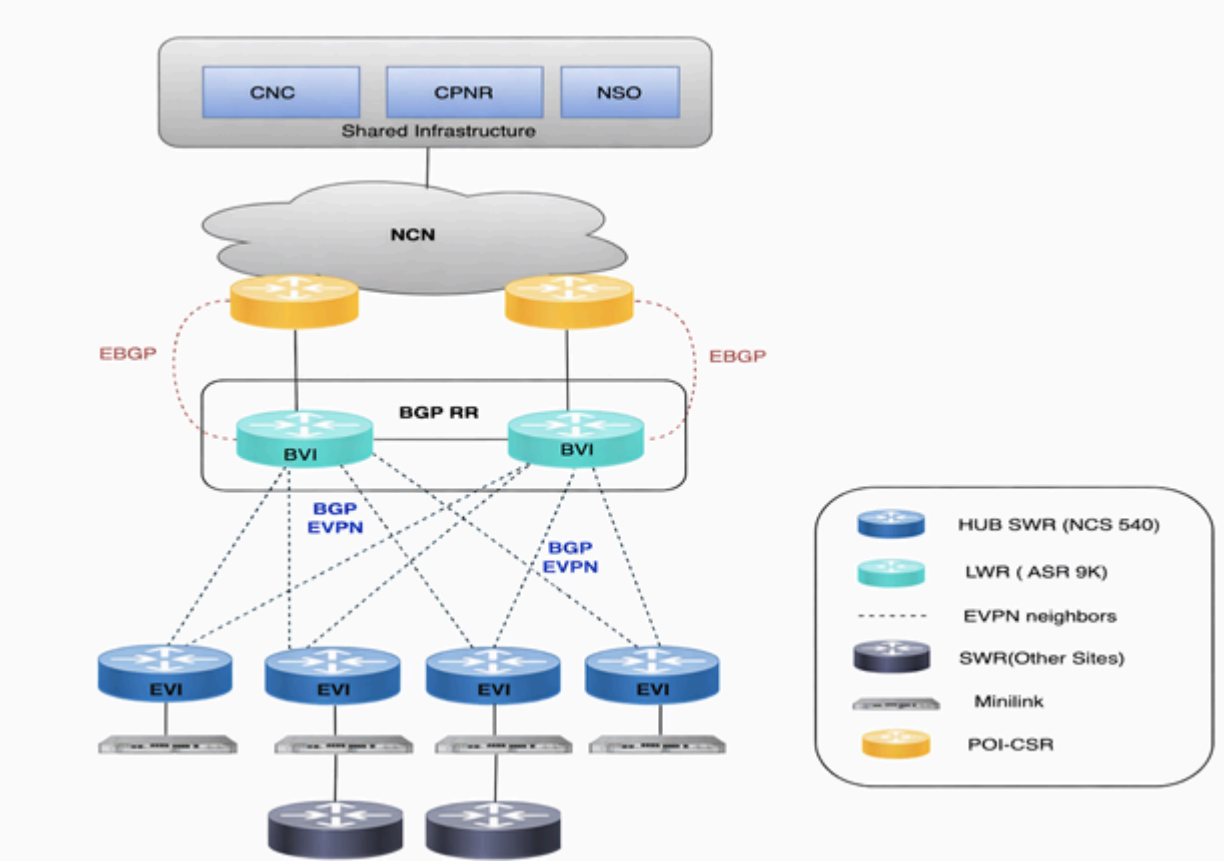


Diagramme du réseau



CNC 4.1 → 7.1 Workflow de migration détaillé

Migration progressive de bout en bout de l'ancienne version 4.1 de CNC vers la version 7.1 de CNC (le même flux peut être suivi pour n'importe quelle mise à niveau de CNC, quelle que soit la version)

Planifier	›	Travaux pratiques	›	Laboratoire client	›	Prêt pour Prod	›	Déploiement de production	›	Période D'Imbibition	›	Transfert	›	Désaffectation

PHASE 1

1 Planification et préparation

PORTÉE ET PLANIFICATION	PLANIFICATION
· Définition du champ	· Modifier l'identification de fenêtre
· Planification des capacités	· Alignement des intervenants

▼

PHASE 2

2 Validation interne des travaux pratiques

INFRASTRUCTURE · Construire CNC 7.1 (hybride/travailleurs) · Installer des applications · Déploiement de NSO avec HA · Déploiement de paires SR-PCE	VALIDATION · Valider tous les cas d'utilisation · Approbation fonctionnelle

▼

PHASE 3

3 Validation de TP client

CONSTRUCTION D'INFRASTRUCTURES · Construire CNC 7.1 (hybride/travailleurs) · Installer des applications · Déploiement de NSO avec HA · Déploiement de paires SR-PCE	MIGRATION DES DONNÉES · Exporter des artefacts CNC 4.1 · Recréer des groupes de périphériques · Importation dans CNC 7.1 · Déploiement des packages NSO	ACCESSIBILITÉ DES PÉRIPHÉRIQUES · Mises à jour ACL · Importation de périphériques et fixation CDG	SERVICES ET OBSERVABILITÉ · Rapprochement et synchronisation des services · Tâches de développement et de collecte des ICP · Activation du script du guide BNM · Observabilité HI/Grafana · Intégration Radius · Intégration de Splunk · Intégration OneFM

			· Activer les sauvegardes CNC

✓ Exécution du programme ATP en laboratoire et obtention de l'approbation

▾

PHASE 4

4 Préparation de la production

SÉCURITÉ ET ACCÈS · Examen de la sécurité · Configuration des contrôles d'accès	INFRASTRUCTURE · Dimensionnement et configuration des machines virtuelles de production · Validation du réseau

▾

PHASE 5

5 Basculement de la production

↻ Répète toutes les étapes de la Phase 3 — dans l'environnement de production

CONSTRUCTION D'INFRASTRUCTURES · Construire CNC 7.1 (hybride/travailleurs) · Installer des applications · Déploiement de NSO avec HA · Déploiement de paires SR-PCE	MIGRATION DES DONNÉES · Exporter des artefacts CNC 4.1 (fournisseurs, profils de justificatifs, guides, étiquettes) · Recréer des groupes de périphériques · Importation dans CNC 7.1	ACCESSIBILITÉ DES PÉRIPHÉRIQUES · Mises à jour ACL · Importation de périphériques et fixation CDG	SERVICES ET OBSERVABILITÉ · Rapprochement et synchronisation des services · Tâches de développement et de collecte des ICP · Activation du guide BNM · HI/Grafana, Splunk, OneFM · Activer les

	· Déploiement des packages NSO		sauvegardes CNC

✓ Déploiement de la production

▼

PHASE 6

6 Période De Trempage

SURVEILLANCE	GESTION DES PROBLÈMES
· Surveillance de la stabilité	· Suivi et résolution des problèmes
· Base de performance	· Processus de remontée

▼

PHASE 7

7 Documentation et transfert

DOCUMENTATION	TRANSFERT
· MOP, documents de conception et documents opérationnels	· Séances de transfert des connaissances
· Diagrammes d'architecture	· Validation du transfert

▼

PHASE 8

8 Déclassement CNC hérité 4.1

CLEANUP	ARCHIVER
· Détacher tous les périphériques de CDG	· Archiver toutes les exportations CNC 4.1

· Supprimer les entrées MDT pointant vers 4.1 MV CDG · Supprimer les machines virtuelles de production	· Vérification finale et approbation	

Scénarios :

Approvisionnement de services L2VPN (basé sur EVPN)

Le service L2VPN fournit une connectivité Ethernet de couche 2 sur plusieurs SWR, certains services étant ancrés sur des LWR. La topologie active CNC est utilisée pour le provisionnement des services, tandis que toute la logique propre à l'environnement est mise en oeuvre via des modèles personnalisés NSO.

La mise en service L2VPN est traitée comme une activité de configuration du jour 2 et nécessite des attributs de service fournis par l'opérateur.

Modèles NSO personnalisés

Plusieurs modèles personnalisés ont été créés pour s'aligner sur les conventions d'attribution de noms et les comportements d'interface spécifiques à l'environnement :

- CT-l2vpn-swr-hub-and-lwr
  Gère les différences d'attribution de noms côté concentrateur f-ou bridge -group et bridge -domain sur les concentrateurs SWR et les LWR.
- CT-l2vpn-swr-nonhub-100 / 101 / 102 / 105
  Supprime l'interface de liaison ascendante ZTP du groupe de pontage EVPN par défaut et du domaine de pontage pour chaque EVI spécifique au VLAN.

Ces modèles garantissent une configuration EVPN cohérente sur l'ensemble du réseau et éliminent les différences de niveau matériel.

Approvisionnement de services L3VPN (basé sur VRF)

L'exemple d'utilisation L3VPN permet la fourniture de services de couche 3 sur plusieurs SWR en tant que point d'extrémité. Le provisionnement est effectué via la topologie active CNC, avec des exigences spécifiques à l'environnement implémentées à l'aide d'un modèle NSO personnalisé.

Comme avec L2VPN, il s'agit d'une action de configuration du jour 2, nécessitant des entrées d'opérateur.

Modèle NSO personnalisé

- CT-l3vpn-swr
  Collecte les paramètres spécifiques au VRF (numéro de système autonome, nom du VRF, ensemble de préfixes, nom de la stratégie de routage, différenciateur de routage) et crée la stratégie d'importation/exportation BGP nécessaire, y compris la redistribution des routes connectées avec une stratégie de routage définie par l'utilisateur.

Ingénierie Du Trafic

L'application Crosswork Optimization Engine (COE) de la suite CNC permet de contrôler les flux de trafic dans le réseau en fonction de l'intention souhaitée.

Il existe deux types de trafic qui nécessitent des intentions différentes (métriques SLA) :

- Trafic TC1 - SLA sensible à la latence pour garantir que le trafic se trouve sur le chemin de latence le plus faible.
- Trafic TC4 - SLA de bande passante minimale pour garantir que la bande passante dédiée est toujours disponible pour le trafic TC4

Trafic TC1 (latence la plus faible)

Pour s'assurer que le trafic TC1 est toujours acheminé sur le chemin à latence la plus faible, une politique de routage de segment (SR) doit être créée sur le routeur SWR de tête de réseau avec des critères de calcul de chemin comme latence.

Pour ce faire, il suffit de définir la configuration ODN (On Demand Next Hop) sur chaque SWR de tête de réseau pour une couleur spécifique 1001 en utilisant CNC pour faciliter la création de politiques SR.

Trafic TC4 (bande passante allouée)

Pour s'assurer que le trafic TC4 est toujours pris sur le chemin avec une bande passante dédiée, il faut avoir une politique SR créée sur le routeur SWR de tête de réseau avec des critères de calcul de chemin comme bande passante.

Pour ce faire, il faut :

- Pack de fonctions Bande passante à la demande (BoD) sur CNC
- Définition de la configuration ODN (On Demand Next Hop) sur chaque SWR de tête de réseau pour une couleur spécifique 1004 à l'aide de la création de politiques CNC SR avec ces configurations

Le pack de fonctions BoD est utilisé pour calculer le chemin pour les stratégies SR qui ont la bande passante comme critère pour le calcul du chemin. Il assure le suivi de la bande passante allouée à une politique et surveille le chemin actuel de la politique pendant son cycle de vie.

À tout moment, si le correctif actuel de la politique BWOD ne dispose pas d'une capacité suffisante pour répondre à la bande passante allouée, il recalcule le chemin de la politique BWOD et réachemine la politique vers un nouveau chemin. Ce réacheminement de la politique BWOD est un processus continu qui ne nécessite aucune intervention manuelle.

D'une certaine manière, le BWOD optimise la bande passante à la volée comme le SR-PCE le fait pour la latence.

Mise en service du périphérique avec sZTP

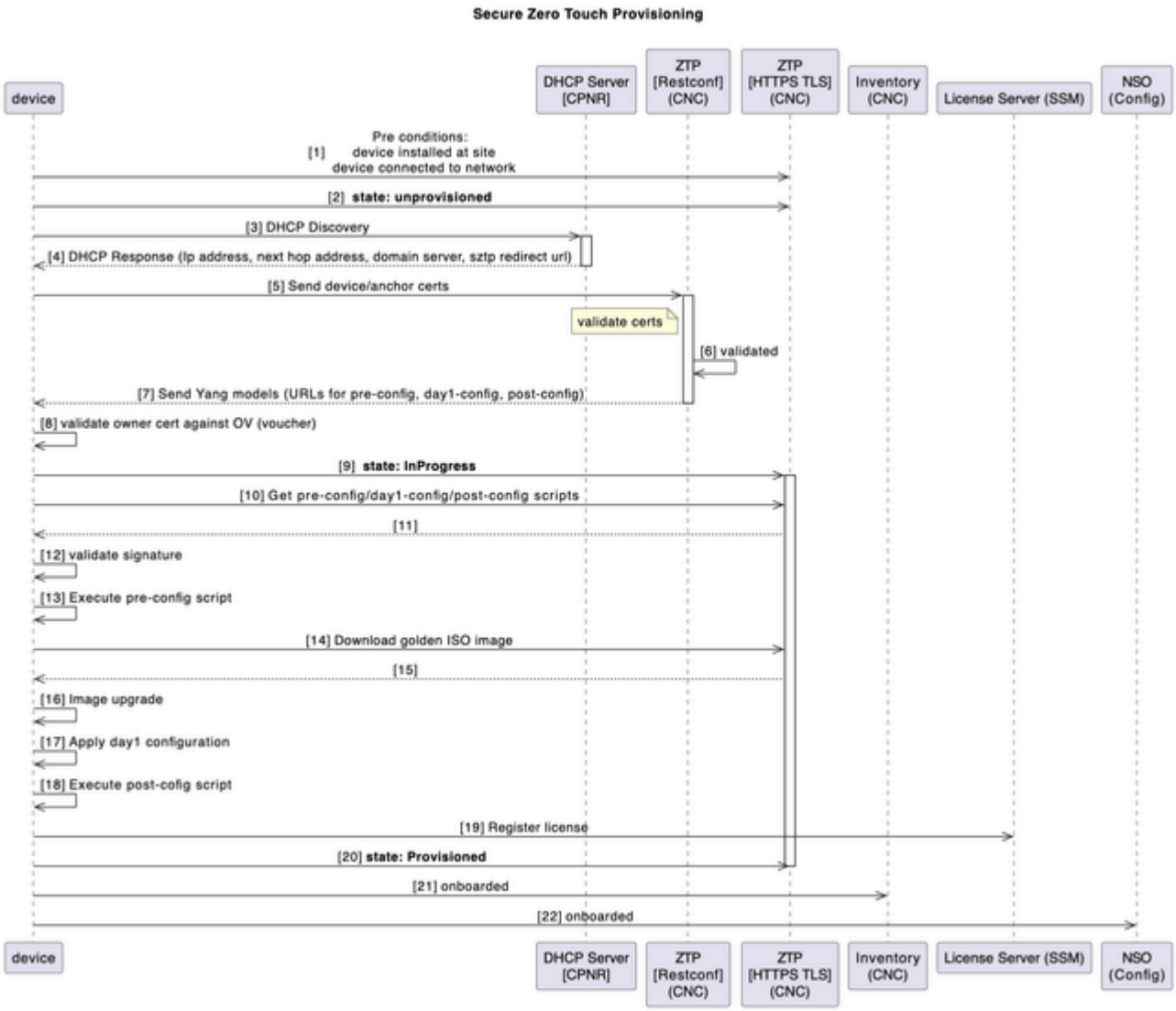
Dans le modèle traditionnel d'installation et de support, le processus d'installation d'un nouveau périphérique nécessitait un certain niveau d'expertise de la part de l'installateur afin d'installer, de configurer et de dépanner l'implémentation d'un nouveau composant. Il peut également y avoir un long processus de préparation de l'équipement à un emplacement hors site, pris en charge par de nombreuses personnes travaillant sur différentes parties de la solution.

Pour les nouveaux périphériques SWR devant être déployés dans votre environnement, ce processus de mise en service des périphériques est automatisé avec l'application ZTP (Zero Touch Provisioning) sécurisée de CNC.

Le workflow ZTP est déclenché lors du premier démarrage du périphérique et télécharge l'image de la plate-forme planifiée et la configuration initiale qui doivent être appliquées sans aucune intervention manuelle.

Le périphérique est également intégré automatiquement sur CNC pour une orchestration plus poussée.

Ce schéma montre le workflow du processus ZTP sécurisé lors de la mise en route du périphérique :



Orchestration post-ZTP (pilotée par l'automatisation)

Une automatisation Python sur l'hôte utilitaire orchestre et audite le processus de bout en bout à l'aide d'une entrée Excel structurée (par chaîne) :

- Génère et télécharge les artefacts de jour 1 et de post-configuration sur CNC.
- Crée des réservations CPNR (entrées DHCP liées au routeur série SWR).
- Ajoute un périphérique dans EPNM (pour la visibilité/l'assurance).
- Maintenance post-ZTP dans CNC :
    - Attribue des SWR aux CDG (destination télémétrique)
    - Se rattache aux groupes et balises de périphériques
    - Met à jour la latitude/longitude pour la visualisation topologique
    - Attache un profil KPI BNM pour activer la transmission en continu de télémétrie

Traitement des messages de notification de bande passante (BNM) dans CNC

Le routeur SWR peut recevoir le BNM du commutateur MiniLink colocalisé qui correspond à la bande passante des ports WAN. Ces messages de notification sont des messages CFM standard qui incluent la bande passante enregistrée courante (RBW) et la bande passante configurée maximale, également appelée bande passante nominale (NBW).

La bande passante actuelle correspond à la bande passante réelle de la liaison WAN hyperfréquence, sur la base des bandes passantes agrégées des liaisons hyperfréquence individuelles et de leurs niveaux de gestion de la qualité de l'air en cours d'exécution. La bande passante nominale est la bande passante WAN maximale possible configurée, sur la base des bandes passantes agrégées de la QAM maximale configurée sur chacune des liaisons micro-ondes individuelles.

L'optimisation de la bande passante est entreprise selon le scénario suivant :

Changement temporaire (événements éphémères)

- Lorsqu'il y a une dégradation ou une panne passagère dans le réseau/la liaison qui est localisée au SWR (par exemple, en raison d'un événement météorologique défavorable qui provoque l'évanouissement du chemin radio micro-ondes et la réduction de la bande passante disponible en raison de changements dans les schémas de modulation), alors la correction de la mise en forme du trafic se produit au SWR local sur l'interface réseau affectée.
- Cela garantit une perte de paquets minimale sur le chemin de transmission affecté.

Lorsqu'un SWR est activé avec l'indicateur de performance clé BNM dans CNC dans le cadre des activités post-sZTP, CNC transfère les configurations de télémétrie dans SWR.

BNM MDT

piloté par modèle de télémétrie

destination-group <NomDGN>

vrf VRF-OMSWR-<AreaCode>1

address-family ipv4 <CDG IPv4Address> port 9010

encoding self-descripting-gpb

protocole tcp

!

!

sensor-group <NomGroupe>

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

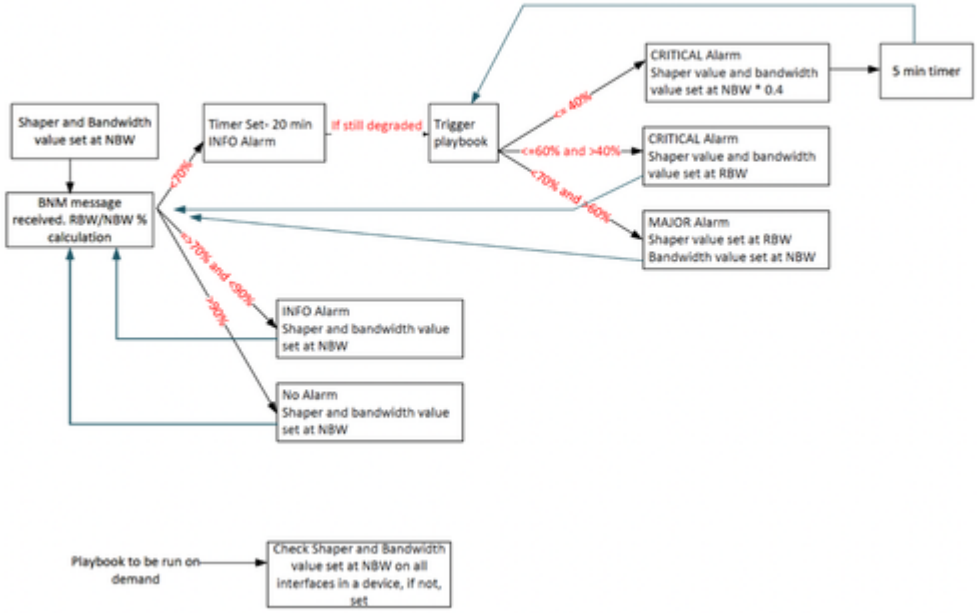
!

CNC traite ces messages BNM reçus par télémétrie et prend des mesures correctives si nécessaire. Voici les 2 composants impliqués dans la commande numérique :

- Health insight (HI) : l'application CNC est utilisée pour ingérer la notification BNM par un KPI personnalisé qui surveille le chemin de capteur spécifique pour les messages BNM. Health Insight est capable de déclencher des alertes au cas où des changements de bande passante seraient importants et nécessiteraient une action.
- L'automatisation des modifications (CA) : l'application CNC est utilisée pour traiter les messages BNM en continu qui ont généré des alertes HI. 2 guides personnalisés sont déployés pour apporter ces modifications à l'interface concernée :
    - Définition du formateur QoS sur le nouveau RBW
    - Définition de la capacité d'interface sur une nouvelle valeur RBW.

Un script Python personnalisé est développé pour exécuter une logique personnalisée et exécuter les guides de CA automatiquement lorsque les indicateurs de performance clés (KPI) HI sont dépassés.

Le script de déclenchement du guide de lecture fonctionne sur la base de cet algorithme :



Ce tableau explique les niveaux d'alerte personnalisés qui ont été définis sur les degrés de dégradation de la bande passante :

Bande passante signalée = RBW

Bande passante nominale = NBW

Valeur des intervalles d'alerte	Niveau de notification
(RBW/NBW)*100 >=70	Informations
(RBW/NBW)*100 <70 et >60	Avertissement
(RBW/NBW)*100 <=60	Critical (critique)

Ce chemin de capteur est surveillé par CNC :

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

Un indicateur de performance clé personnalisé est créé dans CNC pour surveiller le chemin du capteur BNM. Cet indicateur de performance clé est ajouté à un profil d'indicateur de performance clé configuré avec une cadence de 120 secondes et des seuils d'alerte. L'association de routeurs

sans fil à ce profil envoie automatiquement la configuration de télémétrie requise aux périphériques via NSO.

Une fois activés, les périphériques diffusent les données RBW/NBW aux CDG affectés à l'intervalle configuré. Health Insight (HI) calcule le ratio RBW÷NBW et déclenche des alertes lorsque les seuils sont dépassés. Les opérateurs peuvent suivre ces événements dans HI et via les tableaux de bord Grafana.

Un fournisseur d'alertes dans CNC transfère ces alertes au noeud hybride hébergeant l'automatisation Python. Le script analyse les détails du périphérique/interface/RBW/NBW et déclenche les guides Change Automation appropriés : réglage du shaper, mise à jour de la bande passante ou les deux en fonction de la logique de décision définie.

Voici les 2 guides utilisés dans le workflow :

1. Guide pour modifier la valeur du modélisateur

2. Guide pour modifier la bande passante de l’interface

Comme déjà mentionné, le script fait tourner un serveur Web pour agir en tant que fournisseur pour communiquer avec CNC à l'aide de l'API REST. Toute réponse que nous recevons pour une requête POST est capturée ici. Les alertes sont capturées dans le formulaire sur JSON, puis converties en dictionnaire pour extraire les paramètres nécessaires.

Standardiser les opérations réseau du 2e jour grâce à des guides d'automatisation personnalisés

Des guides personnalisés d'automatisation des modifications (CA) ont été développés pour rationaliser et standardiser les opérations critiques du deuxième jour tout au long du cycle de vie du réseau. Il s'agit notamment de la mise en service de bundle Ether, des mises à jour de la description de l'interface de gestion, de l'orchestration en chaîne de CFM, de l'extension transparente de la capacité de liaison, de la désactivation d'eNodeB et de l'intégration Mini-Link efficace. En intégrant les meilleures pratiques opérationnelles dans des workflows réutilisables, ces guides améliorent considérablement la cohérence de l'exécution, minimisent le risque d'erreur humaine et réduisent la dépendance aux interventions manuelles. Dans le cadre d'une mise à niveau Cisco CNC, cette structure d'automatisation joue un rôle essentiel dans l'accélération du redressement opérationnel, la garantie de la continuité des services et la mise en place de processus évolutifs et reproductibles, en adéquation avec les objectifs de transformation du réseau moderne.

Continuité de l'intégration TACACS+ dans la mise à niveau Cisco CNC 7.1

Dans le cadre de la mise à niveau de Cisco CNC 4.1 à 7.1, l'intégration TACACS+ existante a été soigneusement préservée afin d'assurer la continuité de l'authentification et de l'autorisation centralisées. Le processus de mise à niveau a validé et répliqué la configuration TACACS+ dans Cisco CNC 7.1, en maintenant l'alignement avec les politiques de sécurité d'entreprise établies et les mécanismes de contrôle d'accès basé sur les rôles (RBAC).

Transfert de Syslog CNC et CDG vers Splunk

Un transfert syslog est configuré pour transférer les alarmes/événements/syslogs à un serveur Splunk. La fonctionnalité prête à l'emploi de CNC pour configurer le serveur Syslog a été utilisée pour atteindre cet objectif.

Transfert d'alarmes vers OneFM

Les alarmes CNC sont également transmises à un système ascendant comme OneFM en utilisant l'API orientée connexion restconf CNC :

```
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.
```

Automatisation des sauvegardes CNC quotidiennes

Un script automatisé utilise l'API de sauvegarde CNC pour effectuer la sauvegarde complète de CNC et stocke le fichier de sauvegarde dans l'hôte de l'utilitaire. Cette opération est effectuée quotidiennement.

Défis

Big Jump dans la version Crosswork

La mise à niveau de Cross work 4.4 vers 7.1 représentait un saut de version significatif plutôt

qu'une mise à jour incrémentielle de routine. Un tel saut a introduit de nombreuses nouvelles fonctionnalités dans plusieurs applications, ainsi que des améliorations et des modifications architecturales substantielles. Pour cette raison, la mise à niveau CNC n'était pas seulement un simple remplacement de version, elle nécessitait une validation complète pour garantir la compatibilité, la stabilité et la fonctionnalité appropriée de tous les composants intégrés. L'ensemble de fonctionnalités étendu et les améliorations sous-jacentes impliquaient que les workflows, les configurations et les intégrations existants nécessitaient une vérification minutieuse, ce qui rendait les tests et la validation complets essentiels à la réussite de la mise à niveau.

Mise à niveau sans mise en place

CNC ne prend pas en charge un modèle de mise à niveau sur place. Au lieu de cela, les mises à niveau doivent suivre une approche « ascenseur and shift », dans laquelle le déploiement existant est préservé tandis qu'un environnement entièrement nouveau est construit à partir de zéro avec la version cible. Une fois le nouveau système installé, les configurations, les données et les intégrations doivent être soigneusement migrées et validées avant de pouvoir mettre hors service l'ancien environnement.

Cette approche présente plusieurs défis opérationnels :

- Environnements parallèles : Les anciens et les nouveaux environnements CNC doivent s'exécuter simultanément jusqu'à ce que la migration et la validation soient entièrement terminées.
- Pression sur les ressources matérielles : L'exécution de deux environnements complets en parallèle augmente considérablement la demande en ressources de calcul, de stockage et de réseau, ce qui peut surcharger l'infrastructure disponible.
- Effort de validation étendu : Toutes les données, configurations, stratégies et intégrations migrées doivent être vérifiées dans la nouvelle version pour garantir leur fonctionnement correct.
- La migration des données est complexe : Le transfert des données historiques, des configurations d'application et des paramètres opérationnels nécessite une planification minutieuse pour éviter les incohérences ou les pertes de données.
- Désaffectation différée : L'ancien système et ses machines virtuelles ne peuvent pas être supprimés tant que la stabilité du nouveau déploiement n'est pas prouvée, ce qui prolonge l'utilisation des ressources et la surcharge opérationnelle.
- Coordination opérationnelle : Les équipes doivent gérer la synchronisation entre les deux environnements au cours de la période de transition afin d'éviter les dérives de configuration ou les interruptions opérationnelles.
- Conflits d'automatisation en boucle fermée : CNC prend en charge les cas d'utilisation d'automatisation en boucle fermée qui déclenchent dynamiquement des actions en fonction des conditions du réseau en temps réel. Lorsque l'ancien et le nouveau contrôleurs sont actifs pendant la transition, la même logique d'automatisation risque de s'exécuter à partir des deux contrôleurs, ce qui peut entraîner des modifications de configuration en double ou des actions conflictuelles sur le réseau. Cela nécessite un contrôle attentif des politiques

d'automatisation pendant la fenêtre de migration.
- Les données opérationnelles existantes, notamment les alarmes historiques, les événements, les enregistrements d'erreurs et les informations d'audit, ne sont pas migrées vers le nouvel environnement en raison de l'absence de fonctionnalités d'exportation natives. Par conséquent, ces données historiques ne sont pas disponibles dans le système mis à niveau et doivent être traitées comme non récupérables après la migration.

En raison de ces facteurs, le modèle de portance et de décalage rend les mises à niveau CNC plus gourmandes en ressources et plus complexes sur le plan opérationnel qu'une mise à niveau standard sur place.

Les pièges du déploiement sans options de restauration

Certaines erreurs de configuration de déploiement et de post-déploiement dans CNC n'ont pas de chemin de correction et nécessitent un démontage et un redéploiement complets du cluster. Par exemple, un nom de domaine complet incorrect configuré pour le VIP de données croisées , obligatoire pour l'exemple d'utilisation sZTP, a rendu sZTP non fonctionnel. Cette valeur ne pouvant pas être corrigée après le déploiement, un redéploiement complet a été nécessaire.

De même, une configuration incorrecte des informations d'identification de remplacement de périphérique dans l'automatisation des modifications n'a pas pu être corrigée après le déploiement, ce qui a conduit à une nouvelle reconstruction du cluster. D'autres erreurs, telles que des IP de passerelle mal configurées ou des définitions de sous-réseau, sont également identifiées comme non récupérables.

Ces scénarios mettent en évidence l'importance critique de la validation de tous les paramètres immuables lors du déploiement initial. Une planification méticuleuse et une vérification des données sont essentielles pour éviter les retouches coûteuses et l'impact sur le calendrier.

Contraintes de la validation du diagnostic post-déploiement

CNC fournit un utilitaire de diagnostic pour évaluer les paramètres d'intégrité au niveau de la machine virtuelle, tels que la latence de lecture/écriture du disque, les E/S par seconde, la latence de synchronisation, la vitesse de l'interface réseau et la fréquence d'horloge du processeur. L'utilitaire consigne les valeurs mesurées par rapport aux seuils prévus et marque chaque vérification comme réussie ou échouée. Cependant, ces diagnostics ne peuvent être exécutés qu'après le déploiement du cluster, ce qui ne laisse aucun mécanisme pour valider la préparation de l'infrastructure avant le déploiement.

Lors de l'installation, l'indicateur « Ignorer les vérifications de diagnostic » est défini par défaut sur false. En pratique, si une seule vérification échoue, le programme d'installation s'arrête, empêchant ainsi le déploiement de se poursuivre. Par conséquent, les ingénieurs sur site sont souvent obligés d'activer cet indicateur et de contourner entièrement les diagnostics, car même les environnements de production échouent fréquemment à un ou plusieurs contrôles. Cela crée un dilemme opérationnel : les équipes doivent choisir entre appliquer une validation stricte qui bloque le déploiement ou poursuivre sans avoir l'assurance que l'infrastructure sous-jacente répond aux critères de performance recommandés.

Modification de la procédure de création d'indicateurs personnalisés HI

Dans Health Insight 4.1, la création d'indicateurs de performance clés personnalisés reposait sur la logique de script Tick, dans laquelle les définitions d'indicateurs de performance clés et la logique de traitement étaient implémentées à l'aide de scripts dans le cadre Tick. Cependant, dans la version 7.1, cette approche a été remplacée par un cadre basé sur des fichiers de suivi pour définir et gérer les indicateurs de performance clés.

En raison de cette modification architecturale, les indicateurs de performance clés personnalisés existants n'ont pas pu être réutilisés directement et ont dû être retravaillés pour s'aligner sur le nouveau format de fichier de suivi. Cela a nécessité beaucoup de temps et d'efforts pour :

- Comprendre le nouveau cadre : L'équipe a dû étudier la structure, la syntaxe et le comportement opérationnel du modèle de définition d'indicateur de performance clé basé sur des fichiers de suivi introduit dans 7.1.
- Reconcevoir la logique existante : La logique précédemment implémentée dans les scripts Tick a dû être traduite et adaptée au format de fichier tracker.
- Recréer les indicateurs de performance clés BNM : Il a fallu recréer l'indicateur de performance clé personnalisé BNM à l'aide du nouveau cadre pour s'assurer qu'il produisait les mêmes résultats et informations qu'auparavant.
- Valider la précision ICP : Une validation approfondie était nécessaire pour confirmer que les nouvelles mises en oeuvre généraient des mesures cohérentes et correctes par rapport à la version précédente.
- Test et réglage : Le nouveau modèle nécessitait également des tests de performance et de comportement dans des conditions de réseau réelles, suivis d'ajustements si nécessaire.
- Manque d'assistance : Certaines fonctionnalités qui fonctionnaient auparavant avec le script tick n'étaient plus prises en charge avec la nouvelle implémentation du fichier tracker. Il a donc fallu faire des compromis.

Cette modification du mécanisme de création des indicateurs de performance clés a considérablement augmenté l'effort requis pendant la mise à niveau, car elle impliquait à la fois l'apprentissage d'un nouveau système et la réimplémentation de la logique de surveillance personnalisée existante afin d'assurer la continuité des informations opérationnelles.

Délai API dans le script de déclenchement des guides BNM

Les guides BNM sont déclenchés par un script personnalisé qui interagit avec les API CNC. Au cours du processus de mise à niveau et de validation, plusieurs problèmes liés à l'authentification de l'API et au traitement des réponses ont été identifiés et résolus.

Le jeton de l'API CNC a une validité de 8 heures, mais le script d'origine n'incluait pas la logique appropriée pour actualiser le jeton une fois qu'il a expiré. Par conséquent, bien que les alertes KPI dans CNC 4.4 fonctionnaient correctement, le script de déclenchement du guide a cessé de s'exécuter après l'expiration du jeton. Ce problème est passé inaperçu pendant une longue période, ce qui signifie que le script d'automatisation ne fonctionnait pas de manière fiable depuis plus d'un an. Le problème n'est apparu que lors des activités de migration et de validation dans CNC 7.1.

Plusieurs améliorations et raffinements étaient donc nécessaires :

- Logique d'actualisation des jetons : Une logique appropriée a été mise en oeuvre pour détecter l'expiration du jeton et actualiser automatiquement le jeton API, assurant ainsi une exécution ininterrompue du script.
- Modifications des réponses API : Les différences entre les versions CNC ont causé des problèmes supplémentaires. Dans CNC 4.1, une réponse de jeton expirée contenait généralement le message « expiré », alors que dans CNC 7.1, la réponse renvoie « Key not authorized ». La logique de script a dû être mise à jour pour interpréter correctement les nouveaux modèles de réponse dans 7.1.
- Gestion globale des jetons : Auparavant, les jetons étaient stockés et utilisés localement dans les fonctions. Cela a créé des scénarios dans lesquels le jeton était valide lors de la saisie d'une fonction mais a expiré avant les appels API suivants. La mise en oeuvre a été modifiée pour utiliser la gestion globale des jetons, afin d'assurer la cohérence et l'actualisation appropriée de toutes les fonctions.
- Traitement des erreurs amélioré : Dans certains cas, l'API « check sync » du NSO a renvoyé des réponses incomplètes ou différentes de la structure attendue. Cela a provoqué des exceptions KeyError, qui ont suspendu l'exécution du script. Une gestion des exceptions et une logique de validation supplémentaires ont été introduites afin que le script puisse continuer à s'exécuter même lorsque des réponses API inattendues sont reçues.
- Améliorations de la stabilité des scripts : Des mesures de protection et des vérifications supplémentaires ont été ajoutées pour s'assurer que les défaillances de l'API, les problèmes de réponse temporaire ou les événements d'actualisation de jeton ne provoquent pas une interruption inattendue du script.

Ces améliorations ont non seulement permis de résoudre les problèmes mis à jour lors de la mise à niveau, mais ont également considérablement amélioré la fiabilité, la résilience et la maintenabilité de l'infrastructure d'automatisation du guide BNM.

Modification de la conception du déclencheur Traitement BNM et Guide

La logique d'automatisation BNM est basée sur les événements et repose sur les alertes générées par les indicateurs de performance clés dans l'application Health Insight au sein de CNC. Le workflow global fonctionne comme suit :

1. CNC lit les valeurs NB (bande passante nominale) et RBW (bande passante réelle) à partir du périphérique.
2. Il calcule le rapport de bande passante (BW%) à l'aide de ces valeurs.
3. L'indicateur Health Insight évalue ce ratio par rapport à des seuils d'alerte prédéfinis.
4. Lorsqu'une alerte est générée, le script de déclenchement du guide BNM détecte l'alerte et exécute les guides correctifs correspondants

Limitation dans la conception d'alerte d'origine

Les seuils d'alerte configurés étaient :

- % BW < 60 → Critique
- 60 ≤ % P.C. ≤ 70 → Avertissement
- BW% > 90 → Infos

Cette conception a bien fonctionné pour identifier la dégradation de la bande passante, mais elle a créé un écart fonctionnel lors des scénarios de récupération de la bande passante. Plus précisément, la plage de 70 à 90 % n'avait pas de niveau d'alerte défini.

Ceci a conduit à ce comportement :

- Lorsque le pourcentage de bande passante descendait en dessous de 70 %, une alerte critique ou d'avertissement était générée, déclenchant des guides de lecture qui ajustaient les valeurs du modélisateur et de la bande passante.
- Cependant, lorsque la bande passante récupérée et le pourcentage de bande passante augmenté au-dessus de 70 %, l'indicateur de performance clé n'a généré aucune alerte car la valeur est tombée dans la bande 70-90 % sans niveau d'alerte associé.
- Comme le script d'automatisation BNM dépend entièrement de la génération d'alertes pour déclencher des actions, il n'a pas eu l'occasion de lire les valeurs NBW/RBW mises à jour ou d'initier des actions de restauration.
- Par conséquent, la restauration de la bande passante ne s'est pas produite automatiquement, même si une bande passante suffisante était devenue disponible. Il n'y avait pas de logique de restauration aussi bien dans la conception originale.

Cette limitation est devenue visible dans le réseau de production, où les liaisons qui avaient

précédemment subi une réduction de la bande passante sont restées dans un état restreint même après une amélioration des conditions.

Impact de la modification du cadre ICP

Le problème a été encore aggravé par le changement de cadre introduit dans CNC 7.1. Dans Health Insight 4.1, la mise en oeuvre de KPI basés sur Tick a pris en charge jusqu'à cinq niveaux d'alerte, permettant un contrôle plus fin des bandes de seuil et rendant la logique de restauration plus facile à mettre en oeuvre.

Cependant, dans CNC 7.1, le cadre KPI basé sur les fichiers de suivi ne prend en charge que trois niveaux d'alerte, ce qui a réduit la flexibilité de définition de plusieurs seuils de récupération et a nécessité une reconception de la logique d'alerte pour s'adapter à ces contraintes.

Déclenchement excessif du guide

Un autre problème identifié dans la mise en oeuvre originale était la fréquence extrêmement élevée des exécutions de guides. La logique d'automatisation n'incluait aucun temps d'attente ni aucune fenêtre de stabilisation. Dès que la commande numérique a lu une valeur du périphérique qui remplissait la condition d'alerte :

- L'alerte a été immédiatement déclenchée.
- Le script d'automatisation a immédiatement déclenché les guides correctifs.

Comme les valeurs de télémétrie fluctuent fréquemment dans les réseaux en direct, des centaines de guides de lecture sont déclenchés toutes les heures, ce qui n’est pas idéal tant du point de vue de la stabilité du réseau que des performances des applications.

Logique d'automatisation repensée

Pour remédier à ces limitations, la conception de l'automatisation BNM a été remaniée avec plusieurs améliorations :

- Logique de seuil d'alerte révisée : Afin de s'assurer que la bande de récupération a été capturée dans les trois niveaux d'alerte, la logique a été modifiée de sorte que tout % de la BW supérieur à 70 % est maintenant traité comme une alerte de niveau INFO, remplaçant l'approche antérieure où seules les valeurs supérieures à 90 % ont été classifiées comme INFO. Cela a permis d'assurer une surveillance active de la bande de récupération de 70 à 90 %, ce qui permet aux guides de restauration de se déclencher lorsque les conditions de bande passante s'améliorent.

- Introduction du temps d'attente : Un mécanisme de temps d'attente de 20 minutes a été introduit pour s'assurer que les conditions de bande passante restent stables pendant une durée définie avant de déclencher les guides. Cela empêche l'automatisation de réagir aux fluctuations à court terme.
- Exécution contrôlée du guide : Avec la logique et le temps d'attente révisés, la fréquence des exécutions du guide a considérablement diminué, empêchant les actions d'automatisation inutiles.
- Mécanisme de rappel pour dégradation grave : Pour les cas de dégradation importante de la bande passante, une approche de rappel a été introduite. Dans de tels scénarios, l'automatisation ajuste de manière proactive le formateur de trafic et l'allocation de bande passante à 40 % de la bande passante réseau, ce qui permet une récupération plus rapide en cas d'encombrement.
- Stabilité améliorée de l'automatisation : Le workflow reconçu garantit que les scénarios de réduction et de restauration de la bande passante sont traités efficacement, même dans les limites de l'infrastructure KPI basée sur le traqueur.

Résultat

Grâce à ces modifications de conception, associées aux améliorations apportées précédemment en matière de gestion des API, de gestion des jetons et de robustesse des scripts, le cadre d'automatisation BNM fonctionne désormais de manière beaucoup plus stable, efficace et prévisible. Le système peut répondre correctement à la fois aux conditions d'encombrement et de récupération, tout en évitant les exécutions excessives de guides et en garantissant une optimisation fiable de la bande passante du réseau.

Suppression des alarmes des périphériques

Dans CNC 4.1, les alarmes ont été transmises à un système ascendant appelé OneFM via une API RESTCONF. Comme la pile CNC 4.1 n'incluait pas la fonctionnalité EMF, la plate-forme ne générait que des alarmes au niveau du système. Ces alarmes ont été transmises en amont sans aucune complexité liée à la catégorisation des alarmes.

Avec le déploiement de CNC 7.1, l'application EMF a été introduite, élargissant considérablement le modèle d'alarme. Les alarmes sont désormais classées en trois types :

- Alarmes système - relatives à l'état de la plate-forme et des applications CNC
- Alarmes réseau - liées aux conditions de service du réseau
- Alarmes de périphérique : générées directement à partir des périphériques réseau et transmises via CNC

Cependant, il existait déjà un EPNM chargé de collecter et de gérer les alarmes au niveau des

périphériques. Si CNC a également transmis ces alarmes à OneFM, des alarmes en double ont été reçues des deux systèmes. Par conséquent, il était nécessaire d'exclure les alarmes de périphériques du CNC tout en continuant à transférer les alarmes système et réseau.

Le principal défi était une limitation de l'API ascendante RESTCONF utilisée pour transférer les alarmes à OneFM. L'API ne prend pas en charge le filtrage des alarmes en fonction de la catégorie d'alarme. Si un tel filtrage avait été disponible, la solution aurait été simple : excluez simplement les alarmes de périphérique au niveau de l'API avant de les transmettre au système en direction du nord.

Plusieurs solutions possibles ont été évaluées et discutées :

- Arrêt des déroutements de périphérique à la source : Empêchez les périphériques d'envoyer des déroutements à CNC.
- Filtrage des alarmes au niveau du système ascendant (OneFM) : Autoriser CNC à envoyer toutes les alarmes, mais filtrer les alarmes des périphériques dans OneFM.
- Filtrage dans CNC avant le transfert des alarmes.

L'arrêt des déroutements au niveau des périphériques n'a pas été considéré comme viable, car CNC s'appuie sur ces déroutements pour détecter les événements des périphériques et maintenir une connaissance opérationnelle des conditions du réseau. La désactivation des déroutements réduirait considérablement la capacité de CNC à répondre aux problèmes du réseau.

La solution a finalement mis en oeuvre une fonction CNC intégrée appelée Device Alarm Suppression. Cette fonctionnalité permet aux administrateurs de supprimer des types spécifiques d'alarmes de périphériques en fonction des groupes de périphériques, ce qui les empêche d'être traitées ou transférées plus en amont.

En configurant les stratégies de suppression des alarmes des périphériques, le système a pu :

- Supprimer les alarmes générées par les périphériques dans CNC.
- Poursuivre le traitement et le transfert des alarmes système et réseau.
- Empêchez les alarmes de périphériques en double d'atteindre le système OneFM.

Cette approche a fourni une solution propre et évolutive sans perturber la capacité de CNC à recevoir des déroutements des périphériques. Par conséquent, le flux d'alarmes vers OneFM a été rationalisé, garantissant que seules les alarmes système et réseau pertinentes ont été transmises, tout en évitant la duplication avec la gestion des alarmes des périphériques d'EPNM.

Modifications hors bande

Dans la configuration existante, l’équipe d’exploitation s’est souvent appuyée sur des scripts basés sur l’interface de ligne de commande pour transmettre les mises à jour de configuration aux périphériques réseau, en particulier pour des tâches telles que les modifications de liste de contrôle d’accès et les activités de débogage. Bien qu'efficace à court terme, cette approche a entraîné une dérive de la configuration, car les changements apportés à l'extérieur de l'ONS n'ont pas été suivis dans le système. Par conséquent, les workflows de mise en service de NSO ont été affectés en raison d'incohérences entre l'état prévu (modélisé) et les configurations réelles des périphériques, ce qui a entraîné des pannes et des inefficacités opérationnelles.

Rapprochement VPN L2/L3

En raison des modifications apportées à la configuration hors bande : l'équipe réseau avait mis à jour la configuration relative au VPN sur des périphériques en dehors de CNC/NSO et du workflow TSDN. Par conséquent, l'état stocké dans NSO (de l'ère CNC 4.1) ne correspondait pas toujours à l'état des périphériques.

Ces écarts ont entraîné de multiples échecs et incohérences de rapprochement. Dans plusieurs cas, NSO contenait des données de service VPN qui n'existaient plus sur les périphériques (ou qui avaient été modifiées d'une manière que NSO ne reflétait pas). Pour aligner NSO sur le réseau, il était nécessaire de supprimer les entrées de service VPN qui existaient uniquement dans NSO et non sur les périphériques, et de corriger d'autres incohérences causées par des modifications hors bande.

Impact du planning

La résolution de ces problèmes a nécessité environ deux semaines supplémentaires au-delà du plan de rapprochement initial. Le temps supplémentaire a été consacré à l'identification des incohérences, à la validation de l'état du périphérique et au nettoyage ou à la correction en toute sécurité des données CDB NSO.

Observations

1. Autorité de configuration : Les modifications hors bande de la configuration VPN (ou de toute configuration gérée par TSDN) créent une dérive entre NSO et le réseau et compliquent la réconciliation.
2. Base de pré-migration : Une base de référence claire de l'état géré par le CN/l'ONS par rapport à l'état périphérique seul avant la migration aurait facilité la détection et la résolution des divergences.
3. Automatisation et conversion : Les scripts de conversion de charge utile et les personnalisations spécifiques à l'utilisateur étaient essentiels pour gérer de manière cohérente les différences de format et de modèle entre les versions 4.1 et 7.1.

Recommandations pour des mises à niveau similaires

1. Imposer un gel des modifications pour les services VPN (et les autres services gérés par TSDN) pendant la fenêtre de rapprochement, avec des exceptions uniquement via un processus contrôlé.
2. Exécuter un audit de pré-rapprochement comparant la configuration NSO CDB à celle du périphérique afin de quantifier et de répertorier les écarts avant de commencer le rapprochement.
3. Documentez et informez-vous que les modifications apportées au VPN doivent passer par le TSDN CNC/NSO après la mise à niveau afin d'éviter la récurrence de dérive hors bande.
4. Conservez les scripts de conversion et de rapprochement pour les réutiliser lors de futures mises à niveau ou pour le dépannage.

Échec de la sauvegarde CNC en raison des dépendances du mode de maintenance

Le mécanisme de sauvegarde CNC exige que la plate-forme soit mise en mode maintenance avant qu'une opération de sauvegarde puisse être lancée. Par conception, l'API de sauvegarde applique cette condition préalable ; si CNC ne parvient pas à passer en mode maintenance, le processus de sauvegarde est automatiquement abandonné.

En pratique, le passage en mode maintenance échouait souvent en raison d'activités système en cours, notamment :

- Exécutions du guide MOP (Active Change Automation)
- Workflows sZTP en cours
- Opérations de service DLM
- Activités de détachement ou de fixation de profil ICP
- Collections showtech à la demande
- Tâches d'orchestration en arrière-plan

La présence d'une telle activité empêche CNC de passer en mode maintenance, ce qui entraîne l'échec de l'opération de sauvegarde avant l'exécution.

Impact opérationnel

Sauvegardes CNC quotidiennes requises pour la conformité et l'assurance opérationnelle. Cependant, les activités d'automatisation fréquentes, en particulier les guides déclenchés par BNM, ont souvent empêché le système d'entrer en mode maintenance. Par conséquent, les pannes de sauvegarde se sont produites à plusieurs reprises, créant un risque opérationnel

important et nécessitant une intervention manuelle.

Stratégie D'Atténuation

1. Optimisation de la planification de la sauvegarde : une fenêtre de maintenance avec une activité système minimale a été identifiée. D'après l'analyse du trafic et de l'automatisation, la tâche de sauvegarde était planifiée pour 5:00 AM (AEST), heure à laquelle l'orchestration et l'exécution du guide étaient les moins susceptibles d'être actives.

2. Validation de l'activité de pré-sauvegarde : une pré-vérification automatisée a été introduite avant l'appel de l'API de sauvegarde :

- Le script interroge les API CNC pour détecter l'exécution des tâches MOP Change Automation.
- Si une tâche est signalée comme étant en cours d'exécution, le script attend 5 secondes et recommence.
- Cette boucle se poursuit jusqu'à ce que le système ne signale aucune tâche active.
- Ce n'est qu'après confirmation de l'inactivité de l'environnement que le script tente d'activer le mode maintenance et de déclencher la sauvegarde.

Cela a évité les tentatives de sauvegarde inutiles alors que le système était en état de fonctionnement occupé.

3. Mécanismes de reprise et de résilience : Pour tenir compte des états transitoires du système, des garanties supplémentaires ont été ajoutées :

- Jusqu'à trois nouvelles tentatives si l'API de sauvegarde renvoie un échec
- Intervalles de délai courts entre les tentatives
- Traitement des erreurs en douceur pour éviter la fin du script

Résultats et résultats

L'atténuation combinée a considérablement amélioré la fiabilité des sauvegardes :

- Les pannes de sauvegarde ont été considérablement réduites
- Après l'implémentation, seulement deux échecs ont été observés, tous deux causés par un processus sZTP bloqué, qui est hors du contrôle du script.
- L'introduction de retards d'exécution dans l'automatisation du guide BNM a encore réduit les conflits avec le mode maintenance.

Transfert de syslogs vers Splunk

La destination syslog a été configurée dans CNC pour transférer les journaux vers Splunk via TLS. Cependant, une fois reçus, les journaux étaient illisibles du côté du Splunk. En raison de ce problème provenant de l'environnement Splunk, l'option a été choisie pour revenir au transport UDP, après quoi les journaux ont été traités avec succès.

Problème de migration du regroupement de périphériques

L'utilisateur a précédemment créé 18 groupes de périphériques dans CNC 4.1 ; toutefois, cette version ne fournissait aucun mécanisme basé sur l'interface utilisateur ou l'API pour exporter ou importer des groupes de périphériques. Par conséquent, la migration de ces groupes vers CNC 7.1 nécessitait une approche non standard. Deux API CNC internes ont été identifiées : l'une exposant la hiérarchie de groupes de périphériques et l'autre répertoriant les périphériques mappés à chaque noeud de hiérarchie. À l'aide de ces API, tous les groupes de périphériques et leurs périphériques associés ont été extraits et stockés sous forme de sorties JSON. Un script personnalisé a ensuite été développé pour analyser les réponses et extraire uniquement les noms d'hôte des périphériques de chaque groupe.

CNC 7.1 a introduit des fonctionnalités natives d'importation/exportation pour les groupes de périphériques, y compris un modèle d'importation basé sur CSV. Après avoir extrait les noms d'hôte du système hérité, un deuxième script d'automatisation a été créé pour remplir les modèles CSV dans le format requis, afin de garantir que chaque groupe de périphériques puisse être importé de manière précise et indépendante. Cette automatisation était essentielle ; sans elle, la migration des groupes de périphériques vers CNC 7.1 aurait été beaucoup plus longue et plus complexe sur le plan opérationnel.

Isoler les périphériques gravement endommagés en bande passante

Malgré la mise en oeuvre de l'exemple d'utilisation BNM pour corriger automatiquement les faibles rapports RBW/NBW, un sous-ensemble de périphériques est resté dans des états gravement dégradés pendant de longues périodes. Bien que le modélisateur et les guides d'ajustement de la bande passante aient généralement restauré les périphériques peu de temps après les événements de dégradation, plusieurs périphériques sont restés dans un état Critique pendant plus d'une semaine et ont nécessité une intervention manuelle. Toutefois, l'identification de ces dispositifs a posé un défi. Bien que l'interface utilisateur CNC fournisse des visualisations claires des alertes et des mesures de bande passante, elle ne révèle pas facilement les périphériques qui sont restés exclusivement dans un état critique pendant un intervalle prolongé.

Pour combler cette lacune opérationnelle, une solution basée sur une API a été développée. CNC propose une API qui récupère une liste des principaux périphériques générant des alertes sur des périodes configurables (par exemple, 7 jours, un mois). En obtenant ces données et en filtrant les périphériques qui n'ont généré que des alertes critiques au cours de la période sélectionnée, l'équipe a pu isoler rapidement les périphériques nécessitant une correction manuelle. Cette approche automatisée a considérablement amélioré l'efficacité du dépannage et réduit le temps nécessaire à l'identification des cas de dégradation persistante.

Suppression de configuration de télémétrie de périphérique

Dans CNC 4.1, les configurations de télémétrie transmises depuis NSO via le pack de fonctions tm-tcont été appliquées automatiquement lorsqu'un périphérique était associé à un profil d'indicateurs de performance clés Health Insight (HI). Cependant, ces configurations, y compris les références VIP CDG, n'ont pas été supprimées lors du détachement ultérieur du profil KPI. Par conséquent, les périphériques ont accumulé des entrées de télémétrie obsolètes et redondantes au fil du temps.

Ce problème s'est accentué lors de la mise à niveau vers CNC 7.1. Les périphériques conservaient souvent les configurations de télémétrie VIP CDG héritées de CNC 4.1 en plus des nouvelles entrées générées par CNC 7.1, ce qui a entraîné de multiples configurations de télémétrie conflictuelles sur plus de 2 000 périphériques. Des préoccupations ont été soulevées au sujet de l'impact opérationnel et de l'hygiène de la configuration, car seule la configuration CNC 7.1 CDG VIP doit être restée active.

Pour résoudre ce problème, un script automatisé a été développé pour identifier et supprimer les références VIP CDG obsolètes de la configuration de télémétrie de chaque périphérique. Cette solution a permis d'éliminer les incohérences de configuration, de rétablir l'alignement avec le modèle de télémétrie 7.1 attendu et d'éviter ce qui aurait nécessité plusieurs jours de nettoyage manuel sur l'ensemble du parc d'appareils volumineux.

Dépannage de la collection MDT

Dans CNC 7.1, la plupart des collections d'indicateurs de performance clés Health Insight (HI) reposent sur la télémétrie pilotée par modèle (MDT). Lorsqu'un profil ICP est activé sur un périphérique, NSO programme automatiquement les chemins de capteur requis et configure le VIP CDG comme destination de télémétrie. Une fois cette configuration appliquée, une tâche de collecte CDG correspondante est créée pour suivre l'état de télémétrie du périphérique.

Lors de la validation, il a été signalé que plus de 100 périphériques ne disposaient pas de configurations de télémétrie. L'identification de ces périphériques via l'interface utilisateur CNC

s'est avérée peu pratique, car l'interface utilisateur ne prend en charge que le filtrage par périphérique et n'évolue pas efficacement pour un parc dépassant 2 000 périphériques. Cela a nécessité une méthode automatisée pour déterminer quels périphériques n'étaient pas configurés par télémétrie et nécessitaient une réactivation des indicateurs de performance clés.

Pour résoudre ce problème, nous avons utilisé la balise BNM attribuée aux périphériques chaque fois qu'un profil ICP est activé. Tout d'abord, une exportation de tous les périphériques avec l'étiquette BNM a été générée. Un script Python a ensuite été développé pour interagir avec l'API de collection CNC, incorporant une logique de pagination pour récupérer l'ensemble complet des travaux de collection (chaque appel d'API retourne un maximum de 100 entrées). Le script a extrait les noms d'hôte des données de la tâche de collecte et les a comparés à la liste des périphériques balisés BNM exportée.

Cette comparaison a permis d'obtenir la liste des périphériques étiquetés mais qui n'apparaissaient pas dans la tâche de collecte BNM, indiquant que la configuration de télémétrie MDT n'avait pas été appliquée. Le profil ICP a ensuite été réactivé sur ces périphériques et la validation a confirmé que toutes les tâches de collecte correspondantes ont été correctement créées.

Cette automatisation a considérablement rationalisé le processus de dépannage, permettant à l'équipe d'identifier et de corriger tous les périphériques affectés en une seule journée, un effort qui n'aurait pas été possible grâce à une inspection manuelle.

Changements de comportement des AP et ajustement de l'algorithme consensuel dans l'ONS 6.4.1.1

Lors de la mise à niveau de Cisco NSO 5.7.5.1 vers 6.4.1.1 dans le cadre de la transition vers Cisco CNC 7.1, un changement notable a été observé dans le comportement de haute disponibilité (HA) en raison de l'activation implicite de l'algorithme consensus dans la nouvelle version de NSO. Ce n'était pas le comportement par défaut de NSO 5.7.5.1, ce qui a entraîné un changement des caractéristiques de basculement après la mise à niveau. Plus précisément, lorsque le noeud principal a été arrêté, le noeud secondaire est passé à l'état de lecture seule, l'empêchant de gérer les activités d'approvisionnement. De même, lorsque le noeud secondaire est tombé en panne, le noeud principal est passé d'un état principal actif à un état « aucun », ce qui a eu un impact sur la continuité du service.

Pour restaurer le comportement de haute disponibilité attendu aligné sur le déploiement précédent, l'algorithme de consensus a été explicitement désactivé dans NSO 6.4.1.1. Cet ajustement a permis de s'assurer que les noeuds principaux et secondaires ont repris leurs rôles prévus pendant les scénarios de basculement, ce qui a permis une mise en service ininterrompue et le maintien de la stabilité opérationnelle cohérente avec la version NSO précédente.

Mise à niveau de version NSO et améliorations de compatibilité des packages

Dans le cadre de la transition de Cisco CNC 4.1 à 7.1, la version sous-jacente de Cisco NSO a été mise à niveau de 5.7.5.1 à 6.4.1.1. Cette mise à niveau a introduit des modifications dans les structures de modèles XML dans les packages NSO existants, entraînant des échecs dans certains cas de tests de régression qui dépendaient du comportement des modèles hérités.

Pour remédier à ces lacunes en matière de compatibilité, les modèles de package NSO concernés ont été analysés et mis à jour pour s'aligner sur le schéma révisé et les exigences de traitement de NSO 6.4.1.1. Ces améliorations ont permis de garantir que tous les workflows d'automatisation et modèles de service continuent à fonctionner comme prévu, en restaurant la stabilité de régression et en maintenant la cohérence dans l'environnement CNC mis à niveau.

Problèmes liés à l'activation des ICP à grande échelle

CNC fournit un mécanisme d'interface utilisateur prêt à l'emploi pour activer les profils ICP sur les périphériques. Bien que cette approche fonctionne bien pour les petites flottes, elle devient inefficace et peu fiable à grande échelle. Dans ce déploiement, plus de 2 000 périphériques SWR nécessitaient l'activation d'indicateurs de performance clés, et l'interface utilisateur n'offrait pas de moyen efficace de sélectionner ou de traiter les périphériques en bloc.

Initialement, une approche basée sur le marquage a été tentée : tous les périphériques SWR se sont vu attribuer une étiquette SWR, et l'activation des indicateurs de performance clés a été exécutée en utilisant la sélection d'étiquette plutôt que la sélection manuelle des périphériques. Cependant, le traitement de plus de 2 000 périphériques dans un seul workflow a entraîné des défis opérationnels importants. Le travail a duré plus de trois heures et s'est terminé avec des centaines d'échecs. Bien que tous les périphériques aient été inclus dans l'intention, seuls 750 ont reçu l'activation des indicateurs de performance clés avec succès, et les tentatives répétées n'ont produit que des progrès incrémentiels. Cette approche ne s'est révélée ni évolutive, ni reproductible. Il a montré des problèmes importants avec la charge.

Les problèmes de synchronisation des périphériques NSO ont posé un deuxième problème. De nombreuses défaillances ont indiqué que NSO n'était pas synchronisé avec les périphériques correspondants. La tentative de synchronisation manuelle des opérations suivie d'une réactivation des indicateurs de performance clés n'était pas pratique et aurait nécessité un effort important de la part de l'opérateur.

Pour pallier ces limitations, un workflow automatisé et piloté par lots a été développé :

1. Exportez l'inventaire CNC complet.
2. Traiter les périphériques par lots de 50 (identifié comme la taille optimale grâce à l'accord).

3. Pour chaque lot, déclenchez une synchronisation automatique à partir des UUID des périphériques.
4. Exécutez l'activation des indicateurs de performance clés via l'API CNC.
5. Surveiller l'historique des tâches ICP et consigner les échecs par programme.
6. Retraiter les périphériques défaillants en répétant les étapes d'activation de la synchronisation et des indicateurs de performance clés.
7. Une fois le lot terminé, passez à l'ensemble suivant de 50 périphériques.

L'automatisation incluait également la possibilité de désactiver les profils ICP, permettant ainsi une gestion complète du cycle de vie.

Cette solution a fourni un processus rationalisé, déterministe et hautement évolutif pour le provisionnement des indicateurs de performance clés. Elle a éliminé les interventions manuelles, assuré des résultats cohérents et permis d'économiser plusieurs jours d'effort opérationnel. La même automatisation s'est avérée inestimable lorsque les profils KPI ont dû être désactivés et réactivés après le changement de conception BNM, permettant une reconfiguration rapide et sans erreur sur l'ensemble du parc de 2 000 appareils.

API ascendante RESTCONF limitée à l'accès administrateur

L'API ascendante basée sur RESTCONF utilisée pour transférer des alarmes et des événements à partir de CNC a une limitation en vertu de laquelle elle ne peut être appelée qu'à l'aide du compte admin. Les tentatives d'accès à l'API via des comptes de service ont échoué, malgré que ces comptes aient les rôles opérationnels requis. Pour contourner ce problème, l'utilisateur devait utiliser les informations d'identification d'administrateur pour le transfert des alarmes vers le système ascendant, ce qui introduisait une contrainte opérationnelle et limitait l'adhésion aux principes d'accès les moins privilégiés.

L'automatisation en tant qu'activateur stratégique

Compte tenu de l'ampleur et de la complexité du programme de mise à niveau et de migration du CNC, l'exécution manuelle des tâches opérationnelles s'est rapidement avérée intenable. Les activités telles que l'intégration des périphériques, le provisionnement des indicateurs de performance clés, l'alignement de la configuration, la réconciliation et la validation de la télémétrie impliquent des milliers d'éléments réseau et des flux de travail répétés qui sont fortement sujets aux erreurs humaines lorsqu'ils sont effectués manuellement. L'automatisation était donc essentielle non seulement pour accélérer l'exécution, mais également pour garantir la cohérence, réduire le risque opérationnel et libérer les équipes de prestation des tâches répétitives et chronophages.

En systématisant ces processus à l'aide de workflows scriptés et d'opérations basées sur des API, le programme de mise à niveau a réalisé des gains d'efficacité significatifs. L'automatisation a permis d'accélérer l'exécution des tâches, d'améliorer la précision et de prévoir les résultats dans toutes les sections. Les économies qui en ont résulté ont non seulement réduit le délai de déploiement global, mais ont également permis aux ingénieurs de se concentrer sur des efforts de validation et de conception plus importants plutôt que sur des tâches opérationnelles de routine.

Certaines des activités d'automatisation ont été identifiées avant le début du projet de mise à niveau, tandis que d'autres ont évolué lorsque des défis se sont posés. Il y en avait aussi qui étaient nécessaires en raison des questions qui se sont développées au cours du projet.

Ce tableau illustre les domaines dans lesquels l'automatisation a eu un impact important sur l'ensemble du programme.

Description de tâche	Effort manuel (jours)	Effort d'automatisation (jours)	Économies estimées (jours)
Mises à jour ACL (SWR/LWR) (plus de 2 000)	30.0	2.0	28.0
Migration des périphériques et connexion à CDG(2000+)	5	1.0	4.0
Connexion d'indicateurs de performance clés BNM aux périphériques (plus de 2 000)	4.0	1,5 (moyenne)	2.5
Rapprochement des services	7	2.5	4.5
Migration des groupes de périphériques	4	0,5	3.5
Isoler les périphériques à bande passante fortement dégradée	3	0,5	2.5
Dépannage de la collecte MDT	3	0,5	2.5
Totaux	56 jours	8,5 jours	47,5 Jours

Leçons apprises

La mise à niveau n'est pas simple

CNC ne prend pas en charge les mises à niveau sur place, et le modèle « lift-and-shift » introduit une complexité opérationnelle significative. Le processus ne doit jamais être considéré comme simple, surtout lorsque le saut de version est important. Des problèmes inattendus surviennent dans les applications, les intégrations et les workflows, et chacun nécessite du temps, une analyse et une atténuation minutieuse. Un saut majeur dans la version amplifie ce défi, rendant indispensable une planification, une validation et une exécution par phases approfondies. Nous avons dû consacrer beaucoup de temps supplémentaire aux dossiers du centre d'assistance technique et aux efforts de dépannage. Comme nous n'avons pas gardé de temps tampon pour cela, cela est devenu difficile.

CX doit faire le levage lourd

Attendez-vous à un effort considérable de CX pour le déploiement, l'intégration, la migration et la validation de cas d'utilisation de bout en bout. Ne supposez pas que les workflows éprouvés sur l'ancienne version se comportent de manière identique sur la nouvelle.- Beaucoup de dépannage et d'analyse seraient nécessaires pour faire fonctionner les choses.

Automation Toolkit est une nécessité

Le parcours de mise à niveau a démontré que l'automatisation n'est pas une commodité optionnelle, mais une exigence fondamentale pour les déploiements CNC à grande échelle. Nous avons planifié l'automatisation pour les candidats nécessaires au début, mais on ne peut jamais supposer que cela sera suffisant. Au milieu du projet, des problèmes ont pu être identifiés dans les cas d'utilisation où l'automatisation apporterait certainement une valeur ajoutée, comme cela a été démontré dans les sections précédentes.

Éviter les conflits de contrôleur double pendant la migration

Au cours de la mise à niveau, il est essentiel de s'assurer que les anciens et les nouveaux environnements CNC ne sont pas actifs simultanément. Bien qu'une courte période d'imprégnation soit nécessaire pour la validation, l'allonger de façon significative, comme cela s'est produit dans ce projet pendant plus de 2 mois, crée des risques opérationnels. Avec les deux CNC actifs depuis plus de 15 à 20 jours, les fonctions d'automatisation en boucle fermée, telles

que la bande passante à la demande, ont généré des actions incohérentes et contradictoires sur l'ensemble du réseau, puisque la logique d'automatisation s'exécutait à partir de deux contrôleurs à la fois.

L'une des leçons clés consiste à mettre en place des garde-fous clairs lors des migrations. Des mesures telles que la désactivation administrative des périphériques dans l'ancien CNC, la suspension des workflows d'automatisation ou la restriction des abonnements de télémétrie auraient permis d'éviter ces conflits. Les futures mises à niveau doivent prévoir explicitement une isolation stricte des contrôleurs afin d'éviter les interférences entre deux contrôleurs et de garantir un comportement prévisible du réseau.

Les MOP ne sont pas sacro-saintes

Bien que des documents MOP (Method of Procedure) soient créés pour chaque déploiement, intégration et cas d'utilisation, il est irréaliste de supposer qu'un MOP validé dans des conditions de laboratoire se comporte de manière identique en production. L'environnement de production a constamment révélé des écarts, certains mineurs, d'autres significatifs, mettant ainsi en évidence des lacunes qui n'étaient pas visibles lors des tests contrôlés. Les réseaux réels, les comportements hérités, les dépendances externes et les conditions de trafic en direct introduisent des variables que les simulations en laboratoire ne peuvent pas toujours reproduire.

Le principal enseignement à retenir est que les équipes doivent aborder le déploiement de la production en s'attendant à rencontrer des comportements inattendus, des cas extrêmes et de nouvelles découvertes. La flexibilité, la rapidité du dépannage et la capacité à adapter les procédures à la volée sont essentielles pour une exécution réussie à grande échelle.

Efficacité des dossiers TAC

Les problèmes de post-production sont inévitables, et bien que le dépannage initial par l'équipe de livraison soit précieux, le fait de compter uniquement sur les efforts internes peut entraîner des retards inutiles. Il est prudent d'ouvrir un dossier TAC en parallèle comme filet de sécurité, en particulier pour les problèmes liés aux produits ou les comportements complexes qui ne sont pas immédiatement diagnostiquables. Les investigations du TAC demandent souvent du temps, et le fait de retarder la création de dossiers de plusieurs jours peut entraîner une perte significative de la dynamique du projet. L'intervention précoce du TAC garantit la disponibilité d'une assistance spécialisée en cas de besoin, accélère l'identification des causes premières et évite les retards évitables dans les horaires.

Engager la BU CNC pour une assistance efficace

Un soutien solide de la part de l'unité commerciale CNC est très précieux pour tout projet CNC. Les utilisateurs ont souvent besoin d'informations et de clarifications détaillées sur les produits, qui ne sont pas facilement disponibles avec l'équipe de prestation seule. Le fait de disposer d'un contact BU accessible tout au long de la mission accélère la résolution des problèmes, renforce la précision technique et contribue à renforcer la confiance et le rapport utilisateur.

Meilleures pratiques pour la mise à niveau CNC

Planifier une stratégie de mise à niveau optimisée

CNC ne prend pas en charge les mises à niveau sur place, ce qui rend le déploiement parallèle inévitable. Considérez le nouvel environnement comme une nouvelle installation et allouez une capacité de calcul, de stockage et d'administration suffisante pour exécuter deux environnements simultanément. Planifier les étapes de validation, le séquencement de la migration et les activités de mise en service longtemps à l'avance.

Une validation rigoureuse avant déploiement est essentielle, en particulier pour les paramètres immuables

De nombreuses expériences soulignent l'importance cruciale de la diligence au cours du déploiement initial. La validation de toutes les entrées clés à l'avance, en particulier les paramètres de configuration immuables, est essentielle pour éviter les redéploiements coûteux et l'impact sur le calendrier. Il est donc fortement recommandé d'utiliser des listes de contrôle structurées avant le déploiement, des examens par les pairs et des validations à blanc afin de minimiser le risque d'erreurs de configuration irréversibles.

Utiliser un environnement de validation dédié avant d'aborder la production

La mise en place d'un environnement de test/CALO interne au début du projet permet aux équipes d'expérimenter, de valider les workflows, de découvrir les modifications spécifiques aux versions et de renforcer la confiance avant de toucher à la production. Cela réduit considérablement les inconnues lors du déploiement final.

Dimensionnement basé sur des preuves pour les composants de réseau croisé distribué

Lors de la conception de clusters, de distributions CDG et d'allocations PCE, basez les décisions sur les types de périphériques, l'échelle de l'interface, la complexité de la topologie et l'intensité de la collecte plutôt que sur le simple nombre de périphériques. Des distributions équilibrées évitent la surcharge et garantissent des performances prévisibles sur l'ensemble du cluster.

Automatisation des tâches répétitives à volume élevé

Établissez un arriéré d'automatisation au démarrage des tâches répétitives, volumineuses ou critiques sur le plan opérationnel et investissez là où l'automatisation est obligatoire. Validez et affinez d'abord votre automatisation dans l'environnement SIT, en vous assurant que la production ne repose pas sur des correctifs de dernière minute. L'évolutivité amplifie le coût du travail manuel ; l'automatisation standardisée améliore la qualité, la vitesse et le contrôle. Intégrer les résultats sous forme de ressources réutilisables (interfaces documentées, tâches paramétrées, bibliothèques partagées) afin que les équipes puissent tirer parti de la même automatisation pour les futures mises à niveau Crosswork et les projets adjacents, réduisant ainsi le temps de reprise et d'intégration.

Éviter le double contrôle en boucle fermée pendant l'exécution parallèle

Pendant la coexistence, traitez l'automatisation en boucle fermée comme une fonctionnalité d'écriture unique : un seul chemin d'orchestration peut gérer activement la correction ou la configuration basée sur des politiques. Les CLA simultanés sur les anciennes et les nouvelles piles risquent de provoquer des déclencheurs en double et des intentions divergentes, ce qui peut déstabiliser l'état du périphérique. Planifier la mise en service de l'accord de licence de produit comme étape finale, après validation fonctionnelle et basculement définitif vers le nouveau contrôleur.

Évaluation de l'impact de la mise à niveau structurée

Les sauts de version majeurs introduisent de nouvelles fonctionnalités tout en dépréciant ou en modifiant les anciennes. Il est extrêmement important de tenir compte de ces changements. Souvent, la modification ne sera pas documentée dans les notes de version de la version mise à niveau et apparaîtra lorsque nous arriverons sur le terrain. Réaliser des évaluations structurées des éléments suivants :

- API déconseillées
- Modifications du cadre ICP
- Différences de comportement au niveau des applications
- Écarts du modèle de configuration

- Alertes, traitement de la topologie et modifications d'exécution du guide

Tester la compatibilité et le comportement sur la surface d'intégration

CNC interagit avec plusieurs systèmes externes tels que NSO, SSM, CPNR, EPNM, OneFM, Splunk et les structures d'orchestration.
Avant la migration :

- Valider la compatibilité des versions
- Tester toutes les intégrations ascendante/descendante
- Confirmer les modèles de données, les déroutements et les flux télémétriques
- Vérifier le comportement d'authentification SSL/RESTCONF

Les défaillances d'intégration détectées après la migration créent des angles morts opérationnels.

Établir une stratégie robuste d'exportation des données avant la migration

Tout exporter avant de commencer la migration :

- Profils d'identification
- Fournisseurs
- Étiquettes
- Guides personnalisés
- Indicateurs personnalisés
- Rôles et RBAC
- Bons sZTP
- Groupes de périphériques
- Métadonnées du service historique

Migration De Périphériques Par Lots Avec Portes De Validation Intégrées

Lors de la migration de milliers de périphériques, effectuez la migration par lots contrôlés :

- Déplacer les périphériques dans des cohortes fixes (par région, charge CDG ou type de périphérique, par exemple)
- Validez la télémétrie, l'état de synchronisation NSO et l'accessibilité avant de passer au lot suivant

- Revenir au lot si des anomalies persistantes apparaissent

Cela évite une charge élevée sur CDG et CNC dans un court intervalle de temps.

Gestion des modifications de configuration hors bande via l'intégration NSO

Afin de relever le défi hors bande dans le cadre de la mise à niveau de la CNC 4.1 à 7.1, un changement structuré vers des opérations pilotées par les ONS a été mis en oeuvre. L'équipe d'exploitation a obtenu un accès contrôlé basé sur l'utilisateur à l'interface de ligne de commande du NSO, tandis que l'accès administratif direct à l'interface de ligne de commande du périphérique était restreint pour empêcher les modifications hors bande. En outre, les scripts CLI hérités ont été systématiquement convertis en automatisation RESTCONF intégrée à NSO, permettant des fonctionnalités telles que la validation à sec et la restauration transactionnelle. Cette approche a permis de s'assurer que toutes les modifications de configuration étaient gérées de manière centralisée, auditables et cohérentes avec les modèles de service de NSO, éliminant ainsi les dérives de configuration et rétablissant la fiabilité du provisionnement.

Mettre fortement l'accent sur le gel des modifications

Pendant les périodes de migration critiques :

- Geler les modifications du réseau initiées par l'utilisateur
- Restreindre les push de configuration
- Synchronisation avec les équipes sur site et NOC
- Planifiez une fenêtre pour prendre en charge les activités d'urgence telles que le remplacement de périphérique à l'aide de CNC/ZTP, etc.

Cela réduit le bruit et garantit la stabilité de l’état du réseau tout au long de la mise à niveau

Conclusion

La migration de CNC 4.1 vers CNC 7.1 constitue une étude de cas significative dans les complexités inhérentes aux mises à niveau de plate-forme d'orchestration de réseau à grande échelle. Ce projet démontre que de telles transitions ne sont pas simplement des avancées de version, mais des transformations complètes à travers les couches architecturales, les workflows opérationnels et les écosystèmes d'automatisation. L'absence d'un chemin de mise à niveau sur place a nécessité un déploiement complet avec changement de poste et levée, ce qui a introduit des défis d'environnement parallèles et a nécessité une coordination méticuleuse entre CNC, NSO, SR-PCE, CDG et les intégrations de systèmes externes. Le paysage opérationnel qui en a

résulté a souligné l'importance de méthodologies de migration robustes, de cycles de validation exhaustifs et de processus de basculement étroitement contrôlés pour réduire les risques dans les environnements de production.

La mise à niveau a révélé l'importance de l'automatisation en tant que pilier indispensable de l'évolutivité et de la précision. Avec plus de 2 000 périphériques, des configurations télémétriques étendues, plusieurs composants dépendants et des workflows dynamiques d'automatisation en boucle fermée, le projet a mis en évidence les limites des procédures manuelles dans des environnements de cette ampleur. Une automatisation sur mesure couvrant les mises à jour des listes de contrôle d'accès, l'intégration des périphériques, le provisionnement des indicateurs de performance clés, le nettoyage de la télémétrie et l'isolation des pannes s'est avérée essentielle pour assurer le déterminisme, réduire les erreurs humaines et réaliser des gains d'efficacité significatifs. La structure d'automatisation a non seulement permis la continuité opérationnelle pendant la migration, mais a également établi une base durable pour l'optimisation continue du réseau.

Il était tout aussi important de reconnaître que le comportement de production s'écarte nettement des conditions de laboratoire contrôlées. Les modifications apportées au cadre, telles que la transition de la logique ICP basée sur les tops d'horloge vers des définitions basées sur les suivis, ont entraîné des changements de comportement imprévus qui ont nécessité une réorganisation, un nouveau test et un affinement itératif. De même, les défis opérationnels liés à l'automatisation en boucle fermée, à la fiabilité de la télémétrie et au comportement des API ont mis en évidence la nécessité d'un dépannage adaptatif, d'une évaluation proactive des risques et d'un engagement continu avec les experts techniques du TAC et de l'entité. Ensemble, ces facteurs montrent que les transitions majeures des versions nécessitent à la fois une profondeur technique et une préparation organisationnelle. Il reste peu de problèmes à résoudre qui devraient être résolus dans la prochaine version de travail croisé 7.2.

Dans l'ensemble, cette mise à niveau démontre que les migrations CNC à grande échelle réussies reposent sur quatre piliers fondamentaux : une validation rigoureuse du prédéploiement, une automatisation systématique et résiliente, une coordination interfonctionnelle solide et une posture opérationnelle adaptative qui anticipe les divergences entre les environnements de laboratoire et de production. Les connaissances acquises grâce à cet engagement ont non seulement contribué à un déploiement CNC 7.1 stable, mais elles offrent également un plan pour les transitions futures, en éclairant les meilleures pratiques, en renforçant les garde-fous architecturaux et en renforçant les connaissances institutionnelles pour l'évolution ultérieure de votre écosystème d'automatisation du réseau.

Glossaire des termes

Terme	Définition

BNM	Message de notification de bande passante.
CAT	Topologie active croisée
CCA	Automatisation des modifications transversales
CDG	Passerelle de données croisée
CHI	Crosswork Health Insight
CNC	Contrôleur réseau Cisco Crosswork
COE	Moteur D'Optimisation Crosswork
RPNC	Cisco Prime Network Registrar
MCG	Gestionnaire de Workflow Crosswork
CEM	Fonctions de gestion des éléments
ICP	indicateur clé de performance
LWR	Grand routeur sans fil
HAR	Télémesure pilotée par modèle
SERPILLIÈRE	Méthode de procédure
NOUVELLE-GUERRE	Bande passante nominale
NSO	Network Services Orchestrator
RBW	Bande passante enregistrée

SR-PCE	Élément De Calcul Du Chemin De Routage Du Segment
SSM	Cisco Smart Software Manager
TOUR	Petit routeur sans fil
TAC	centre d'assistance technique
TSDN	Réseaux définis par logiciel de transport
ZTP	Provisionnement sans intervention
RR	Réflecteur De Route
RP	Profil de route
POI	Point D'Interconnexion
EVPN	Réseau privé virtuel Ethernet.

Références

- Cisco Systems, Notes de mise à jour de Cisco Crosswork Network Controller, version 7.1.0
- Cisco Systems, Guide d'installation de Cisco Crosswork Infrastructure 7.1
- Cisco Systems, Guide d'administration de Cisco Crosswork Infrastructure 7.1 - Présentation des concepts :
- Cisco Systems, Guide d'ingénierie et d'optimisation du trafic des contrôleurs réseau croisés, version 7.1
- Cisco Systems, Cisco Crosswork Health Insights User Guide, version 7.1
- Cisco Systems, guide de déploiement ZTP (Crosswork Zero Touch Provisioning)
- Cisco Systems, Cisco NSO Transport SDN Function Pack Guide d'installation, version 7.1.0
- Cisco Systems,Guide de configuration de Cisco SR-PCE

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.