

# Estudo de caso de upgrade do CNC

## Contents

---

[Introdução](#)

[Resumo](#)

[Background](#)

[Rede de produção](#)

[Fluxo de trabalho de migração do CNC 4.1 para o CNC 7.1](#)

[Arquitetura CNC e integração com outros componentes](#)

[Diagrama de arquitetura](#)

[Diagrama de Rede](#)

[Fluxo de trabalho de migração detalhado do CNC 4.1 → 7.1](#)

[Casos de uso](#)

[Provisionamento de serviços L2VPN \(com base em EVPN\)](#)

[Modelos NSO Personalizados](#)

[Provisionamento de serviços L3VPN \(com base em VRF\)](#)

[Modelo NSO personalizado](#)

[Engenharia de tráfego](#)

[Tráfego TC1 \(menor latência\)](#)

[Tráfego TC4 \(largura de banda comprometida\)](#)

[Ativação de dispositivo usando sZTP](#)

[Orquestração pós-ZTP \(orientada por automação\)](#)

[Processamento de mensagem de notificação de largura de banda \(BNM\) no CNC](#)

[Alteração Temporária \(Eventos Fugazes\)](#)

[MDT BNM](#)

[Padronize as operações de rede do dia seguinte por meio de manuais de atividades de automação personalizada](#)

[Continuidade da integração TACACS+ na atualização do Cisco CNC 7.1](#)

[Encaminhamento de syslog CNC e CDG para Splunk](#)

[Encaminhamento de Alarmes para o OneFM](#)

[Automação de Backups CNC diários](#)

[Desafios](#)

[Big Jump na versão Crosswork](#)

[Não há atualização no local](#)

[Ocorrências de implantação sem opções de reversão](#)

[Restrições da Validação de Diagnóstico Pós-Implantação](#)

[Alteração de Procedimento de Criação de KPI Personalizado HI](#)

[Tempo Limite de API no Script de Disparo de Playbooks BNM](#)

[Alteração de Design do Disparador do Manual e do Processamento do BNM](#)

[Limitação no Design de alerta original](#)

[Impacto da Alteração da Estrutura de KPI](#)

[Disparo Excessivo do Manual](#)

[Lógica de automação reprojeta](#)

[Resultado](#)

---

[Supressão de Alarmes do Dispositivo](#)

[Alterações fora da banda](#)

[Reconciliação de VPN L2/L3](#)

[Impacto da Agenda](#)

[Observações](#)

[Recomendações para atualizações semelhantes](#)

[Falha de backup do CNC devido a dependências do modo de manutenção](#)

[Impacto operacional](#)

[Estratégia de mitigação](#)

[Resultados e resultado](#)

[Encaminhando syslogs para Splunk](#)

[Problema de Migração do Agrupamento de Dispositivos](#)

[Isole Dispositivos Degradados Com Grande Largura De Banda](#)

[Remoção da configuração de telemetria do dispositivo](#)

[Solucionar problemas da coleção MDT](#)

[Mudanças de comportamento de HA e ajuste de algoritmo de consenso em NSO 6.4.1.1](#)

[Aprimoramentos de Atualização de Versão NSO e Compatibilidade de Pacote](#)

[Problemas com a habilitação de KPI em escala](#)

[RESTCONF API ascendente restrita ao acesso do administrador](#)

## [Automação como um viabilizador estratégico](#)

### [Lições aprendidas](#)

[A atualização não é simples](#)

[CX tem que fazer o levantamento pesado](#)

[O kit de ferramentas de automação é uma necessidade](#)

[Evite conflitos de controlador duplo durante a migração](#)

[MOPs não são sagrados](#)

[Eficácia dos casos TAC](#)

[Envolve a CNC BU para um suporte de conhecimento eficaz](#)

## [Melhores práticas para atualização do CNC](#)

[Planeje uma estratégia de atualização otimizada](#)

[A validação pré-implantação rigorosa é essencial especialmente para parâmetros imutáveis](#)

[Use um ambiente de validação dedicado antes de tocar na produção](#)

[Dimensionamento baseado em evidências para componentes de trabalho cruzado distribuído](#)

[Automação para trabalho repetitivo e de alto volume](#)

[Evite o controle de loop fechado duplo durante a execução paralela](#)

[Executar Avaliação de Impacto de Upgrade Estruturado](#)

[Teste a compatibilidade e o comportamento na superfície de integração](#)

[Estabelecer uma estratégia robusta de exportação de dados antes da migração](#)

[Migração De Dispositivos Em Lote Com Portas De Validação Integradas](#)

[Lidar com alterações de configuração fora da banda por meio da integração de NSO](#)

[Coloque forte ênfase no congelamento de mudanças](#)

## [Conclusão](#)

## [Glossário de termos](#)

## [Referências](#)

---

# Introdução

Este documento descreve um estudo de caso de uma migração complexa e em larga escala de uma rede sem fio fixa do Cisco CNC 4.1 para 7.1 via lift-and-shift.

## Resumo

Este documento apresenta um estudo de caso detalhado da migração de uma rede sem fio fixa de grande escala do Cisco Crosswork Network Controller (CNC) versão 4.1 para a versão 7.1. Devido à ausência de um mecanismo de atualização no local, a transição exigiu uma implantação de elevação e deslocamento total, introduzindo complexidade significativa de arquitetura, operacional e integração em mais de 2.000 dispositivos de rede e vários sistemas interdependentes. O estudo examina os desafios encontrados - em várias áreas.

Um resultado importante destaca o papel essencial da automação em garantir escalabilidade, precisão e determinismo operacional, especialmente para fluxos de trabalho de alto volume. Os resultados demonstram ainda que os ambientes de produção divergem consideravelmente das condições controladas em laboratório, necessitando de solução adaptativa de problemas, validação iterativa e envolvimento contínuo com as equipes de engenharia do TAC e da unidade de negócios. Esse trabalho contribui com insights práticos, metodologias validadas e melhores práticas recomendadas que servem como modelo de referência para futuras atualizações de CNC e transições de plataforma de orquestração em grande escala.

## Background

A proliferação de redes 5G, a rápida adoção de dispositivos conectados e a digitalização de ambientes corporativos e de consumo levaram a um aumento significativo no volume de tráfego e na diversidade de serviços que devem ser fornecidos de forma segura e confiável em escala. Os provedores de serviços de comunicação (CSPs) agora operam redes altamente dinâmicas, em que ferramentas operacionais tradicionais em silos frequentemente criam complexidade, degradam a experiência do usuário e geram despesas operacionais (OpEx) mais altas.

Para se manterem competitivas, as operadoras estão adotando cada vez mais modelos operacionais modernizados baseados em automação, virtualização, princípios de SDN e redes orientadas por análise e auto-otimização.

O Cisco Crosswork Network Controller (CNC) foi projetado para oferecer suporte a essa transformação, simplificando os fluxos de trabalho operacionais, reduzindo o custo total de

propriedade (TCO) e permitindo a automação baseada em intenção em redes de transporte de vários fornecedores. O CNC fornece uma plataforma unificada para provisionamento de serviços, monitoramento da integridade da rede e otimização em tempo real, oferecendo aos operadores um único painel de controle para gerenciar redes IP de grande escala de forma mais proativa e eficiente.

A Crosswork Infrastructure subjacente oferece uma estrutura de cluster resiliente e escalável na qual todos os aplicativos CNC são executados. Para o CNC 7.1, isso inclui módulos como Mecanismo de Otimização, Topologia Ativa, Automação de Alterações, Percepções de Integridade, Funções de Gerenciamento de Elementos (EMF), Integridade do Serviço e Crosswork Workflow Manager (CWM), cada um contribuindo para a orquestração e a garantia de ponta a ponta.

A atualização do CNC, no entanto, apresenta desafios únicos. O CNC não oferece suporte a atualizações no local, exigindo uma implantação de substituição completa, em que o novo ambiente é criado em paralelo com o existente, e todos os dados e serviços são migrados para a nova versão. Este estudo de caso examina uma atualização em grande escala do CNC 4.1 para o CNC 7.1 para um agregador de serviços australiano de grande porte que oferece serviço de backbone para todos os outros provedores de serviços.

A migração foi especialmente complexa devido a vários manuais de atividades de automação de alterações personalizados, KPIs de informações de saúde personalizados, requisitos de reconciliação de serviços VPN L2/L3 e a necessidade de ZTP seguro.

O grande salto de versão introduziu incerteza adicional, dadas as mudanças internas de arquitetura e comportamento que dificultaram a previsão de como os casos de uso existentes se comportariam na nova versão. Isso exigiu validação e alinhamento abrangentes em todos os casos de uso.

Um planejamento significativo foi investido na determinação da alocação ideal de recursos, incluindo contagens de nós híbridos/de trabalhadores, distribuição CDG e dimensionamento PCE, e se o volume de recursos existente poderia ser mantido.

A implantação e validação iniciais do CNC 7.1 foram realizadas em um laboratório interno de CALO, proporcionando um ambiente seguro para experimentação, refinamento de configurações e construção de confiança. Isso foi seguido pela implantação no ambiente de teste interno, que espelha a produção. A fase final envolveu a implantação do CNC 7.1 na produção, a aplicação de alterações de configuração no nível do dispositivo e a execução de uma migração em fases de todos os dispositivos e serviços associados para o novo controlador.

## Rede de produção

A rede de produção de ar-gapped é espalhada por amplas partes da Austrália. Com a presença de dispositivos 2K+, variando de NCS a ASR9Ks, a CNC gerenciou todos esses dispositivos fornecendo uma visualização topológica ao vivo. Aproximadamente 2K dispositivos eram NCS540s localmente conhecidos como SWR (Small Wireless Router) executando IOS-XR 24.3.2 e 30 eram ASR-9Ks (Versão 7.5.2) localmente conhecidos como LWRs (Large Wireless Router).

A configuração Crosswork consistia em 3 nós híbridos e 2 nós de trabalho. Havia um total de 5 CDGs para os dispositivos, sendo 4 ativos e 1 nó em espera. Isso proporcionou proteção limitada, já que o pool tinha apenas 1 CDG em espera. Mas considerando suas exigências, isso foi dado o sinal verde. O fato de todas as VMs estarem em um único data center também facilitou a decisão de continuar com apenas 1 em espera.

O CDG é o componente que manipula a coleta de dados de dispositivos através de vários protocolos como SNMP, CLI e GNMI. Os dados coletados pelo CDG são expostos ao Crosswork através do kafka interno. Um dispositivo integrado ao Crosswork deve ser conectado a um CDG, que permite que o gateway de dados se conecte ao dispositivo e obtenha os dados do dispositivo.

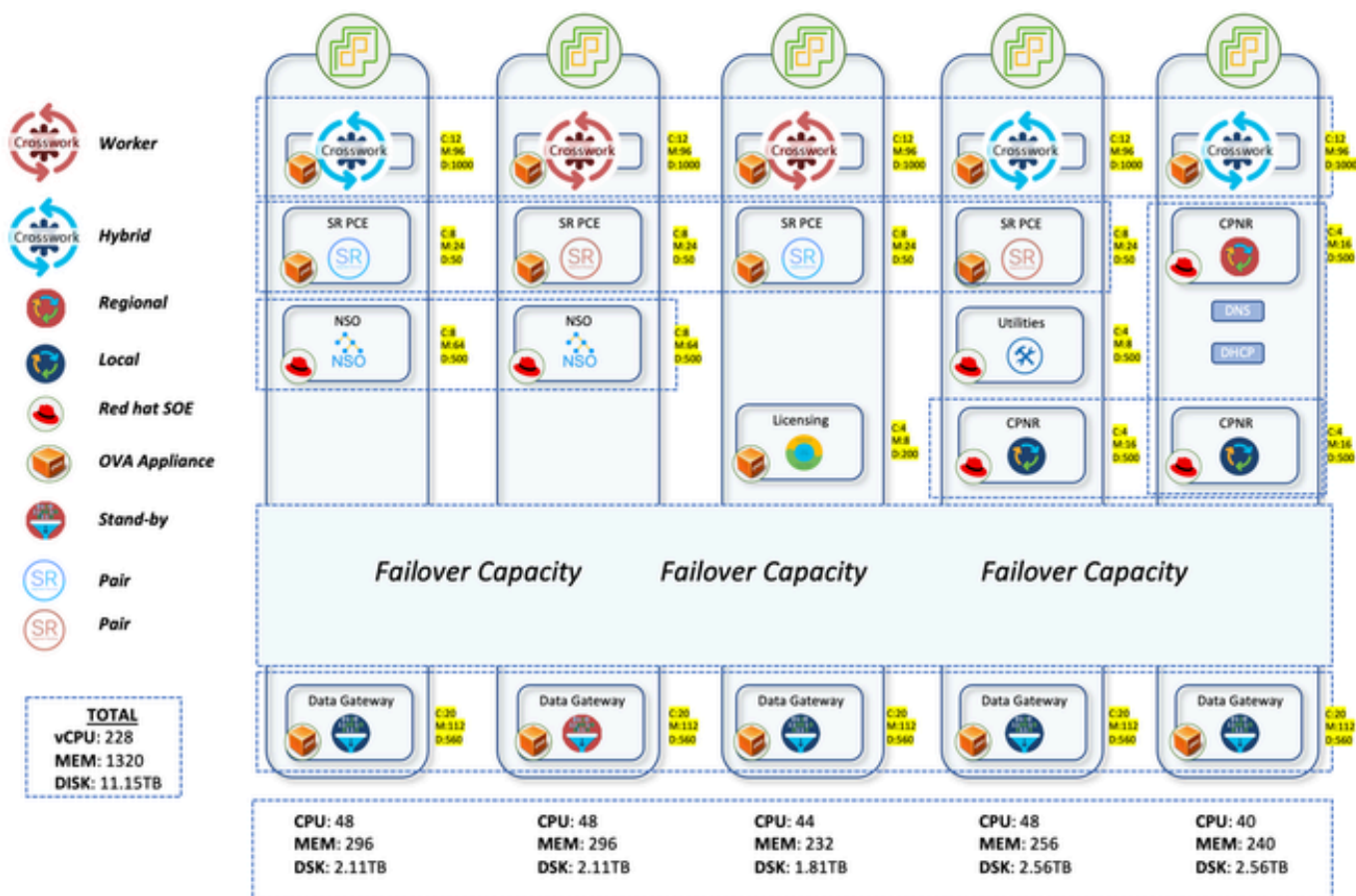
A distribuição de dispositivos para os CDGs também recebeu muita reflexão. A implantação anterior distribuiu aleatoriamente os dispositivos entre os CDGs. Isso deu origem a uma distribuição muito enviesada, com alguns CDGs carregando mais dispositivos, enquanto havia de 1 a 2 CDGs com menos dispositivos. Tal conduziu a um consumo excessivo e a uma sobrecarga de alguns CDG, enquanto outros foram subprovisionados.

O processo de pensamento aqui na atualização foi distribuir 700 SWRs cada para os 4 CDGs ativos. Isso representou 2100 SWRs sendo acomodados nos três primeiros CDGs. Os LWRs que eram muito pesados na interface foram todos reservados para o quarto CDG. Embora fossem um número muito pequeno com uma contagem de 30, essa alocação assegurou que, mesmo se mais coletas fossem feitas desses dispositivos, não haveria carga pesada sobre o CDG. Qualquer integração posterior de SWR também iria para o 4º CDG. Isso garantiu uma distribuição uniforme nos três primeiros CDGs com mais espaço disponível no quarto para receber novos dispositivos.

O SR-PCE foi implantado em 2 pares, o que significa 4 VMs distribuídas em máquinas host diferentes. Um par gerencia 7 sites POI e o outro gerencia os 8 sites POI restantes. As atualizações de topologia na GUI do CNC são feitas através do uso do SR-PCE. Ele aprende a topologia da rede através do peering BGP-LS com outros roteadores LWR. Esse componente também é usado em todos os casos de uso de engenharia de tráfego em que ele desempenha o papel do controlador para direcionar o tráfego para caminhos diferentes.

Para lidar com todos os casos de uso de provisionamento de serviços e configuração de dispositivos, o NSO precisa ser usado em conjunto com o CNC. Para a rede de produção, dois NSOs com a versão 6.4.1.1 foram implantados para trabalhar em conjunto no modo de alta disponibilidade. SR-PCE (Segment Routing Path Computation Element) é o componente necessário para fornecer as atualizações de topologia ao CNC e também para lidar com casos de

uso de engenharia de tráfego em tempo real. Quatro SR-PCEs com a versão 25.2.1 foram implantados aqui, com cada PCE sendo correspondido a dois LWRs diferentes.



## Fluxo de trabalho de migração do CNC 4.1 para o CNC 7.1



Para a implantação do CNC, a escolha preferida era seguir em frente com o docker baseado. Mas como o cliente não aprovou a configuração do docker em suas instalações, não havia outra opção além de prosseguir com a implantação manual usando o vCenter. Isso leva mais tempo para ser

implantado em comparação com o script, pois exige que forneçamos entradas várias vezes na GUI do vCenter.

Depois que a implantação do CNC foi feita, todos os aplicativos necessários foram implantados com o arquivo de instalação de ação automática fornecido pela BU que carrega e ativa os aplicativos todos de uma vez, reduzindo assim o tempo necessário para fazê-lo manualmente. A camada principal foi implantada, incluindo Mecanismo de Otimização de Trabalho Cruzado, Topologia Ativa, Integridade do Serviço, Funções de Gerenciamento de Elementos, Gerenciador de Fluxo de Trabalho Cruzado. Junto com isso, os pacotes complementares também foram configurados, o que inclui a automação de alterações e o Health Insight.

CWM e SH não tinham casos de uso. No entanto, eles foram implantados, pois estavam interessados em alguns dos casos de uso oferecidos por esses aplicativos na próxima versão.

Uma vez configurados os aplicativos, o próximo passo era migrar os dados da versão antiga do CNC. Isso consiste principalmente nos perfis de credencial, provedores, tags, playbooks personalizados, KPIs personalizados, funções, vouchers sZTP e quaisquer outros dados. CNC fornece a opção de exportação para todos estes que podem ser alavancados e, em seguida, importados para o novo CNC.

Uma vez configurados, é prudente iniciar a migração do dispositivo. Em caso de atualizações, se o novo CNC for implantado em uma nova sub-rede em comparação com a mais antiga, há a necessidade de fazer alterações de ACL em dispositivos para fornecer acessibilidade com o novo CNC. Esse é um processo demorado, pois exige que um faça login manualmente em cada dispositivo e altere a configuração.

Depois que essas alterações de ACL forem feitas, a próxima etapa será importar os dispositivos para o novo CNC e anexá-los aos CDGs. Se a acessibilidade for apropriada e as credenciais SSH e SNMP estiverem corretas, os dispositivos serão mostrados como alcançáveis no CNC e também serão integrados ao NSO (Network Services Orchestrator).

Na frente da NSO, todos os pacotes necessários precisam estar no lugar e operacionalmente ativos para garantir que a CNC possa falar com a NSO e vice-versa. Por exemplo, para integrar automaticamente os dispositivos ao NSO da CNC, o pacote de funções da DLM é obrigatório. Da mesma forma, se houver qualquer requisito para que o NSO configure caminhos do sensor MDT no dispositivo, o pacote TM-TC deverá ser implantado no NSO. A essência é que, dependendo do caso de uso, o pacote relevante deve ser implantado no NSO.

Em vez de usar a abordagem manual para implantar esses pacotes necessários, especialmente os Transport-SDN, um script automatizado foi desenvolvido para provisionamento. Com a atualização do CNC 7.1, foram introduzidas atualizações nos pacotes TSDN. Esses pacotes atualizados destinam-se à implantação no servidor NSO para garantir o suporte contínuo para o

provisionamento de L2/L3 no ambiente atualizado. O script automatiza a instalação dos pacotes TSDN atualizados e carrega os metadados necessários no NSO, permitindo que ele provisione serviços conforme necessário.

Uma instância do servidor de licenciamento Cisco Smart Software Manager (SSM) e três instâncias do Cisco Prime Network Registrar (CPNR) também podem ser implantadas em hosts diferentes.

## Arquitetura CNC e integração com outros componentes

O CNC fornece uma única plataforma para provisionamento, otimização e visualização de serviços implantados por meio de uma IU unificada. Aqui está um breve resumo dos componentes internos do CNC que residem no conjunto de plataformas CNC e os casos de uso.

- Topologia ativa de trabalho cruzado (CAT):
  - Aplicação de componente interno distribuída através de nós de VM CNC
  - Fornece visibilidade completa em tempo real do inventário reconciliado
  - Integra informações de inventário de várias fontes de dados em uma única exibição
  - Computação de caminho de rede de transporte
  - Descoberta de topologia
- Mecanismo de otimização de trabalho cruzado (COE):
  - Aplicação de componente interno distribuída através de nós de VM CNC
  - Otimização da rede em tempo real
  - Visualização da topologia em tempo real
  - Visualizações e provisionamento SR-TE
  - Visualização e provisionamento RSVP-TE
  - Largura de banda sob demanda
- Ideias de saúde de trabalho cruzado (CHI):
  - Aplicação de componente interno distribuída através de nós de VM CNC
  - Monitoramento de KPI
  - Painel de alerta
- Automação de alteração de trabalho cruzado (CCA):
  - Aplicação de componente interno distribuída através de nós de VM CNC
  - Ferramenta Dev-ops com livros de reprodução prontos para uso
  - Recurso de agendamento para executar reproduções no horário desejado
  - Os KPIs de alta qualidade alertam sobre a suposição de itens sugeridos como correção

Diagrama de arquitetura

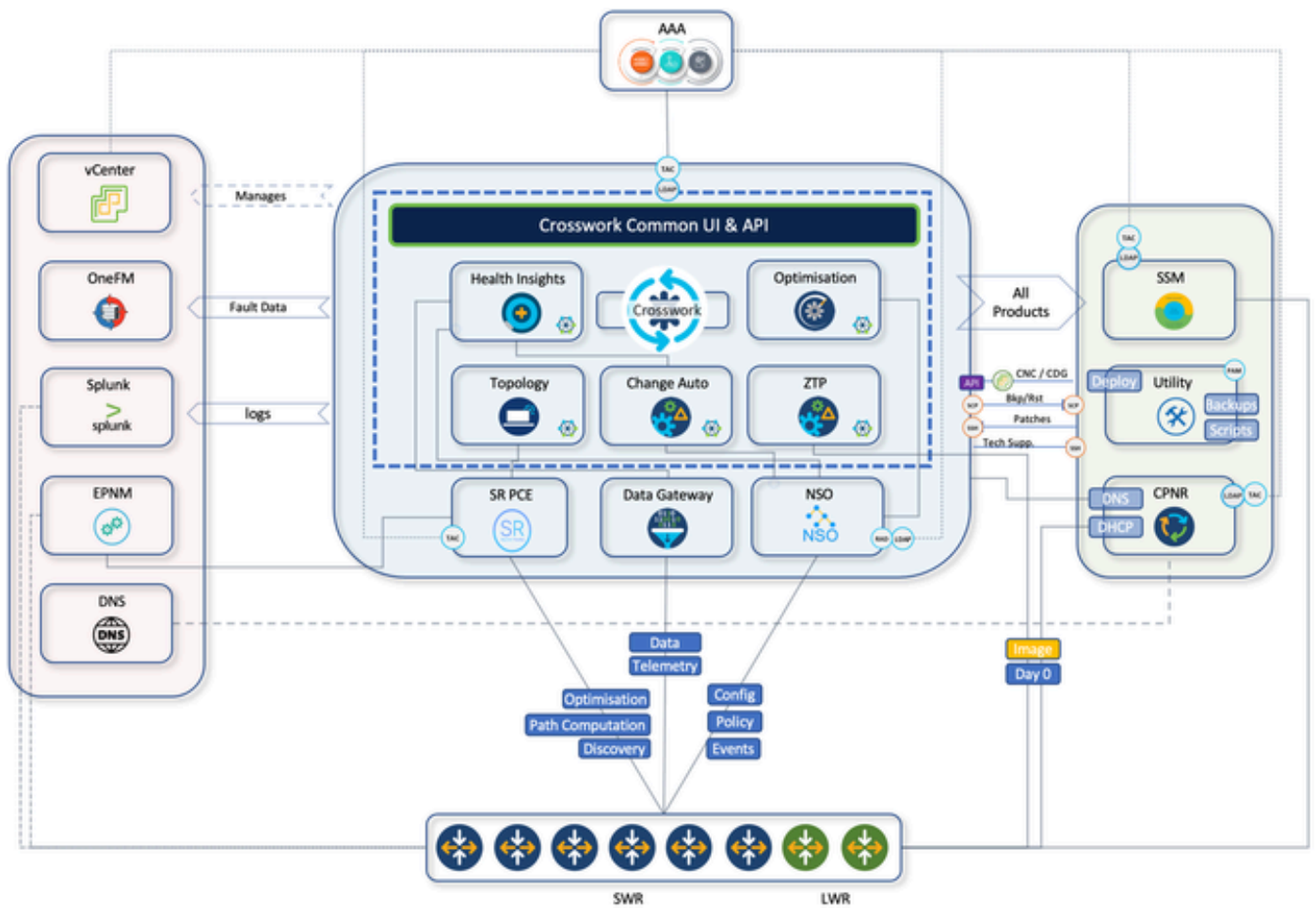
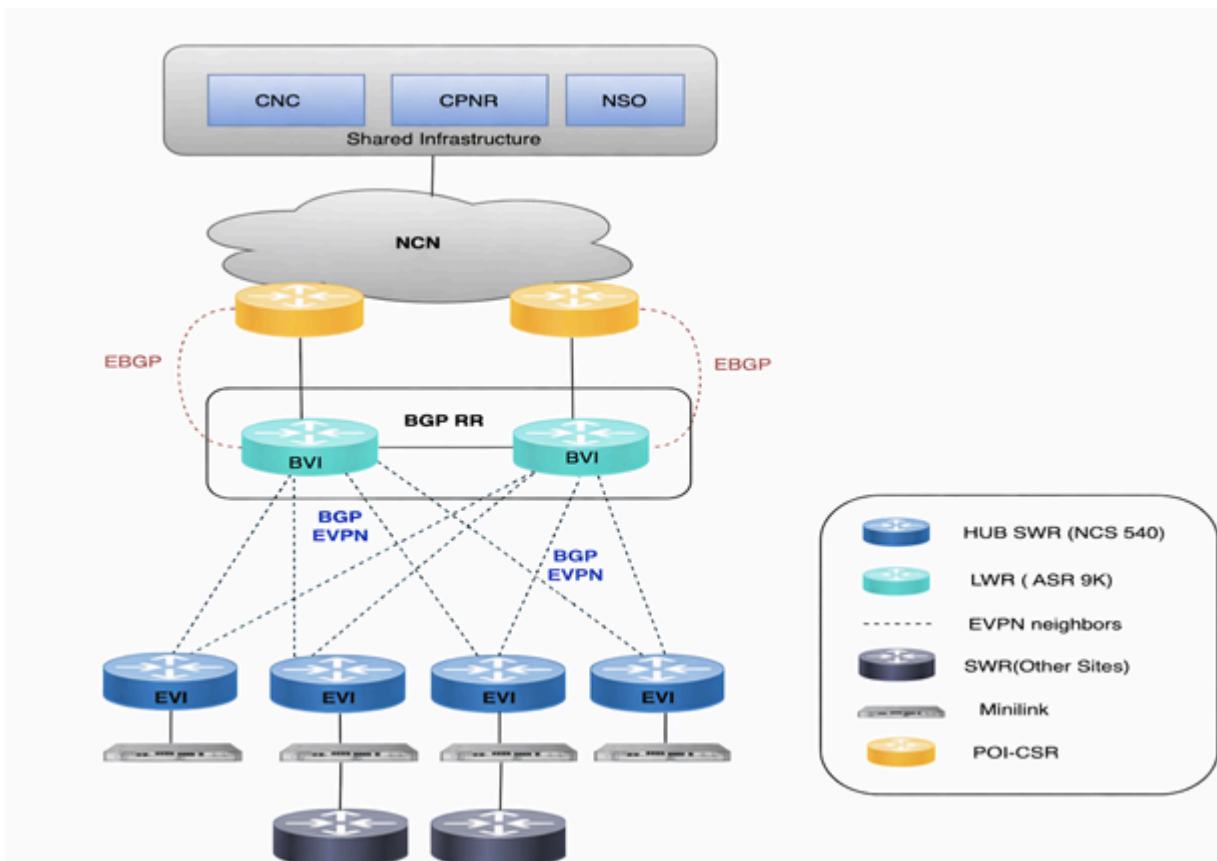


Diagrama de Rede



## Fluxo de trabalho de migração detalhado do CNC 4.1 → 7.1

Migração em fases de ponta a ponta do antigo CNC 4.1 para o CNC 7.1 (O mesmo fluxo pode ser seguido para qualquer Atualização do CNC, independentemente das versões)

Planejar	Laboratório	Laboratório do cliente	Pronto para produção	Distribuição da produção	Período de impregnação	Entrega	Desativação		
<p>FASE 1</p> <p>1 Planejamento e preparação</p> <table border="1"> <tr> <td> <p>ESCOPO E PLANEJAMENTO</p> <ul style="list-style-type: none"> <li>Definição do âmbito</li> <li>Planejamento de capacidade</li> </ul> </td> <td> <p>PROGRAMAÇÃO</p> <ul style="list-style-type: none"> <li>Alterar a identificação da janela</li> <li>Alinhamento das partes interessadas</li> </ul> </td> </tr> </table>								<p>ESCOPO E PLANEJAMENTO</p> <ul style="list-style-type: none"> <li>Definição do âmbito</li> <li>Planejamento de capacidade</li> </ul>	<p>PROGRAMAÇÃO</p> <ul style="list-style-type: none"> <li>Alterar a identificação da janela</li> <li>Alinhamento das partes interessadas</li> </ul>
<p>ESCOPO E PLANEJAMENTO</p> <ul style="list-style-type: none"> <li>Definição do âmbito</li> <li>Planejamento de capacidade</li> </ul>	<p>PROGRAMAÇÃO</p> <ul style="list-style-type: none"> <li>Alterar a identificação da janela</li> <li>Alinhamento das partes interessadas</li> </ul>								
▼									

FASE 2

2 Validação interna do laboratório

<p>INFRAESTRUTURA</p> <ul style="list-style-type: none"><li>· Construir CNC 7.1 (híbrido/trabalhadores)</li><li>· Instalar aplicativos</li><li>· Implantar NSO com HA</li><li>· Implantar pares SR-PCE</li></ul>	<p>VALIDAÇÃO</p> <ul style="list-style-type: none"><li>· Validar todos os casos de uso</li><li>· Aprovação funcional</li></ul>
--	--



FASE 3

3 Validação do laboratório do cliente

<p>CRIAÇÃO DE INFRAESTRUTURA</p> <ul style="list-style-type: none"><li>· Construir CNC 7.1 (híbrido/trabalhadores)</li><li>· Instalar aplicativos</li><li>· Implantar NSO com HA</li><li>· Implantar pares SR-PCE</li></ul>	<p>MIGRAÇÃO DE DADOS</p> <ul style="list-style-type: none"><li>· Exportar artefatos CNC 4.1</li><li>· Recriar grupos de dispositivos</li><li>· Importação para CNC 7.1</li><li>· Implantar pacotes NSO</li></ul>	<p>ALCANCE DO DISPOSITIVO</p> <ul style="list-style-type: none"><li>· Atualizações de ACL</li><li>· Importação de dispositivos e anexo CDG</li></ul>	<p>SERVIÇOS E OBSERVABILIDADE</p> <ul style="list-style-type: none"><li>· Reconciliação e sincronização de serviços</li><li>· Capacitação de KPI e trabalhos de coleta</li><li>· Ativação do script do manual de atividades do BNM</li><li>· Observabilidade HI/Grafana</li><li>· Integração Radius</li><li>· Integração do Splunk</li><li>· Integração do OneFM</li></ul>
---	--	--	--

			· Ativar backups CNC				
✓ Executar ATP no Laboratório e Obter Aprovação							
▼							
<p>FASE 4</p> <p>4 Preparação da produção</p> <table border="1"> <tr> <td> <p>SEGURANÇA E ACESSO</p> <ul style="list-style-type: none"> <li>· Análise de segurança</li> <li>· Configuração de controles de acesso</li> </ul> </td> <td> <p>INFRAESTRUTURA</p> <ul style="list-style-type: none"> <li>· Dimensionamento e configuração de VMs de produção</li> <li>· Validação da rede</li> </ul> </td> </tr> </table>				<p>SEGURANÇA E ACESSO</p> <ul style="list-style-type: none"> <li>· Análise de segurança</li> <li>· Configuração de controles de acesso</li> </ul>	<p>INFRAESTRUTURA</p> <ul style="list-style-type: none"> <li>· Dimensionamento e configuração de VMs de produção</li> <li>· Validação da rede</li> </ul>		
<p>SEGURANÇA E ACESSO</p> <ul style="list-style-type: none"> <li>· Análise de segurança</li> <li>· Configuração de controles de acesso</li> </ul>	<p>INFRAESTRUTURA</p> <ul style="list-style-type: none"> <li>· Dimensionamento e configuração de VMs de produção</li> <li>· Validação da rede</li> </ul>						
▼							
<p>FASE 5</p> <p>5 Conversão da produção</p> <p>↻ Repete todas as etapas da Fase 3 — no ambiente de produção</p> <table border="1"> <tr> <td> <p>CRIAÇÃO DE INFRAESTRUTURA</p> <ul style="list-style-type: none"> <li>· Construir CNC 7.1 (híbrido/trabalhadores)</li> <li>· Instalar aplicativos</li> <li>· Implantar NSO com HA</li> <li>· Implantar pares SR-PCE</li> </ul> </td> <td> <p>MIGRAÇÃO DE DADOS</p> <ul style="list-style-type: none"> <li>· Exportar artefatos CNC 4.1(Provedores, perfis de credencial, playbooks, tags)</li> <li>· Recriar grupos de dispositivos</li> <li>· Importação para CNC 7.1</li> <li>· Implantar pacotes</li> </ul> </td> <td> <p>ALCANCE DO DISPOSITIVO</p> <ul style="list-style-type: none"> <li>· Atualizações de ACL</li> <li>· Importação de dispositivos e anexo CDG</li> </ul> </td> <td> <p>SERVIÇOS E OBSERVABILIDADE</p> <ul style="list-style-type: none"> <li>· Reconciliação e sincronização de serviços</li> <li>· Capacitação de KPI e trabalhos de coleta</li> <li>· Ativação do manual de atividades do BNM</li> <li>· HI/Grafana, Splunk, OneFM</li> </ul> </td> </tr> </table>				<p>CRIAÇÃO DE INFRAESTRUTURA</p> <ul style="list-style-type: none"> <li>· Construir CNC 7.1 (híbrido/trabalhadores)</li> <li>· Instalar aplicativos</li> <li>· Implantar NSO com HA</li> <li>· Implantar pares SR-PCE</li> </ul>	<p>MIGRAÇÃO DE DADOS</p> <ul style="list-style-type: none"> <li>· Exportar artefatos CNC 4.1(Provedores, perfis de credencial, playbooks, tags)</li> <li>· Recriar grupos de dispositivos</li> <li>· Importação para CNC 7.1</li> <li>· Implantar pacotes</li> </ul>	<p>ALCANCE DO DISPOSITIVO</p> <ul style="list-style-type: none"> <li>· Atualizações de ACL</li> <li>· Importação de dispositivos e anexo CDG</li> </ul>	<p>SERVIÇOS E OBSERVABILIDADE</p> <ul style="list-style-type: none"> <li>· Reconciliação e sincronização de serviços</li> <li>· Capacitação de KPI e trabalhos de coleta</li> <li>· Ativação do manual de atividades do BNM</li> <li>· HI/Grafana, Splunk, OneFM</li> </ul>
<p>CRIAÇÃO DE INFRAESTRUTURA</p> <ul style="list-style-type: none"> <li>· Construir CNC 7.1 (híbrido/trabalhadores)</li> <li>· Instalar aplicativos</li> <li>· Implantar NSO com HA</li> <li>· Implantar pares SR-PCE</li> </ul>	<p>MIGRAÇÃO DE DADOS</p> <ul style="list-style-type: none"> <li>· Exportar artefatos CNC 4.1(Provedores, perfis de credencial, playbooks, tags)</li> <li>· Recriar grupos de dispositivos</li> <li>· Importação para CNC 7.1</li> <li>· Implantar pacotes</li> </ul>	<p>ALCANCE DO DISPOSITIVO</p> <ul style="list-style-type: none"> <li>· Atualizações de ACL</li> <li>· Importação de dispositivos e anexo CDG</li> </ul>	<p>SERVIÇOS E OBSERVABILIDADE</p> <ul style="list-style-type: none"> <li>· Reconciliação e sincronização de serviços</li> <li>· Capacitação de KPI e trabalhos de coleta</li> <li>· Ativação do manual de atividades do BNM</li> <li>· HI/Grafana, Splunk, OneFM</li> </ul>				

	NSO		· Ativar backups CNC		
✓ Distribuição da produção					
▼					
<p>FASE 6</p> <p>6 Período de impregnação</p> <table border="1"> <tr> <td> <p>MONITORAMENTO</p> <ul style="list-style-type: none"> <li>· Monitorização da estabilidade</li> <li>· Linha de base de desempenho</li> </ul> </td> <td> <p>GERENCIAMENTO DE PROBLEMAS</p> <ul style="list-style-type: none"> <li>· Acompanhamento e resolução de problemas</li> <li>· Processo de encaminhamento</li> </ul> </td> </tr> </table>				<p>MONITORAMENTO</p> <ul style="list-style-type: none"> <li>· Monitorização da estabilidade</li> <li>· Linha de base de desempenho</li> </ul>	<p>GERENCIAMENTO DE PROBLEMAS</p> <ul style="list-style-type: none"> <li>· Acompanhamento e resolução de problemas</li> <li>· Processo de encaminhamento</li> </ul>
<p>MONITORAMENTO</p> <ul style="list-style-type: none"> <li>· Monitorização da estabilidade</li> <li>· Linha de base de desempenho</li> </ul>	<p>GERENCIAMENTO DE PROBLEMAS</p> <ul style="list-style-type: none"> <li>· Acompanhamento e resolução de problemas</li> <li>· Processo de encaminhamento</li> </ul>				
▼					
<p>FASE 7</p> <p>7 Documentação e transferência</p> <table border="1"> <tr> <td> <p>DOCUMENTAÇÃO</p> <ul style="list-style-type: none"> <li>· MOPs, documentos de projeto e documentos operacionais</li> <li>· Diagramas de arquitetura</li> </ul> </td> <td> <p>TRANSFERÊNCIA</p> <ul style="list-style-type: none"> <li>· Sessões de transferência de conhecimento</li> <li>· Aprovação de transferência</li> </ul> </td> </tr> </table>				<p>DOCUMENTAÇÃO</p> <ul style="list-style-type: none"> <li>· MOPs, documentos de projeto e documentos operacionais</li> <li>· Diagramas de arquitetura</li> </ul>	<p>TRANSFERÊNCIA</p> <ul style="list-style-type: none"> <li>· Sessões de transferência de conhecimento</li> <li>· Aprovação de transferência</li> </ul>
<p>DOCUMENTAÇÃO</p> <ul style="list-style-type: none"> <li>· MOPs, documentos de projeto e documentos operacionais</li> <li>· Diagramas de arquitetura</li> </ul>	<p>TRANSFERÊNCIA</p> <ul style="list-style-type: none"> <li>· Sessões de transferência de conhecimento</li> <li>· Aprovação de transferência</li> </ul>				
▼					
<p>FASE 8</p> <p>8 Descomissionamento de CNC antigo 4.1</p> <table border="1"> <tr> <td> <p>CLEANUP</p> <ul style="list-style-type: none"> <li>· Desconecte todos os dispositivos do CDG</li> </ul> </td> <td> <p>ARQUIVO</p> <ul style="list-style-type: none"> <li>· Arquivar todas as exportações CNC 4.1</li> </ul> </td> </tr> </table>				<p>CLEANUP</p> <ul style="list-style-type: none"> <li>· Desconecte todos os dispositivos do CDG</li> </ul>	<p>ARQUIVO</p> <ul style="list-style-type: none"> <li>· Arquivar todas as exportações CNC 4.1</li> </ul>
<p>CLEANUP</p> <ul style="list-style-type: none"> <li>· Desconecte todos os dispositivos do CDG</li> </ul>	<p>ARQUIVO</p> <ul style="list-style-type: none"> <li>· Arquivar todas as exportações CNC 4.1</li> </ul>				

<ul style="list-style-type: none"> <li>· Excluir entradas MDT que apontam para 4.1 CDG VMs</li> <li>· Excluir VMs de produção</li> </ul>	<ul style="list-style-type: none"> <li>· Auditoria final e aprovação</li> </ul>	
--	---	--

## Casos de uso

### Provisionamento de serviços L2VPN (com base em EVPN)

O serviço L2VPN fornece conectividade Ethernet de Camada 2 através de vários SWRs, com alguns serviços ancorados em LWRs. A Topologia Ativa CNC é usada para o provisionamento de serviços, enquanto toda a lógica específica do ambiente é implementada através de modelos personalizados NSO.

O provisionamento de L2VPN é tratado como uma atividade de configuração de Dia2 e requer atributos de serviço fornecidos pelo operador.

#### Modelos NSO Personalizados

Vários modelos personalizados foram criados para alinhar-se com convenções de nomenclatura específicas do ambiente e comportamentos de interface:

- CT-l2vpn-swr-hub-and-lwr  
Trata as diferenças de nomeação do lado do hub para bridge -group e bridge -domain em hubs SWR e LWRs.
- CT-l2vpn-swr-nonhub-100 / 101 / 102 / 105  
Remove a interface de uplink ZTP do grupo de pontes EVPN padrão e do domínio de pontes para cada EVI específico de VLAN.

Esses modelos garantem uma configuração de EVPN consistente em toda a rede e abstraem as diferenças de nível de hardware.

### Provisionamento de serviços L3VPN (com base em VRF)

O caso de uso da L3VPN permite a entrega de serviços de Camada 3 através de vários SWRs como endpoint. O provisionamento é realizado por meio da Topologia Ativa do CNC, com requisitos específicos do ambiente implementados usando um modelo NSO personalizado.

Como no L2VPN, essa é uma ação de configuração de Dia 2, exigindo entradas do operador.

## Modelo NSO personalizado

- CT-l3vpn-sw  
Coleta parâmetros específicos de VRF (número AS, nome VRF, conjunto de prefixos, nome de política de rota, diferenciador de rota) e cria a política de importação/exportação de BGP necessária, incluindo a redistribuição de rotas conectadas com uma política de rota definida pelo usuário.

## Engenharia de tráfego

A aplicação Crosswork Optimization Engine (COE) do conjunto CNC ajuda a controlar os fluxos de tráfego na rede com base na intenção desejada.

Há dois tipos de tráfego que exigem propósitos diferentes (métricas de SLA):

- Tráfego TC1 - SLA sensível à latência para garantir que o tráfego esteja no caminho de latência mais baixa.
- Tráfego TC4 - SLA de largura de banda mínima para garantir que a largura de banda dedicada esteja sempre disponível para o tráfego TC4

### Tráfego TC1 (menor latência)

Para garantir que o tráfego TC1 seja sempre usado no caminho de latência mais baixa, é necessário ter uma política de roteamento de segmento (SR) criada no SWR do headend com critérios de computação de caminho como latência.

Isso é obtido definindo a configuração On Demand Next Hop (ODN) em cada SWR de headend para a cor específica 1001 usando o CNC para facilitar a criação da política de SR.

### Tráfego TC4 (largura de banda comprometida)

Para garantir que o tráfego TC4 seja sempre usado no caminho com largura de banda dedicada, é necessário ter uma política SR criada no SWR do headend com critérios de computação de caminho como largura de banda.

Isso é obtido por:

- Largura de banda sob demanda (BoD) pacote de função no CNC
- Definindo a configuração de ODN (On Demand Next Hop, próximo salto sob demanda) em cada SWR de headend para a cor específica 1004 usando a criação de política do CNC SR com essas configurações

O pacote de funções BoD é usado para calcular o caminho para políticas SR que têm a largura de banda como critério para o cálculo do caminho. Ele rastreia a largura de banda comprometida com uma política e monitora o caminho atual da política durante seu ciclo de vida.

A qualquer momento, se o patch atual da política de BWOD não tiver capacidade suficiente disponível para atender à largura de banda comprometida, ele recalcula o caminho da política de BWOD e redireciona a política para o novo caminho. Esse novo roteamento de política BWOD é um processo contínuo e não precisa de intervenção manual.

De certa forma, o BWOD otimiza a largura de banda imediatamente, da mesma forma que o SR-PCE faz com a latência.

## Ativação de dispositivo usando sZTP

No antigo modelo tradicional de instalação e suporte, o processo de ativar um novo dispositivo exigia um certo nível de experiência do instalador para instalar, configurar e solucionar problemas da implementação de um novo componente. Também pode haver um longo processo de pré-transferência do equipamento em um local externo, com o suporte de muitas pessoas que trabalham em diferentes partes da solução.

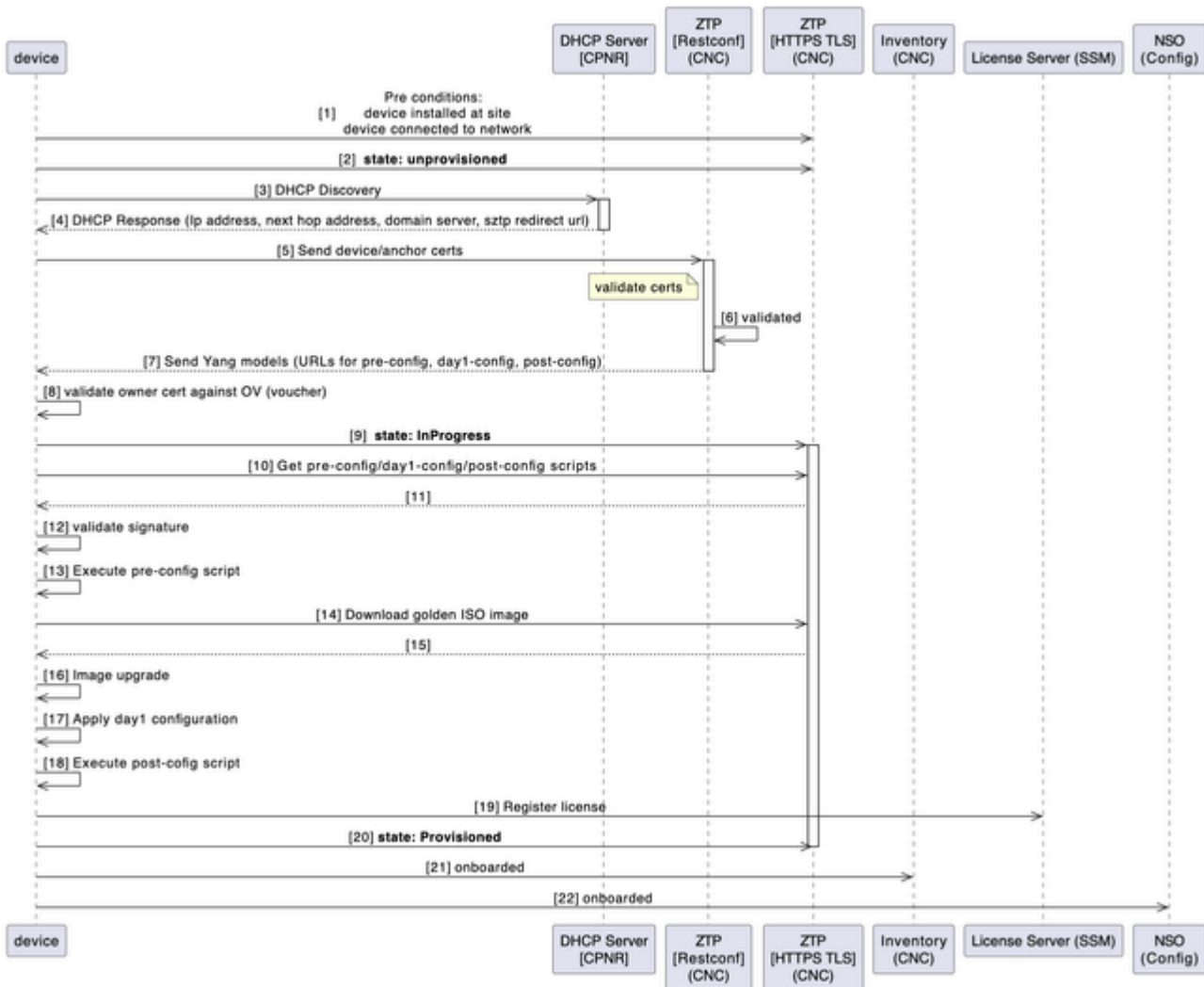
Para novos dispositivos SWR planejados para serem implantados em seu ambiente, esse processo de ativação do dispositivo é automatizado com a aplicação ZTP (Zero Touch Provisioning) segura do CNC.

O fluxo de trabalho do ZTP é acionado na primeira inicialização do dispositivo e ele faz o download da imagem da plataforma planejada e da configuração inicial que precisa ser aplicada sem qualquer intervenção manual.

O dispositivo também é integrado automaticamente no CNC para posterior orquestração.

Este diagrama mostra o fluxo de trabalho do processo ZTP seguro na ativação do dispositivo:

### Secure Zero Touch Provisioning



### Orquestração pós-ZTP (orientada por automação)

Uma automação Python no host de utilitários orquestra e audita o processo completo usando uma entrada estruturada do Excel (por cadeia):

- Gera e carrega artefatos de Dia-1 e pós-configuração no CNC.
- Cria reservas CPNR (entradas DHCP associadas ao SWR serial).
- Adiciona dispositivo no EPNM (para visibilidade/garantia).
- Limpeza pós-ZTP em CNC:
  - Atribui SWRs aos CDGs (destino de telemetria)
  - Anexa a grupos de dispositivos e marcas
  - Atualiza latitude/longitude para visualização de topologia
  - Anexa o perfil de KPI do BNM para habilitar o streaming de telemetria

Processamento de mensagem de notificação de largura de banda (BNM) no CNC

O SWR pode receber o BNM do switch MiniLink co-localizado, que corresponde à largura de banda das portas WAN. Essas mensagens de notificação são mensagens CFM baseadas em padrão, que incluem a largura de banda gravada atual (RBW) e a largura de banda máxima configurada, também conhecida como largura de banda nominal (NBW).

A largura de banda atual é a largura de banda real em execução do link da WAN de micro-ondas, com base nas larguras de banda agregadas dos links de micro-ondas individuais e seus níveis de QAM em execução. A largura de banda nominal é a largura de banda máxima de WAN possível configurada, com base nas larguras de banda agregadas do QAM máximo configurado em cada um dos links de micro-ondas individuais.

A otimização da largura de banda é realizada com base neste cenário:

#### Alteração Temporária (Eventos Fugazes)

- Quando há uma degradação ou falha passageira na rede/link localizado no SWR (por exemplo, devido a um evento climático adverso que causa enfraquecimento do caminho de rádio de micro-ondas e redução na largura de banda disponível devido a alterações nos esquemas de modulação), a correção da modelagem de tráfego ocorre no SWR local na interface de rede afetada.
- Isso garante que ocorra perda mínima de pacotes no caminho de transmissão afetado.

Quando um SWR é ativado com KPI BNM no CNC como parte de atividades pós-sZTP, o CNC envia configurações de telemetria para o SWR.

#### MDT BNM

orientado por modelo de telemetria

```
destination-group <DGName>
```

```
vrf VRF-OMSWR-<AreaCode>1
```

```
address-family ipv4 <CDG IPv4Address> porta 9010
```

```
encoding self-describe-gpb
```

```
protocolo tcp
```

!

!

sensor-group <GroupName>

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

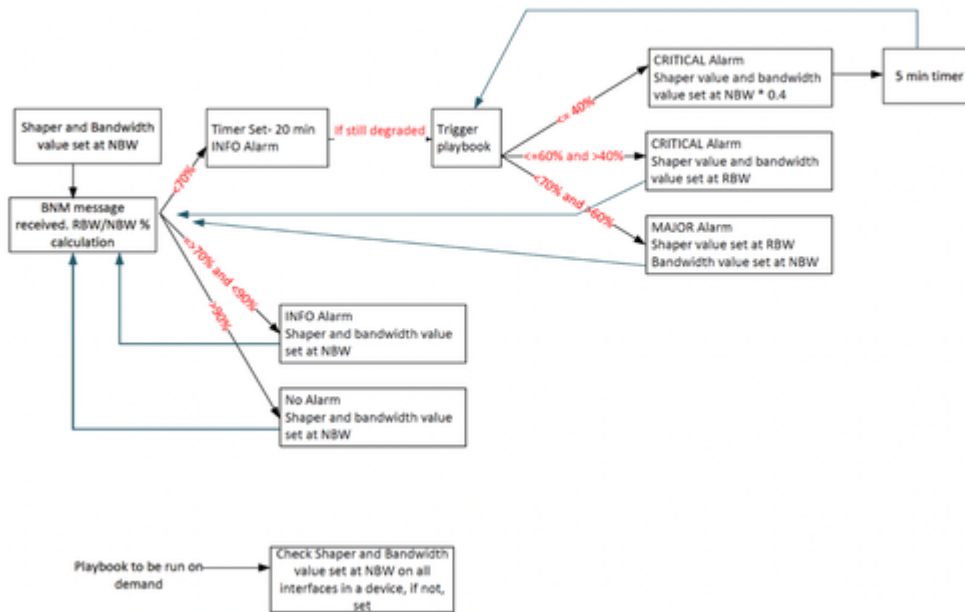
!

O CNC processa essas mensagens BNM recebidas por telemetria e toma medidas corretivas, se necessário. Aqui estão os 2 componentes envolvidos no CNC:

- HI (Health insight, insight da integridade): o aplicativo CNC é usado para incluir a notificação BNM por um KPI personalizado que monitora o caminho específico do sensor para mensagens BNM. O Health Insight é capaz de emitir alertas caso as alterações na largura de banda sejam significativas para serem seguidas.
- Automação de alterações (CA): o aplicativo CNC é usado para atuar na transmissão de mensagens BNM que causaram alertas HI. 2 manuais de atividades personalizados são implantados para fazer essas alterações na interface afetada:
  - Definindo o formador de QoS como novo RBW
  - Definindo a capacidade da interface para o novo valor RBW.

Um script Python personalizado é desenvolvido para executar lógica personalizada e executar os manuais de atividades da CA automaticamente quando KPIs HI são violados.

O script de disparo do manual de atividades opera com base neste algoritmo:



Esta tabela explica os níveis de alerta personalizados que foram definidos em graus de degradação da largura de banda:

Largura de banda reportada = RBW

Largura de banda nominal = NBW

Valor dos intervalos de alerta	Nível de notificação
$(RBW/NBW) * 100 \geq 70$	Informações
$(RBW/NBW) * 100 < 70$ e $> 60$	Aviso
$(RBW/NBW) * 100 \leq 60$	Crítico

Esse caminho do sensor é monitorado pelo CNC:

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

Um KPI personalizado é criado no CNC para monitorar o caminho do sensor BNM. Esse KPI é adicionado a um perfil de KPI configurado com uma cadência de 120 segundos e limites de alerta. Anexar SWRs a esse perfil automaticamente envia a configuração de telemetria necessária aos

dispositivos por meio do NSO.

Uma vez ativados, os dispositivos transmitem dados RBW/NBW para os CDGs atribuídos no intervalo configurado. O Health Insight (HI) calcula a proporção RBW+NBW e gera alertas quando os limites são ultrapassados; os operadores podem monitorar esses eventos em HI e por meio de painéis Grafana.

Um provedor de alertas no CNC encaminha esses alertas para o nó híbrido que hospeda a automação Python. O script analisa os detalhes do dispositivo/interface/RBW/NBW e aciona os manuais de atividades apropriados do Change Automation: ajuste do modelador, atualização da largura de banda ou ambos com base na lógica de decisão definida.

Estes são os dois manuais de atividades usados no fluxo de trabalho:

1. Manual para alterar o valor do modelador
2. Manual para alterar a largura de banda da interface

Como já mencionado, o script gira um servidor Web para atuar como provedor para se comunicar com o CNC usando a API REST. Qualquer resposta recebida para uma solicitação POST é capturada aqui. Os alertas são capturados no formulário em JSON e, em seguida, convertidos em dicionário para extrair os parâmetros necessários.

**Padronize as operações de rede do dia seguinte por meio de manuais de atividades de automação personalizada**

Os manuais de atividades da automação de alterações personalizadas (CA) foram desenvolvidos para simplificar e padronizar as operações críticas do dia 2 em todo o ciclo de vida da rede. Isso inclui provisionamento de Bundle-Ether, atualizações de descrição de interface de gerenciamento, orquestração de encadeamento em cascata CFM, expansão contínua da capacidade do link, desativação do eNodeB e integração eficiente do MiniLink. Com a incorporação de práticas recomendadas operacionais em fluxos de trabalho reutilizáveis, esses manuais de atividades melhoram significativamente a consistência da execução, minimizam o risco de erro humano e reduzem a dependência de intervenções manuais. No contexto de uma atualização do Cisco CNC, essa estrutura de automação desempenha um papel fundamental na aceleração da recuperação operacional, garantindo a continuidade do serviço e permitindo processos escaláveis e repetíveis alinhados com os objetivos de transformação de rede modernos.

**Continuidade da integração TACACS+ na atualização do Cisco CNC 7.1**

Como parte da atualização do Cisco CNC 4.1 para 7.1, a integração TACACS+ existente foi cuidadosamente preservada para garantir a continuidade da Autenticação e Autorização centralizadas. O processo de atualização validou e replicou a configuração TACACS+ no Cisco CNC 7.1, mantendo o alinhamento com políticas de segurança corporativa estabelecidas e mecanismos de controle de acesso baseado em funções (RBAC).

## Encaminhamento de syslog CNC e CDG para Splunk

Um encaminhamento de syslog é configurado para encaminhar os alarmes/eventos/syslogs para um servidor Splunk. A capacidade de configuração imediata do CNC para configurar o Servidor syslog foi usada para conseguir isso.

## Encaminhamento de Alarmes para o OneFM

Os alarmes CNC também são encaminhados para um sistema ascendente como o OneFM, utilizando a API orientada para conexão CNC restconf:

```
curl -L --request GET \  
--url https://{server_ip}:30603/crosswork/notification/restconf/streams/v2/alarm.json \  
--header 'Accept: application/txt'). This API must be used over a websocket connection config.
```

## Automação de Backups CNC diários

Um script automatizado usa a API de backup do CNC para fazer o backup completo do CNC e armazena o arquivo de backup no host do utilitário. Esta operação é feita diariamente.

## Desafios

### Big Jump na versão Crosswork

A atualização do Cross work 4.4 para 7.1 representou um salto significativo na versão, em vez de uma atualização incremental de rotina. Um salto tão grande introduziu inúmeros novos recursos em vários aplicativos, juntamente com aprimoramentos substanciais e alterações de arquitetura. Por causa disso, a atualização do CNC não era apenas uma substituição simples de versão, exigia validação completa para garantir compatibilidade, estabilidade e funcionalidade adequada

em todos os componentes integrados. O conjunto expandido de recursos e as melhorias subjacentes significaram que os fluxos de trabalho, configurações e integrações existentes precisavam de verificação cuidadosa, tornando testes e validações abrangentes essenciais para o sucesso da atualização.

## Não há atualização no local

O CNC não suporta um modelo de atualização no local. Em vez disso, as atualizações devem seguir uma abordagem de substituição, em que a implantação existente é preservada, enquanto um ambiente completamente novo é criado do zero com a versão de destino. Depois que o novo sistema é instalado, as configurações, os dados e as integrações devem ser cuidadosamente migrados e validados antes que o ambiente mais antigo possa ser descomissionado.

Essa abordagem apresenta vários desafios operacionais:

- **Ambientes paralelos:** Tanto o antigo como o novo ambiente CNC devem ser executados simultaneamente até que a migração e a validação sejam totalmente concluídas.
- **Pressão dos recursos de hardware:** A execução de dois ambientes completos em paralelo aumenta significativamente a demanda por recursos de computação, armazenamento e rede, o que pode sobrecarregar a infraestrutura disponível.
- **Esforço de validação estendido:** Todos os dados, configurações, políticas e integrações migrados devem ser verificados na nova versão para garantir que funcionem exatamente como esperado.
- **Complexidade da migração de dados:** A transferência de dados históricos, configurações de aplicativos e configurações operacionais exige um planejamento cuidadoso para evitar inconsistências ou perda de dados.
- **Encerramento diferido:** O sistema mais antigo e suas VMs não podem ser excluídos até que a nova implantação seja comprovadamente estável, prolongando o uso de recursos e a sobrecarga operacional.
- **Coordenação operacional:** As equipes devem gerenciar a sincronização entre os dois ambientes durante o período de transição para evitar interrupções na configuração ou interrupções operacionais.
- **Conflitos de automação de loop fechado:** O CNC suporta casos de uso de automação de loop fechado que acionam ações dinamicamente com base em condições de rede em tempo real. Quando os controladores antigos e os novos estão ativos durante a transição, há um risco de que a mesma lógica de automação possa ser executada em ambos os controladores, resultando potencialmente em alterações de configuração duplicadas ou ações conflitantes na rede. Isso exige controle cuidadoso das políticas de automação durante a janela de migração.
- **Os dados operacionais antigos, incluindo alarmes históricos, eventos, registros de falhas e informações de auditoria, não são migrados para o novo ambiente devido à ausência de recursos nativos de exportação. Como resultado, esses dados históricos não estão disponíveis no sistema atualizado e devem ser tratados como não recuperáveis após a migração.**

Devido a esses fatores, o modelo de elevação e deslocamento torna as atualizações do CNC mais intensas em recursos e mais complexas operacionalmente em comparação com uma atualização padrão no local.

## Ocorrências de implantação sem opções de reversão

Certos erros de configuração de implantação e pós-implantação no CNC não têm caminho de correção e exigem uma desmontagem e reimplantação completa do cluster. Por exemplo, um FQDN incorreto configurado para o VIP de dados de Crosswork , obrigatório para o caso de uso sZTP, tornou o sZTP não funcional. Como esse valor não pode ser corrigido após a implantação, uma reimplantação completa foi necessária.

Da mesma forma, a configuração incorreta de credenciais de substituição de dispositivo na Automação de Alterações não pôde ser retificada após a implantação, levando a outra recriação de cluster. Outros erros, como IPs de gateway configurados incorretamente ou definições de sub-rede, também são identificados como não recuperáveis.

Esses cenários destacam a importância crítica de validar todos os parâmetros imutáveis durante a implantação inicial. O planejamento meticuloso e a verificação de entrada são essenciais para evitar o dispendioso retrabalho e o impacto na programação.

## Restrições da Validação de Diagnóstico Pós-Implantação

O CNC fornece um utilitário de diagnóstico para avaliar os parâmetros de integridade no nível da VM, como latência de leitura/gravação de disco, IOPS, latência de sincronização, velocidade da interface de rede e frequência de clock da CPU. O utilitário reporta os valores medidos em relação aos limites esperados e marca cada verificação como aprovada ou reprovada. No entanto, esses diagnósticos podem ser executados somente após a implantação do cluster, não deixando nenhum mecanismo para validar a prontidão da infraestrutura antes da implantação.

Durante a instalação, o indicador "Ignorar verificações de diagnóstico" é definido como falso por padrão. Na prática, se uma única verificação falhar, o instalador será interrompido, impedindo que a implantação continue. Como resultado, os engenheiros de campo são frequentemente obrigados a ativar esse indicador e ignorar totalmente os diagnósticos, já que até mesmo os ambientes de produção frequentemente falham em uma ou mais verificações. Isso cria um dilema operacional: as equipes devem escolher entre aplicar validação rigorosa que bloqueie a implantação ou prossiga sem a garantia de que a infraestrutura subjacente atende aos parâmetros de desempenho recomendados.

## Alteração de Procedimento de Criação de KPI Personalizado HI

No Health Insight 4.1, a criação personalizada de KPI contou com a lógica do script Tick, em que as definições de KPI e a lógica de processamento foram implementadas usando scripts na estrutura Tick. No entanto, na versão 7.1, essa abordagem foi substituída por uma estrutura baseada em arquivos de rastreamento para definir e gerenciar KPIs.

Devido a essa alteração de arquitetura, os KPIs personalizados existentes não puderam ser reutilizados diretamente e exigiram retrabalho para alinhar com o novo formato de arquivo do rastreador. Isso exigiu uma quantidade substancial de tempo e esforço para:

- Entenda a nova estrutura: A equipe teve que estudar a estrutura, a sintaxe e o comportamento operacional do modelo de definição de KPI baseado em arquivos do rastreador introduzido na versão 7.1.
- Reprojetar a lógica existente: A lógica anteriormente implementada em scripts Tick tinha que ser traduzida e adaptada para o formato de arquivo tracker.
- Recriar KPIs do BNM: O KPI do BNM personalizado teve que ser recriado usando a nova estrutura para garantir que produzissem os mesmos resultados e insights de antes.
- Validar precisão do KPI: Uma validação extensiva foi necessária para confirmar que as novas implementações geraram métricas consistentes e corretas em comparação com a versão anterior.
- Teste e ajuste: O novo modelo também exigia testes de desempenho e comportamento em condições reais de rede, seguidos de ajustes quando necessário.
- Falta de suporte: Alguns recursos que funcionavam anteriormente com o script tick não eram mais suportados com a implementação do novo arquivo tracker. Por conseguinte, foi necessário estabelecer alguns compromissos.

Essa alteração no mecanismo de criação de KPI aumentou significativamente o esforço necessário durante a atualização, pois envolveu o aprendizado de um novo sistema e a reimplementação da lógica de monitoramento personalizada existente para garantir a continuidade dos insights operacionais.

## Tempo Limite de API no Script de Disparo de Playbooks BNM

Os manuais de atividades do BNM são acionados através de um script personalizado que interage com APIs CNC. Durante o processo de atualização e validação, vários problemas relacionados à autenticação e ao tratamento de resposta da API foram identificados e abordados.

O token de API do CNC tem uma validade de 8 horas, mas o script original não incluía a lógica apropriada para atualizar o token quando ele expirasse. Como resultado, embora os alertas de KPI no CNC 4.4 estivessem funcionando corretamente, o script de disparo do manual de

reprodução parou de ser executado após a expiração do token. Esse problema passou despercebido por um longo período, o que significa que o script de automação não estava sendo executado de forma confiável há mais de um ano. O problema só ficou visível durante as atividades de migração e validação no CNC 7.1.

Por conseguinte, foram necessárias várias melhorias e aperfeiçoamentos:

- Lógica de atualização de token: A lógica correta foi implementada para detectar a expiração do token e atualizar automaticamente o token de API, garantindo a execução ininterrupta do script.
- Alterações de resposta de API: As diferenças entre as versões do CNC causaram problemas adicionais. No CNC 4.1, uma resposta de token expirado normalmente continha a mensagem "expirado", enquanto no CNC 7.1, a resposta retorna "Chave não autorizada". A lógica do script tinha que ser atualizada para interpretar corretamente os novos padrões de resposta na versão 7.1.
- Manipulação global de token: Anteriormente, os tokens eram armazenados e usados localmente nas funções. Isso criou cenários em que o token era válido ao entrar em uma função, mas expirava antes das chamadas de API subsequentes. A implementação foi modificada para usar manipulação global de token, garantindo consistência e atualização adequada em todas as funções.
- Tratamento de erros aprimorado: Em alguns casos, a API de "sincronização de verificação" do NSO retornou respostas que estavam incompletas ou diferentes da estrutura esperada. Isso causou exceções `KeyError`, que suspenderam a execução do script. Lógica de validação e tratamento de exceções adicionais foram introduzidas para que o script possa continuar em execução mesmo quando respostas inesperadas de API são recebidas.
- Aprimoramentos de estabilidade de script: Proteções e verificações adicionais foram adicionadas para garantir que falhas de API, problemas de resposta temporária ou eventos de atualização de token não causem o encerramento inesperado do script.

Essas melhorias não só resolveram os problemas descobertos durante a atualização, mas também melhoraram significativamente a confiabilidade, resiliência e capacidade de manutenção da estrutura de automação do manual de atividades do BNM.

## Alteração de Design do Disparador do Manual e Processamento do BNM

A lógica de automação do BNM é orientada por eventos e se baseia em alertas gerados por KPIs no aplicativo Health Insight no CNC. O fluxo de trabalho geral opera da seguinte maneira:

1. O CNC lê os valores de NB (largura de banda nominal) e RBW (largura de banda real) do dispositivo.
2. Ele calcula a taxa de largura de banda (BW%) usando esses valores.
3. O KPI de Informações de Integridade avalia essa proporção em relação aos limites de alerta

predefinidos.

4. Quando um alerta é gerado, o script de disparo de manual de atividades do BNM detecta o alerta e executa os manuais de atividades corretivos correspondentes

### Limitação no Design de alerta original

Os limites de alerta configurados foram:

- $BW\% < 60$  → Crítico
- $60 \leq BW\% \leq 70$  → Aviso
- $BW\% > 90$  → Informações

Esse projeto funcionou bem para identificar a degradação da largura de banda, mas criou uma lacuna funcional durante os cenários de recuperação de largura de banda. Especificamente, a faixa de 70 a 90% não tinha um nível de alerta definido.

Isso levou a este comportamento:

- Quando o BW% cai abaixo de 70%, um alerta Crítico ou de Aviso é gerado, acionando os manuais de atividades que ajustam os valores do modelador e da largura de banda.
- No entanto, quando a largura de banda foi recuperada e o BW% aumentou acima de 70%, o KPI não gerou nenhum alerta porque o valor caiu na faixa de 70-90% sem nenhum nível de alerta associado.
- Como o script de automação BNM depende inteiramente da geração de alertas para acionar ações, ele não teve oportunidade de ler valores NBW/RBW atualizados ou iniciar ações de restauração.
- Como resultado, a restauração da largura de banda não ocorreu automaticamente, mesmo que uma largura de banda suficiente tenha se tornado disponível. Não havia lógica de restauração também no projeto original.

Essa limitação tornou-se visível na rede de produção, onde os links que tinham anteriormente sofrido redução de largura de banda permaneceram em um estado restrito mesmo depois que as condições melhoraram.

### Impacto da Alteração da Estrutura de KPI

O problema foi ainda agravado pela mudança de estrutura introduzida no CNC 7.1. No Health Insight 4.1, a implementação do KPI baseado em Tick suportou até cinco níveis de alerta, permitindo um melhor controle das faixas de limiar e tornando a lógica de restauração mais fácil de implementar.

No entanto, no CNC 7.1, a estrutura de KPI baseada em arquivos do rastreador suporta apenas três níveis de alerta, o que reduziu a flexibilidade na definição de vários limites de recuperação e exigiu a reprojeção da lógica de alerta para se ajustar a essas restrições.

## Disparo Excessivo do Manual

Outra questão identificada na implementação original foi a frequência extremamente alta de execuções do manual de atividades. A lógica de automação não incluiu nenhum tempo de espera ou janela de estabilização. Assim que o CNC ler um valor do dispositivo que atende à condição de alerta:

- O alerta foi emitido imediatamente.
- O script de automação acionou imediatamente os manuais de atividades corretivos.

Como os valores de telemetria flutuam com frequência nas redes ativas, isso fez com que centenas de manuais de atividades fossem acionados a cada hora, o que não era ideal do ponto de vista da estabilidade da rede e do desempenho de aplicativos.

## Lógica de automação reprojeta

Para lidar com essas limitações, o projeto de automação do BNM foi reformulado com várias melhorias:

- Lógica de limite de alerta revisado: Para garantir que a banda de recuperação fosse capturada dentro dos três níveis de alerta, a lógica foi modificada para que qualquer BW% maior que 70% seja tratado como um alerta de nível INFO, substituindo a abordagem anterior, onde apenas valores acima de 90% foram classificados como INFO. Isso garantiu que a banda de recuperação de 70 a 90% fosse monitorada ativamente, permitindo que os manuais de reprodução de restauração fossem acionados quando as condições de largura de banda melhorassem.
- Introdução do tempo de espera: Um mecanismo de tempo de espera de 20 minutos foi introduzido para garantir que as condições de largura de banda permaneçam estáveis por uma duração definida antes de acionar os manuais de atividades. Isso evita que a automação reaja a flutuações de curto prazo.
- Execução controlada do manual: Com a lógica revisada e o tempo de espera, a frequência de execuções do manual de atividades foi reduzida drasticamente, evitando ações de automação desnecessárias.
- Mecanismo de reforço para degradação grave: Nos casos de degradação severa da largura de banda, foi introduzida uma abordagem de reforço. Nesses cenários, a automação ajusta proativamente o modelador de tráfego e a alocação de largura de banda para 40% do NBW, permitindo uma recuperação mais rápida do congestionamento.
- Melhor estabilidade de automação: O fluxo de trabalho reprojeta garante que a redução

da largura de banda e os cenários de restauração da largura de banda sejam manipulados de forma eficaz, mesmo dentro das limitações da estrutura de KPI com base no rastreador.

## Resultado

Com essas alterações de design, combinadas com as melhorias anteriores no tratamento de API, gerenciamento de token e robustez de script, a estrutura de automação do BNM agora opera de uma maneira muito mais estável, eficiente e previsível. O sistema pode responder corretamente ao congestionamento e às condições de recuperação, evitando execuções excessivas do manual de atividades e garantindo uma otimização confiável da largura de banda da rede.

## Supressão de Alarmes do Dispositivo

No CNC 4.1, os alarmes foram encaminhados para um sistema ascendente chamado OneFM através de uma API RESTCONF. Como a pilha CNC 4.1 não incluía a funcionalidade EMF, a plataforma gerou apenas alarmes em nível de sistema. Esses alarmes foram encaminhados upstream sem qualquer complexidade relacionada à categorização de alarmes.

Com a implantação do CNC 7.1, a aplicação EMF foi introduzida, expandindo significativamente o modelo de alarme. Agora, os alarmes foram categorizados em três tipos:

- Alarmes do sistema - relacionados com a plataforma CNC e saúde da aplicação
- Alarmes de rede - relacionados às condições do serviço de rede
- Alarmes de dispositivos - gerados diretamente de dispositivos de rede e encaminhados através do CNC

No entanto, já havia um EPNM responsável por coletar e gerenciar alarmes em nível de dispositivo. Se o CNC também encaminhou esses alarmes para o OneFM, isso resultou em alarmes duplicados sendo recebidos de ambos os sistemas. Portanto, o requisito era excluir os alarmes de dispositivos do CNC enquanto ainda encaminhava os alarmes de rede e do sistema.

O principal desafio foi uma limitação da API ascendente RESTCONF usada para encaminhar alarmes para o OneFM. A API não oferece suporte à filtragem de alarmes com base na categoria de alarme. Se essa filtragem estivesse disponível, a solução teria sido simples: simplesmente exclua os alarmes de dispositivos no nível da API antes de encaminhá-los para o sistema ascendente.

Várias soluções potenciais foram avaliadas e discutidas:

- Interrupção de armadilhas de dispositivos na origem: Impeça que os dispositivos enviem armadilhas para o CNC.
- Alarmes de filtragem no sistema ascendente (OneFM): Permitir que o CNC envie todos os alarmes, exceto os alarmes do dispositivo de filtro, no OneFM.
- Filtragem no CNC antes de encaminhar alarmes.

A interrupção de armadilhas no nível do dispositivo não foi considerada viável porque o CNC conta com essas armadilhas para detectar eventos do dispositivo e manter a consciência operacional das condições da rede. Desabilitar armadilhas reduziria significativamente a capacidade do CNC de responder a problemas de rede.

A solução finalmente implementada aproveitou um recurso CNC incorporado chamado Supressão de Alarme de Dispositivo. Esse recurso permite que os administradores suprimam tipos específicos de alarmes de dispositivos com base em grupos de dispositivos, impedindo que eles sejam processados ou encaminhados mais upstream.

Ao configurar políticas de supressão de alarme de dispositivo, o sistema foi capaz de:

- Suprima alarmes gerados por dispositivos dentro do CNC.
- Continue processando e encaminhando os alarmes do sistema e da rede.
- Impeça que alarmes de dispositivos duplicados acessem o sistema OneFM.

Essa abordagem proporcionou uma solução limpa e escalável sem interromper a capacidade da CNC de receber armadilhas de dispositivos. Como resultado, o fluxo de alarme para o OneFM foi otimizado, garantindo que apenas os alarmes relevantes do sistema e da rede fossem encaminhados, evitando a duplicação com o gerenciamento de alarmes do dispositivo do EPNM.

## Alterações fora da banda

Na configuração existente, a equipe de operações frequentemente dependia de scripts diretos baseados em CLI para enviar atualizações de configuração para dispositivos de rede, particularmente para tarefas como modificações de ACL e atividades de depuração. Embora eficaz a curto prazo, essa abordagem levou a um desvio de configuração, pois as alterações feitas fora do NSO não foram rastreadas dentro do sistema. Como resultado, os fluxos de trabalho de provisionamento do NSO foram afetados devido a inconsistências entre o estado pretendido (modelado) e as configurações reais do dispositivo, levando a falhas e ineficiências operacionais.

## Reconciliação de VPN L2/L3

Devido a alterações de configuração fora da banda: a equipe de rede atualizou a configuração relacionada à VPN em dispositivos fora do CNC/NSO e do fluxo de trabalho TSDN. Como resultado, o estado armazenado na NSO (da era CNC 4.1) nem sempre correspondia ao estado nos dispositivos.

Essas discrepâncias causaram várias falhas e inconsistências de reconciliação. Em vários casos, o NSO continha dados de serviço VPN que não existiam mais nos dispositivos (ou que tinham sido modificados de uma forma que o NSO não refletia). Para alinhar o NSO com a rede, foi necessário remover as entradas de serviço VPN que existiam apenas no NSO e não nos dispositivos e corrigir outras incompatibilidades causadas por alterações fora da banda.

## Impacto da Agenda

A resolução desses problemas exigiu aproximadamente duas semanas adicionais em relação ao plano de reconciliação original. O tempo extra foi gasto identificando incompatibilidades, validando o estado do dispositivo e limpando ou corrigindo com segurança os dados NSO CDB.

## Observações

1. Autoridade de configuração: As alterações fora de banda na configuração da VPN (ou em qualquer configuração gerenciada por TSDN) criam um descompasso entre o NSO e a rede e complicam a reconciliação.
2. Linha de base pré-migração: Uma linha de base clara do estado NC/NSO-managed vs device-only antes da migração teria facilitado a detecção e a resolução de discrepâncias.
3. Automação e conversão: Scripts de conversão de payload e personalizações específicas do usuário foram essenciais para lidar com diferenças de formato e modelo entre 4.1 e 7.1 de forma consistente.

## Recomendações para atualizações semelhantes

1. Imponha um congelamento de alteração para serviços VPN (e outros serviços gerenciados por TSDN) durante a janela de reconciliação, com exceções somente por meio de um processo controlado.
2. Executar uma auditoria de pré-reconciliação comparando o NSO CDB com a configuração do dispositivo para quantificar e listar as discrepâncias antes de iniciar a reconciliação.
3. Documente e socialize que as alterações de VPN devem passar pelo CNC/NSO TSDN após a atualização para evitar a recorrência de desvio fora da banda.
4. Manter scripts de conversão e reconciliação para reutilização em atualizações futuras ou para solução de problemas.

## Falha de backup do CNC devido a dependências do modo de manutenção

O mecanismo de backup CNC exige que a plataforma seja colocada em modo de manutenção antes que uma operação de backup possa ser iniciada. Por projeto, a API de backup aplica esse pré-requisito; se o CNC não conseguir fazer a transição para o modo de manutenção, o processo de backup será automaticamente anulado.

Na prática, entrar no modo de manutenção frequentemente falhou devido a atividades contínuas do sistema, incluindo:

- Execuções do Active Change Automation playbook (MOP)
- Fluxos de trabalho sZTP contínuos
- Operações de serviço DLM
- Anexação de perfil de KPI ou atividades de desanexação
- Coleções de showtech sob demanda
- Tarefas de orquestração em segundo plano

A presença de qualquer atividade impede o CNC de entrar no modo de manutenção, fazendo com que a operação de backup falhe antes da execução.

### Impacto operacional

Os backups CNC diários necessários para conformidade e garantia operacional. No entanto, a atividade de automação frequente, particularmente os manuais de atividades acionados pelo BNM, significava que o sistema muitas vezes era incapaz de entrar no modo de manutenção. Como resultado, as falhas de backup ocorreram repetidamente, criando um risco operacional significativo e necessitando de intervenção manual.

### Estratégia de mitigação

1. Otimização da programação de backup: Foi identificada uma janela de manutenção com atividade mínima do sistema. Com base na análise de tráfego e automação, o trabalho de backup foi agendado para as 5:00 da manhã (AEST), quando a orquestração e a execução do manual tinham menor probabilidade de estar ativas.

2. Validação da atividade de pré-backup: uma pré-verificação automatizada foi introduzida antes da chamada da API de backup:

- O script consulta APIs CNC para detectar trabalhos MOP de Alterar Automação em execução.

- Se algum trabalho for relatado comoRunning, o script aguardará 5 segundos e tentará novamente.
- Esse loop continua até que o sistema informe que não há trabalhos ativos.
- Somente depois que o ambiente for confirmado como ocioso, o script tentará ativar o modo de manutenção e acionar o backup.

Isso evitou tentativas desnecessárias de backup enquanto o sistema estava em um estado operacional ocupado.

3. Mecanismos de repetição e resiliência: Para acomodar estados de sistema transitórios, salvaguardas adicionais foram adicionadas:

- Até três novas tentativas se a API de backup retornar uma falha
- Intervalos de atraso curtos entre novas tentativas
- Manuseio de erros harmonioso para evitar o término do script

## Resultados e resultado

A mitigação combinada melhorou significativamente a confiabilidade do backup:

- As falhas de backup foram drasticamente reduzidas
- Após a implementação, apenas duas falhas foram observadas, ambas causadas por um processo sZTP travado, que está fora do controle do script.
- A introdução de atrasos de execução na automação do manual de atividades do BNM reduziu ainda mais a contenção com o modo de manutenção.

## Encaminhando syslogs para Splunk

O destino syslog foi configurado no CNC para encaminhar logs para Splunk sobre TLS. No entanto, uma vez recebidos, os logs estavam ilegíveis no lado do Splunk. Devido a esse problema originário do ambiente Splunk, a opção foi escolhida para reverter para o transporte UDP, após o qual os logs foram processados com êxito.

## Problema de Migração do Agrupamento de Dispositivos

O usuário criou previamente 18 grupos de dispositivos no CNC 4.1; no entanto, essa versão não forneceu nenhum mecanismo baseado em UI ou orientado por API para exportar ou importar grupos de dispositivos. Como resultado, a migração desses grupos para o CNC 7.1 exigiu uma

abordagem não padrão. Foram identificadas duas APIs CNC internas: um expondo a hierarquia de grupo de dispositivos e outro listando os dispositivos mapeados para cada nó da hierarquia. Usando essas APIs, todos os grupos de dispositivos e seus dispositivos associados foram extraídos e armazenados como saídas JSON. Um script personalizado foi desenvolvido para analisar as respostas e extrair apenas os nomes de host do dispositivo de cada grupo.

O CNC 7.1 introduziu capacidades nativas de importação/exportação para grupos de dispositivos, incluindo um modelo de importação baseado em CSV. Depois de extrair os nomes de host do sistema legado, um segundo script de automação foi criado para preencher os modelos CSV no formato necessário, garantindo que cada grupo de dispositivos pudesse ser importado de forma precisa e independente. Essa automação foi essencial; sem ele, a migração dos grupos de dispositivos para o CNC 7.1 teria sido significativamente mais demorada e operacionalmente complexa.

## Isole Dispositivos Degradados Com Grande Largura De Banda

Apesar da implementação do caso de uso de BNM para corrigir automaticamente as baixas taxas de RBW/NBW, um subconjunto de dispositivos continuou a permanecer em estados gravemente degradados por períodos prolongados. Embora os manuais de ferramentas de modelagem e ajuste de largura de banda normalmente restaurassem dispositivos logo após eventos de degradação, vários dispositivos persistiram em um estado crítico por mais de uma semana e exigiram intervenção manual. Identificar esses dispositivos, no entanto, representou um desafio. Embora a IU CNC forneça visualizações claras de alertas e métricas de largura de banda, ela não revela facilmente dispositivos que permaneceram exclusivamente em um estado Crítico durante um intervalo prolongado.

Para resolver essa lacuna operacional, foi desenvolvida uma solução orientada por API. O CNC oferece uma API que recupera uma lista dos principais dispositivos geradores de alertas em janelas de tempo configuráveis (por exemplo, 7 dias, um mês). Ao obter esses dados e filtrar por dispositivos que geraram apenas alertas críticos durante o período selecionado, a equipe conseguiu isolar rapidamente os dispositivos que exigem correção manual. Essa abordagem automatizada melhorou significativamente a eficiência da solução de problemas e reduziu o tempo necessário para identificar casos de degradação persistente.

## Remoção da configuração de telemetria do dispositivo

No CNC 4.1, as configurações de telemetria enviadas do NSO através do pacote thetm-tcf function foram aplicadas automaticamente quando um dispositivo foi associado a um perfil KPI de Insight de Saúde (HI). No entanto, essas configurações, incluindo referências VIP de CDG, não foram removidas quando o perfil de KPI foi desanexado posteriormente. Como resultado, os dispositivos

acumularam entradas de telemetria obsoletas e redundantes ao longo do tempo.

Este problema tornou-se mais pronunciado durante a atualização para o CNC 7.1. Os dispositivos muitas vezes mantiveram as configurações de telemetria CDG VIP legadas do CNC 4.1, juntamente com as novas entradas geradas pelo CNC 7.1, levando a várias configurações de telemetria conflitantes em mais de 2.000 dispositivos. Foram levantadas preocupações sobre o impacto operacional e a higiene da configuração, já que apenas a configuração VIP do CNC 7.1 CDG deve ter permanecido ativa.

Para resolver isso, um script automatizado foi desenvolvido para identificar e remover referências VIP CDG obsoletas da configuração de telemetria de cada dispositivo. Essa solução eliminou as inconsistências de configuração, restaurou o alinhamento com o modelo de telemetria 7.1 esperado e impediu o que teria sido vários dias de esforço de limpeza manual em toda a grande frota de dispositivos.

## Solucionar problemas da coleção MDT

No CNC 7.1, a maioria das coleções de KPI de Insight de Saúde (HI) dependem da Telemetria Controlada por Modelo (MDT). Quando um perfil de KPI é ativado em um dispositivo, o NSO programa automaticamente os caminhos do sensor necessários e configura o CDG VIP como o destino de telemetria. Uma vez aplicada essa configuração, um trabalho de coleta de CDG correspondente é criado para rastrear o status de telemetria do dispositivo.

Durante a validação, foi relatado que mais de 100 dispositivos não tinham configurações de telemetria. A identificação desses dispositivos através da interface de usuário do CNC mostrou-se impraticável, já que a IU suporta apenas a filtragem por dispositivo e não escala eficientemente para uma frota superior a 2.000 dispositivos. Isso exigia um método automatizado para determinar quais dispositivos não tinham configuração de telemetria e precisavam de reativação de KPI.

Para resolver isso, utilizamos a marca BNM atribuída aos dispositivos sempre que um perfil de KPI é ativado. Primeiro, foi gerada uma exportação de todos os dispositivos com a marca BNM. Um script Python foi desenvolvido para interagir com a API de coleta CNC, incorporando a lógica de paginação para recuperar o conjunto completo de trabalhos de coleta (cada chamada de API retorna um máximo de 100 entradas). O script extraiu nomes de host dos dados de trabalho de coleção e os comparou com a lista de dispositivos com marcas BNM exportada.

Essa comparação rendeu a lista de dispositivos que foram marcados, mas não apareceram no trabalho de coleta do BNM, indicando que a configuração de telemetria do MDT não foi aplicada. O perfil de KPI foi reativado nesses dispositivos, e a validação confirmou que todos os trabalhos de coleta correspondentes foram criados corretamente.

Essa automação otimizou significativamente o processo de solução de problemas, permitindo que a equipe identificasse e corrigisse todos os dispositivos afetados em um único dia, um esforço que não seria viável através da inspeção manual.

## Mudanças de comportamento de HA e ajuste de algoritmo de consenso em NSO 6.4.1.1

Durante a atualização do Cisco NSO 5.7.5.1 para 6.4.1.1 como parte da transição do Cisco CNC 7.1, uma mudança notável foi observada no comportamento de Alta Disponibilidade (HA) devido à habilitação implícita do algoritmo de consenso na versão mais recente do NSO. Esse não era o comportamento padrão no NSO 5.7.5.1, levando a uma mudança nas características de failover após o upgrade. Especificamente, quando o nó primário foi desativado, o nó secundário passou para um estado somente leitura, impedindo que manipulasse as atividades de provisionamento. Da mesma forma, quando o nó secundário é desativado, o nó primário passa de um estado primário ativo para um estado "nenhum", afetando a continuidade do serviço.

Para restaurar o comportamento de HA esperado alinhado com a implantação anterior, o algoritmo de consenso foi explicitamente desabilitado no NSO 6.4.1.1. Esse ajuste garantiu que os nós primário e secundário retomassem suas funções pretendidas durante cenários de failover, permitindo provisionamento ininterrupto e mantendo a estabilidade operacional consistente com a versão anterior do NSO.

## Aprimoramentos de Atualização de Versão NSO e Compatibilidade de Pacote

Como parte da transição do Cisco CNC 4.1 para 7.1, a versão subjacente do Cisco NSO foi atualizada de 5.7.5.1 para 6.4.1.1. Esta atualização de versão introduziu alterações nas estruturas de modelo XML dentro dos pacotes NSO existentes, levando a falhas em certos casos de teste de regressão que dependiam do comportamento do modelo legado.

Para resolver essas lacunas de compatibilidade, os modelos de pacote NSO afetados foram analisados e atualizados para se alinharem com o esquema revisado e os requisitos de processamento do NSO 6.4.1.1. Essas melhorias garantiram que todos os fluxos de trabalho de automação e modelos de serviço continuassem a funcionar como esperado, restaurando a estabilidade de regressão e mantendo a consistência em todo o ambiente CNC atualizado.

## Problemas com a habilitação de KPI em escala

O CNC fornece um mecanismo de interface de usuário pronto para ativar perfis de KPI em dispositivos. Embora esta abordagem funcione bem para as pequenas frotas, torna-se ineficiente e pouco fiável em larga escala. Nessa implantação, mais de 2.000 dispositivos SWR exigiam a

habilitação de KPI, e a interface do usuário não oferecia uma maneira eficaz de selecionar ou processar dispositivos em massa.

Inicialmente, foi tentada uma abordagem baseada em marcação: todos os dispositivos SWR receberam uma marca SWR e a habilitação de KPI foi executada usando a seleção de marca em vez da seleção manual de dispositivos. No entanto, o processamento de mais de 2.000 dispositivos em um único fluxo de trabalho levou a desafios operacionais significativos. O trabalho foi executado por mais de três horas e concluído com centenas de falhas. Embora todos os dispositivos tenham sido incluídos na intenção, apenas ~750 receberam com êxito a habilitação de KPI, e tentativas repetidas produziram apenas progresso incremental. Essa abordagem não se mostrou escalável nem repetitiva. Ele mostrou problemas significativos com a carga.

Um segundo desafio surgiu de problemas de sincronização de dispositivos NSO. Muitas falhas indicaram que o NSO não foi sincronizado com os dispositivos correspondentes. A tentativa de operações manuais de sincronização seguidas pela reativação de KPI era impraticável e exigiria um grande esforço do operador.

Para lidar com essas limitações, foi desenvolvido um fluxo de trabalho automatizado e controlado por lote:

1. Exportar o inventário completo do CNC.
2. Processar dispositivos em lotes de 50 (identificados como o tamanho ideal por meio de ajuste).
3. Para cada lote, acione uma sincronização automatizada usando UUIDs de dispositivo.
4. Execute a habilitação de KPI por meio da API do CNC.
5. Monitore programaticamente o histórico de trabalhos de KPI e registre falhas.
6. Reprosse os dispositivos com falha repetindo as etapas de sincronização e habilitação de KPI.
7. Quando um lote for concluído com êxito, passe para o próximo conjunto de 50 dispositivos.

A automação também incluiu a capacidade de desabilitar perfis de KPI, permitindo o gerenciamento do ciclo de vida completo.

Essa solução forneceu um processo otimizado, determinístico e altamente escalável para provisionamento de KPI. Ela eliminou a intervenção manual, garantiu resultados consistentes e economizou vários dias de esforço operacional. A mesma automação provou-se inestimável quando os perfis de KPI tiveram que ser desabilitados e reabilitados após a alteração do design do BNM, permitindo uma reconfiguração rápida e sem erros em toda a frota de 2.000 dispositivos.

RESTCONF API ascendente restrita ao acesso do administrador

A API ascendente baseada em RESTCONF usada para encaminhar alarmes e eventos do CNC tem uma limitação em que ela pode ser chamada somente usando a conta admin. As tentativas de acessar a API por meio de contas de serviço não tiveram êxito, apesar dessas contas terem as funções operacionais necessárias. Como solução alternativa, o usuário foi solicitado a usar as credenciais de administrador para o encaminhamento de alarme para o sistema ascendente, introduzindo uma restrição operacional e limitando a adesão aos princípios de acesso de privilégio mínimo.

## Automação como um viabilizador estratégico

Dada a escala e a complexidade do programa de atualização e migração do CNC, a execução manual de tarefas operacionais rapidamente se revelou insustentável. Atividades como integração de dispositivos, provisionamento de KPI, alinhamento de configuração, reconciliação e validação de telemetria envolvem milhares de elementos de rede e fluxos de trabalho repetidos que são altamente propensos a erro humano quando executados manualmente. Portanto, a automação era essencial não apenas para acelerar a execução, mas também para garantir a consistência, reduzir o risco operacional e liberar as equipes de entrega de tarefas repetitivas e demoradas.

Ao sistematizar esses processos por meio de fluxos de trabalho com script e operações orientadas por API, o programa de atualização obteve ganhos de eficiência significativos. A automação permitiu a conclusão mais rápida de tarefas, maior precisão e resultados previsíveis em todas as seções. A economia resultante não só reduziu o cronograma geral de implantação, como também permitiu que os engenheiros se concentrassem em esforços de validação e projeto de valor mais alto, em vez de tarefas operacionais de rotina.

Algumas das atividades de automação foram identificadas antes do início do projeto de atualização, enquanto outras evoluíram quando surgiram desafios. Houve também alguns que foram necessários pelas questões que se desenvolveram durante o curso do projeto.

Esta tabela ilustra as áreas em que a automação gerou um impacto substancial no programa.

Descrição da Tarefa	Esforço Manual (Dias)	Esforço de automação (dias)	Economia estimada (dias)
Atualizações de ACL (SWR/LWR)(2K+)	30.0	2.0	28.0
Migração e conexão de dispositivos ao CDG(2.000+)	5	1.0	4,0

Descrição da Tarefa	Esforço Manual (Dias)	Esforço de automação (dias)	Economia estimada (dias)
Conexão de KPI BNM a dispositivos (2K+)	4,0	1,5 (média)	2.5
Reconciliação de serviço	7	2.5	4.5
Migração de Grupos de Dispositivos	4	0,5	3.5
Isolar dispositivos com largura de banda muito degradada	3	0,5	2.5
Troubleshooting de coleta de MDT	3	0,5	2.5
Totais	56 dias	8,5 dias	47,5 dias

## Lições aprendidas

### A atualização não é simples

O CNC não suporta atualizações no local, e o modelo de elevação e troca introduz uma complexidade operacional significativa. O processo nunca deve ser considerado simples, especialmente quando o salto de versão é grande. Problemas inesperados surgem em aplicativos, integrações e fluxos de trabalho, e cada um exige tempo, análise e mitigação cuidadosa. Um grande salto na versão amplifica esse desafio, tornando essencial o planejamento completo, a validação e a execução em fases. Tivemos que gastar muito tempo extra em casos de TAC e esforços de solução de problemas. Como não mantivemos o tempo de buffer para isso, tornou-se desafiador.

### CX tem que fazer o levantamento pesado

Espere um esforço substancial do CX em implantações, integrações, migração e validação completa de casos de uso. Não presuma que os fluxos de trabalho comprovados na versão antiga

se comportam de forma idêntica na nova versão.- Várias análises e soluções de problemas seriam necessárias para fazer as coisas funcionarem.

## O kit de ferramentas de automação é uma necessidade

A jornada de atualização demonstrou que a automação não é uma conveniência opcional, mas um requisito fundamental para implantações CNC em larga escala. Planejamos a automação para os candidatos necessários no início, mas nunca se pode supor que isso seja suficiente. No meio do projeto, problemas podem ser identificados em casos de uso em que a automação definitivamente agregaria valor, como demonstrado nas seções anteriores.

## Evite conflitos de controlador duplo durante a migração

Durante a atualização, é essencial garantir que os ambientes CNC antigos e novos não estejam ativos simultaneamente. Embora seja necessário um curto período de impregnação para a validação, o seu prolongamento significativo, como aconteceu neste projeto durante mais de dois meses, cria riscos operacionais. Com ambos os CNCs ativos por mais de 15-20 dias, os recursos de automação de loop fechado, como Largura de Banda Sob Demanda, geraram ações inconsistentes e conflitantes em toda a rede, uma vez que a lógica de automação estava sendo executada a partir de dois controladores de uma só vez.

Uma lição importante é implementar barreiras de proteção claras durante a migração. Medidas como desativar administrativamente dispositivos no antigo CNC, pausar fluxos de trabalho de automação ou restringir assinaturas de telemetria teriam evitado esses conflitos. Atualizações futuras devem planejar explicitamente o isolamento estrito do controlador para evitar a interferência de dois controladores e garantir um comportamento de rede previsível.

## MOPs não são sagrados

Embora os documentos do Método de Procedimento (MOP) sejam criados para todas as implantações, integrações e casos de uso, não é realista supor que um MOP validado em condições de laboratório comporte-se de forma idêntica na produção. O ambiente de produção revelou consistentemente desvios, alguns menores, alguns significativos, destacando assim lacunas que não eram visíveis durante os testes controlados. Redes reais, comportamentos antigos, dependências externas e condições de tráfego ao vivo introduzem variáveis que as simulações de laboratório nem sempre podem replicar.

O aprendizado principal é que as equipes devem abordar a implantação da produção com a

expectativa de encontrar comportamentos inesperados, casos avançados e novas descobertas. Flexibilidade, capacidade rápida de solução de problemas e prontidão para adaptar procedimentos em tempo real são essenciais para uma execução bem-sucedida em escala.

## Eficácia dos casos TAC

Os problemas de pós-produção são inevitáveis e, embora a solução inicial de problemas pela equipe de entrega seja valiosa, depender exclusivamente do esforço interno pode levar a atrasos desnecessários. É prudente abrir um caso de TAC em paralelo como uma rede de segurança, especialmente para problemas relacionados a produtos ou comportamentos complexos que não são imediatamente diagnosticáveis. As investigações do TAC geralmente exigem tempo, e atrasar a criação do caso por vários dias pode resultar em perda significativa do momentum do projeto. Envolver o TAC antecipadamente garante que a assistência especializada esteja disponível quando necessário, acelera a identificação da causa básica e evita deslizamentos evitáveis na programação.

## Envolve a CNC BU para um suporte de conhecimento eficaz

Forte apoio da Unidade de Negócios CNC é altamente valioso durante qualquer projeto CNC. Os usuários frequentemente precisam de informações e esclarecimentos detalhados sobre o produto que não estão prontamente disponíveis apenas com a equipe de entrega. Ter um contato de BU acessível durante todo o contrato acelera a resolução de problemas, reforça a precisão técnica e ajuda a criar maior confiança e afinidade do usuário.

## Melhores práticas para atualização do CNC

### Planeje uma estratégia de atualização otimizada

O CNC não suporta atualizações no local, tornando a implantação paralela inevitável. Trate o novo ambiente como uma nova instalação e aloque computação, armazenamento e capacidade administrativa suficientes para executar dois ambientes simultaneamente. Planeje estágios de validação, sequenciamento de migração e atividades de transição com bastante antecedência.

A validação pré-implantação rigorosa é essencial especialmente para parâmetros imutáveis

Muitas experiências destacam a importância crítica da diligência durante a implantação inicial. A validação prévia de todas as principais entradas, particularmente de parâmetros de configuração imutáveis, é essencial para evitar reimplementações dispendiosas e impacto no cronograma. Portanto, o uso de listas de verificação pré-implantação estruturadas, revisões por colegas e validações de simulação é altamente recomendado para minimizar o risco de erros de configuração irreversíveis.

## Use um ambiente de validação dedicado antes de tocar na produção

O estabelecimento de um ambiente interno de CALO/teste no início do projeto permite que as equipes testem, validem fluxos de trabalho, descubram alterações específicas de versão e criem confiança antes de tocar na produção. Isso reduz significativamente as incógnitas durante a implantação final.

## Dimensionamento baseado em evidências para componentes de trabalho cruzado distribuído

Ao projetar clusters, distribuições de CDG e alocações de PCE, baseie as decisões em tipos de dispositivos, escala de interface, complexidade de topologia e intensidade de coleta em vez de contagens simples de dispositivos. Distribuições balanceadas evitam sobrecarga e garantem desempenho previsível em todo o cluster.

## Automação para trabalho repetitivo e de alto volume

Estabeleça um registro posterior de automação no início das tarefas que são repetitivas, de alto volume ou críticas em termos operacionais e invista onde a automação é obrigatória. Valide e refine sua automação no ambiente de SIT primeiro, garantindo que a produção não dependa de correções de última hora. A escala amplifica o custo do trabalho manual; a automação padronizada melhora a qualidade, a velocidade e o controle. Os resultados do pacote são ativos reutilizáveis (interfaces documentadas, tarefas parametrizadas, bibliotecas compartilhadas) para que as equipes possam aproveitar a mesma automação para futuras atualizações de Crosswork e projetos adjacentes, reduzindo o tempo de retrabalho e de integração.

## Evite o controle de loop fechado duplo durante a execução paralela

Durante a coexistência, trate a automação de loop fechado como um recurso de gravador único: somente um caminho de orquestração pode conduzir ativamente a correção ou a configuração

orientada por políticas. O CLA simultâneo em pilhas antigas e novas corre o risco de acionadores duplicados e intenções divergentes, o que pode desestabilizar o estado do dispositivo. Planeje o lançamento do CLA como uma etapa da fase final, após a validação funcional e a transição definitiva para o novo controlador.

## Executar Avaliação de Impacto de Upgrade Estruturado

Os saltos de versão principal introduzem novos recursos ao mesmo tempo em que substituem ou alteram os antigos. É extremamente importante ter em conta estas mudanças. Muitas vezes, a alteração não será documentada nas notas de versão da versão atualizada e será exibida quando chegarmos ao campo. Conduzir avaliações estruturadas de:

- APIs preteridas
- Alterações de estrutura de KPI
- Diferenças de comportamento no nível do aplicativo
- Desvios do modelo de configuração
- Alertas, processamento de topologia e alterações na execução do manual

## Teste a compatibilidade e o comportamento na superfície de integração

O CNC interage com vários sistemas externos, como NSO, SSM, CPNR, EPNM, OneFM, Splunk e estruturas de orquestração.

Antes da migração:

- Validar compatibilidade de versão
- Testar todas as integrações ascendente/descendente
- Confirmar modelos de dados, armadilhas, fluxos de telemetria
- Verificar comportamento de autenticação SSL/RESTCONF

As falhas de integração detectadas após a migração criam pontos cegos operacionais.

## Estabelecer uma estratégia robusta de exportação de dados antes da migração

Exportar tudo antes de iniciar a migração:

- Perfis de credencial
- Provedores

- Tags
- Playbooks personalizados
- KPIs Personalizados
- Funções e RBAC
- Comprovantes sZTP
- Grupos de dispositivos
- Metadados de serviço de histórico

## Migração De Dispositivos Em Lote Com Portas De Validação Integradas

Ao migrar milhares de dispositivos, faça a migração em lotes controlados:

- Mover dispositivos em coortes fixas (por exemplo, por região, carga CDG ou tipo de dispositivo)
- Valide a telemetria, o estado de sincronização NSO e a acessibilidade antes de passar para o próximo lote
- Reverter o lote se forem exibidas anomalias persistentes

Isso evita a alta carga no CDG e no CNC em um curto intervalo de tempo.

## Lidar com alterações de configuração fora da banda por meio da integração de NSO

Para enfrentar o desafio fora da banda como parte da atualização do CNC 4.1 para 7.1, foi implementada uma mudança estruturada para operações conduzidas pelo NSO. A equipe de operações recebeu acesso controlado e baseado no usuário à CLI do NSO, enquanto o acesso administrativo direto à CLI do dispositivo foi restrito para evitar alterações fora da banda. Além disso, os scripts legados da CLI foram sistematicamente convertidos em automação baseada em RESTCONF integrada com NSO, permitindo recursos como validação de execução a seco e reversão transacional. Essa abordagem garantiu que todas as alterações de configuração fossem gerenciadas centralmente, auditáveis e consistentes com os modelos de serviço do NSO, eliminando efetivamente o desvio de configuração e restaurando a confiabilidade do provisionamento.

## Coloque forte ênfase no congelamento de mudanças

Durante as janelas de migração críticas:

- Congelar alterações de rede iniciadas pelo usuário
- Restringir envios de configuração
- Sincronizar com equipes de campo e NOC
- Planeje alguma janela para acomodar atividades de emergência, como a substituição de dispositivos usando o CNC/ZTP e assim por diante.

Isso reduz o ruído e garante que o estado da rede permaneça estável durante toda a atualização

## Conclusão

A migração do CNC 4.1 para o CNC 7.1 constitui um estudo de caso significativo nas complexidades inerentes às atualizações de plataforma de orquestração de rede em grande escala. Esse projeto demonstra que essas transições não são apenas avanços de versão, mas transformações abrangentes em camadas arquitetônicas, fluxos de trabalho operacionais e ecossistemas de automação. A ausência de um caminho de atualização in-loco exigiu uma implantação de elevação e deslocamento total, introduzindo desafios de ambiente paralelos e exigindo uma coordenação meticulosa entre as integrações de CNC, NSO, SR-PCE, CDG e sistema externo. O cenário operacional resultante ressaltou a importância de metodologias de migração robustas, ciclos de validação exaustivos e processos de cutover rigorosamente controlados para mitigar o risco em ambientes de produção.

A atualização revelou ainda mais a importância da automação como um pilar indispensável para escalabilidade e precisão. Com mais de 2.000 dispositivos, amplas configurações de telemetria, vários componentes dependentes e fluxos de trabalho dinâmicos de automação de loop fechado, o projeto destacou as limitações dos procedimentos manuais em ambientes dessa magnitude. A automação desenvolvida especificamente, abrangendo atualizações de ACL, integração de dispositivos, provisionamento de KPI, limpeza de telemetria e isolamento de falhas, se mostrou essencial para garantir o determinismo, reduzir o erro humano e obter ganhos significativos de eficiência. A estrutura de automação não apenas permitiu a continuidade operacional durante a migração, mas também estabeleceu uma base sustentável para a otimização contínua da rede.

Igualmente importante foi o reconhecimento de que o comportamento de produção se desvia marcadamente das condições controladas em laboratório. As alterações de estrutura, como a transição da lógica KPI baseada em Tick para definições baseadas em rastreador, introduziram mudanças de comportamento não antecipadas que exigiram reengenharia, retestes e refinamento iterativo. Da mesma forma, os desafios operacionais relacionados à automação de loop fechado, confiabilidade de telemetria e comportamento de API destacaram a necessidade de solução adaptável de problemas, avaliação proativa de riscos e envolvimento contínuo com especialistas do TAC e da unidade de negócios. Esses fatores ilustram coletivamente que as transições de versão principais exigem profundidade técnica e preparação organizacional. Ainda restam alguns problemas em aberto que devem ser resolvidos na próxima versão 7.2 do crosswork.

No geral, essa atualização demonstra que as migrações bem-sucedidas de CNC de grande escala dependem de quatro pilares básicos: validação rigorosa de pré-implantação, automação sistemática e resiliente, coordenação interfuncional forte e uma postura operacional adaptável que antecipe a divergência entre ambientes de laboratório e de produção. Os insights obtidos com esse engajamento não só contribuíram para uma implantação estável do CNC 7.1, mas também oferecem um modelo para transições futuras, informando as melhores práticas, reforçando os resguardos arquitetônicos e o conhecimento institucional para a evolução subsequente do ecossistema de automação de rede.

## Glossário de termos

Termo	Definição
BNM	Bandwidth Notification Message (Mensagem de notificação de largura de banda).
CAT	Topologia Ativa de Crosswork
CCA	Crosswork Change Automation
CDG	Gateway de dados de trabalho cruzado
CHI	Crosswork Health Insight
CNC	Controlador de rede Cisco Crosswork
COE	Mecanismo de Otimização de Trabalho Cruzado
CPNR	Cisco Prime Network Registrar
CWM	Gerenciador de Fluxo de Trabalho Cruzado
EMF	Funções de Gerenciamento de Elementos
KPI	Indicador Chave de Desempenho

LWR	Roteador sem fio grande
MDT	Telemetria orientada por modelo
MOP	Método de Procedimento
NBW	Largura de banda nominal
NSO	Network Services Orchestrator
RBW	Largura de Banda Gravada
SR-PCE	Elemento de computação de caminho de roteamento de segmento
SSM	Cisco Smart Software Manager
SWR	Roteador sem fio pequeno
TAC	Centro de Assistência Técnica
TSDN	Rede definida por software de transporte
ZTP	Provisionamento Zero Touch
RR	Refletor de rota
RP	Perfil da rota
POI	Ponto De Interconexão
EVPN	Ethernet Virtual Private Network (Rede virtual privada Ethernet).

# Referências

- [Cisco Systems, Notas de versão do Cisco Crosswork Network Controller, Versão 7.1.0](#)
- [Cisco Systems, Guia de instalação do Cisco Crosswork Infrastructure 7.1](#)
- [Cisco Systems, Guia de Administração do Cisco Crosswork Infrastructure 7.1 — Visão Geral dos Conceitos:](#)
- [Cisco Systems, Guia de otimização e engenharia de tráfego de controlador de rede de trabalho cruzado, versão 7.1](#)
- [Cisco Systems, Guia do Usuário do Cisco Crosswork Health Insights, Versão 7.1](#)
- [Cisco Systems, Guia de implantação de provisionamento automatizado \(ZTP\) Crosswork](#)
- [Cisco Systems, Guia de Instalação do Pacote de Função Cisco NSO Transport SDN, Versão 7.1.0](#)
- [Cisco Systems, Guia de configuração do Cisco SR-PCE](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.