CNC升级案例研究

目录

- 简介
- 摘要
- 背景
- 生产网络
- 从CNC 4.1到CNC 7.1的迁移工作流程
- CNC架构和与其他组件的集成
  - 架构图
  - 网络图
  - CNC 4.1 → 7.1详细迁移工作流程
- 使用案例
  - L2VPN（基于EVPN）服务调配
    - 自定义NSO模板
  - L3VPN（基于VRF）服务调配
    - 自定义NSO模板
  - 流量工程
    - TC1流量（最低延迟）
    - TC4流量（承诺带宽）
  - 使用sZTP打开设备
    - 后ZTP协调（自动化驱动）
  - CNC中的带宽通知消息(BNM)处理
    - 临时（短暂事件）更改
    - BNM MDT
  - 通过自定义自动化攻略实现第2天网络运营标准化
  - 思科CNC 7.1升级中的TACACS+集成连续性
  - CNC和CDG系统日志转发到Splunk
  - 警报转发到OneFM
  - 日常CNC备份自动化
- 挑战
  - Crosswork版本中的大跳跃
  - 无就地升级
  - 无回滚选项的部署缺陷
  - 部署后诊断验证的限制
  - HI自定义KPI创建过程更改
  - BNM手册触发器脚本中的API超时
  - BNM处理和手册触发器设计更改
    - 原始警报设计中的限制
    - KPI框架更改的影响
    - 过度触发攻略
    - 重新设计的自动化逻辑
    - 结果

- 设备警报抑制
- 带外更改
- L2/L3 VPN协调
  - 计划影响
  - 观察结果
  - 类似升级的建议
- CNC备份因维护模式依赖性而失败
  - 运营影响
  - 缓解策略
  - 结果和结果
- 将系统日志转发到Splunk
- 设备分组迁移问题
- 隔离带宽严重下降的设备
- 设备遥测配置删除
- 排除MDT集合故障
- NSO 6.4.1.1中HA行为变化及一致性算法调整
- NSO版本升级和软件包兼容性增强功能
- 大规模实施KPI的问题
- RESTCONF北向API限制为管理员访问

自动化作为战略推动力

所学课程

- 升级并不简单
- CX必须完成繁重的工作
- 自动化工具包势在必行
- 避免迁移期间发生双控制器冲突
- MOP不是神圣不可侵犯的
- TAC案例的有效性
- 与CNC BU接洽，提供有效的知识支持

CNC升级的最佳实践

- 规划优化的升级策略
- 严格的部署前验证对于不可变的参数尤其重要
- 在接触生产之前使用专用验证环境
- 基于证据的分布式交叉工作组件规模确定
- 自动化重复的大量工作
- 避免并行运行时的双闭环控制
- 执行结构化的升级影响评估
- 测试整个集成表面的兼容性和行为
- 制定稳健的迁移前数据导出策略
- 带内置验证门的批处理设备迁移
- 通过NSO集成处理带外配置更改
- 大力强调变更冻结

结论

术语词汇表

参考

简介

本文档介绍固定无线网络从Cisco CNC 4.1到7.1通过提举和移位进行复杂的大规模迁移的案例研究。

摘要

本白皮书详细介绍了大规模固定无线网络从Cisco Crosswork Network Controller(CNC)4.1版迁移到7.1版的案例研究。由于没有就地升级机制，此过渡需要完全升降式部署，从而在2000多个网络设备和多个相互依赖的系统之间引入显着的架构、操作和集成复杂性。该研究分析了在多个领域遇到的挑战。

一项重要成果强调了自动化在确保可扩展性、准确性和操作决定性（尤其是对于大批量工作流程）方面的重要作用。这些结果进一步表明，生产环境与受控实验室条件存在很大差异，这要求适应性故障排除、迭代验证以及与TAC和业务部门工程团队的持续接触。此工作提供实际见解、验证方法和推荐的最佳实践，作为未来CNC升级和大规模协调平台过渡的参考蓝图。

背景

5G网络的迅速普及、连接设备的迅速普及，以及企业和消费者环境的数字化，已导致流量显着增加，必须大规模安全可靠地交付多种服务。通信服务提供商(CSP)现在运营高度动态的网络，传统孤立运营工具通常导致复杂性、降低用户体验和增加运营成本(OpEx)。

为了保持竞争力，运营商越来越多地采用建立在自动化、虚拟化、SDN原则以及分析驱动的自我优化网络基础上的现代化运营模式。

Cisco Crosswork Network Controller(CNC)旨在通过简化运营工作流、降低总拥有成本(TCO)以及跨多供应商传输网络实现基于意图的自动化来支持这种转型。CNC为服务调配、网络运行状况监控和实时优化提供统一平台，为运营商提供单一管理平台，以便更主动且高效地管理大型IP网络。

底层Crosswork基础设施提供可恢复的、可扩展的集群框架，所有CNC应用都运行在该框架上。对于CNC 7.1，此模块包括优化引擎、活动拓扑、变更自动化、运行状况见解、元素管理功能(EMF)、服务运行状况和交互工作流程管理器(CWM)等模块，每个模块都有助于端到端协调和保证。

然而，升级CNC带来了独特的挑战。CNC不支持就地升级，需要完全升降式部署，其中新环境与现有环境并行构建，所有数据和服务都迁移到新版本。本案例研究考察了一个从CNC 4.1到CNC

7.1的大规模升级，该升级适用于支持为所有其他服务提供商提供主干服务的澳大利亚主要服务集成商。

由于多个自定义的变更自动化行动手册、自定义的运行状况见解KPI、L2/L3 VPN服务协调要求以及安全ZTP的需要，迁移变得特别复杂。

由于内部架构和行为方面的变化，很难预测现有使用案例在新版本中的行为方式，因此大版本升级带来了额外的不确定性。这就需要跨所有使用案例进行全面验证和协调。

在决定最佳资源分配（包括混合/员工节点计数、CDG分配和PCE规模确定）以及您的现有资源足迹是否可以保留方面，进行了大量的规划。

CNC 7.1初始部署和验证在内部的CALO实验室中执行，为实验、优化配置和建立信心提供了安全的环境。其次是在内部测试环境中部署，该环境密切地反映了生产情况。最后阶段包括在生产中部署CNC 7.1，应用设备级配置更改，以及执行所有设备和相关服务到新控制器的分阶段迁移。

生产网络

气隙式生产网络遍布澳大利亚的广大地区。在NCS到ASR9Ks的2000多个设备出现后，CNC通过实时拓扑视图管理所有这些设备。大约2000台设备是运行IOS-XR 24.3.2的NCS540(本地称为SWR（小型无线路由器）),30台是ASR-9Ks（版本7.5.2）(本地称为LWR（大型无线路由器）)。

Crosswork设置由3个混合节点和2个工作节点组成。设备共有5个CDG，其中4个为主用节点，1个为备用节点。这提供了有限的保护，因为池只有1个备用CDG。但是考虑到你的要求，这已经是允许了。由于所有虚拟机都位于单个数据中心上，因此仅使用1个备用虚拟机也能更轻松地做出决策。

CDG是处理通过SNMP、CLI和GNMI等各种协议从设备收集数据的组件。CDG收集的数据通过内部kafka暴露于Crosswork中。注册到Crosswork的设备必须连接到CDG，CDG使数据网关能够连接到该设备并获取设备数据。

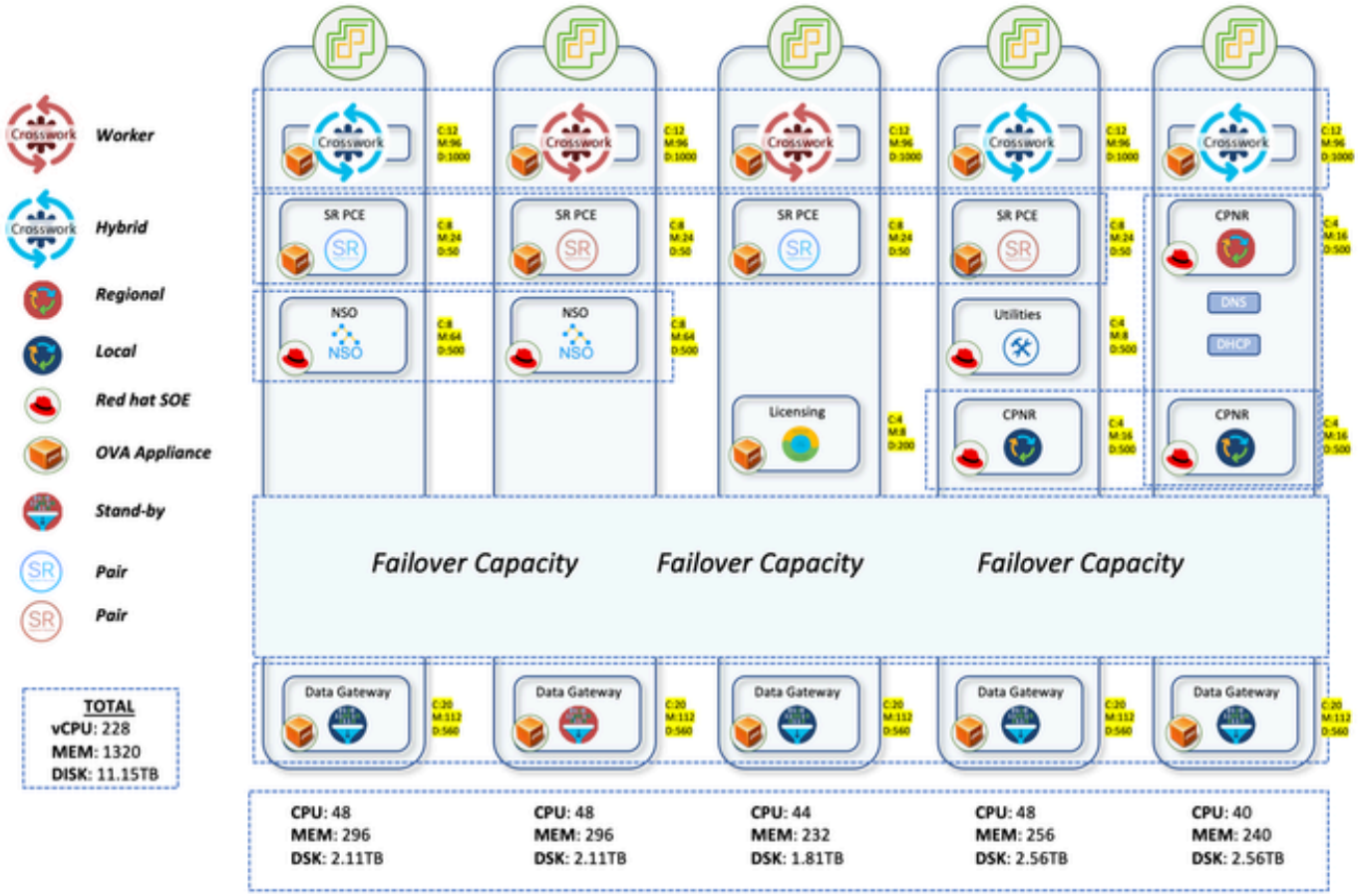
同时，对CDG的器件分布也进行了详细的考虑。早期部署在CDG之间随机分配了设备。这导致了非常不均衡的分布，一些CDG承载更多设备，而有1-2个CDG承载的设备非常少。这导致某些CDG过度消耗和过重的负担，而其他的CDG调配不足。

此处的升级思路是将每个700个SWR分配到4个活动CDG。前三个CDG中容纳了2100个SWR。 接口前部的LWR非常重，均预留给第四个CDG。尽管它们数量很小，数量为30，但此分配可确保即使从这些设备完成更多收集，也不会对CDG造成过大负载。任何后续的SWR入职也将转至第四届CDG。这确保了前三个CDG的统一分布，而第四个CDG有更多空间可供新设备使用。

SR-PCE以2对的方式部署，这意味着有4台虚拟机分布在不同主机上。一对管理7个POI站点，另一

对管理其余8个POI站点。CNC GUI上的拓扑更新通过使用SR-PCE来完成。它通过与其他LWR路由器的BGP-LS对等获取网络拓扑。此组件还用于所有流量工程使用案例，在这些使用案例中，它充当控制器的角色，将流量引导到不同的路径。

要处理所有服务调配和设备配置使用案例，需要将NSO与CNC配合使用。对于生产网络，部署了两个版本为6.4.1.1的NSO，以在高可用性模式下协同工作。SR-PCE(Segment Routing Path Computation Element)是为CNC提供拓扑更新以及处理实时流量工程使用案例所需的组件。此处部署了四个版本为25.2.1的SR-PCE，每个PCE与两个不同的LWR对等。



从CNC 4.1到CNC 7.1的迁移工作流程



对于CNC部署，首选是采用基于docker的部署。但是，由于客户端未批准在其本地设置docker，因此别无选择，只能使用vCenter进行手动部署。与基于脚本的部署相比，这要花费更长的时间，因为它要求我们在vCenter GUI中提供多次输入。

完成CNC部署后，所有需要的应用都与BU一起部署，BU提供自动操作安装文件，可一次性上传和激活应用，从而减少手动执行所需的时间。主要层部署包括Crosswork Optimization Engine、Active Topology、Service Health、Element Management Functions和Crosswork Workflow Manager。除此之外，还设置了包括Change Automation和Health Insight在内的附加包。

CWM和SH没有任何使用案例。但是，由于他们对这些应用程序在下一版本中提供的一些使用案例感兴趣，所以还是部署了这些应用程序。

安装应用程序后，下一步是迁移旧版本的CNC中的数据。这主要包括凭证配置文件、提供商、标记、自定义手册、自定义KPI、角色、sZTP凭证和任何其他数据。CNC提供可用于所有这些CNC的导出选项，然后将其导入到新的CNC。

设置这些设备后，开始设备迁移是审慎之举。在升级时，如果新的CNC部署在新子网中，而旧子网部署在新子网中，则需要在设备上执行ACL更改，以提供与新的CNC的可达性。这是一个非常耗时的过程，因为它需要手动登录每台设备并更改配置。

完成这些ACL更改后，下一步是将设备导入新的CNC并将其连接到CDG。如果可达性正确，并且SSH和SNMP凭证正确，则设备在CNC上显示为可达状态，并且还注册到NSO（网络服务协调器）。

在NSO方面，所有必需的软件包都必须准备妥当，并在操作性上达到要求，以确保CNC可以与NSO通信，反之亦然。例如，要从CNC自动将设备安装到NSO，必须使用DLM功能包。同样，如果有任何要求NSO在设备上配置MDT传感器路径，则必须在NSO上部署TM-TC软件包。要点是，根据使用案例，相关软件包必须部署在NSO上。

我们开发了一个用于调配的自动脚本，而不是采用手动方法来部署这些所需的软件包，尤其是

Transport-SDN软件包。随着CNC 7.1的升级，更新已引入到TSDN包。这些更新的软件包用于在NSO服务器上部署，以确保在升级的环境中继续支持L2/L3调配。该脚本自动安装更新的TSDN包并将必要的元数据加载到NSO，使其能够根据需要调配服务。

思科智能软件管理器(SSM)许可服务器的一个实例和Cisco Prime Network Registrar(CPNR)的3个实例也部署在不同主机上。

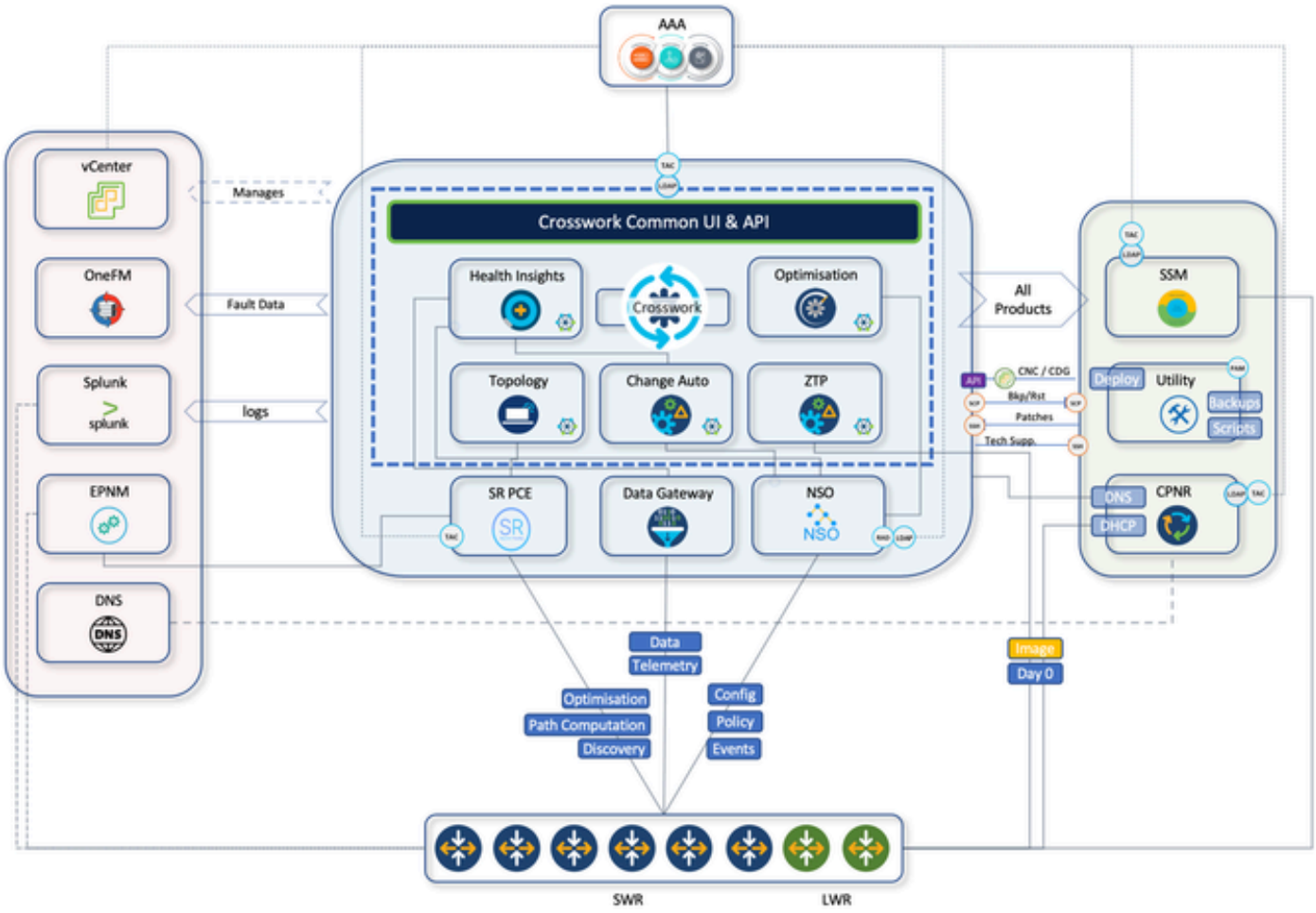
CNC架构和与其他组件的集成

CNC通过统一的UI为调配、优化和可视化部署的服务提供了单一平台。这里简要总结了驻留在CNC平台套件中的CNC内部组件及其使用案例。

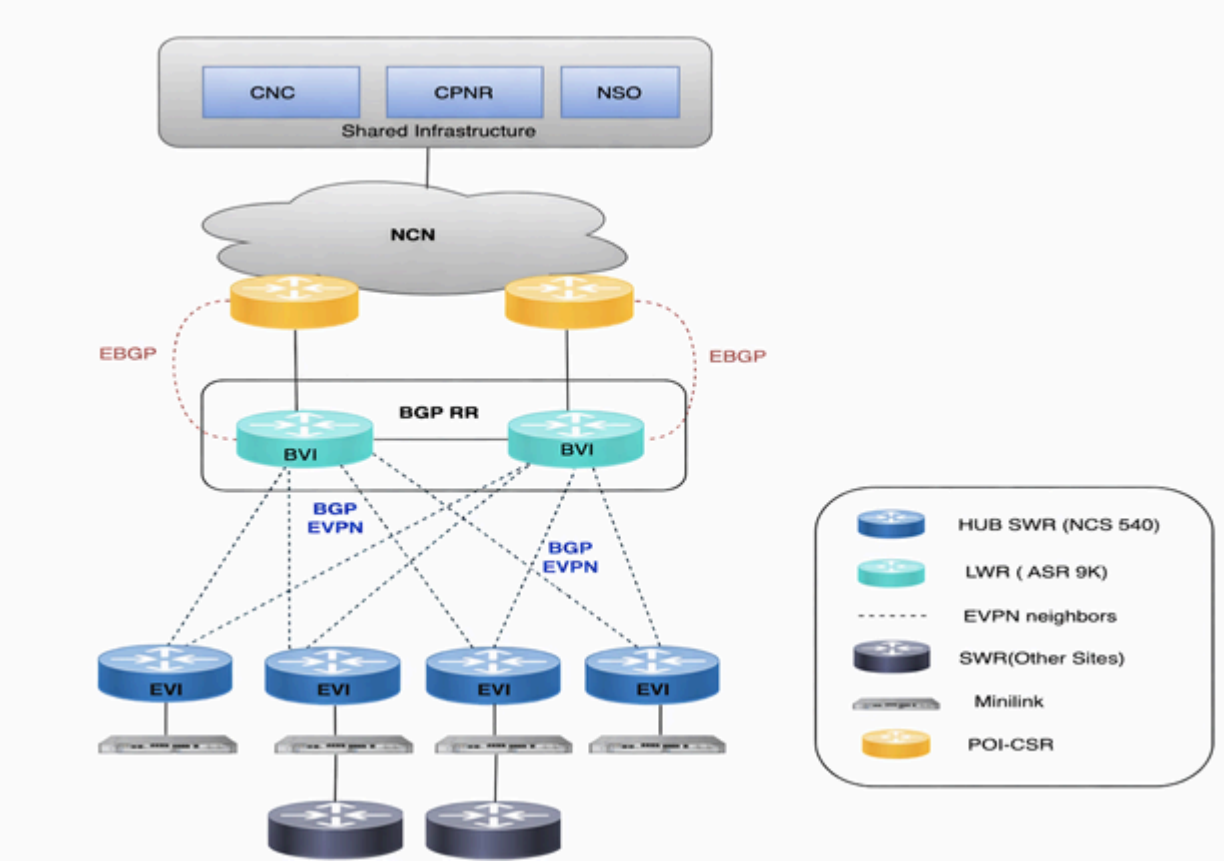
- 交叉工作活动拓扑(CAT):
    - 分布在CNC VM节点上的内部组件应用
    - 提供协调库存的实时端到端可视性
    - 将来自多个数据源的库存信息集成到单个显示中
    - 传输网络路径计算
    - 拓扑发现

- Crosswork优化引擎(COE):
    - 分布在CNC VM节点上的内部组件应用
    - 实时网络优化
    - 实时拓扑可视化
    - SR-TE可视化和调配
    - RSVP-TE可视化和调配
    - 按需带宽
- Crosswork health insight(CHI):
    - 分布在CNC VM节点上的内部组件应用
    - KPI监控
    - 警报控制面板
- Crosswork变更自动化(CCA):
    - 分布在CNC VM节点上的内部组件应用
    - 配备开箱即用的实战手册的开发运营工具
    - 安排在所需时间运行播放的功能
    - HI KPI警报作为补救措施与建议的实演进行拼接

架构图


AAA
vCenter
Manages
OneFM
Fault Data
Splunk
logs
EPNM
DNS
Crosswork Common UI & API
Health Insights
Crosswork
Optimisation
Topology
Change Auto
ZTP
SR PCE
Data Gateway
NSO
All Products
SSM
CNC / CDG
Bkp/Rst
Patches
Tech Supp.
Deploy
Utility
Backups
Scripts
DNS
DHCP
CPNR
Data
Telemetry
Optimisation
Path Computation
Discovery
Config
Policy
Events
Image
Day 0
SWR
LWR

网络图



CNC 4.1 → 7.1详细迁移工作流程

从传统CNC 4.1到CNC 7.1的端到端分阶段迁移（无论版本如何，任何CNC升级都可以遵循相同的流程）

计划	实验	客户实验室	生产就绪	生产推广	吸收期	切换	停用

第 1 阶段

1计划和准备

范围和规划	安排
·范围定义	·更改窗口标识
•容量规划	·利益相关方协调

▼

第 2 阶段

2内部实验室验证

基础设施 ·构建CNC 7.1（混合/工作） ·安装应用 ·使用高可用性部署NSO ·部署SR-PCE对	验证 ·验证所有使用案例 ·功能签核

▼

第 3 阶段

3客户实验室验证

基础设施构建 ·构建CNC 7.1（混合/工作） ·安装应用 ·使用高可用性部署NSO ·部署SR-PCE对	数据迁移 ·导出CNC 4.1工件 ·重新创建设备组 ·导入CNC 7.1 ·部署NSO包	设备可达性 · ACL更新 ·设备导入和CDG附件	服务和可观察性 ·服务协调与同步 · KPI支持和收集作业 · BNM手册脚本支持 ·HI/Grafana可观测性 · Radius集成 · Splunk集成 · OneFM集成 ·启用CNC备份

✓在实验室中执行ATP并签核

▼

第 4 阶段

4生产就绪性

安全和访问 •安全检查 ·访问控制设置	基础设施 ·生产VM调整和设置 ·网络验证

▼

第 5 阶段

5生产转换

⟲在生产环境中重复第3阶段的所有步骤

基础设施构建 ·构建CNC 7.1（混合/工作） ·安装应用 ·使用高可用性部署NSO ·部署SR-PCE对	数据迁移 ·导出CNC 4.1对象（提供商、凭证配置文件、攻略、标签） ·重新创建设备组 ·导入CNC 7.1 ·部署NSO包	设备可达性 · ACL更新 ·设备导入和CDG附件	服务和可观察性 ·服务协调与同步 · KPI支持和收集作业 · BNM手册支持 · HI/Grafana、Splunk、OneFM ·启用CNC备份

✓生产推广

▼

第 6 阶段

6浸透期

监控 ·稳定监控 ·性能基线	问题管理 ·问题跟踪和解决 ·上报流程

▼

第 7 阶段

7文档和交接

文档	切换
·MOP、设计文档和操作文档 ·架构图	·知识传授课程 ·交接签核

▼

第 8 阶段

8 停用传统CNC 4.1

清理	ARCHIVE
·从CDG中分离所有设备 ·删除指向4.1 CDG虚拟机的MDT条目 ·删除生产VM	·存档所有CNC 4.1出口 ·最终审核与签核

使用案例

L2VPN（基于EVPN）服务调配

L2VPN服务跨多个SWR提供第2层以太网连接，部分服务锚定在LWR上。CNC活动拓扑用于服务调配，而所有特定于环境的逻辑通过NSO自定义模板实施。

L2VPN调配被视为Day2配置活动，需要运营商提供的服务属性。

自定义NSO模板

创建了多个自定义模板，以与环境特定的命名约定和接口行为保持一致：

- CT-l2vpn-swr-hub-and-lwr
  处理SWR集线器和LWR上的集线器端命名差异（或网桥组和网桥域）。
- CT-l2vpn-swr-nonhub-100 / 101 / 102 / 105
  从默认EVPN网桥组和网桥域中删除每个VLAN特定EVI的ZTP上行链路接口。

这些模板可确保网络中的EVPN配置保持一致，并消除硬件级别的差异。

L3VPN（基于VRF）服务调配

L3VPN使用案例支持作为终端跨多个SWR的第3层服务交付。调配通过CNC活动拓扑执行，使用自定义NSO模板实施特定于环境的需求。

与L2VPN一样，这是第2天配置操作，需要操作员输入。

自定义NSO模板

- CT-l3vpn-swr
  收集特定于VRF的参数（AS编号、VRF名称、前缀集、路由策略名称、路由区分器）并构建必要的BGP导入/导出策略，包括使用用户定义的路由策略重分布连接的路由。

流量工程

CNC套件的交叉工作优化引擎(COE)应用有助于根据期望的意图控制网络中的流量。

有两种流量类型需要不同的用途（SLA指标）：

- TC1流量 — 对延迟敏感的SLA，用于确保流量位于最低延迟路径上。
- TC4流量 — 最小带宽SLA，确保专用带宽始终可用于TC4流量

TC1流量（最低延迟）

要确保TC1流量始终采用最低延迟路径，必须在前端SWR上创建分段路由(SR)策略，将路径计算标准作为延迟。

这可以通过使用CNC定义每个前端SWR上特定颜色1001的按需下一跳(ODN)配置来实现，以便创建SR策略。

TC4流量（承诺带宽）

要确保TC4流量始终采用具有专用带宽的路径，必须在前端SWR上创建SR策略，并将路径计算标准作为带宽。

这通过以下方式实现：

- CNC上的按需带宽(BoD)功能包
- 使用这些配置创建CNC　SR策略，为每个前端SWR定义特定颜色1004的按需下一跳(ODN)配置

BoD函数包用于计算SR策略的路径，SR策略将带宽作为路径计算的标准。它跟踪承诺用于策略的带宽，并在策略的生命周期中持续监控策略的当前路径。

在任何时间点，如果BWOD策略的当前补丁没有足够的可用容量来满足已提交的带宽，它会重新计算BWOD策略路径并将策略重新路由到新路径。此BWOD策略重新路由是一个持续的过程，无需手动干预。

在某种程度上，BWOD可以像SR-PCE一样动态优化带宽，从而解决延迟问题。

使用sZTP打开设备

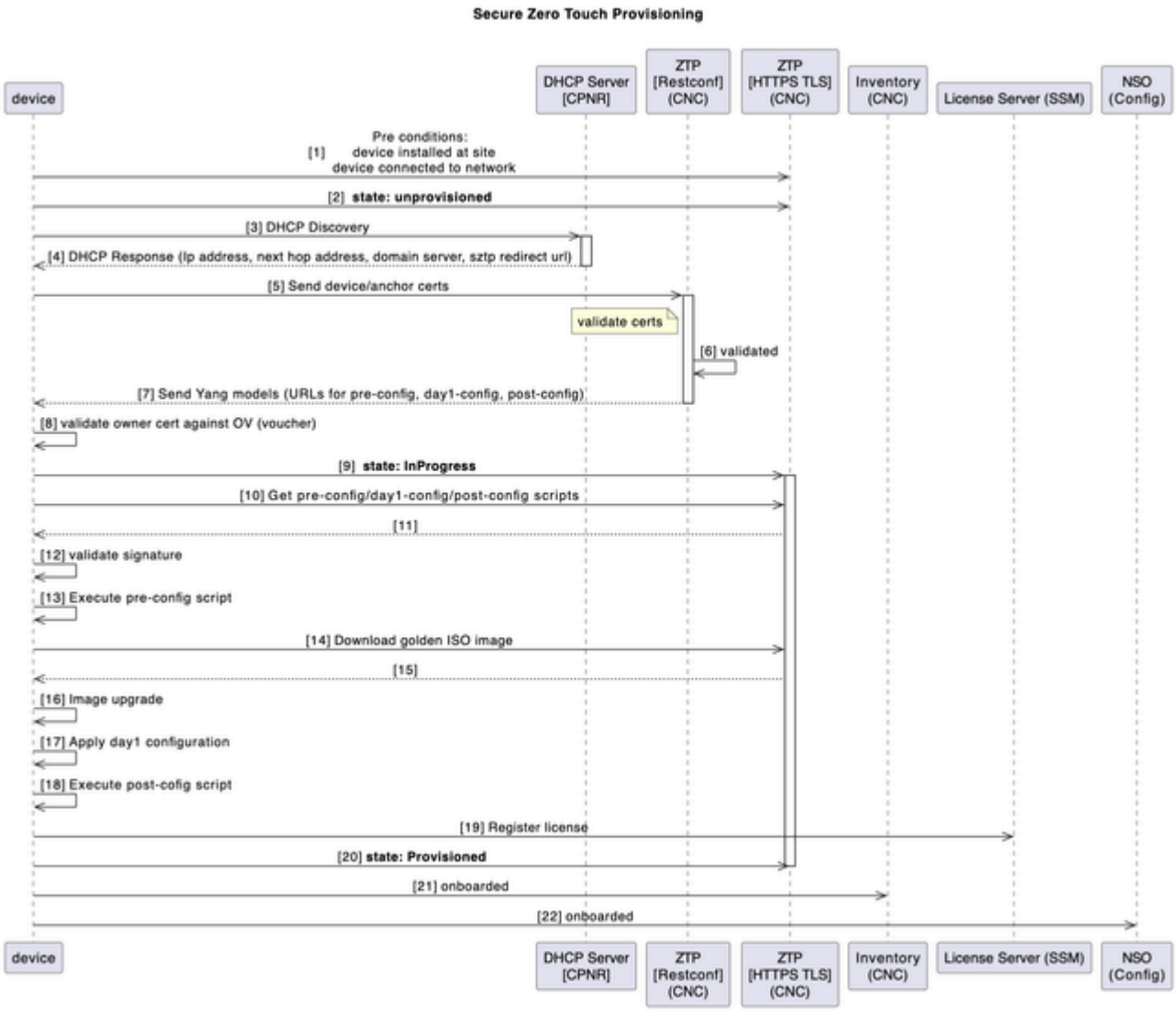
在以往的传统的安装和支持模式中，安装新设备的过程需要安装人员具备一定水平的专业知识，以便安装、配置新组件并对实施进行故障排除。在异地预调试设备也可能是一个漫长的过程，由处理解决方案不同部分的许多人员来支持。

对于计划在您的环境中部署的新SWR设备，通过安全的ZTP（零接触调配）CNC应用自动执行设备启用过程。

ZTP工作流程在首次设备启动时触发，它将下载需要应用的计划平台映像和初始配置，无需任何手动干预。

该设备还自动连接到CNC进行进一步协调。

此图显示了设备启动时安全ZTP流程的工作流程：



后ZTP协调（自动化驱动）

实用程序主机上的Python自动化使用结构化Excel输入（按链）协调和审核端到端流程：

- 生成第1天和配置后工件并将其上传到CNC。
- 创建CPNR保留（绑定到SWR串行的DHCP条目）。
- 在EPNM中添加设备（用于可视性/保证）。
- CNC中的ZTP后内部管理：
  - 将SWR分配到CDG（遥测目的地）
  - 附加到设备组和标记
  - 更新纬度/经度以实现拓扑可视化
  - 附加BNM KPI配置文件以启用遥测流

CNC中的带宽通知消息(BNM)处理

SWR可以从共置的MiniLink交换机接收与WAN端口带宽对应的BNM。这些通知消息是基于标准的CFM消息，包括当前运行的记录带宽(RBW)和最大配置带宽(也称为额定带宽(NBW))。

当前带宽是微波WAN链路的实际运行带宽，基于单个微波链路的聚合带宽及其运行QAM级别。标称带宽是配置的最大可能广域网带宽，基于每个单个微波链路上配置的最大QAM的聚合带宽。

根据以下场景进行带宽优化：

临时（短暂事件）更改

- 当局限于SWR的网络/链路出现短暂的降级或中断（例如，由于不利天气事件，导致微波无线电路径衰落，并且由于调制方案的改变导致可用带宽减少），则流量整形校正发生在受影响的网络接口的本地SWR。
- 这样可以确保在受影响的传输路径上出现最小的数据包丢失。

在CNC中启用SWR时，CNC会将BNM KPI作为sZTP后活动的一部分，并将遥测配置推送到SWR中。

BNM MDT

遥测模型驱动

```
destination-group <DGName>
 vrf VRF-OMSWR-<AreaCode>1
 address-family ipv4 <CDG IPv4Address>端口9010
  encoding self-describing-gpb
  protocol tcp
 !
!
sensor-group
```

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

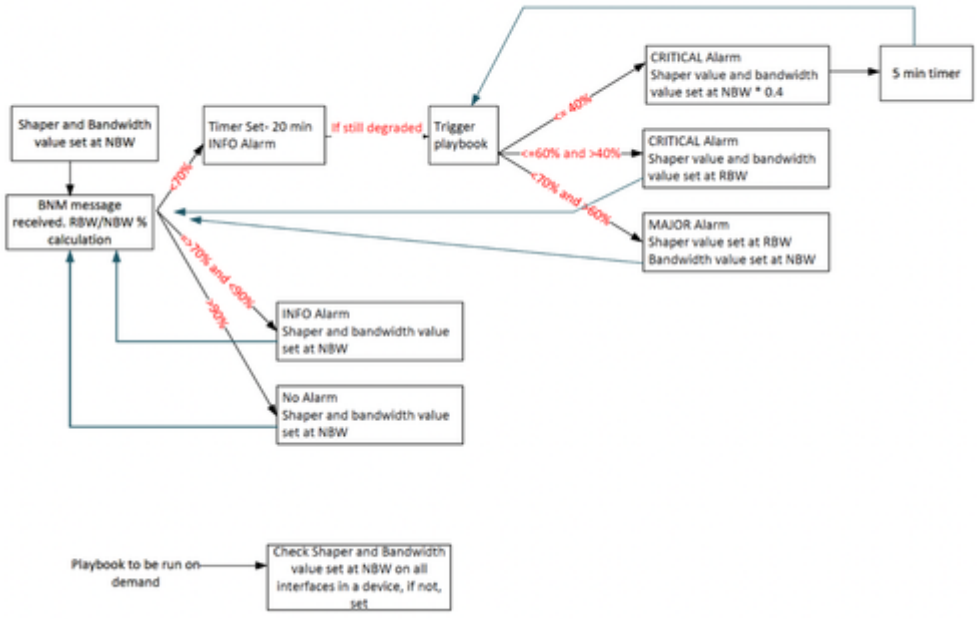
!

CNC会处理通过遥测接收的这些BNM消息，并在需要时采取补救措施。下面是CNC涉及的两个组件：

- Health insight(HI):CNC应用程序用于通过自定义KPI接收BNM通知，自定义KPI可监控BNM消息的特定传感器路径。Health Insight能够在带宽变化很大时发出警报，以便采取措施。
- 变更自动化(CA):CNC应用用于处理导致HI警报的BNM消息流。部署了2个自定义手册，以便在受影响的界面上进行以下更改：
  - 将QoS整形器设置为新RBW
  - 将接口容量设置为新的RBW值。

开发自定义Python脚本以执行自定义逻辑，并在违反HI KPI时自动执行CA手册。

手册触发脚本基于以下算法运行：



下表说明已针对带宽下降程度设置的自定义警报级别：

报告的带宽= RBW

额定带宽= NBW

警报间隔值	通知级别
(RBW/NBW)*100 >=70	信息
(RBW/NBW)*100 <70和>60	警告
(RBW/NBW)*100 <=60	关键

此传感器路径由CNC监控：

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

在CNC中创建自定义KPI以监控BNM传感器路径。此KPI已添加到配置了120秒的周期和警报阈值的KPI配置文件中。将SWR连接到此配置文件会自动将所需的遥测配置通过NSO推送到设备。

启用后，设备会按配置的时间间隔将RBW/NBW数据流式传输到分配的CDG。运行状况分析(HI)会计算RBW÷NBW比率，并在超过阈值时发出警报；操作员可以在HI和Grafana控制面板中监控这些事件。

CNC中的警报提供商将这些警报转发到托管Python自动化的混合节点。该脚本解析设备/接口/RBW/NBW详细信息并触发相应的变更自动化操作手册：根据定义的决策逻辑调整整形器、带宽更新或两者。

以下是工作流程中使用的2个攻略：

1.改变整形器价值的攻略

2.更改接口带宽的攻略

如前所述，该脚本会启动Web服务器，作为使用REST　API与CNC通信的提供商。此处捕获我们获得的POST请求的任何响应。警报在JSON上以形式捕获，然后转换为字典以提取必要的参数。

通过自定义自动化攻略实现第2天网络运营标准化

定制变更自动化(CA)手册旨在简化和标准化整个网络生命周期中的第2天关键操作。这些功能包括捆绑以太调配、管理接口描述更新、CFM菊花链协调、无缝链路容量扩展、eNodeB停用以及高效

的小型链路自注册。通过将操作最佳实践嵌入可重用工作流程，这些攻略可显着增强执行一致性，最大限度地降低人为错误风险，并降低对手动干预的依赖。在思科CNC升级的背景下，此自动化框架在加速运营周转、确保服务连续性和实现符合现代网络转型目标的可扩展、可重复流程方面发挥着关键作用。

思科CNC 7.1升级中的TACACS+集成连续性

作为Cisco CNC 4.1到7.1升级的一部分，现有的TACACS+集成被谨慎保留，以确保集中式身份验证和授权的连续性。升级过程验证并复制了Cisco CNC 7.1中的TACACS+配置，保持与既定的企业安全策略和基于角色的访问控制(RBAC)机制保持一致。

CNC和CDG系统日志转发到Splunk

系统日志转发设置为将警报/事件/系统日志转发到Splunk服务器。利用CNC开箱即用的功能设置syslog服务器来实现这一点。

警报转发到OneFM

CNC警报也使用CNC restconf面向连接的API转发到OneFM等北向系统：

```
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.
```

日常CNC备份自动化

自动脚本利用CNC备份API进行CNC的完全备份，并将备份文件存储在实用程序主机中。此操作每天完成。

挑战

Crosswork版本中的大跳跃

从Cross work 4.4升级到7.1是一个重大的版本飞跃，而不是例行的增量更新。如此大的跳变跨多个应用引入了大量新功能，以及实质性的改进和架构变更。因此，CNC升级不仅仅是一个简单的版本替换，它需要彻底验证以确保所有集成组件的兼容性、稳定性和正确功能。扩展的功能集和基础改进意味着现有的工作流程、配置和集成需要进行仔细的验证，这使得全面的测试和验证对升级的成功至关重要。

无就地升级

CNC不支持就地升级模式。相反，升级必须采用一举一动的方法，即保留现有部署，同时使用目标版本从头构建全新的环境。安装新系统后，必须仔细迁移和验证配置、数据和集成，才能停用较旧的环境。

此方法会带来以下几个操作挑战：

- 并行环境：旧的和新的CNC环境必须同时运行，直到完全完成迁移和验证。
- 硬件资源压力：并行运行两个完整环境会显着增加对计算、存储和网络资源的需求，这可能会使可用基础设施承受压力。
- 扩展验证工作：必须在新版本中验证所有迁移的数据、配置、策略和集成，以确保它们完全按照预期运行。
- 数据迁移复杂性：历史数据、应用配置和操作设置的传输需要精心规划，以避免不一致或数据丢失。
- 延迟停用：在新部署被证明稳定之前，不能删除旧系统及其VM，从而延长资源使用率和运营开销。
- 运营协调：在过渡期间，团队必须管理两个环境之间的同步，以防止配置漂移或运营中断。
- 闭环自动化冲突：CNC支持闭环自动化使用案例，这些使用案例可以根据实时网络条件动态触发操作。当旧控制器和新控制器在转换期间都处于活动状态时，两个控制器可能会执行相同的自动化逻辑，这可能导致网络中的配置更改重复或操作冲突。这需要在迁移期间仔细控制自动化策略。
- 由于缺少本地导出功能，旧版操作数据（包括历史警报、事件、故障记录和审计信息）无法迁移到新环境。因此，升级后的系统中没有这些历史数据，迁移后必须将其视为不可恢复。

由于这些因素，升降和移位模式使得与标准就地升级相比，CNC升级更耗费资源且操作更复杂。

无回滚选项的部署缺陷

CNC中的某些部署和部署后配置错误没有补救路径，并且需要完整的集群中断和重新部署。例如，为Crosswork数据VIP配置的FQDN不正确（对于sZTP使用案例是必需的），导致sZTP无法正常工作。由于这一数值在部署后无法修正，因此需要进行全部重新部署。

同样，部署后无法纠正更改自动化中设备覆盖凭证配置不正确的问题，导致重建另一个集群。其他

错误（例如网关IP配置错误或子网定义）也标识为不可恢复。

这些场景强调了初始部署期间验证所有不可变参数的至关重要性。精心规划和输入验证对于避免代价高昂的返工和计划影响至关重要。

部署后诊断验证的限制

CNC提供诊断实用程序来评估VM级别的运行状况参数，例如磁盘读/写延迟、IOPS、同步延迟、网络接口速度和CPU时钟频率。实用程序根据预期阈值报告测量值，并将每次检查标记为通过或失败。但是，这些诊断只能在部署群集后执行，因此没有在部署之前验证基础架构就绪性的机制。

安装期间，“忽略诊断检查”(Ignore Diagnostic Checks)标志默认设置为false。在实践中，如果任何一次检查失败，安装程序将停止，导致部署无法继续。因此，现场工程师经常被迫启用此标志并完全绕过诊断，因为即使生产级环境也经常无法通过一次或多次检查。这造成了一个运营难题：团队必须选择实施阻止部署的严格验证，还是在不确保底层基础设施满足建议的性能基准的情况下继续操作。

HI自定义KPI创建过程更改

在Health Insight 4.1中，自定义KPI创建依赖于Tick脚本逻辑，其中KPI定义和处理逻辑使用Tick框架中的脚本来实施。但是，在7.1版本中，此方法被用于定义和管理KPI的基于跟踪器的框架所取代。

由于此架构更改，现有自定义KPI无法直接重复使用，需要重新处理才能与新跟踪器文件格式保持一致。这需要大量的时间和精力：

- 了解新框架：该团队必须研究7.1中引入的基于跟踪器文件的KPI定义模型的结构、语法和操作行为。
- 重新设计现有逻辑：之前在Tick脚本中实现的逻辑必须被转换并改编为跟踪器文件格式。
- 重新创建BNM KPI:必须使用新框架重新创建自定义BNM KPI，以确保它们产生与以前相同的结果和见解。
- 验证KPI准确性：需要进行广泛的验证，以确认新的实施与以前的版本相比产生了一致和正确的指标。
- 测试和调整：新模型还需要测试真实网络条件下的性能和行为，并在必要时进行调整。
- 缺少支持：新的tracker文件实现不再支持之前使用tick脚本的一些功能。因此，必须做出一些妥协。

KPI创建机制的这一更改显着增加了升级期间的工作量，因为它涉及学习新系统和重新实施现有自定义监控逻辑以确保运营见解的连续性。

BNM手册触发器脚本中的API超时

BNM手册通过与CNC API交互的自定义脚本触发。在升级和验证过程中，发现并解决了一些与API身份验证和响应处理相关的问题。

CNC API令牌的有效期为8小时，但原始脚本不包含用于在其过期后刷新令牌的正确逻辑。因此，尽管CNC 4.4中的KPI警报运行正常，但手册触发脚本在令牌过期后停止执行。此问题在很长一段时间内未注意到，这意味着自动化脚本实际上已超过一年未可靠运行。此问题仅在CNC 7.1中的迁移和验证活动中可见。

因此，需要做出一些改进和改进：

- 令牌刷新逻辑：实施适当的逻辑来检测令牌到期并自动刷新API令牌，确保脚本的不间断执行。
- API响应更改：CNC版本之间的差异导致了其他问题。在CNC 4.1中，过期的令牌响应通常包含消息“expired”，而在CNC 7.1中，响应返回“Key not authorized”。 必须更新脚本逻辑，才能正确解释7.1中的新响应模式。
- 全局令牌处理：以前，令牌在函数内进行本地存储和使用。这样创建的场景中，令牌在输入函数时有效，但在后续API调用之前过期。该实现被修改为使用全局令牌处理，以确保所有功能之间的一致性和适当的刷新。
- 改进了错误处理：在某些情况下，NSO“check sync” API返回的响应不完整或与预期结构不同。这导致KeyError异常，从而暂停了脚本执行。引入了额外的异常处理和验证逻辑，这样即使收到意外的API响应，脚本也可以继续运行。
- 脚本稳定性增强：添加了额外的保护和检查，以确保API故障、临时响应问题或令牌刷新事件不会导致脚本意外终止。

这些改进不仅解决了升级期间发现的问题，还显着增强了BNM攻略自动化框架的可靠性、可复原性和可维护性。

BNM处理和手册触发器设计更改

BNM自动化逻辑是事件驱动的，并依赖于CNC内Health Insight应用程序中的KPI生成的警报。整体工作流程如下：

1. CNC从设备读取NB（额定带宽）和RBW（实际带宽）值。
2. 它使用这些值计算带宽比率(BW%)。
3. Health Insight KPI根据预定义的警报阈值评估此比率。
4. 当生成警报时，BNM手册触发脚本检测该警报并执行相应的纠正手册

原始警报设计中的限制

配置的警报阈值为：

- BW% < 60 → Critical
- 60 ≤ BW% ≤ 70 → Warning
- BW% > 90 → Info

此设计在识别带宽降级方面效果不错，但在带宽恢复方案期间造成了功能缺口。具体来说，70-90%范围没有定义警报级别。

这导致了以下行为：

- 当BW%降至70%以下时，将生成严重或警告警报，触发调整整形器和带宽值的手册。
- 但是，当带宽恢复且BW%增长到70%以上时，KPI不会生成警报，因为值会降到70-90%的范围内，并且没有关联的警报级别。
- 由于BNM自动化脚本完全依赖警报生成来触发操作，因此它没有机会读取更新的NBW/RBW值或启动恢复操作。
- 因此，即使有足够的带宽可用，也不会自动恢复带宽。原始设计中没有恢复逻辑。

这一限制在生产网络中显而易见，以前经过带宽缩减的链路即使在条件改善后仍保持受限状态。

KPI框架更改的影响

CNC 7.1中引入的框架更改进一步加剧了这一问题。在Health Insight 4.1中，基于Tick的KPI实施支持最多五个警报级别，允许更精细地控制阈值范围，并使恢复逻辑更易于实施。

但是，在CNC 7.1中，基于tracker文件的KPI框架仅支持三个警报级别，这降低了定义多个恢复阈值的灵活性，并且需要重新设计警报逻辑以适合这些限制。

过度触发攻略

在初始实施中发现的另一个问题是手册执行频率极高。自动化逻辑不包括任何保持时间或稳定窗口。当CNC从符合警报条件的设备读取值后：

- 警报立即响起。
- 自动化脚本立即触发了纠正手册。

由于实时网络中的遥测值频繁波动，因此每小时都会触发数百个手册，从网络稳定性和应用性能角度来看都不理想。

重新设计的自动化逻辑

为了解决这些限制，我们对BNM自动化设计进行了一些改进：

- 修订警报阈值逻辑：为了确保恢复频段捕获在三个警报级别内，对逻辑进行了修改，将任何大于70%的BW%现在视为INFO级别警报，取代了之前仅将大于90%的值归类为INFO的方法。这确保了70-90%的恢复频段受到主动监控，使恢复手册可以在带宽条件改善时触发。
- 保留时间简介：引入了20分钟的保持时间机制，以确保带宽条件在定义的持续时间内保持稳定，然后触发攻略。这可以防止自动化对短期波动做出反应。
- 受控手册执行：随着修改后的逻辑和保持时间，实战手册执行频率显着降低，从而阻止不必要的自动化操作。
- 严重退化的助推器机制：对于带宽严重下降的情况，引入了增强器方法。在这种情况下，自动化会主动将流量整形器和带宽分配调整为NBW的40%，从而更快地从拥塞中恢复。
- 提高自动化稳定性：重新设计的工作流程可确保有效处理带宽减少和带宽恢复方案，即使在基于跟踪器的KPI框架的限制内也是如此。

结果

通过这些设计变更，再加上以前在API处理、令牌管理和脚本稳定性方面的改进，BNM自动化框架现在能够以更加稳定、高效和可预测的方式运行。系统可以正确响应拥塞和恢复条件，同时避免执行过多的手册，并确保可靠的网络带宽优化。

设备警报抑制

在CNC 4.1中，警报通过RESTCONF API转发到名为OneFM的北向系统。由于CNC 4.1堆栈不包含EMF功能，因此平台仅生成系统级警报。这些警报是在没有任何警报分类相关复杂性的情况下向上游转发的。

随着CNC 7.1的部署，EMF的应用被引入，大大扩展了告警模型。警报现在分为三种类型：

- 系统警报 — 与CNC平台和应用运行状况相关
- 网络警报 — 与网络服务条件相关
- 设备警报 — 直接从网络设备生成并通过CNC转发

但是，已经有一个负责收集和管理设备级警报的EPNM。如果CNC也将这些警报转发给OneFM，则会导致两个系统收到重复的警报。因此，要求从CNC中排除设备警报，同时仍转发系统和网络警报

。

主要挑战在于用于向OneFM转发警报的RESTCONF北向API的限制。API不支持根据警报类别过滤警报。如果能够进行此类过滤，解决方案将非常简单：只需在API级别排除设备警报，然后将其转发到北向系统。

对几种可能的解决方案进行了评估和讨论：

- 停止源设备陷阱：防止设备向CNC发送陷阱。
- 在北向系统(OneFM)上过滤警报：允许CNC发送所有警报，但过滤OneFM内的设备警报。
- 在转发警报之前在CNC中过滤。

在设备级别停止陷阱不可行，因为CNC依靠这些陷阱来检测设备事件并保持对网络条件的操作感知。禁用陷阱会显着降低CNC响应网络问题的能力。

该解决方案最终利用了一个称为“设备警报抑制”的内置CNC功能。此功能允许管理员根据设备组抑制特定类型的设备警报，从而防止这些警报被进一步处理或转发到上游。

通过配置设备警报抑制策略，系统能够：

- 在CNC中抑制设备生成的警报。
- 继续处理和转发系统和网络警报。
- 防止重复的设备警报到达OneFM系统。

此方法提供了安全且可扩展的解决方案，不会影响CNC从设备接收陷阱的能力。因此，流向OneFM的警报流得以简化，确保仅转发相关的系统和网络警报，同时避免与EPNM的设备警报管理重复。

带外更改

在现有设置中，操作团队经常依靠直接的基于CLI的脚本将配置更新推送到网络设备，尤其是诸如ACL修改和调试活动等任务。尽管这种方法在短期内有效，但会导致配置漂移，因为系统不会跟踪在NSO之外进行的更改。因此，NSO的调配工作流程因目标（建模）状态和实际设备配置之间的不一致而受到影响，导致故障和运营效率低下。

L2/L3 VPN协调

由于带外配置更改：网络团队更新了CNC/NSO和TSDN工作流程之外的设备上的VPN相关配置。因

此，NSO中存储的状态（从CNC 4.1时代）并不总是与设备上的状态匹配。

这些差异导致多次协调失败和不一致。在若干情况下，NSO包含的VPN服务数据不再存在于设备上（或者已以NSO未反映的方式进行了修改）。 要使NSO与网络保持一致，必须删除仅存在于NSO中而不存在于设备上的VPN服务条目，并更正因带外更改而导致的其他不匹配。

计划影响

解决这些问题需要在最初协调计划之外再执行大约两周的时间。额外的时间用于识别不匹配、验证设备状态以及安全地清理或纠正NSO CDB数据。

观察结果

1. 配置权限：对VPN（或任何受TSDN管理的）配置进行带外更改会导致NSO与网络之间的漂移，并使协调复杂化。
2. 迁移前基线：在迁移之前，NC/NSO管理的状态与仅设备状态的明确基线会使差异更易于检测和解决。
3. 自动化和转换：负载转换脚本和特定于用户的自定义对于以一致的方式处理4.1和7.1之间的格式和模式差异至关重要。

类似升级的建议

1. 在协调窗口期间对VPN（和其他TSDN管理的）服务执行变更冻结，但仅通过受控进程执行例外。
2. 运行协调前审核，比较NSO CDB与设备配置，以量化并列出差异，然后开始协调。
3. 记录并宣传VPN更改必须通过CNC/NSO TSDN升级后才能避免带外漂移的重复发生。
4. 保留转换和协调脚本，以便在将来的升级或故障排除时重复使用。

CNC备份因维护模式依赖性而失败

CNC备份机制要求在启动备份操作之前将平台置于维护模式。根据设计，备份API实施此前提条件；如果CNC无法转换到维护模式，备份过程将自动中止。

在实践中，由于持续的系统活动，进入维护模式经常失败，包括：

- 主动变更自动化(MOP)执行
- 持续的sZTP工作流程
- DLM服务操作
- KPI配置文件附加或分离活动

- 按需showtech集合
- 后台协调任务

任何此类活动的存在都会阻止CNC进入维护模式，从而导致备份操作在执行之前失败。

运营影响

所需的每日CNC备份，以确保合规性和运营。但是，频繁的自动化活动，特别是BNM触发的攻略，意味着系统通常无法进入维护模式。因此，备份故障会反复发生，从而带来巨大的操作风险，需要手动干预。

缓解策略

1.备份计划优化：确定了一个系统活动最小的维护窗口。根据流量和自动化分析，备份作业安排在凌晨5:00（美国东部标准时间），那时协调和实战手册执行最不可能处于活动状态。

2.备份前活动验证：在调用备份API之前引入了自动预检查：

- 该脚本查询CNC API以检测正在运行的Change Automation MOP作业。
- 如果任何作业报告为Running，脚本将等待5秒并重试。
- 此循环一直持续到系统报告无活动作业为止。
- 只有在确认环境空闲后，脚本才会尝试启用维护模式并触发备份。

这可在系统处于忙碌操作状态时防止不必要的备份尝试。

3.重试和复原机制：为适应暂时的系统状态，增加了额外的保障措施：

- 如果备份API返回失败，最多尝试三次重试
- 重试之间的短延迟间隔
- 平稳的错误处理，避免脚本终止

结果和结果

组合缓解显着提高了备份可靠性：

- 备份故障显着减少
- 实施后，只观察到两个故障，两者都是由于脚本控制之外的sZTP进程停滞造成的。
- 在BNM手册自动化中引入的执行延迟进一步减少了与维护模式的争用。

将系统日志转发到Splunk

系统日志目标在CNC中配置为通过TLS将日志转发到Splunk。然而，一旦收到，Splunk一侧的日志是无法读取的。由于此问题源自Splunk环境，因此选择恢复到UDP传输，之后成功处理日志。

设备分组迁移问题

用户之前在CNC 4.1中创建了18个设备组；但是，该版本未提供任何基于UI或API驱动的机制来导出或导入设备组。因此，将这些组迁移到CNC 7.1需要采用非标准方法。确定了两个内部CNC API:一个显示设备组层次结构，另一个列出映射到每个层次结构节点的设备。使用这些API，提取所有设备组及其相关设备并将其存储为JSON输出。然后开发自定义脚本来解析响应并仅从每个组提取设备主机名。

CNC 7.1引入了设备组的本地导入/导出功能，包括基于CSV的导入模板。在从旧系统中提取主机名后，又创建了第二个自动化脚本以所需格式填充CSV模板，从而确保可以准确独立地导入每个设备组。这种自动化至关重要；如果没有它，将设备组迁移到CNC 7.1将会非常耗时且操作复杂。

隔离带宽严重下降的设备

尽管实施了BNM使用案例以自动修复低RBW/NBW比率，但部分设备在较长时间内仍保持严重降级状态。虽然整形器和带宽调整手册通常在降级事件后不久恢复设备，但多个设备持续处于严重状态达一周以上，并且需要手动干预。但是，确定这些设备是一项挑战。虽然CNC UI提供警报和带宽指标的清晰可视化，但它不会轻易显示长时间间隔内完全处于“严重”状态的设备。

为了解决这一操作缺口，开发了API驱动的解决方案。CNC提供一个API，用于检索可配置时间窗口（例如，7天，一个月）内顶级警报生成设备的列表。 通过获取此数据并过滤在所选时段内仅生成严重警报的设备，该团队能够快速隔离需要手动补救的设备。这种自动化方法显着提高了故障排除效率，并减少了确定持续性降级案例所需的时间。

设备遥测配置删除

在CNC 4.1中，当设备与Health Insight(HI)KPI配置文件关联时，会自动应用通过tm-tcfunction pack从NSO推送的遥测配置。但是，这些配置（包括CDG VIP参考）在稍后分离KPI配置文件时未删除。因此，随着时间的推移，设备会积累陈旧和冗余的遥测条目。

在升级到CNC 7.1期间，这个问题变得更加突出。设备通常会保留来自CNC 4.1的传统CDG VIP遥测配置，以及CNC 7.1生成的新条目，导致超过2000个设备上的多个冲突遥测配置。由于只有CNC

7.1 CDG VIP配置必须保持活动状态，因此对运营影响和配置安全提出了担忧。

为了解决这个问题，我们开发了一个自动脚本，用于识别并从每个设备的遥测配置中删除过时的CDG VIP参考。此解决方案消除了配置不一致的情况，恢复了与预期的7.1遥测模式的一致性，并避免了大型设备机群中几天的人工清理工作。

排除MDT集合故障

在CNC 7.1中，大多数运行状况见解(HI)KPI集合依赖于模型驱动遥测(MDT)。 当在设备上启用KPI配置文件时，NSO会自动对所需的传感器路径进行编程，并将CDG VIP配置为遥测目标。应用此配置后，将创建相应的CDG收集作业以跟踪设备的遥测状态。

在验证期间，据报告有100多个设备缺少遥测配置。通过CNC用户界面识别这些设备已被证明是不切实际的，因为UI仅支持每个设备的过滤，并且对于超过2,000台设备的机群无法有效扩展。这就需要采用自动化方法来确定哪些设备缺少遥测配置和所需的KPI重新启用。

为了解决这个问题，我们利用KPI配置文件激活时分配给设备的BNM标记。首先，生成带有BNM标记的所有设备的导出。然后，开发一个Python脚本与CNC收集API交互，合并分页逻辑以检索完整集合作业（每个API调用最多返回100个条目）。 脚本从收集作业数据中提取主机名，并将其与导出的BNM标记设备列表进行比较。

此比较产生了已标记但未出现在BNM收集作业中的设备的列表，表明尚未应用MDT遥测配置。然后在这些设备上重新启用KPI配置文件，验证确认正确创建了所有相应的收集作业。

这种自动化显着简化了故障排除流程，使团队能够在一天之内确定并修复所有受影响的设备，而通过手动检查无法实现这一目的。

NSO 6.4.1.1中HA行为变化及一致性算法调整

从Cisco NSO 5.7.5.1升级到6.4.1.1期间，作为Cisco CNC 7.1过渡的一部分，由于新版NSO中隐式启用共识算法，高可用性(HA)行为发生了显着变化。这不是NSO 5.7.5.1中的默认行为，导致升级后故障切换特征发生改变。具体而言，当主节点关闭时，辅助节点转换为只读状态，阻止其处理调配活动。同样，当辅助节点关闭时，主节点从活动主节点状态移动到“无”状态，从而影响服务连续性。

为了恢复与先前部署一致的预期HA行为，NSO 6.4.1.1中明确禁用了一致性算法。此调整确保主节点和辅助节点在故障切换方案期间恢复其预期角色，允许不间断调配，并保持与早期NSO版本一致的操作稳定性。

NSO版本升级和软件包兼容性增强功能

作为从Cisco CNC 4.1到7.1的过渡的一部分，基础Cisco NSO版本从5.7.5.1升级到6.4.1.1。此版本升级导致现有NSO包中XML模板结构的更改，导致某些依赖于传统模板行为的回归测试案例出现故障。

为了弥补这些兼容性差距，对受影响的NSO软件包模板进行了分析和更新，以与NSO 6.4.1.1的修订方案和处理要求保持一致。这些增强确保了所有的自动化工作流程和服务模式都能继续按预期运行，恢复回归稳定，并在升级后的CNC环境中保持一致性。

大规模实施KPI的问题

CNC提供开箱即用的UI机制，用于在设备上启用KPI配置文件。尽管这种方法对小型舰队非常有效，但在大规模上却变得低效且不可靠。在此部署中，超过2,000台SWR设备需要KPI支持，而UI无法提供批量选择或处理设备的有效方式。

最初，尝试了一种基于标记的方法：为所有SWR设备分配了一个SWR标签，并且使用标签选择而非手动设备选择执行KPI启用。但是，在单个工作流程中处理2,000多个设备会导致重大运营挑战。这份工作持续了三个多小时，并且失败了数百次。虽然所有设备都包含在意向中，但只有约750个设备成功获得KPI支持，重复尝试仅产生递增的进度。事实证明，这种方法既不可扩展，也不可重复。它显示了负载的严重问题。

NSO设备同步问题带来了第二个挑战。许多故障表明NSO未与相应的设备同步。尝试手动同步操作后进行KPI重新启用是不切实际的，需要操作员进行大量的工作。

为了解决这些限制，我们开发了一个自动化的、批处理驱动的工作流程：

1. 导出完整的CNC清单。
2. 批量处理设备50（通过调整确定为最佳大小）。
3. 对于每个批处理，使用设备UUID触发自动同步。
4. 通过CNC API执行KPI启用。
5. 以编程方式监视KPI作业历史记录和日志失败。
6. 通过重复同步和KPI启用步骤重新处理故障设备。
7. 成功完成批处理后，请转到下一组50台设备。

自动化还包括禁用KPI配置文件，从而实现完整的生命周期管理。

此解决方案为KPI调配提供了简化、确定性和高度可扩展的流程。它消除了手动干预，确保了一致的结果，并节省了数天的运营工作。当KPI配置文件在BNM设计更改后必须禁用和重新启用时，这种自动化证明非常宝贵，可以在整个2,000个设备群中进行快速且无错误的重新配置。

RESTCONF北向API限制为管理员访问

用于从CNC转发警报和事件的RESTCONF北向API具有限制，因此只能使用admin帐户调用。尝试通过服务帐户访问API失败，尽管这些帐户具有所需的操作角色。作为解决方法，用户需要使用管理员凭证将警报转发到北向系统，引入操作限制并限制对最低权限访问原则的遵守。

自动化作为战略推动力

鉴于CNC升级和迁移计划的规模和复杂性，操作任务的手动执行很快就证明是不可持续的。设备自注册、KPI调配、配置调整、协调和遥测验证等活动涉及数千个网络元素和重复的工作流程，这些元素在手动执行时极易出现人为错误。因此，自动化不仅对于加快执行速度，而且对于确保一致性、降低运营风险以及让交付团队从时间密集型重复任务中解放出来至关重要。

通过脚本化工作流程和API驱动的操作将这些流程系统化，升级计划实现了显着的效率提升。自动化加快了任务完成速度，提高了准确性，在所有部分都实现了可预测的结果。由此带来的节省不仅缩短了整体部署时间，而且使工程师能够将精力集中在价值更高的验证和设计工作上，而不是放在日常运营任务上。

有些自动化活动是在升级项目开始之前确定的，而有些活动是在出现挑战时演变而来的。有些问题是在项目过程中出现的问题所造成的。

此表说明了自动化对计划产生重大影响的领域。

任务说明	手动工作（天）	自动化工作（天）	估计节省额（天）
ACL更新(SWR/LWR)(2K+)	30.0	2.0	28.0
设备迁移和连接至CDG(2K+)	5	1.0	4.0
BNM KPI连接到设备(2K+)	4.0	1.5（平均值）	2.5
服务协调	7	2.5	4.5
设备组迁移	4	0.5	3.5

任务说明	手动工作（天）	自动化工作（天）	估计节省额（天）
隔离带宽严重下降的设备	3	0.5	2.5
MDT集合故障排除	3	0.5	2.5
总计	56 天	8.5 天	47.5 天

所学课程

升级并不简单

CNC不支持就地升级，而升降和移位模式会引入极大的操作复杂性。绝不能认为过程非常简单，特别是当版本跳转较大时。意外问题会出现在各种应用、集成和工作流程中，每个问题都需要时间、分析和谨慎的缓解措施。主要版本的飞跃放大了这一挑战，使得彻底的规划、验证和阶段性执行变得必不可少。我们不得不在TAC案例和故障排除方面花费大量额外时间。由于我们没有为此保持缓冲时间，这变得很有挑战性。

CX必须完成繁重的工作

期望在部署、集成、迁移和端到端使用案例验证方面投入大量的CX工作。不要认为在旧版本上验证的工作流程在新版本上表现相同。 — 需要进行大量的故障排除和分析，才能使工作顺利进行。

自动化工具包势在必行

升级过程表明，自动化不是可选的便利性而是大规模CNC部署的基本要求。我们早就为必要的候选人规划了自动化流程，但没人能想当然地认为这已经足够了。在项目进行过程中，可以在使用案例中发现问题，使用案例中自动化肯定会增加价值，如前面的部分所示。

避免迁移期间发生双控制器冲突

在升级过程中，确保旧的和新的CNC环境不能同时处于活动状态至关重要。虽然验证需要较短的吸收期，但是将其大幅延长（例如在此项目中超过2个月）会带来操作风险。由于两个CNC都处于活

动状态，且活动时间超过15-20天，Bandwidth On Demand（按需带宽）等闭环自动化功能会在网络中产生不一致和冲突的操作，因为自动化逻辑同时从两个控制器运行。

关键教训是在迁移期间实施清晰的护栏。管理性禁用旧CNC中的设备、暂停自动化工作流程或限制遥测订用等措施可以防止这些冲突。未来的升级必须明确规划严格的控制器隔离，以避免双控制器干扰并确保可预测的网络行为。

MOP不是神圣不可侵犯的

虽然过程方法(MOP)文档针对每个部署、集成和使用案例创建，但假定在实验室条件下验证的MOP在生产中行为一致是不现实的。生产环境始终显示偏差，有些偏差很小，有些偏差很大，从而突显了控制测试中看不到的差距。真实网络、传统行为、外部依赖项和实时流量条件引入实验室模拟无法始终复制的变量。

主要学习是，团队必须在进行生产部署时，期望遇到意外行为、重大案例和新发现。灵活性、快速故障排除能力以及随时调整程序的就绪性是大规模成功执行的关键。

TAC案例的有效性

生产后问题不可避免，尽管交付团队进行初步故障排除很有价值，但仅依赖内部努力可能会导致不必要的延迟。谨慎的做法是将TAC案例作为安全网络并行打开，尤其是对于与产品相关或无法立即诊断的复杂行为。TAC调查通常需要时间，将问题创建时间推迟几天会导致项目动力严重受损。尽早与TAC接洽，可确保必要时提供专家协助，加快根本原因的确定，并防止可避免的进度延后。

与CNC BU接洽，提供有效的知识支持

在任何CNC项目期间，CNC业务部的大力支持都是非常有价值的。用户通常需要详细的产品见解和说明，而仅交付团队无法轻松获得这些见解和说明。在整个合作过程中均可访问业务部门联系人，可加快问题解决速度、提高技术准确性，并有助于建立更大的信心和用户关系。

CNC升级的最佳实践

规划优化的升级策略

CNC不支持就地升级，因此并行部署不可避免。将新环境视为全新安装，并分配足够的计算、存储和管理容量来同时运行两个环境。尽早规划验证阶段、迁移排序和移交活动。

严格的部署前验证对于不可变的参数尤其重要

许多经验表明，在初始部署期间，尽职调查至关重要。预先验证所有关键输入，特别是不可变的配置参数，对于防止成本高昂的重新部署和计划影响至关重要。因此，强烈建议使用结构化的预部署检查表、对等体检查和模拟验证，以最大程度降低不可逆配置错误的风险。

在接触生产之前使用专用验证环境

在项目早期阶段建立内部CALO/测试环境允许团队进行试验、验证工作流程、发现版本特定的更改，以及在进入生产阶段之前建立信任。这显着减少了最终推广期间的未知数。

基于证据的分布式交叉工作组件规模确定

在设计集群、CDG分布和PCE分配时，决策依据的是设备类型、接口规模、拓扑复杂性和收集强度，而不是简单的设备计数。均衡的分发可防止过载，并确保跨群集的可预测性能。

自动化重复的大量工作

建立自动化积压工作，处理重复性、大量或操作关键的启动任务，并在需要自动化的情况下进行投资。首先在SIT环境中验证和优化您的自动化，确保生产不依赖于最后一分钟的修复。规模增加了手动工作的成本；标准化自动化可提高质量、速度和控制。将结果打包为可重复使用的资产（已记录的接口、参数化作业、共享库），这样团队就可以在未来的Crosswork升级和相邻项目中使用相同的自动化功能，从而减少返工和入职时间。

避免并行运行时的双闭环控制

在共存期间，将闭环自动化视为单写入器功能：只有一个协调路径可以主动推动补救或策略驱动的配置。在旧堆栈和新堆栈上并发CLA可能产生重复触发和不同意图的风险，从而破坏设备状态的稳定。在功能验证和最终移交给新控制器后，将CLA作为后期阶段里程碑进行上线规划。

执行结构化的升级影响评估

主要版本跳转引入新功能，同时弃用或更改旧功能。在这些更改中考虑因素非常重要。很多时候，升级版本的版本说明中不会记录此更改，我们到达现场后会弹出。对以下内容进行结构化评估：

- 弃用的API
- KPI框架更改
- 应用级行为差异
- 配置模型偏差
- 警报、拓扑处理和手册执行更改

测试整个集成表面的兼容性和行为

CNC与多个外部系统交互，例如NSO、SSM、CPNR、EPNM、OneFM、Splunk和协调框架。迁移前：

- 验证版本兼容性
- 测试所有北向/南向集成
- 确认数据模型、陷阱、遥测流
- 检查SSL/RESTCONF身份验证行为

迁移后发现的集成故障会造成操作盲点。

制定稳健的迁移前数据导出策略

在开始迁移之前导出所有内容：

- 凭证配置文件
- 提供商
- 标签
- 自定义手册
- 自定义KPI
- 角色和RBAC
- sZTP优惠券
- 设备组
- 历史服务元数据

带内置验证门的批处理设备迁移

当迁移数千台设备时，按受控批次执行迁移：

- 在固定队列中移动设备（例如，按区域、CDG负载或设备类型）
- 在移至下一批之前验证遥测、NSO同步状态和可达性
- 如果出现持续异常，请回滚批次

这可以防止CDG和CNC在短时间内承受高负荷。

通过NSO集成处理带外配置更改

为了解决CNC 4.1到7.1升级中的带外挑战，实施了向NSO驱动操作的结构化转变。运营团队可以对NSO CLI进行基于用户的受控访问，而设备CLI的直接管理访问受到限制，以防止带外更改。此外，传统CLI脚本被系统性地转换为基于RESTCONF的自动化并与NSO集成，从而实现了诸如试运行验证和事务回滚等功能。此方法可确保所有配置更改都集中管理、可审计且与NSO的服务模式保持一致，从而有效地消除配置漂移并恢复调配可靠性。

大力强调变更冻结

在关键迁移期间：

- 冻结用户发起的网络更改
- 限制配置推送
- 与现场团队和NOC团队同步
- 规划一些窗口，以适应紧急活动，如使用CNC/ZTP更换设备等。

这样可以降低噪音，并确保网络状态在整个升级过程中保持稳定

结论

从CNC 4.1迁移到CNC 7.1构成大规模网络协调平台升级固有的复杂性的重要案例研究。此项目证明，此类过渡不仅仅是版本改进，而是跨架构层、运营工作流和自动化生态系统的全面转型。由于缺少就地升级路径，需要进行完全升降和移位部署，这就带来了并行环境挑战，并需要在CNC、NSO、SR-PCE、CDG和外部系统集成之间进行细致的协调。由此产生的运营状况强调了稳健的迁移方法、详尽的验证周期和严格控制的转换过程对于降低生产环境中的风险的重要性。

此次升级进一步表明了自动化作为可扩展性和准确性不可或缺支柱的重要性。该项目拥有2,000多台设备、广泛的遥测配置、多个相关组件和动态闭环自动化工作流程，突出显示了如此规模的环境中的手动操作流程的局限性。经过实践证明，专用的自动化跨越ACL更新、设备自注册、KPI调配、遥测清理和故障隔离对于确保确定性、减少人为错误以及显着提高效率至关重要。自动化框架不仅在迁移期间实现了运营连续性，还为持续的网络优化奠定了坚实的基础。

同样重要的是认识到生产行为明显背离了受控的实验室条件。框架更改（例如从基于Tick的KPI逻辑过渡到基于跟踪器的定义）引入了意外行为转变，需要重新设计、重新测试和迭代优化。同样，围绕闭环自动化、遥测可靠性和API行为的运营挑战也突出表明需要自适应故障排除、主动风险评估，以及持续与TAC和业务部门主题专家接洽。这些因素共同表明，主要版本的过渡需要技术深度和组织就绪性。仍有一些未解决的问题需要在下一个交互工作版本7.2中解决。

总体而言，此次升级表明，成功的大规模CNC迁移依赖于以下四个基本支柱：严格的预部署验证、系统和弹性自动化、强大的跨职能协调，以及可预知实验室和生产环境差异的自适应操作状态。通过此次合作获得的洞察不仅有助于稳定部署CNC 7.1，而且还可为未来过渡提供蓝图、介绍最佳实践、加强架构护栏，并强化机构知识，以便进一步完善您的网络自动化生态系统。

术语词汇表

期限	定义
BNM	带宽通知消息。
CAT	Crosswork活动拓扑
CCA	Crosswork变更自动化
CDG	Crosswork数据网关
CHI	Crosswork Health Insight
CNC	Cisco Crosswork网络控制器
COE	Crosswork优化引擎
CPNR	Cisco Prime Network Registrar

CWM	Crosswork Workflow Manager
EMF	元素管理功能
KPI	关键绩效指标(KPI)
LWR	大型无线路由器
MDT	模型驱动的遥测
MOP	程序方法
NBW	额定带宽
NSO	网络服务协调器
RBW	记录的带宽
SR-PCE	分段路由路径计算元素
SSM	思科智能软件管理器
SWR	小型无线路由器
TAC	技术支持中心
TSDN	传输软件定义的网络
ZTP	零接触调配
RR	路由反射器
RP	路由配置文件
POI	互联点

EVPN	以太网虚拟专用网络。

参考

- Cisco Systems， Cisco Crosswork Network Controller Release Notes， Release 7.1.0
- Cisco Systems， Cisco Crosswork Infrastructure 7.1安装指南
- Cisco Systems， Cisco Crosswork Infrastructure 7.1管理指南 — 概念概述:
- Cisco Systems， Crosswork Network Controller Traffic Engineering and Optimization Guide，版本7.1
- Cisco Systems， Cisco Crosswork Health Insights用户指南，版本7.1
- Cisco Systems， Crosswork Zero Touch Provisioning(ZTP)部署指南
- Cisco Systems， Cisco NSO Transport SDN Function Pack Bundle Installation Guide， Release 7.1.0
- Cisco Systems，Cisco SR-PCE配置指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。