Caso di studio sull'aggiornamento di CNC

Sommario

Introduzione

Questo documento descrive un caso aziendale di migrazione complessa e su larga scala di una rete wireless fissa da Cisco CNC 4.1 a 7.1 tramite lift-and-shift.

Riassunto

Questo documento presenta un caso di studio dettagliato sulla migrazione di una rete fissa wireless su larga scala da Cisco Crosswork Network Controller (CNC) versione 4.1 alla versione 7.1. A causa dell'assenza di un meccanismo di aggiornamento sul posto, la transizione ha richiesto un'installazione completa lift-and-shift, introducendo una notevole complessità architetturale, operativa e di integrazione tra più di 2.000 dispositivi di rete e più sistemi interdipendenti. Lo studio esamina le sfide incontrate in diversi settori.

Un risultato chiave evidenzia il ruolo essenziale dell'automazione nel garantire scalabilità, accuratezza e determinismo operativo, in particolare per i flussi di lavoro di grandi volumi. I risultati dimostrano inoltre che gli ambienti di produzione divergono notevolmente dalle condizioni di laboratorio controllate, richiedendo la risoluzione adattiva dei problemi, la convalida iterativa e l'impegno costante con i team tecnici di TAC e Business Unit. Questo lavoro fornisce informazioni pratiche, metodologie convalidate e best practice consigliate che fungono da modello di riferimento per futuri aggiornamenti CNC e transizioni di piattaforme di orchestrazione su larga scala.

Introduzione

La proliferazione delle reti 5G, la rapida adozione di dispositivi connessi e la digitalizzazione degli ambienti aziendali e di consumo hanno portato a un significativo aumento del volume di traffico e alla diversità dei servizi che devono essere forniti in modo sicuro e affidabile su scala. I provider di servizi di comunicazione (CSP, Communications Service Provider) gestiscono ora reti altamente dinamiche, in cui gli strumenti operativi tradizionali a silo spesso creano complessità, peggiorano l'esperienza utente e aumentano le spese operative (OpEx).

Per rimanere competitivi, gli operatori stanno adottando sempre più modelli operativi modernizzati basati su automazione, virtualizzazione, principi SDN e reti basate sull'analisi e con ottimizzazione automatica.

Cisco Crosswork Network Controller (CNC) è progettato per supportare questa trasformazione semplificando i flussi di lavoro operativi, riducendo il costo totale di proprietà (TCO) e consentendo

l'automazione basata su intento nelle reti di trasporto multifornitore. Il CNC fornisce una piattaforma unificata per il provisioning dei servizi, il monitoraggio dello stato della rete e l'ottimizzazione in tempo reale, offrendo agli operatori un'unica console per gestire le reti IP su larga scala in modo più proattivo ed efficiente.

Crosswork Infrastructure sottostante offre un framework cluster resiliente e scalabile su cui vengono eseguite tutte le applicazioni CNC. Per il CNC 7.1, questo include moduli come Optimization Engine, Active Topology, Change Automation, Health Insights, Element Management Functions (EMF), Service Health e Crosswork Workflow Manager (CWM), ognuno dei quali contribuisce all'orchestrazione e alla garanzia end-to-end.

L'aggiornamento di un CNC, tuttavia, presenta problematiche uniche. Il CNC non supporta gli aggiornamenti sul posto, che richiedono un'installazione "lift-and-shift" completa in cui il nuovo ambiente viene creato in parallelo a quello esistente e tutti i dati e i servizi vengono migrati alla nuova versione. Questo caso di studio esamina un upgrade su larga scala da CNC 4.1 a CNC 7.1 per un importante aggregatore di servizi australiano che fornisce servizi backbone per tutti gli altri fornitori di servizi.

La migrazione è stata particolarmente complessa a causa di più playbook personalizzati per l'automazione delle modifiche, KPI personalizzati di Health Insight, requisiti di riconciliazione dei servizi VPN L2/L3 e la necessità di un ZTP sicuro.

Il salto di versione di grandi dimensioni ha introdotto ulteriore incertezza, date le modifiche architetturali e comportamentali interne che hanno reso difficile prevedere come si sarebbero comportati gli attuali casi d'uso nella nuova release. Ciò ha richiesto una convalida e un allineamento completi in tutti i casi di utilizzo.

È stata investita una pianificazione significativa per determinare l'allocazione ottimale delle risorse, inclusi il conteggio dei nodi ibridi/di lavoro, la distribuzione CDG e il dimensionamento PCE, nonché per stabilire se è possibile mantenere l'ingombro delle risorse esistenti.

L'installazione e la convalida iniziali di CNC 7.1 sono state eseguite in un laboratorio CALO interno, fornendo un ambiente sicuro per sperimentare, perfezionare le configurazioni e creare fiducia. A ciò ha fatto seguito l'installazione nell'ambiente di test interno, che rispecchia da vicino la produzione. La fase finale prevedeva l'installazione di CNC 7.1 in produzione, l'applicazione delle modifiche alla configurazione a livello di dispositivo e l'esecuzione di una migrazione a fasi di tutti i dispositivi e i servizi associati al nuovo controller.

Rete di produzione

La rete di produzione con interruzioni d'aria è diffusa in ampie parti dell'Australia. Con la presenza

di dispositivi 2K+, che vanno dalla NCS all'ASR9K, CNC ha gestito tutti questi dispositivi fornendo una vista topologica dal vivo. Circa 2K dispositivi erano NCS540 localmente noti come SWR (Small Wireless Router) con IOS-XR 24.3.2 e 30 erano ASR-9K (versione 7.5.2) localmente noti come LWR (Large Wireless Router).

La configurazione di Crosswork consisteva di 3 nodi ibridi e 2 nodi di lavoro. C'erano un totale di 5 CDG per i dispositivi con 4 attivi e 1 il nodo di standby. Ciò garantiva una protezione limitata in quanto il pool aveva solo 1 CDG in standby. Ma considerate le vostre esigenze, questo è stato dato il via libera. Il fatto che tutte le VM si trovassero in un unico centro dati ha facilitato la decisione di procedere con un solo standby.

Il CDG è il componente che gestisce la raccolta dei dati dai dispositivi tramite vari protocolli come SNMP, CLI e GNMI. I dati raccolti da CDG sono esposti a Crosswork attraverso la kafka interna. Un dispositivo caricato su Crosswork deve essere collegato a un CDG, il che consente al gateway dati di connettersi al dispositivo e di ottenere i dati del dispositivo.

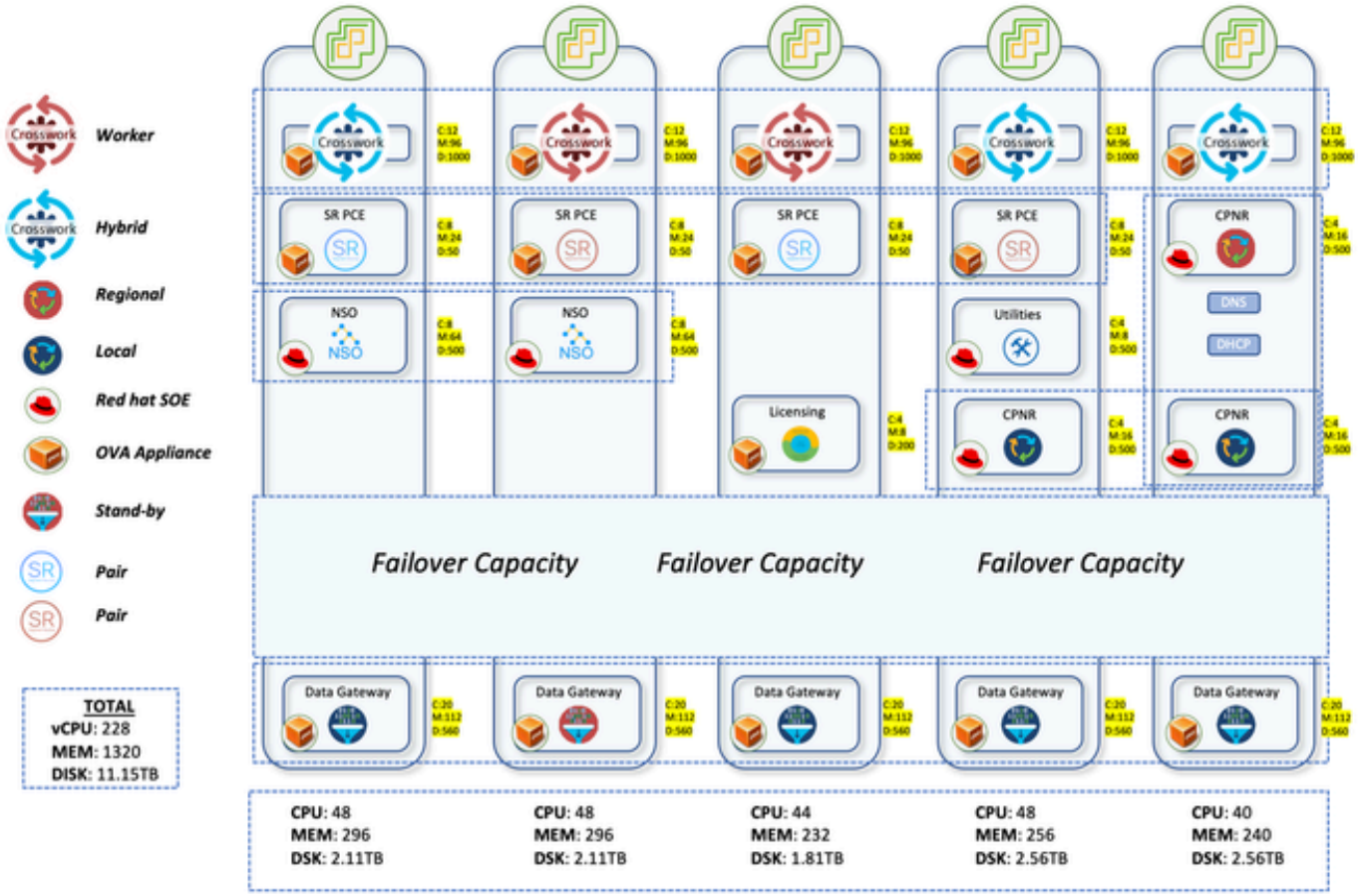
Anche la distribuzione dei dispositivi per i CDG è stata oggetto di molte riflessioni. La distribuzione precedente aveva distribuito casualmente i dispositivi tra i CDG. Ciò ha dato origine ad una distribuzione molto asimmetrica con alcuni CDG che trasportavano più dispositivi, mentre c'erano 1-2 CDG con meno dispositivi. Ciò ha portato a un sovraconsumo e a un sovraccarico di alcuni CDG, mentre altri sono stati sottoforniti.

Il processo di aggiornamento prevedeva la distribuzione di 700 CDG ciascuno ai 4 CDG attivi. In questo modo, nei primi tre CDG sono stati accolti 2100 CFA. I LWR molto pesanti sul fronte di interfaccia erano tutti riservati per il quarto CDG. Anche se erano un numero molto piccolo con un conteggio di 30, questa assegnazione assicurava che anche se fossero state fatte più raccolte da questi dispositivi, non ci sarebbe stato alcun carico pesante sul CDG. Eventuali successive registrazioni di CFA andrebbero anche al 4º CDG. Ciò ha assicurato una distribuzione uniforme nei primi tre CDG con più spazio disponibile nel 4^{esimo} CDG per l'introduzione di nuovi dispositivi.

SR-PCE è stato implementato in 2 coppie, il che significa 4 VM distribuite su diverse macchine host. Una coppia gestisce 7 siti POI e l'altra gli altri 8 siti POI. Gli aggiornamenti della topologia sull'interfaccia utente del CNC vengono eseguiti tramite l'utilizzo di SR-PCE. Apprende la topologia della rete tramite il peer BGP-LS con altri router LWR. Questo componente viene inoltre utilizzato in tutti i casi di utilizzo di ingegneria del traffico in cui svolge il ruolo di controller per indirizzare il traffico su percorsi diversi.

Per gestire tutti i casi di utilizzo del provisioning dei servizi e della configurazione dei dispositivi, l'NSO deve essere utilizzato insieme al CNC. Per la rete di produzione, due NSO con versione 6.4.1.1 sono stati implementati per funzionare in tandem in modalità ad alta disponibilità. SR-PCE (Segment Routing Path Computation Element) è il componente necessario per fornire gli aggiornamenti della topologia a CNC e anche per la gestione dei casi di utilizzo di ingegneria del traffico in tempo reale. Quattro SR-PCE con la versione 25.2.1 sono stati implementati qui con

ciascun PCE che è stato associato a due diversi LWR.



Flusso di lavoro di migrazione da CNC 4.1 a CNC 7.1

Per l'installazione CNC, la scelta preferita era quella di procedere con quella basata sul docker. Tuttavia, poiché il client non ha approvato la configurazione del docker presso la propria sede, non vi era altra opzione se non quella di procedere con l'installazione manuale utilizzando vCenter. L'installazione richiede più tempo rispetto a quella basata su script, in quanto è necessario fornire

più volte gli input nell'interfaccia utente di vCenter.

Una volta completata l'installazione CNC, tutte le applicazioni richieste sono state distribuite con l'unità di business fornito file di installazione di azione automatica che carica e attiva le applicazioni tutte contemporaneamente, riducendo così il tempo necessario per farlo manualmente. È stato implementato il livello Premier che include Crosswork Optimization Engine, Active Topology, Service Health, Element Management Functions, Crosswork Workflow Manager. Insieme a questo, sono stati impostati anche i pacchetti aggiuntivi che includono Change Automation e Health Insight.

CWM e SH non avevano casi di utilizzo. Tuttavia, sono stati implementati poiché erano interessati ad alcuni dei casi di utilizzo offerti da queste applicazioni nella versione successiva.

Una volta installate le applicazioni, il passaggio successivo consisteva nel migrare i dati dalla vecchia versione di CNC. Comprende principalmente profili di credenziali, provider, tag, playbook personalizzati, KPI personalizzati, ruoli, voucher sZTP e altri dati. CNC fornisce l'opzione di esportazione per tutti questi che possono essere utilizzati e poi importati nel nuovo CNC.

Una volta configurati questi elementi, è prudente avviare la migrazione dei dispositivi. In caso di aggiornamenti, se il nuovo CNC viene implementato in una nuova subnet rispetto a quella precedente, è necessario apportare modifiche ACL ai dispositivi per garantire la raggiungibilità con il nuovo CNC. Si tratta di un processo che richiede molto tempo, in quanto richiede l'accesso manuale a ciascun dispositivo e la modifica della configurazione.

Una volta apportate le modifiche agli ACL, il passo successivo è importare i dispositivi nel nuovo CNC e collegarli ai CDG. Se la raggiungibilità è corretta e le credenziali SSH e SNMP sono corrette, i dispositivi vengono mostrati come raggiungibili sul CNC e vengono anche collegati all'NSO (Network Services Orchestrator).

Sul fronte dell'NSO, tutti i pacchetti richiesti devono essere in posizione e operativi per garantire che il CNC possa parlare con l'NSO e viceversa. Ad esempio, per collegare automaticamente i dispositivi all'NSO dal CNC, il pacchetto funzioni DLM è obbligatorio. Analogamente, se l'NSO deve configurare i percorsi dei sensori MDT sul dispositivo, il pacchetto TM-TC deve essere distribuito sull'NSO. In sostanza, a seconda del caso di utilizzo, il pacchetto deve essere distribuito sull'NSO.

Anziché adottare l'approccio manuale per l'installazione dei pacchetti richiesti, in particolare di quelli Transport-SDN, è stato sviluppato uno script automatizzato per il provisioning. Con l'aggiornamento a CNC 7.1, sono stati introdotti aggiornamenti ai pacchetti TSDN. Questi pacchetti aggiornati sono destinati all'installazione sul server NSO per garantire il supporto continuo per il provisioning L2/L3 nell'ambiente aggiornato. Lo script automatizza l'installazione dei pacchetti TSDN aggiornati e carica i metadati necessari nell'NSO, consentendo il provisioning dei

servizi in base alle esigenze.

Su host diversi vengono implementate anche un'istanza del server licenze Cisco Smart Software Manager (SSM) e 3 istanze di Cisco Prime Network Registrar (CPNR).

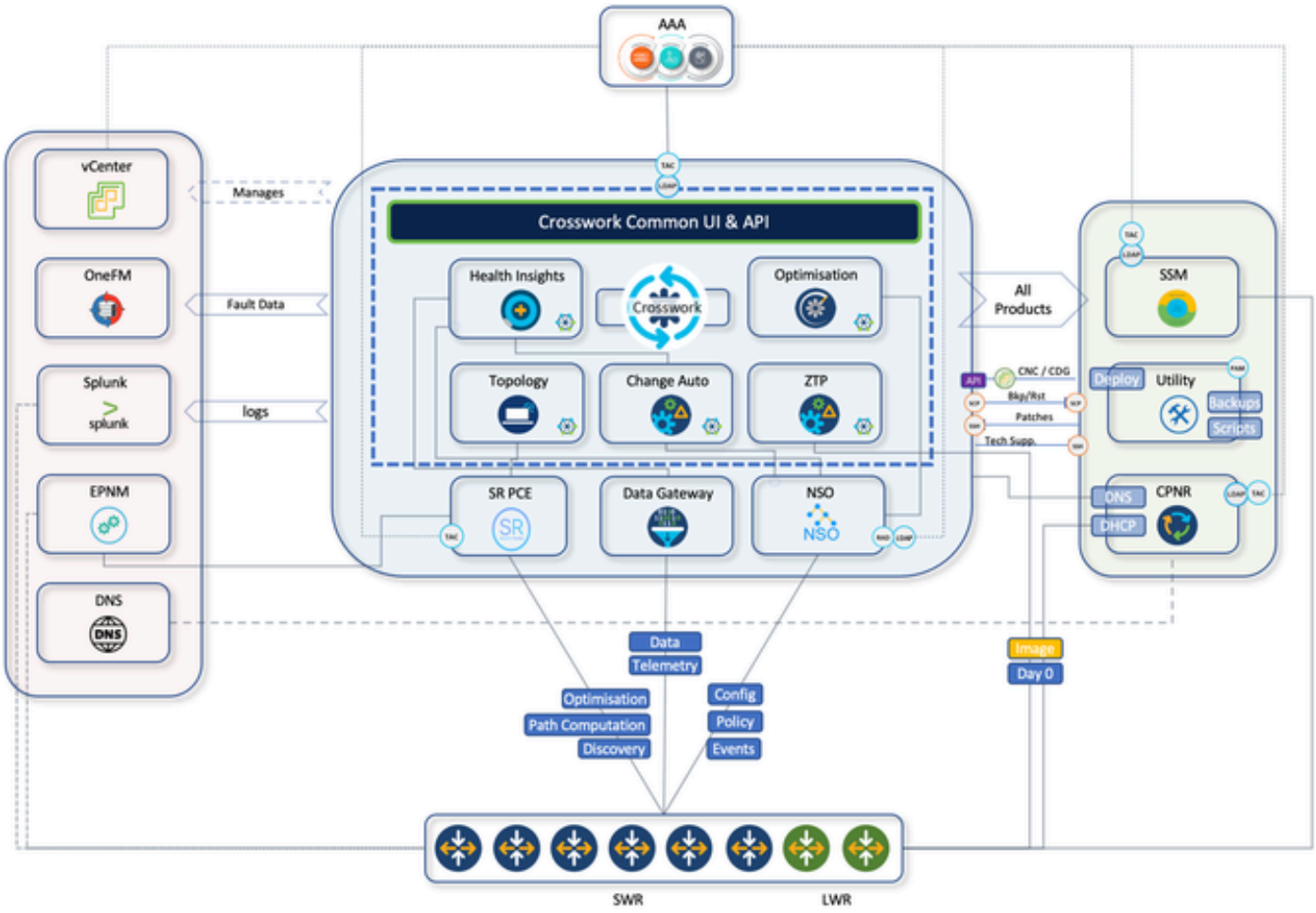
Architettura CNC e integrazione con altri componenti

Il CNC fornisce un'unica piattaforma per il provisioning, l'ottimizzazione e la visualizzazione dei servizi distribuiti tramite un'interfaccia utente unificata. Di seguito è riportato un breve riepilogo dei componenti interni CNC che risiedono nella suite di piattaforme CNC e i casi di utilizzo.

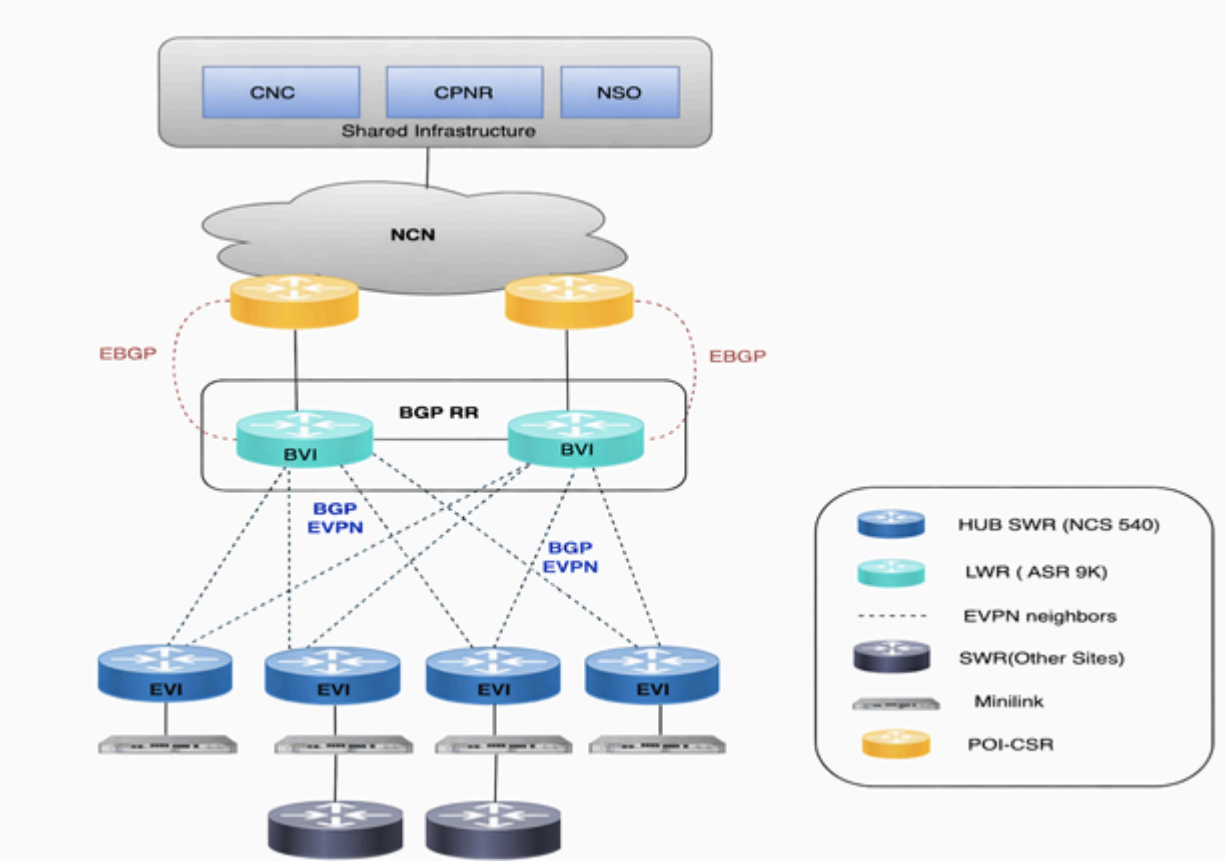
- Crosswork active topology (CAT):
  - Applicazione componente interna distribuita su nodi VM CNC
  - Visibilità end-to-end in tempo reale dell'inventario riconciliato
  - Integrazione delle informazioni di inventario provenienti da più origini dati in un unico schermo
  - Calcolo del percorso di rete del trasporto
  - Individuazione topologia

- Crosswork Optimization Engine (COE):
  - Applicazione componente interna distribuita su nodi VM CNC
  - Ottimizzazione in tempo reale della rete
  - Visualizzazione della topologia in tempo reale
  - Visualizzazioni e provisioning SR-TE
  - Visualizzazione e provisioning RSVP-TE
  - Larghezza di banda su richiesta
- Crosswork health insight (CHI):
  - Applicazione componente interna distribuita su nodi VM CNC
  - Monitoraggio KPI
  - Dashboard avvisi
- Crosswork change automation (CCA):
  - Applicazione componente interna distribuita su nodi VM CNC
  - Strumento Dev-ops con playbook pronti all'uso
  - Pianificazione della capacità di eseguire le riproduzioni all'ora desiderata
  - Collegamento avvisi indicatori KPI HI a riproduzioni suggerite come correzione

Diagramma dell'architettura



Esempio di rete



CNC 4.1 → 7.1 Flusso di lavoro di migrazione dettagliato

Migrazione end-to-end graduale dal precedente CNC 4.1 al CNC 7.1 (lo stesso flusso può essere seguito per qualsiasi aggiornamento CNC indipendentemente dalle versioni)

Pianificazione	Laboratorio	Laboratorio per i clienti	Pronto per la produzione	Distribuzione produzione	Periodo di immersione	Consegna	Smantellar

FASE 1

1 Pianificazione e preparazione

AMBITO E PIANIFICAZIONE	PROGRAMMAZIONE
· Definizione dell'ambito · Pianificazione della capacità	· Identificazione della finestra di modifica · Allineamento delle parti interessate

▾ B

FASE 2

2 Convalida Lab Interna

INFRASTRUTTURA · Creazione CNC 7.1 (ibrido/lavoratori) · Installare le app · Installazione di NSO con HA · Implementazione di coppie SR-PCE	CONVALIDA · Convalida di tutti i casi di utilizzo · Approvazione funzionale

▼ B

FASE 3

3 Convalida laboratorio cliente

CREAZIONE INFRASTRUTTURA · Creazione CNC 7.1 (ibrido/lavoratori) · Installare le app · Installazione di NSO con HA · Implementazione di coppie SR-PCE	MIGRAZIONE DEI DATI · Esportazione di artefatti CNC 4.1 · Ricreazione dei gruppi di dispositivi · Importazione in CNC 7.1 · Distribuire pacchetti NSO	RAGGIUNGIBILITÀ DEL DISPOSITIVO · Aggiornamenti ACL · Importazione di dispositivi e collegamento CDG	SERVIZI E OSSERVABILITÀ · Riconciliazione e sincronizzazione dei servizi · Processi di attivazione e raccolta degli indicatori KPI · Abilitazione script playbook BNM · Osservabilità Hi/Grafana · Integrazione Radius · Integrazione con Splunk · Integrazione con OneFM

			· Abilitazione dei backup CNC

†Esegui ATP in Lab e ottieni l'approvazione

▾ B

FASE 4

4 Fattibilità della produzione

SICUREZZA E ACCESSO · Revisione della sicurezza · Configurazione dei controlli di accesso	INFRASTRUTTURA · Dimensionamento e configurazione delle VM di produzione · Convalida della rete

▾ B

FASE 5

5 Cutover produzione

↻ Ripete tutti i passaggi della Fase 3 nell'ambiente di produzione

CREAZIONE INFRASTRUTTURA · Creazione CNC 7.1 (ibrido/lavoratori) · Installare le app · Installazione di NSO con HA · Implementazione di coppie SR-PCE	MIGRAZIONE DEI DATI · Esportazione di artefatti CNC 4.1 (provider, profili credenziali, playbook, tag) · Ricreazione dei gruppi di dispositivi · Importazione in CNC 7.1 · Distribuire pacchetti NSO	RAGGIUNGIBILITÀ DEL DISPOSITIVO · Aggiornamenti ACL · Importazione di dispositivi e collegamento CDG	SERVIZI E OSSERVABILITÀ · Riconciliazione e sincronizzazione dei servizi · Processi di attivazione e raccolta degli indicatori KPI · Abilitazione playbook BNM · Hi/Grafana, Splunk, OneFM

			· Abilitazione dei backup CNC

†Implementazione della produzione

▾ B

FASE 6

6 Periodo di immersione

MONITORAGGIO · Monitoraggio della stabilità · Prestazioni di base	GESTIONE DEI PROBLEMI · Monitoraggio e risoluzione dei problemi · Processo di escalation

▾ B

FASE 7

7 Documentazione e passaggio di consegne

DOCUMENTAZIONE · MOP, documenti di progettazione e documenti operativi · Diagrammi dell'architettura	CONSEGNA · Sessioni di trasferimento delle conoscenze · Firma di trasferimento

▾ B

FASE 8

8 Smantellare il CNC legacy 4.1

PULIZIA · Scollegare tutti i dispositivi da CDG	ARCHIVIO · Archiviare tutte le esportazioni CNC 4.1

	· Eliminare le voci MDT che fanno riferimento a VM CDG 4.1 · Eliminazione delle VM di produzione	· Audit finale e approvazione

Scenari d'uso

Provisioning dei servizi L2VPN (basato su EVPN)

Il servizio L2VPN fornisce connettività Ethernet di layer 2 su più CAVI, con alcuni servizi ancorati ai CAVI LWR. La topologia attiva CNC viene utilizzata per il provisioning dei servizi, mentre tutta la logica specifica dell'ambiente viene implementata tramite modelli personalizzati NSO.

Il provisioning L2VPN viene trattato come un'attività di configurazione del giorno 2 e richiede attributi del servizio forniti dall'operatore.

Modelli NSO personalizzati

Sono stati creati diversi modelli personalizzati per allinearsi alle convenzioni di denominazione e ai comportamenti di interfaccia specifici dell'ambiente:

- CT-l2vpn-swr-hub-and-lwr
  Gestisce le differenze di denominazione lato hub per bridge -group e bridge -domain su hub SWR e LWR.
- CT-l2vpn-swr-nonhub-100/101/102/105
  Rimuove l'interfaccia uplink ZTP dal gruppo di bridge EVPN e dal dominio di bridge predefiniti per ciascuna VLAN.

Questi modelli garantiscono una configurazione EVPN coerente in tutta la rete e rimuovono le differenze a livello di hardware.

Provisioning del servizio L3VPN (basato su VRF)

Lo Use Case L3VPN consente la fornitura di servizi di livello 3 su più SWR come endpoint. Il provisioning viene eseguito tramite la topologia attiva CNC, con requisiti specifici dell'ambiente implementati utilizzando un modello NSO personalizzato.

Come per L2VPN, questa è un'azione di configurazione del giorno 2, che richiede l'intervento

dell'operatore.

Modello NSO personalizzato

- CT-l3vpn-swr
  Raccoglie i parametri specifici di VRF (numero AS, nome VRF, set di prefissi, nome dei criteri di route, identificatore di route) e crea i criteri di importazione/esportazione BGP necessari, inclusa la ridistribuzione delle route connesse con un criterio di route definito dall'utente.

Progettazione del traffico

L'applicazione Crosswork Optimization Engine (COE) della suite CNC aiuta a controllare i flussi di traffico in rete in base all'intento desiderato.

Esistono due tipi di traffico che richiedono diversi intenti (metriche SLA):

- Traffico TC1 - SLA sensibile alla latenza per garantire che il traffico si trovi sul percorso con la latenza più bassa.
- Traffico TC4 - SLA larghezza di banda minima per garantire che la larghezza di banda dedicata sia sempre disponibile per il traffico TC4

Traffico TC1 (latenza più bassa)

Per garantire che il traffico TC1 venga sempre indirizzato al percorso con latenza più bassa, è necessario creare una policy di routing del segmento (SR) sul file SWR dell'headend con criteri di calcolo del percorso come latenza.

A tal fine, è necessario definire la configurazione On Demand Next Hop (ODN) su ciascun CFA headend per il colore 1001 specifico utilizzando un CNC per facilitare la creazione della policy SR.

Traffico TC4 (larghezza di banda vincolata)

Per garantire che il traffico TC4 sia sempre indirizzato al percorso con larghezza di banda dedicata, è necessario creare una policy SR sul file SWR dell'headend con criteri di calcolo del percorso come larghezza di banda.

Questo obiettivo è conseguito mediante:

- Pacchetto funzioni larghezza di banda su richiesta (BoD) su CNC
- Definizione della configurazione ODN (On Demand Next Hop) su ciascun headend SWR per il colore specifico 1004 mediante la creazione di policy CNC SR con queste configurazioni

Il pacchetto di funzioni BoD viene utilizzato per calcolare il percorso per i criteri SR con larghezza di banda come criterio per il calcolo del percorso. Tiene traccia della larghezza di banda assegnata a una regola e mantiene il monitoraggio del percorso corrente della regola durante il suo ciclo di vita.

In qualsiasi momento, se la patch corrente del criterio BWOD non dispone di capacità sufficiente per soddisfare la larghezza di banda impegnata, ricalcola il percorso del criterio BWOD e instrada nuovamente il criterio al nuovo percorso. Questo reindirizzamento delle policy BWOD è un processo continuo e non richiede alcun intervento manuale.

In un certo senso, il BWOD ottimizza immediatamente la larghezza di banda allo stesso modo in cui l'SR-PCE la ottimizza per la latenza.

Accensione dispositivo con sZTP

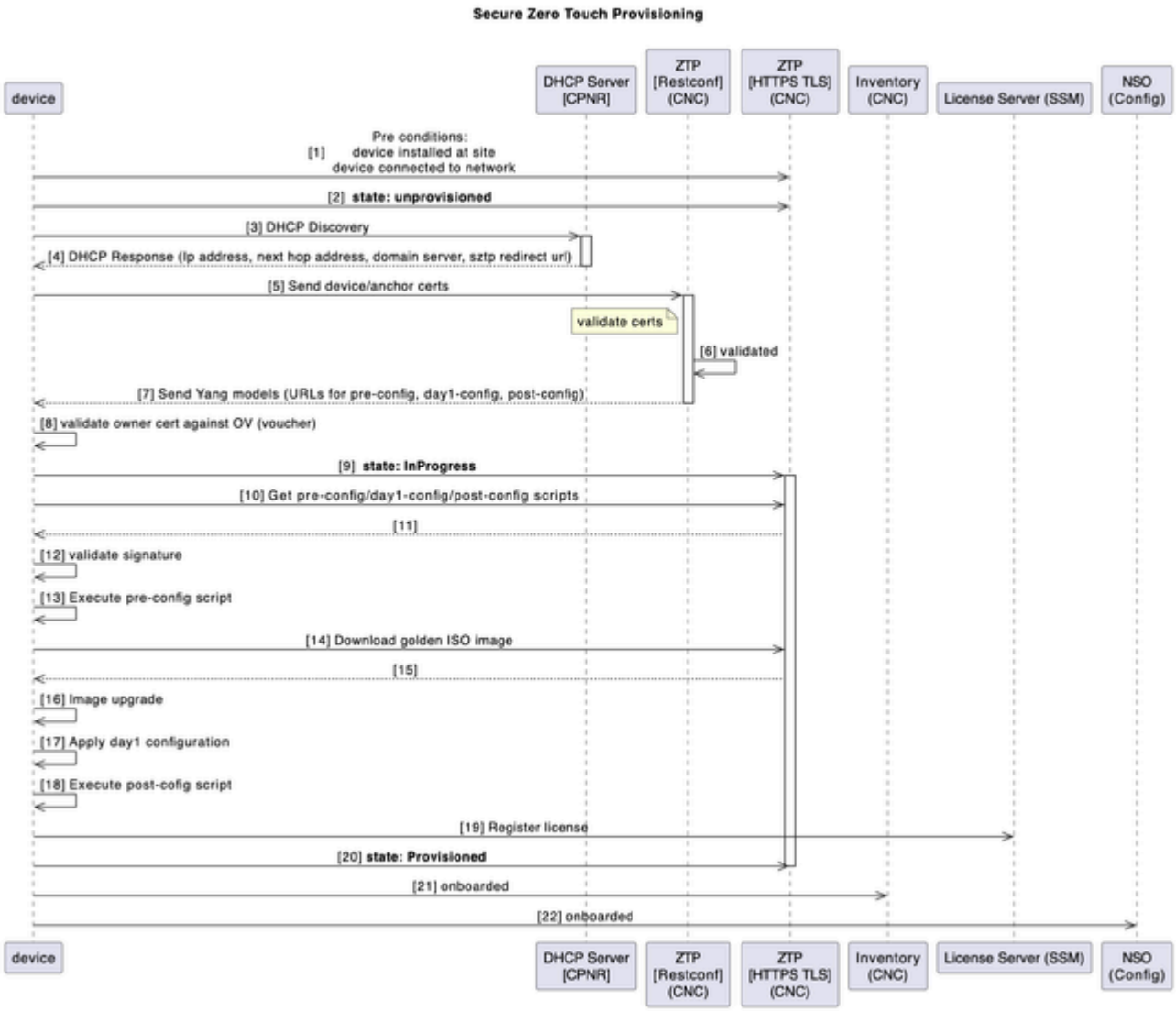
In passato, il processo di installazione di un nuovo dispositivo richiedeva un certo livello di esperienza da parte dell'installatore per installare, configurare e risolvere i problemi relativi all'implementazione di un nuovo componente. Potrebbe inoltre essere necessario un lungo processo di pre-installazione dell'apparecchiatura in un sito remoto, supportato da molte persone che lavorano su parti diverse della soluzione.

Per i nuovi dispositivi SWR da installare nell'ambiente, questo processo di accensione del dispositivo è automatizzato con l'applicazione ZTP (Zero Touch Provisioning) protetta del CNC.

Il flusso di lavoro ZTP viene attivato al primo avvio del dispositivo e scarica l'immagine della piattaforma pianificata e la configurazione iniziale che deve essere applicata senza alcun intervento manuale.

Il dispositivo è anche auto onboarding su CNC per ulteriori orchestrazioni.

Il diagramma mostra il flusso di lavoro del processo ZTP sicuro all'accensione del dispositivo:



Orchestrazione post-ZTP (guidata da automazione)

Un'automazione Python sull'host utility coordina e controlla il processo end-to-end utilizzando un input Excel strutturato (per catena):

- Genera e carica elementi Day-1 e post-config nel CNC.
- Crea prenotazioni CPNR (voci DHCP associate al numero di serie SWR).
- Aggiunge un dispositivo in EPNM (per visibilità/garanzia).
- Manutenzione post-ZTP in CNC:
    - Assegna i CDG (destinazione di telemetria)
    - Collegamento a gruppi di dispositivi e tag
    - Aggiorna latitudine/longitudine per la visualizzazione della topologia
    - Collega il profilo KPI BNM per abilitare il flusso di telemetria

Elaborazione BNM (Bandwidth Notification Message) in CNC

Il SWR può ricevere BNM dallo switch MiniLink nella stessa posizione che corrisponde alla larghezza di banda delle porte WAN. Questi messaggi di notifica sono messaggi CFM basati su standard che includono la larghezza di banda registrata corrente (RBW) e la larghezza di banda configurata massima, nota anche come larghezza di banda nominale (NBW).

La larghezza di banda corrente è l'effettiva larghezza di banda corrente del collegamento WAN a microonde, basata sulle larghezze di banda aggregate dei singoli collegamenti a microonde e i relativi livelli QAM in esecuzione. La larghezza di banda nominale è la larghezza di banda WAN massima configurata, basata sulle larghezze di banda aggregate del QAM massimo configurato su ciascuno dei singoli collegamenti a microonde.

L'ottimizzazione della larghezza di banda viene eseguita in base a questo scenario:

Modifica temporanea (eventi flessibili)

- Quando si verifica un degrado o un'interruzione improvvisa della rete o del collegamento localizzati in SWR (ad esempio, a causa di un evento meteorologico avverso che provoca la perdita del percorso radio delle microonde e la riduzione della larghezza di banda disponibile a causa di cambiamenti negli schemi di modulazione), la correzione del traffic shaping si verifica nel SWR locale sull'interfaccia di rete interessata.
- Questo assicura che si verifichi una perdita minima del pacchetto sul percorso di trasmissione interessato.

Quando un CFA viene abilitato con l'indicatore KPI BNM in un CNC come parte delle attività post-ZTP, il CNC inserisce le configurazioni di telemetria nel CFA.

BNM MDT

basato su modelli di telemetria

destination-group <NomeDGN>

vrf VRF-OMSWR-<indicativo località>1

address-family ipv4 <indirizzo IPv4CDG> porta 9010

codifica gpb autodescrittivo

protocol tcp

!

!

sensor-group <NomeGruppo>

percorso-sensore Cisco-IOS-XR-ethernet-cfm-oper:cfm/nodi/nodo/larghezza di banda-notifiche/larghezza di banda-notifica

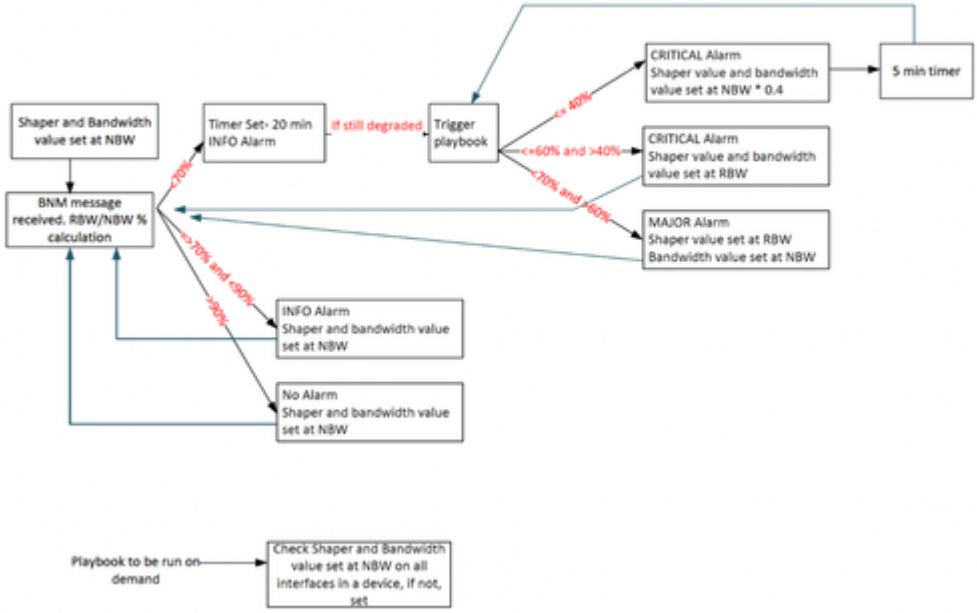
!

Il CNC elabora questi messaggi BNM ricevuti tramite telemetria e, se necessario, intraprende azioni correttive. Ecco i 2 componenti coinvolti nel CNC:

- Health insight (HI): l'applicazione CNC viene utilizzata per acquisire la notifica BNM da un indicatore KPI personalizzato che monitora il percorso specifico del sensore per i messaggi BNM. Health Insight è in grado di generare allarmi nel caso in cui le modifiche della larghezza di banda siano significative e debbano essere implementate.
- Automazione delle modifiche (CA): l'applicazione CNC viene utilizzata per eseguire lo streaming dei messaggi BNM che hanno causato allarmi Hi. 2 playbook personalizzati vengono distribuiti per apportare queste modifiche all'interfaccia interessata:
    - Impostazione dello shaper QoS su un nuovo RBW
    - Impostazione della capacità dell'interfaccia sul nuovo valore RBW.

Uno script Python personalizzato viene sviluppato per eseguire la logica personalizzata ed eseguire automaticamente i playbook CA quando vengono violati gli indicatori KPI HI.

Lo script di attivazione della playbook funziona in base a questo algoritmo:



In questa tabella vengono illustrati i livelli di attenzione personalizzati impostati in base ai gradi di riduzione della larghezza di banda:

Larghezza di banda segnalata = RBW

Larghezza di banda nominale = NBW

Valore intervalli avvisi	Livello di notifica
(RBW/NBW)*100 >=70	Informazioni
(RBW/NBW)*100 <70 e >60	Avviso
(RBW/NBW)*100 <=60	Critico

Questo percorso del sensore è monitorato dal CNC:

Cisco-IOS-XR-ethernet-cfm-oper:cfm/nodi/nodi/notifiche-larghezza di banda/notifiche-larghezza di banda

Un indicatore KPI personalizzato viene creato nel CNC per monitorare il percorso del sensore BNM. Questo indicatore KPI viene aggiunto a un profilo KPI configurato con una cadenza di 120

secondi e soglie di avviso. Collegando i CFA a questo profilo, la configurazione di telemetria richiesta viene automaticamente inviata ai dispositivi tramite NSO.

Una volta abilitati, i dispositivi inviano i dati RBW/NBW ai CDG assegnati all'intervallo configurato. Health Insight (HI) calcola il rapporto RBW - NBW e genera avvisi quando le soglie vengono superate; gli operatori possono monitorare questi eventi in Hi e tramite dashboard Grafana.

Un provider di avvisi nel CNC inoltra questi avvisi al nodo ibrido che ospita l'automazione Python. Lo script analizza i dettagli relativi a dispositivo/interfaccia/RBW/NBW e attiva i playbook di Change Automation appropriati: regolazione dello shaper, aggiornamento della larghezza di banda o entrambi in base alla logica di decisione definita.

Di seguito sono riportati i due playbook utilizzati nel flusso di lavoro:

1. Playbook per modificare il valore della forma

2. Playbook per modificare la larghezza di banda dell'interfaccia

Come già accennato, lo script fa girare un server Web per fungere da provider per comunicare con CNC utilizzando l'API REST. Qualsiasi risposta ricevuta per una richiesta POST viene acquisita qui. Gli avvisi vengono acquisiti nel modulo in JSON e quindi convertiti in dizionario per estrarre i parametri necessari.

Standardizzazione delle operazioni di rete del secondo giorno tramite playbook di automazione personalizzata

I playbook CA (Custom Change Automation) sono stati sviluppati per semplificare e standardizzare le operazioni critiche del secondo giorno durante l'intero ciclo di vita della rete. tra cui il provisioning Bundle-Ether, gli aggiornamenti delle descrizioni dell'interfaccia di gestione, l'orchestrazione a margherita CFM, l'espansione senza problemi della capacità di collegamento, lo smantellamento di eNodeB e l'onboarding efficiente di Mini-Link. Integrando le procedure ottimali operative in workflow riutilizzabili, questi playbook migliorano notevolmente la coerenza dell'esecuzione, riducono al minimo il rischio di errore umano e riducono la dipendenza dagli interventi manuali. Nell'ambito di un upgrade Cisco CNC, questa struttura di automazione svolge un ruolo fondamentale nell'accelerare l'operatività, garantendo la continuità del servizio e abilitando processi scalabili e ripetibili in linea con gli obiettivi di trasformazione della rete moderna.

Continuità di integrazione TACACS+ in aggiornamento Cisco CNC 7.1

Nell'ambito dell'aggiornamento da Cisco CNC 4.1 a 7.1, l'integrazione TACACS+ esistente è stata attentamente preservata per garantire la continuità dell'autenticazione e dell'autorizzazione centralizzate. Il processo di aggiornamento ha convalidato e replicato la configurazione TACACS+ in Cisco CNC 7.1, mantenendo l'allineamento con le policy di sicurezza aziendali e i meccanismi di controllo degli accessi basato sui ruoli (RBAC).

CNC e CDG Syslog inoltro a Splunk

L'inoltro syslog è configurato per inoltrare allarmi/eventi/syslog a un server Splunk. A tale scopo è stata utilizzata la funzionalità preconfigurata del CNC per l'installazione del server syslog.

Inoltro di allarmi a OneFM

Gli allarmi CNC vengono inoltrati anche ad un sistema in direzione nord come OneFM, utilizzando l'API CNC restconf orientato alla connessione:

```
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.
```

Automazione dei backup giornalieri CNC

Uno script automatizzato utilizza l'API di backup CNC per eseguire il backup completo del CNC e memorizza il file di backup nell'host dell'utilità. Questa operazione viene eseguita giornalmente.

Sfide

Grande salto nella versione Crosswork

L'aggiornamento da Cross work 4.4 a 7.1 ha rappresentato un significativo salto di versione piuttosto che un aggiornamento incrementale di routine. Un salto di tale portata ha introdotto numerose nuove funzioni in più applicazioni, oltre a sostanziali miglioramenti e modifiche architetturali. Per questo motivo, l'aggiornamento del CNC non è stato solo una semplice sostituzione della versione, ma ha richiesto una convalida completa per garantire compatibilità, stabilità e funzionalità adeguate in tutti i componenti integrati. L'ampliamento della serie di

funzionalità e i relativi miglioramenti hanno fatto sì che i workflow, le configurazioni e le integrazioni esistenti richiedessero un'attenta verifica, rendendo il testing e la convalida completi fondamentali per il successo dell'upgrade.

Nessun aggiornamento sul posto

Il CNC non supporta un modello di aggiornamento sul posto. Al contrario, gli aggiornamenti devono seguire un approccio "lift-and-shift", in cui l'implementazione esistente viene preservata mentre un ambiente completamente nuovo viene creato da zero con la versione di destinazione. Una volta installato il nuovo sistema, le configurazioni, i dati e le integrazioni devono essere attentamente migrati e convalidati prima di poter rimuovere le autorizzazioni dall'ambiente precedente.

Questo approccio introduce diverse sfide operative:

- Ambienti paralleli: Sia il vecchio che il nuovo ambiente CNC devono essere eseguiti contemporaneamente fino al completamento della migrazione e della convalida.
- Pressione delle risorse hardware: L'esecuzione in parallelo di due ambienti completi aumenta in modo significativo la richiesta di risorse di elaborazione, storage e rete, che possono sovraccaricare l'infrastruttura disponibile.
- Risorsa di convalida estesa: Tutti i dati, le configurazioni, i criteri e le integrazioni migrati devono essere verificati nella nuova versione per garantire che funzionino esattamente come previsto.
- Complessità della migrazione dei dati: Il trasferimento di dati cronologici, configurazioni delle applicazioni e impostazioni operative richiede un'attenta pianificazione per evitare incoerenze o perdite di dati.
- Disattivazione ritardata: Il sistema precedente e le relative VM non possono essere eliminati finché la nuova implementazione non viene dimostrata stabile, prolungando l'utilizzo delle risorse e il sovraccarico operativo.
- Coordinamento operativo: I team devono gestire la sincronizzazione tra entrambi gli ambienti durante il periodo di transizione per evitare deviazioni della configurazione o interruzioni operative.
- Conflitti di automazione a loop chiuso: Il CNC supporta casi di utilizzo dell'automazione a loop chiuso che attivano dinamicamente azioni basate su condizioni di rete in tempo reale. Quando sia il controller precedente che quello nuovo sono attivi durante la transizione, esiste il rischio che la stessa logica di automazione possa essere eseguita da entrambi i controller, con il rischio di causare modifiche di configurazione duplicate o azioni in conflitto nella rete. Ciò richiede un attento controllo delle regole di automazione durante la finestra di migrazione.
- I dati operativi legacy, inclusi gli allarmi cronologici, gli eventi, i record di errore e le informazioni di audit, non vengono migrati nel nuovo ambiente a causa dell'assenza di funzionalità di esportazione native. Di conseguenza, questi dati cronologici non sono disponibili nel sistema aggiornato e devono essere trattati come non recuperabili dopo la migrazione.

A causa di questi fattori, il modello lift-and-shift rende gli aggiornamenti CNC più complessi dal punto di vista operativo e delle risorse rispetto a un aggiornamento standard sul posto.

Problemi di distribuzione senza opzioni di rollback

Alcuni errori di configurazione di distribuzione e post-distribuzione nel CNC non dispongono di un percorso di correzione e richiedono un ripristino completo del cluster. Ad esempio, un FQDN non corretto configurato per Crosswork Data VIP , obbligatorio per lo Use Case sZTP, ha reso sZTP non funzionante. Poiché questo valore non può essere corretto dopo la distribuzione, è necessaria una ridistribuzione completa.

Analogamente, non è stato possibile correggere la configurazione errata delle credenziali di override del dispositivo in Change Automation dopo la distribuzione, determinando la ricostruzione di un altro cluster. Anche altri errori, quali la configurazione errata degli IP dei gateway o delle definizioni delle subnet, vengono identificati come non recuperabili.

Questi scenari evidenziano l'importanza critica della convalida di tutti i parametri non modificabili durante la distribuzione iniziale. Una pianificazione meticolosa e una verifica accurata degli input sono essenziali per evitare l'impatto di costose rilavorazioni e programmazioni.

Vincoli della convalida diagnostica post-distribuzione

Il CNC fornisce un'utilità di diagnostica per valutare i parametri di integrità a livello di VM, quali latenza di lettura/scrittura su disco, IOPS, latenza di sincronizzazione, velocità dell'interfaccia di rete e frequenza di clock della CPU. L'utility riporta i valori misurati rispetto alle soglie previste e contrassegna ogni controllo come superato o non riuscito. Tuttavia, queste operazioni di diagnostica possono essere eseguite solo dopo l'installazione del cluster, senza lasciare alcun meccanismo per convalidare la fattibilità dell'infrastruttura prima dell'installazione.

Durante l'installazione, il flag "Ignore Diagnostic Checks" (Ignora controlli diagnostici) è impostato su false per impostazione predefinita. In pratica, se un singolo controllo ha esito negativo, l'Installer si interrompe, impedendo l'avanzamento dell'installazione. Di conseguenza, i tecnici sul campo sono spesso costretti ad attivare questo flag e a ignorare completamente la diagnostica, in quanto anche gli ambienti di produzione spesso non superano uno o più controlli. Questo crea un dilemma operativo: i team devono scegliere tra l'implementazione di una convalida rigorosa che blocchi l'installazione o l'esecuzione di un'operazione senza la garanzia che l'infrastruttura sottostante soddisfi i benchmark delle prestazioni consigliati.

Modifica procedura creazione indicatore KPI personalizzato HI

In Health Insight 4.1, la creazione di KPI personalizzati si basava sulla logica dello script Tick, in cui le definizioni KPI e la logica di elaborazione venivano implementate utilizzando gli script all'interno del framework Tick. Tuttavia, nella versione 7.1, questo approccio è stato sostituito da un framework basato su file di rilevamento per la definizione e la gestione degli indicatori KPI.

A causa di questa modifica dell'architettura, gli indicatori KPI personalizzati esistenti non possono essere riutilizzati direttamente e richiedono una rielaborazione per l'allineamento con il nuovo formato del file di rilevamento. Ciò ha richiesto molto tempo e sforzi per:

- Comprendere il nuovo framework: Il team ha dovuto studiare la struttura, la sintassi e il comportamento operativo del modello di definizione degli indicatori KPI basato su file di tracciamento introdotto nella versione 7.1.
- Riprogettare la logica esistente: La logica implementata in precedenza negli script Tick doveva essere tradotta e adattata nel formato di file tracker.
- Ricrea indicatori KPI BNM: È stato necessario ricreare l'indicatore KPI BNM personalizzato utilizzando il nuovo framework per garantire che producesse gli stessi risultati e informazioni dettagliate di prima.
- Convalida precisione indicatore KPI: È stata richiesta una convalida completa per confermare che le nuove implementazioni generano metriche coerenti e corrette rispetto alla versione precedente.
- Test e ottimizzazione: Il nuovo modello ha inoltre richiesto la verifica delle prestazioni e del comportamento in condizioni reali di rete, seguita da eventuali modifiche.
- Mancanza di supporto: Alcune funzionalità che funzionavano in precedenza con lo script tick non erano più supportate con la nuova implementazione del file tracker. Quindi, bisognava scendere a dei compromessi.

Questo cambiamento nel meccanismo di creazione degli indicatori KPI ha notevolmente aumentato lo sforzo richiesto durante l'upgrade, poiché ha comportato sia l'apprendimento di un nuovo sistema che la reimplementazione della logica di monitoraggio personalizzata esistente per garantire la continuità delle informazioni operative.

Timeout API in script trigger playbooks BNM

I playbook BNM vengono attivati tramite uno script personalizzato che interagisce con le API CNC. Durante il processo di aggiornamento e convalida, sono stati identificati e risolti diversi problemi relativi all'autenticazione API e alla gestione delle risposte.

Il token API CNC ha una validità di 8 ore, ma lo script originale non include la logica corretta per aggiornare il token una volta scaduto. Di conseguenza, sebbene gli allarmi KPI nel CNC 4.4

funzionassero correttamente, lo script di attivazione del playbook cessò di essere eseguito dopo la scadenza del token. Questo problema è passato inosservato per un lungo periodo, il che significa che lo script di automazione non era stato effettivamente eseguito in modo affidabile per più di un anno. Il problema è diventato visibile solo durante le attività di migrazione e convalida del CNC 7.1.

Sono stati pertanto necessari diversi miglioramenti e perfezionamenti:

- Logica di aggiornamento token: È stata implementata la logica corretta per rilevare la scadenza del token e aggiornare automaticamente il token API, garantendo l'esecuzione ininterrotta dello script.
- Modifiche alla risposta API: Le differenze tra le versioni CNC hanno causato problemi aggiuntivi. In CNC 4.1, una risposta token scaduta conteneva in genere il messaggio "scaduto", mentre in CNC 7.1, la risposta restituisce "Chiave non autorizzata". È stato necessario aggiornare la logica dello script per interpretare correttamente i nuovi modelli di risposta in 7.1.
- Gestione token globale: In precedenza, i token venivano archiviati e utilizzati localmente all'interno delle funzioni. Questo ha creato scenari in cui il token era valido quando si immette una funzione, ma è scaduto prima delle successive chiamate API. L'implementazione è stata modificata in modo da utilizzare la gestione globale dei token, garantendo coerenza e un aggiornamento corretto di tutte le funzioni.
- Gestione degli errori migliorata: In alcuni casi, l'API "check sync" dell'NSO ha restituito risposte incomplete o diverse dalla struttura prevista. Ciò ha causato eccezioni KeyError che hanno sospeso l'esecuzione dello script. Sono state introdotte ulteriori regole di gestione e convalida delle eccezioni in modo che lo script possa continuare a essere eseguito anche quando vengono ricevute risposte API impreviste.
- Miglioramenti della stabilità dello script: Sono state aggiunte misure di protezione e controlli aggiuntivi per garantire che errori API, problemi di risposta temporanei o eventi di aggiornamento del token non causino l'interruzione imprevista dello script.

Questi miglioramenti non solo hanno risolto i problemi scoperti durante l'upgrade, ma hanno anche migliorato significativamente l'affidabilità, la resilienza e la manutenibilità del framework di automazione dei playbook BNM.

Modifica alla progettazione del trigger di elaborazione e playbook BNM

La logica di automazione BNM è basata sugli eventi e si basa sugli avvisi generati dagli indicatori KPI nell'applicazione Health Insight all'interno di CNC. Il flusso di lavoro complessivo funziona come segue:

1. Il CNC legge i valori NB (Nominal Bandwidth) e RBW (Real Bandwidth) dal dispositivo.
2. Calcola il rapporto larghezza di banda (BW%) utilizzando questi valori.

3. L'indicatore prestazioni chiave di Health Insight valuta questo rapporto rispetto alle soglie di allarme predefinite.
4. Quando viene generato un avviso, lo script di attivazione del playbook BNM rileva l'avviso ed esegue i playbook correttivi corrispondenti

Limitazione nella progettazione originale degli avvisi

Soglie di avviso configurate:

- BW% < 60 → Critico
- 60 ≤ BW% ≤ 70 → Avvertenza
- BW% > 90 → Info

Questo design ha funzionato bene per identificare la riduzione della larghezza di banda, ma ha creato un gap funzionale durante gli scenari di recupero della larghezza di banda. In particolare, per l'intervallo 70-90% non è stato definito alcun livello di avviso.

Questo ha portato a questo comportamento:

- Quando BW% scende al di sotto del 70%, viene generato un allarme critico o di avvertenza, che attiva playbook che regolano i valori di shaper e larghezza di banda.
- Tuttavia, quando la larghezza di banda è stata ripristinata e la percentuale di larghezza di banda è aumentata oltre il 70%, l'indicatore KPI non ha generato alcun avviso perché il valore è sceso nella banda del 70-90% senza alcun livello di avviso associato.
- Poiché lo script di automazione BNM dipende interamente dalla generazione di avvisi per attivare le azioni, non ha avuto la possibilità di leggere i valori NBW/RBW aggiornati o avviare azioni di ripristino.
- Di conseguenza, il ripristino della larghezza di banda non è stato eseguito automaticamente, anche se era disponibile una larghezza di banda sufficiente. Non c'era una logica di restauro anche nel progetto originale.

Questa limitazione è diventata visibile nella rete di produzione, dove i collegamenti che in precedenza avevano subito una riduzione della larghezza di banda rimanevano in uno stato di restrizione anche dopo il miglioramento delle condizioni.

Impatto della modifica della struttura degli indicatori KPI

Il problema è stato ulteriormente aggravato dalla modifica del framework introdotta nel CNC 7.1. In Health Insight 4.1, l'implementazione di indicatori KPI basati su Tick ha supportato fino a cinque livelli di allarme, consentendo un controllo più accurato delle bande di soglia e rendendo più facile l'implementazione della logica di ripristino.

Tuttavia, nel CNC 7.1, il framework KPI basato su file di rilevamento supporta solo tre livelli di avviso, il che ha ridotto la flessibilità nella definizione di più soglie di recupero e ha richiesto la riprogettazione della logica di avviso per adattarla a questi vincoli.

Attivazione eccessiva playbook

Un altro problema identificato nell'implementazione originale era la frequenza estremamente elevata di esecuzioni di playbook. La logica di automazione non include alcun tempo di attesa o finestra di stabilizzazione. Non appena il CNC legge un valore dal dispositivo che soddisfa la condizione di avviso:

- L'allerta è stata immediatamente attivata.
- Lo script di automazione ha immediatamente attivato i playbook correttivi.

Poiché i valori di telemetria fluttuano frequentemente nelle reti in tempo reale, questo provocava l'attivazione di centinaia di playbook ogni ora, il che non era ideale dal punto di vista della stabilità della rete e delle prestazioni delle applicazioni.

Logica di automazione riprogettata

Per superare questi limiti, la progettazione dell'automazione BNM è stata rielaborata con diversi miglioramenti:

- Logica di soglia di avviso rivista: Per garantire che la banda di recupero sia stata acquisita entro i tre livelli di alert, la logica è stata modificata in modo che qualsiasi % della larghezza di banda superiore al 70% venga ora considerato come un alert di livello INFO, sostituendo l'approccio precedente in cui solo i valori superiori al 90% sono stati classificati come INFO. Ciò ha garantito il monitoraggio attivo della banda di ripristino del 70-90%, consentendo l'attivazione dei playbook di ripristino in caso di miglioramento delle condizioni di larghezza di banda.
- Introduzione del tempo di attesa: È stato introdotto un meccanismo di tempo di attesa di 20 minuti per garantire che le condizioni di larghezza di banda rimangano stabili per una determinata durata prima di attivare i playbook. In questo modo si evita che l'automazione reagisca alle fluttuazioni a breve termine.
- Esecuzione controllata di playbook: Con la nuova logica e il tempo di attesa, la frequenza delle esecuzioni dei playbook si è ridotta drasticamente, impedendo azioni di automazione non necessarie.
- Meccanismo di richiamo per una degradazione grave: Nei casi di grave degradazione della larghezza di banda, è stato introdotto un approccio di potenziamento. In questi scenari, l'automazione regola proattivamente l'allocazione della larghezza di banda e della riduzione del traffico al 40% della NBW, consentendo un ripristino più rapido dalla congestione.
- Maggiore stabilità dell'automazione: Il flusso di lavoro riprogettato garantisce che gli scenari

di riduzione e ripristino della larghezza di banda siano gestiti in modo efficace, anche entro i limiti del framework KPI basato su tracker.

Risultato

Con queste modifiche progettuali, combinate con i precedenti miglioramenti nella gestione delle API, nella gestione dei token e nella solidità degli script, la struttura di automazione BNM ora funziona in modo molto più stabile, efficiente e prevedibile. Il sistema è in grado di rispondere correttamente sia alle condizioni di congestione che di ripristino, evitando un numero eccessivo di esecuzioni di playbook e assicurando un'ottimizzazione affidabile della larghezza di banda della rete.

Eliminazione avvisi dispositivi

Nel CNC 4.1, gli allarmi sono stati inoltrati ad un sistema in direzione nord chiamato OneFM attraverso un'API RESTCONF. Poiché lo stack CNC 4.1 non includeva la funzionalità EMF, la piattaforma generava solo allarmi a livello di sistema. Questi allarmi sono stati inoltrati a monte senza alcuna complessità relativa alla classificazione.

Con l'installazione di CNC 7.1, è stata introdotta l'applicazione EMF, ampliando significativamente il modello di allarme. Gli allarmi sono stati ora suddivisi in tre categorie:

- Allarmi di sistema - relativi allo stato della piattaforma CNC e dell'applicazione
- Allarmi di rete - relativi alle condizioni del servizio di rete
- Allarmi sui dispositivi - generati direttamente dai dispositivi di rete e inoltrati tramite CNC

Tuttavia, esisteva già un EPNM responsabile della raccolta e della gestione degli allarmi a livello di dispositivo. Se anche il CNC inoltrava questi allarmi a OneFM, ciò provocava la ricezione di doppi allarmi da entrambi i sistemi. Pertanto, il requisito era quello di escludere gli allarmi dei dispositivi dal CNC mentre ancora inoltrava gli allarmi del sistema e della rete.

La sfida principale era una limitazione dell'API RESTCONF northbound utilizzata per inoltrare gli allarmi a OneFM. L'API non supporta il filtro degli allarmi in base alla categoria dell'allarme. Se tale filtraggio fosse stato disponibile, la soluzione sarebbe stata semplice: è sufficiente escludere gli allarmi dei dispositivi a livello API prima di inoltrarli al sistema in direzione nord.

Sono state valutate e discusse diverse possibili soluzioni:

- Interruzione dei trap all'origine: Impedire ai dispositivi di inviare trap al CNC.

- Filtraggio degli allarmi sul sistema in direzione nord (OneFM): Consenti al CNC di inviare tutti gli allarmi ma filtra gli allarmi del dispositivo all'interno di OneFM.
- Filtraggio all'interno del CNC prima dell'inoltro degli allarmi.

Non è stato possibile arrestare le trap a livello di dispositivo perché il CNC si basa su tali trap per rilevare gli eventi del dispositivo e mantenere la consapevolezza operativa delle condizioni della rete. La disattivazione delle trap ridurrebbe in modo significativo la capacità del CNC di rispondere ai problemi della rete.

L'implementazione finale della soluzione si è basata su una funzionalità CNC integrata chiamata soppressione degli allarmi dei dispositivi. Questa funzione consente agli amministratori di eliminare determinati tipi di allarmi dei dispositivi in base ai gruppi di dispositivi, impedendo loro di essere elaborati o inoltrati ulteriormente a monte.

Configurando i criteri di soppressione degli allarmi dei dispositivi, il sistema è stato in grado di:

- Sopprimere gli allarmi generati dal dispositivo all'interno del CNC.
- Continuare l'elaborazione e l'inoltro degli allarmi di sistema e di rete.
- Impedire che gli allarmi dei dispositivi duplicati raggiungano il sistema OneFM.

Questo approccio ha fornito una soluzione pulita e scalabile senza compromettere la capacità del CNC di ricevere trappole dai dispositivi. Di conseguenza, il flusso di allarmi verso OneFM è stato semplificato, garantendo che solo gli allarmi di sistema e di rete rilevanti siano stati inoltrati, evitando la duplicazione con la gestione degli allarmi dei dispositivi di EPNM.

Modifiche fuori banda

Nell'installazione esistente, il team operativo si basava spesso su script diretti basati su CLI per eseguire il push degli aggiornamenti della configurazione ai dispositivi di rete, in particolare per attività quali le modifiche ACL e le attività di debug. Anche se efficace nel breve termine, questo approccio ha portato a una deviazione della configurazione, in quanto le modifiche effettuate al di fuori dell'NSO non sono state tracciate all'interno del sistema. Di conseguenza, i flussi di lavoro di provisioning NSO sono stati influenzati da incoerenze tra lo stato previsto (modellato) e le configurazioni effettive dei dispositivi, con conseguenti guasti e inefficienze operative.

Riconciliazione VPN L2/L3

Modifiche alla configurazione fuori banda: il team di rete ha aggiornato la configurazione VPN su dispositivi esterni al CNC/NSO e al flusso di lavoro TSDN. Di conseguenza, lo stato memorizzato in NSO (dall'era CNC 4.1) non sempre corrispondeva allo stato sui dispositivi.

Queste discrepanze hanno causato più errori e incoerenze di riconciliazione. In diversi casi, NSO conteneva dati del servizio VPN che non esistevano più sui dispositivi (o erano stati modificati in un modo che NSO non rifletteva). Per allineare NSO alla rete, è stato necessario rimuovere le voci del servizio VPN presenti solo in NSO e non sui dispositivi e correggere altre mancate corrispondenze causate da modifiche fuori banda.

Impatto sulla programmazione

La risoluzione di questi problemi ha richiesto circa due settimane in più rispetto al piano di riconciliazione originale. Il tempo aggiuntivo è stato impiegato per identificare le mancate corrispondenze, convalidare lo stato del dispositivo e pulire o correggere in modo sicuro i dati CDB NSO.

Osservazioni

1. Autorità di configurazione: Le modifiche fuori banda apportate alla configurazione VPN (o a qualsiasi configurazione gestita da TSDN) creano uno scostamento tra l'NSO e la rete e complicano la riconciliazione.
2. Base di riferimento pre-migrazione: Una linea di base chiara dello stato gestito da NC/NSO rispetto a quello gestito solo dal dispositivo prima della migrazione avrebbe semplificato il rilevamento e la risoluzione delle discrepanze.
3. Automazione e conversione: Gli script di conversione del payload e le personalizzazioni specifiche dell'utente erano essenziali per gestire in modo coerente le differenze di formato e modello tra 4.1 e 7.1.

Suggerimenti per aggiornamenti simili

1. Imponi un blocco delle modifiche per i servizi VPN (e altri servizi gestiti da TSDN) durante la finestra di riconciliazione, con eccezioni solo tramite un processo controllato.
2. Eseguire un controllo di pre-riconciliazione confrontando il CDB NSO con la configurazione del dispositivo per quantificare ed elencare le discrepanze prima di avviare la riconciliazione.
3. Documentare e socializzare che le modifiche VPN devono passare attraverso CNC/NSO TSDN post-aggiornamento per evitare il ripetersi di deviazioni fuori banda.
4. Conservare gli script di conversione e riconciliazione per riutilizzarli in aggiornamenti futuri o per la risoluzione dei problemi.

Backup CNC non riuscito a causa delle dipendenze della modalità di manutenzione

Il meccanismo di backup CNC richiede che la piattaforma venga messa in modalità di manutenzione prima di poter avviare un'operazione di backup. In base alla progettazione, l'API di

backup applica questo prerequisito; se il CNC non passa alla modalità di manutenzione, il processo di backup viene interrotto automaticamente.

In pratica, l'attivazione della modalità di manutenzione spesso non è riuscita a causa di attività di sistema in corso, tra cui:

- Esecuzioni MOP (Change Automation playbook) attive
- Workflow sZTP in corso
- Operazioni del servizio DLM
- Attività di collegamento o scollegamento del profilo KPI
- Raccolte showtech su richiesta
- Attività orchestrazione in background

La presenza di tali attività impedisce al CNC di entrare in modalità di manutenzione, causando il fallimento dell'operazione di backup prima dell'esecuzione.

Impatto operativo

I backup giornalieri CNC richiesti per la conformità e la garanzia operativa. Tuttavia, le frequenti attività di automazione, in particolare i playbook attivati da BNM, impedivano al sistema di entrare in modalità manutenzione. Di conseguenza, gli errori di backup si sono verificati ripetutamente, creando un rischio operativo significativo e richiedendo l'intervento manuale.

Strategia di mitigazione

1. Ottimizzazione della pianificazione del backup: è stata identificata una finestra di manutenzione con attività di sistema minima. In base all'analisi del traffico e dell'automazione, il processo di backup è stato pianificato per le 5:00 AM (AEST), quando l'orchestrazione e l'esecuzione del playbook avevano meno probabilità di essere attivi.

2. Convalida dell'attività di pre-backup: è stato introdotto un pre-controllo automatico prima di richiamare l'API di backup:

- Lo script esegue una query sulle API CNC per rilevare l'esecuzione dei processi MOP di Change Automation.
- Se un processo viene segnalato come In esecuzione, lo script attende 5 secondi e riprova.
- Questo ciclo continua finché il sistema non segnala alcun processo attivo.
- Solo dopo la conferma dell'inattività dell'ambiente, lo script tenta di attivare la modalità di manutenzione e attivare il backup.

In questo modo è stato possibile evitare tentativi di backup non necessari quando il sistema era in uno stato operativo occupato.

3. Meccanismi di nuovi tentativi e resilienza: per adattarsi a stati di sistema transitori, sono state aggiunte garanzie aggiuntive:

- Fino a tre tentativi se l'API di backup restituisce un errore
- Intervalli di ritardo brevi tra i tentativi
- Gestione accurata degli errori per evitare la terminazione dello script

Risultati e risultati

L'attenuazione combinata ha migliorato notevolmente l'affidabilità dei backup:

- Riduzione drastica degli errori di backup
- Dopo l'implementazione, sono stati osservati solo due errori, entrambi causati da un processo sZTP bloccato, che è al di fuori del controllo dello script.
- L'introduzione di ritardi di esecuzione nell'automazione del playbook BNM ha ulteriormente ridotto la contesa con la modalità di manutenzione.

Inoltro dei syslog a Splunk

La destinazione syslog è stata configurata nel CNC per l'inoltro dei log a Splunk su TLS. Tuttavia, una volta ricevuti, i log erano illeggibili sul lato Splunk. A causa di questo problema generato dall'ambiente Splunk, è stata scelta l'opzione di ripristinare il trasporto UDP, dopo di che i log sono stati elaborati correttamente.

Problema di migrazione raggruppamento dispositivi

L'utente ha creato in precedenza 18 gruppi di dispositivi in CNC 4.1; tuttavia, tale release non forniva alcun meccanismo basato su UI o su API per esportare o importare gruppi di dispositivi. Di conseguenza, la migrazione di questi gruppi al CNC 7.1 richiedeva un approccio non standard. Sono state identificate due API CNC interne: una espone la gerarchia dei gruppi di dispositivi e un'altra elenca i dispositivi mappati a ciascun nodo della gerarchia. Utilizzando queste API, tutti i gruppi di dispositivi e i dispositivi associati sono stati estratti e archiviati come output JSON. È stato quindi sviluppato uno script personalizzato per analizzare le risposte ed estrarre solo i nomi host dei dispositivi da ciascun gruppo.

Il CNC 7.1 ha introdotto funzionalità native di importazione/esportazione per i gruppi di dispositivi, tra cui un modello di importazione basato su CSV. Dopo aver estratto i nomi host dal sistema legacy, è stato creato un secondo script di automazione per popolare i modelli CSV nel formato richiesto, garantendo che ogni gruppo di dispositivi potesse essere importato in modo accurato e indipendente. Questa automazione era essenziale; senza di essa, la migrazione dei gruppi di dispositivi al CNC 7.1 sarebbe stata molto più lunga e complessa dal punto di vista operativo.

Isolamento dei dispositivi con una larghezza di banda notevolmente ridotta

Nonostante l'implementazione del caso di utilizzo BNM per correggere automaticamente rapporti RBW/NBW bassi, un sottoinsieme di dispositivi ha continuato a rimanere in stato di grave degrado per lunghi periodi. Sebbene i playbook di regolazione della larghezza di banda e della shaper in genere ripristinassero i dispositivi subito dopo gli eventi di degradazione, diversi dispositivi persistevano in uno stato Critico per più di una settimana e richiedevano un intervento manuale. L'identificazione di questi dispositivi, tuttavia, ha presentato una sfida. Mentre l'interfaccia utente CNC fornisce una chiara visualizzazione degli allarmi e delle metriche della larghezza di banda, non rivela facilmente i dispositivi che sono rimasti esclusivamente in uno stato Critico per un intervallo prolungato.

Per colmare questa lacuna operativa, è stata sviluppata una soluzione basata su API. Il CNC offre un'API che recupera un elenco dei dispositivi che generano allarmi più in alto su intervalli di tempo configurabili (ad esempio, 7 giorni, un mese). Ottenendo questi dati e filtrando i dispositivi che hanno generato solo avvisi critici durante il periodo selezionato, il team è stato in grado di isolare rapidamente i dispositivi che richiedono interventi di ripristino manuali. Questo approccio automatizzato ha migliorato in modo significativo l'efficienza della risoluzione dei problemi e ridotto il tempo necessario per identificare i casi di deterioramento persistente.

Rimozione configurazione telemetria dispositivo

Nel CNC 4.1, le configurazioni di telemetria inviate dall'NSO tramite il pacchetto temm-tcfunction sono state applicate automaticamente quando un dispositivo è stato associato a un profilo KPI di Health Insight (HI). Tuttavia, queste configurazioni, inclusi i riferimenti VIP CDG, non sono state rimosse quando il profilo KPI è stato successivamente scollegato. Di conseguenza, i dispositivi hanno accumulato nel tempo voci di telemetria obsolete e ridondanti.

Questo problema divenne più evidente durante l'aggiornamento a CNC 7.1. I dispositivi spesso mantenevano le precedenti configurazioni di telemetria VIP CDG da CNC 4.1 insieme alle nuove voci generate da CNC 7.1, portando a più configurazioni di telemetria in conflitto su più di 2.000 dispositivi. Sono state sollevate preoccupazioni riguardo all'impatto operativo e all'igiene della configurazione, in quanto solo la configurazione VIP CDG 7.1 del CNC deve essere rimasta attiva.

Per risolvere questo problema, è stato sviluppato uno script automatizzato per identificare e rimuovere i riferimenti VIP obsoleti del CDG dalla configurazione di telemetria di ciascun dispositivo. Questa soluzione ha eliminato le incoerenze di configurazione, ha ripristinato l'allineamento con il modello di telemetria 7.1 previsto e ha impedito quello che sarebbe stato diversi giorni di lavoro manuale di pulizia in tutto il parco di dispositivi di grandi dimensioni.

Risolvere i problemi relativi alla raccolta MDT

In CNC 7.1, la maggior parte delle raccolte di indicatori KPI di Health Insight (HI) si basa sulla telemetria guidata dal modello (MDT). Quando un profilo KPI è abilitato su un dispositivo, NSO programma automaticamente i percorsi dei sensori richiesti e configura il VIP del CDG come destinazione di telemetria. Una volta applicata questa configurazione, viene creato un processo di raccolta CDG corrispondente per tenere traccia dello stato di telemetria del dispositivo.

Durante la convalida, è stato segnalato che più di 100 dispositivi mancano delle configurazioni di telemetria. L'identificazione di questi dispositivi tramite l'interfaccia utente CNC si è rivelata poco pratica, in quanto l'interfaccia utente supporta solo il filtraggio per dispositivo e non è scalabile in modo efficiente per un parco che supera i 2.000 dispositivi. Ciò ha reso necessario un metodo automatizzato per determinare quali dispositivi non avevano una configurazione di telemetria e richiedevano la riattivazione degli indicatori KPI.

Per risolvere questo problema, è stato utilizzato il tag BNM assegnato ai dispositivi ogni volta che viene attivato un profilo KPI. Innanzitutto, è stata generata un'esportazione di tutti i dispositivi con il tag BNM. È stato poi sviluppato uno script Python per interagire con l'API della raccolta CNC, incorporando la logica di paginazione per recuperare l'intero set di lavori di raccolta (ogni chiamata API restituisce un massimo di 100 voci). Lo script ha estratto i nomi host dai dati del processo di raccolta e li ha confrontati con l'elenco dei dispositivi con tag BNM esportati.

Questo confronto ha restituito l'elenco di dispositivi contrassegnati ma non visualizzati nel processo di raccolta BNM, indicando che la configurazione di telemetria MDT non è stata applicata. Il profilo KPI è stato quindi riattivato su questi dispositivi e la convalida ha confermato che tutti i processi di raccolta corrispondenti sono stati creati correttamente.

Questa automazione ha semplificato notevolmente il processo di risoluzione dei problemi, consentendo al team di identificare e correggere tutti i dispositivi interessati in un solo giorno, un'operazione che non sarebbe stata possibile attraverso l'ispezione manuale.

Modifiche del comportamento HA e regolazione dell'algoritmo di consenso in NSO 6.4.1.1

Durante l'aggiornamento da Cisco NSO 5.7.5.1 a 6.4.1.1 come parte della transizione Cisco CNC 7.1, è stata osservata una notevole modifica nel comportamento ad alta disponibilità (HA) a causa dell'attivazione implicita dell'algoritmo di consenso nella nuova versione NSO. Questo non era il comportamento predefinito in NSO 5.7.5.1, che ha comportato un cambiamento nelle caratteristiche di failover dopo l'aggiornamento. In particolare, quando il nodo primario è stato disattivato, il nodo secondario è passato a uno stato di sola lettura, impedendo la gestione delle attività di provisioning. Analogamente, quando il nodo secondario è diventato inattivo, il nodo primario è passato da uno stato primario attivo a uno stato "none", con un impatto sulla continuità del servizio.

Per ripristinare il comportamento HA previsto in linea con la distribuzione precedente, l'algoritmo di consenso è stato esplicitamente disabilitato in NSO 6.4.1.1. Questa modifica ha garantito che i nodi primario e secondario riprendessero i ruoli previsti durante gli scenari di failover, consentendo il provisioning ininterrotto e mantenendo la stabilità operativa coerente con la versione precedente di NSO.

Miglioramenti compatibilità pacchetti e aggiornamento versione NSO

Nell'ambito della transizione da Cisco CNC 4.1 a 7.1, la versione sottostante di Cisco NSO è stata aggiornata dalla versione 5.7.5.1 alla 6.4.1.1. Questo aggiornamento della versione ha introdotto modifiche nelle strutture dei modelli XML all'interno dei pacchetti NSO esistenti, portando a errori in alcuni casi di test di regressione che dipendevano dal comportamento del modello legacy.

Per risolvere queste lacune di compatibilità, i modelli di pacchetto NSO interessati sono stati analizzati e aggiornati per allinearsi allo schema e ai requisiti di elaborazione rivisti di NSO 6.4.1.1. Questi miglioramenti hanno garantito che tutti i flussi di lavoro di automazione e i modelli di servizio continuassero a funzionare come previsto, ripristinando la stabilità di regressione e mantenendo la coerenza nell'ambiente CNC aggiornato.

Problemi relativi all'abilitazione degli indicatori KPI su scala

Il CNC fornisce un meccanismo di interfaccia utente preconfigurato per l'attivazione dei profili KPI sui dispositivi. Se da un lato questo approccio funziona bene per le piccole flotte, dall'altro diventa inefficiente e inaffidabile su larga scala. In questa implementazione, oltre 2.000 dispositivi SWR hanno richiesto l'abilitazione degli indicatori KPI e l'interfaccia utente non ha offerto un modo efficace per selezionare o elaborare i dispositivi in blocco.

Inizialmente è stato tentato un approccio basato sul tagging: a tutti i dispositivi SWR è stato assegnato un tag SWR e l'attivazione degli indicatori KPI è stata eseguita utilizzando la selezione dei tag anziché la selezione manuale dei dispositivi. Tuttavia, l'elaborazione di oltre 2.000 dispositivi in un singolo workflow ha portato a notevoli sfide operative. Il processo è durato più di tre ore ed è stato completato con centinaia di errori. Sebbene tutti i dispositivi siano stati inclusi

nell'intento, solo circa 750 hanno ricevuto l'abilitazione KPI e ripetuti tentativi hanno prodotto solo progressi incrementali. Questo approccio non si è dimostrato né scalabile né ripetibile. Ha mostrato problemi significativi con il carico.

Una seconda sfida è emersa dai problemi di sincronizzazione dei dispositivi NSO. Molti errori hanno indicato che NSO non era sincronizzato con i dispositivi corrispondenti. Il tentativo di eseguire operazioni di sincronizzazione manuali seguite dalla riattivazione dell'indicatore KPI non è stato pratico e avrebbe richiesto un notevole sforzo da parte dell'operatore.

Per risolvere queste limitazioni, è stato sviluppato un flusso di lavoro automatizzato basato su batch:

1. Esportate l'inventario completo di un CNC.
2. Dispositivi di processo in lotti di 50 (identificati come dimensioni ottimali tramite tuning).
3. Per ogni batch, attiva una sincronizzazione automatica da tramite gli UUID dei dispositivi.
4. Eseguire l'abilitazione KPI tramite l'API CNC.
5. Monitorare la cronologia dei processi KPI e registrare gli errori a livello di programmazione.
6. Rielaborare i dispositivi con errori ripetendo i passaggi di abilitazione sincronizzazione e KPI.
7. Una volta completato un batch, passare al successivo gruppo di 50 dispositivi.

L'automazione includeva anche la possibilità di disabilitare i profili KPI, consentendo una gestione completa del ciclo di vita.

Questa soluzione ha fornito un processo semplificato, deterministico e altamente scalabile per il provisioning degli indicatori KPI. Ha eliminato l'intervento manuale, assicurato risultati coerenti e risparmiato più giorni di sforzo operativo. La stessa automazione si è rivelata preziosa quando i profili KPI hanno dovuto essere disabilitati e riabilitati dopo la modifica del progetto BNM, consentendo una riconfigurazione rapida e senza errori nell'intero parco di 2.000 dispositivi.

RESTCONF API Northbound con accesso amministrativo limitato

L'API basata su RESTCONF northbound utilizzata per inoltrare allarmi ed eventi dal CNC ha un limite in base al quale può essere richiamata solo utilizzando l'account admin. I tentativi di accedere all'API tramite gli account del servizio non sono riusciti, nonostante tali account dispongano dei ruoli operativi richiesti. Come soluzione alternativa, all'utente è stato richiesto di utilizzare le credenziali di amministratore per l'inoltro degli allarmi al sistema in direzione nord, introducendo un vincolo operativo e limitando l'aderenza ai principi di accesso con privilegi minimi.

Automazione come attivatore strategico

Data la portata e la complessità del programma di aggiornamento e migrazione CNC, l'esecuzione manuale delle attività operative si è rivelata rapidamente insostenibile. Attività quali l'onboarding dei dispositivi, il provisioning degli indicatori KPI, l'allineamento della configurazione, la riconciliazione e la convalida telemetrica coinvolgono migliaia di elementi di rete e flussi di lavoro ripetuti che sono altamente soggetti a errori umani quando vengono eseguiti manualmente. L'automazione era quindi essenziale non solo per accelerare l'esecuzione, ma anche per garantire la coerenza, ridurre i rischi operativi e liberare i team di consegna dalle attività ripetitive e dispendiose in termini di tempo.

Attraverso la sistematizzazione di questi processi attraverso workflow basati su script e operazioni basate su API, il programma di upgrade ha ottenuto significativi miglioramenti in termini di efficienza. L'automazione ha consentito il completamento più rapido delle attività, una maggiore precisione e risultati prevedibili in tutte le sezioni. Il risparmio ottenuto non solo ha ridotto la tempistica complessiva dell'installazione, ma ha anche consentito ai tecnici di concentrarsi su attività di convalida e progettazione di valore superiore, piuttosto che su attività operative di routine.

Alcune delle attività di automazione sono state identificate prima dell'avvio del progetto di upgrade, mentre altre si sono evolute quando si sono verificati problemi. C'erano anche alcune cose che erano necessarie per le questioni che si sono sviluppate durante il corso del progetto.

Nella tabella sono illustrate le aree in cui l'automazione ha avuto un impatto significativo sul programma.

Descrizione attività	Impegno manuale (giorni)	Impegno di automazione (giorni)	Risparmi stimati (giorni)
Aggiornamenti ACL (SWR/LWR)(2K+)	30.0	2.0	28.0
Migrazione e collegamento di dispositivi a CDG(2K+)	5	1.0	4.0
Collegamento degli indicatori KPI BNM ai dispositivi (oltre 2K)	4.0	1,5 (media)	2.5
Riconciliazione dei servizi	7	2.5	4.5
Migrazione gruppi di dispositivi	4	0.5	3.5

Descrizione attività	Impegno manuale (giorni)	Impegno di automazione (giorni)	Risparmi stimati (giorni)
Isolamento dei dispositivi con larghezza di banda ridotta	3	0.5	2.5
Risoluzione dei problemi della raccolta MDT	3	0.5	2.5
Totali	56 giorni	8,5 giorni	47,5 giorni

Lezioni apprese

L'aggiornamento non è semplice

Il CNC non supporta gli aggiornamenti sul posto e il modello lift-and-shift introduce una notevole complessità operativa. Il processo non deve mai essere considerato semplice, specialmente quando il salto di versione è grande. I problemi imprevisti emergono in tutte le applicazioni, le integrazioni e i flussi di lavoro e richiedono tempi, analisi e un'attenta mitigazione. Un importante passo avanti in termini di versione rafforza questa sfida, rendendo essenziali una pianificazione, una convalida e un'esecuzione graduale. Abbiamo dovuto dedicare molto tempo in più ai casi TAC e alle attività di risoluzione dei problemi. Dal momento che non abbiamo tenuto il tempo di tampone per questo, è diventato impegnativo.

CX deve eseguire il sollevamento pesante

Previsione di un notevole impegno da parte del sistema CX in termini di implementazione, integrazione, migrazione e convalida completa dei casi di utilizzo. Non partire dal presupposto che i flussi di lavoro testati nella versione precedente si comportano in modo identico a quelli della versione successiva.- Per garantire il corretto funzionamento delle operazioni sono necessarie numerose attività di analisi e risoluzione dei problemi.

Automation Toolkit è una necessità

Il percorso di aggiornamento ha dimostrato che l'automazione non è un vantaggio opzionale, ma

un requisito fondamentale per le installazioni CNC su larga scala. Abbiamo pianificato presto l'automazione per i candidati necessari, ma non si può mai supporre che sarà sufficiente. A metà del progetto, è stato possibile identificare i problemi nei casi di utilizzo in cui l'automazione apporterebbe un valore aggiunto, come è stato dimostrato nelle sezioni precedenti.

Evitare conflitti tra due controller durante la migrazione

Durante l'aggiornamento, è fondamentale garantire che gli ambienti legacy e new CNC non siano attivi contemporaneamente. Benché sia necessario un breve periodo di immersione per la convalida, un prolungamento significativo di tale periodo, come è avvenuto in questo progetto per più di due mesi, comporta rischi operativi. Con entrambi i CNC attivi per oltre 15-20 giorni, le funzioni di automazione a loop chiuso come Bandwidth On Demand generarono azioni incoerenti e in conflitto sulla rete, dal momento che la logica di automazione veniva eseguita da due controller contemporaneamente.

Una lezione fondamentale è l'implementazione di procedure chiare durante la migrazione. Misure come la disabilitazione amministrativa dei dispositivi nel vecchio CNC, la sospensione dei flussi di lavoro di automazione o la limitazione delle sottoscrizioni di telemetria avrebbero evitato questi conflitti. Gli aggiornamenti futuri devono prevedere esplicitamente un rigoroso isolamento dei controller per evitare interferenze a doppio controller e garantire un comportamento di rete prevedibile.

I pacchetti MOP non sono sacrosant

Sebbene i documenti MOP (Method of Procedure) vengano creati per ogni distribuzione, integrazione e caso di utilizzo, non è realistico supporre che un MOP convalidato in condizioni di laboratorio si comporti in modo identico in fase di produzione. L'ambiente di produzione ha rivelato costantemente deviazioni, alcune minime, alcune significative, evidenziando così lacune che non erano visibili durante i test controllati. Le reti del mondo reale, i comportamenti legacy, le dipendenze esterne e le condizioni del traffico in tempo reale introducono variabili che le simulazioni di laboratorio non sempre possono replicare.

Il concetto chiave è che i team devono affrontare l'implementazione della produzione con l'aspettativa di incontrare comportamenti imprevisti, casi limite e nuove scoperte. Flessibilità, capacità di risoluzione rapida dei problemi e prontezza di adattamento immediato delle procedure sono essenziali per un'esecuzione efficace su vasta scala.

Efficacia dei casi di TAC

I problemi di post-produzione sono inevitabili e, mentre la risoluzione iniziale dei problemi da parte del team di consegna è preziosa, affidarsi esclusivamente allo sforzo interno può portare a inutili ritardi. è prudente aprire un caso TAC in parallelo come rete di sicurezza, soprattutto per problemi relativi ai prodotti o comportamenti complessi che non sono diagnosticabili immediatamente. Le ricerche TAC richiedono spesso tempo e ritardare la creazione dei casi di diversi giorni può comportare una perdita significativa dello slancio del progetto. Il coinvolgimento tempestivo di TAC assicura la disponibilità dell'assistenza di esperti quando necessario, accelera l'identificazione della root cause e impedisce che si verifichino slittamenti nella pianificazione.

Coinvolgi l'unità CNC per un efficace supporto della conoscenza

Un forte supporto da parte della CNC Business Unit è molto prezioso durante qualsiasi progetto CNC. Gli utenti spesso richiedono informazioni dettagliate sui prodotti e chiarimenti che non sono immediatamente disponibili solo con il team di distribuzione. La possibilità di accedere a un contatto per l'unità aziendale durante l'intero progetto accelera la risoluzione dei problemi, rafforza l'accuratezza tecnica e contribuisce a creare maggiore fiducia e un rapporto più proficuo tra gli utenti.

Best practice per l'aggiornamento CNC

Pianificazione di una strategia di aggiornamento ottimizzata

Il CNC non supporta gli aggiornamenti sul posto, rendendo inevitabile l'installazione parallela. Trattare il nuovo ambiente come una nuova installazione e allocare una capacità di elaborazione, storage e amministrazione sufficiente per eseguire due ambienti contemporaneamente. Pianificare le fasi di convalida, il sequenziamento della migrazione e le attività di cutover con molto anticipo.

Una rigorosa convalida pre-distribuzione è essenziale soprattutto per i parametri non modificabili

Molte esperienze sottolineano l'importanza critica della diligenza durante la distribuzione iniziale. La convalida anticipata di tutti gli input chiave, in particolare dei parametri di configurazione non modificabili, è essenziale per evitare costose ridistribuzioni e un impatto sulla pianificazione. Per ridurre al minimo il rischio di errori irreversibili di configurazione, si consiglia pertanto di utilizzare elenchi di controllo pre-distribuzione strutturati, revisioni peer e convalide a secco.

Utilizzare un ambiente di convalida dedicato prima di toccare la produzione

La creazione di un ambiente di prova/CALO interno all'inizio del progetto consente ai team di sperimentare, convalidare i workflow, scoprire le modifiche specifiche delle versioni e creare fiducia prima di intervenire sulla produzione. Ciò riduce sensibilmente le incognite durante il rollout finale.

Dimensionamento basato su prove per componenti Crosswork distribuiti

Nella progettazione di cluster, distribuzioni CDG e allocazioni PCE, le decisioni si basano sui tipi di dispositivi, la scala dell'interfaccia, la complessità della topologia e l'intensità di raccolta, anziché sul semplice numero di dispositivi. Le distribuzioni bilanciate evitano il sovraccarico e garantiscono prestazioni prevedibili nel cluster.

Automazione per lavori ripetitivi e ad alto volume

Stabilire un backlog di automazione per le attività di avvio ripetitive, con volumi elevati o critiche a livello operativo e investire dove l'automazione è obbligatoria. Convalidare e perfezionare l'automazione nell'ambiente SIT, assicurandosi che la produzione non si basi su correzioni dell'ultimo minuto. La scalabilità amplifica il costo del lavoro manuale; l'automazione standardizzata migliora qualità, velocità e controllo. Creazione di pacchetti di risultati come risorse riutilizzabili (interfacce documentate, processi con parametri, librerie condivise) in modo che i team possano sfruttare la stessa automazione per i futuri aggiornamenti Crosswork e i progetti adiacenti, riducendo i tempi di rielaborazione e caricamento.

Evitare il controllo a doppio loop chiuso durante l'esecuzione parallela

Durante la coesistenza, trattare l'automazione a loop chiuso come una funzionalità di scrittura singola: solo un percorso di orchestrazione può attivare il monitoraggio e l'aggiornamento o la configurazione basata su regole. La presenza contemporanea di CLA sugli stack vecchi e nuovi comporta il rischio di duplicazione dei trigger e di intento divergente, che può destabilizzare lo stato del dispositivo. Pianificare il lancio di CLA come fase avanzata, dopo la convalida funzionale e il passaggio definitivo al nuovo controller.

Valutazione dell'impatto dell'aggiornamento strutturato

I salti di versione principali introducono nuove funzionalità mentre deprecano o modificano quelle precedenti. È estremamente importante tenere conto di questi cambiamenti. Molte volte, la modifica non sarà documentata nelle note di rilascio della versione aggiornata e apparirà quando arriveremo sul campo. Effettuare valutazioni strutturate di:

- API obsolete
- Modifiche al framework KPI
- Differenze di comportamento a livello di applicazione
- Deviazioni dal modello di configurazione
- Avvisi, elaborazione della topologia e modifiche all'esecuzione della playbook

Verifica della compatibilità e del comportamento nell'area di integrazione

Il CNC interagisce con più sistemi esterni come NSO, SSM, CPNR, EPNM, OneFM, Splunk e strutture di orchestrazione.
Prima della migrazione:

- Convalida compatibilità versioni
- Testare tutte le integrazioni in direzione nord/sud
- Conferma modelli di dati, trap, flussi di telemetria
- Verifica comportamento autenticazione SSL/RESTCONF

Gli errori di integrazione rilevati dopo la migrazione creano punti ciechi operativi.

Definizione di una solida strategia di esportazione dei dati prima della migrazione

Esporta tutto prima di iniziare la migrazione:

- Profili credenziali
- Provider
- Tag
- Playbook personalizzati
- Indicatori KPI personalizzati
- Ruoli e RBAC
- Giustificativi sZTP
- Gruppi di dispositivi
- Metadati cronologici dei servizi

Migrazione Di Dispositivi In Batch Con Gate Di Convalida Integrate

Quando si esegue la migrazione di migliaia di dispositivi, eseguire la migrazione in batch controllati:

- Spostare i dispositivi in una coorte fissa (ad esempio, per area geografica, carico CDG o tipo di dispositivo)
- Convalida telemetria, stato di sincronizzazione NSO e raggiungibilità prima di passare al batch successivo
- Esegui il rollback del batch se vengono visualizzate anomalie persistenti

Ciò previene un carico elevato su CDG e CNC in un breve intervallo di tempo.

Gestione delle modifiche alla configurazione fuori banda tramite l'integrazione NSO

Per affrontare la sfida fuori banda nell'ambito dell'aggiornamento CNC da 4.1 a 7.1, è stato implementato un passaggio strutturato verso le operazioni guidate da NSO. Al team operativo è stato fornito un accesso controllato e basato sull'utente alla CLI NSO, mentre l'accesso amministrativo diretto alla CLI del dispositivo è stato limitato per impedire modifiche fuori banda. Inoltre, gli script CLI legacy sono stati convertiti in modo sistematico in un'automazione basata su RESTCONF integrata con NSO, consentendo funzionalità quali la convalida dell'esecuzione a secco e il rollback delle transazioni. Questo approccio garantiva che tutte le modifiche alla configurazione fossero gestite centralmente, verificabili e coerenti con i modelli di servizio NSO, eliminando in modo efficace le deviazioni della configurazione e ripristinando l'affidabilità del provisioning.

Enfasi forte sul blocco delle modifiche

Durante le finestre di migrazione critiche:

- Blocca modifiche di rete avviate dall'utente
- Limita push di configurazione
- Sincronizza con i team sul campo e NOC
- Pianificare alcune finestre per ospitare attività di emergenza come la sostituzione del dispositivo utilizzando CNC/ZTP e così via.

Ciò riduce il rumore e garantisce la stabilità dello stato della rete durante l'upgrade

Conclusioni

La migrazione da CNC 4.1 a CNC 7.1 costituisce un caso di studio significativo nelle complessità inerenti agli aggiornamenti della piattaforma di orchestrazione di rete su larga scala. Questo progetto dimostra che tali transizioni non sono solo miglioramenti di versione, ma trasformazioni complete tra livelli di architettura, flussi di lavoro operativi ed ecosistemi di automazione. L'assenza di un percorso di upgrade sul posto ha richiesto un'installazione completa, che ha introdotto sfide ambientali parallele e richiede un coordinamento meticoloso tra CNC, NSO, SR-PCE, CDG e integrazioni di sistemi esterni. Il panorama operativo che ne risulta ha evidenziato l'importanza di metodologie di migrazione affidabili, cicli di convalida completi e processi di cutover strettamente controllati per ridurre i rischi negli ambienti di produzione.

L'aggiornamento ha ulteriormente rivelato la criticità dell'automazione come un pilastro indispensabile per la scalabilità e l'accuratezza. Con oltre 2.000 dispositivi, configurazioni di telemetria estese, più componenti dipendenti e flussi di lavoro dinamici di automazione a loop chiuso, il progetto ha evidenziato i limiti delle procedure manuali in ambienti di questa portata. L'automazione mirata basata su aggiornamenti ACL, l'onboarding dei dispositivi, il provisioning degli KPI, la pulizia della telemetria e l'isolamento degli errori si sono rivelati essenziali per garantire il determinismo, ridurre l'errore umano e ottenere notevoli miglioramenti in termini di efficienza. La struttura di automazione non solo ha consentito la continuità operativa durante la migrazione, ma ha anche creato una base sostenibile per l'ottimizzazione continua della rete.

Altrettanto importante è stato il riconoscimento che il comportamento di produzione si discosta notevolmente dalle condizioni di laboratorio controllato. Le modifiche della struttura, come la transizione dalla logica degli indicatori KPI basati su tick a quella basata su tracciatori, hanno introdotto cambiamenti di comportamento imprevisti che hanno richiesto una riprogettazione, un nuovo test e un perfezionamento iterativo. Analogamente, le sfide operative relative all'automazione a loop chiuso, all'affidabilità della telemetria e al comportamento delle API hanno evidenziato la necessità di una risoluzione dei problemi adattiva, di una valutazione proattiva dei rischi e di un impegno continuo con gli esperti in materia di TAC e Business Unit. Questi fattori illustrano collettivamente che le transizioni delle versioni principali richiedono sia approfondimento tecnico che preparazione organizzativa. Rimangono ancora poche questioni in sospeso che dovrebbero essere risolte nella prossima versione 7.2 di crosswork.

Nel complesso, questo aggiornamento dimostra che il successo delle migrazioni di CNC su larga scala si basa su quattro pilastri fondamentali: rigorosa convalida pre-installazione, automazione sistematica e resiliente, forte coordinamento interfunzionale e postura operativa adattiva che anticipa la divergenza tra ambienti di laboratorio e di produzione. Le conoscenze acquisite da questo impegno non solo hanno contribuito a un'installazione CNC 7.1 stabile, ma hanno anche offerto un piano per le transizioni future, informando le best practice, rafforzando i presidi architetturali e rafforzando la conoscenza istituzionale per la successiva evoluzione dell'ecosistema di automazione di rete.

Glossario dei termini

Termine	Definizione
BNM	Messaggio di notifica larghezza di banda.
GATTO	Crosswork Active Topology
CCA	Crosswork Change Automation
CDG	Crosswork Data Gateway
CHI	Crosswork Health Insight
CNC	Cisco Crosswork Network Controller
COE	Crosswork Optimization Engine
CPNR	Cisco Prime Network Registrar
CWM	Crosswork Workflow Manager
EMF	Funzioni di gestione degli elementi
KPI	Indicatore prestazioni chiave
LWR	Grande router wireless
MDT	Telemetria guidata dal modello
MOP	Metodo di procedura
NBW	Larghezza di banda nominale

NSO	Network Services Orchestrator
RBW	Larghezza di banda registrata
SR-PCE	Elemento calcolo percorso ciclo segmento
SSM	Cisco Smart Software Manager
CFA	Router wireless di piccole dimensioni
TAC	Technical Assistance Center
TSDN	Transport Software-Defined Networking
ZTP	Provisioning Zero Touch
RR	Riflettore route
RP	Profilo ciclo di lavorazione
POI	Punto Di Interconnessione
EVPN	Rete privata virtuale Ethernet.

Riferimenti

- Cisco Systems, Cisco Crosswork Network Controller Release Notes, versione 7.1.0
- Guida all'installazione di Cisco Systems, Cisco Crosswork Infrastructure 7.1
- Cisco Systems, Cisco Crosswork Infrastructure 7.1 Administration Guide - Panoramica dei concetti:
- Cisco Systems, Crosswork Network Controller Traffic Engineering and Optimization Guide, versione 7.1
- Cisco Systems, Cisco Crosswork Health Insights User Guide, versione 7.1
- Guida all'installazione di Cisco Systems e Crosswork Zero Touch Provisioning (ZTP)
- Cisco Systems, Cisco NSO Transport SDN Function Pack Installation Guide, versione 7.1.0
- Cisco Systems, Guida alla configurazione di Cisco SR-PCE

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).