Realizar verificação de integridade e configuração do Nexus

Contents

Introdução

Este documento descreve o procedimento e os requisitos para executar verificações automáticas de integridade e configuração para plataformas Nexus 3000/9000 e 7000.

Pré-requisitos

Requisitos

A verificação automatizada de integridade e configuração é compatível apenas com as plataformas Nexus que executam o software NX-OS independente, e não com os switches que executam o software ACI.

Estas plataformas de hardware são suportadas:

- Switches Nexus 3000/9000 Series que executam a imagem do software NX-OS unificado: 7.0(3)Ix ou mais recente
- Switches Nexus 7000/7700 Series com software NX-OS versão 7.x ou mais recente

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Procedimento de verificação de integridade e configuração

Colete show tech-support detailsoushow tech-support registros do switch Nexus para o qual você deseja executar a verificação de integridade e configuração. Oshow tech-support detailsé altamente recomendável, pois oferece maior valor com mais verificações feitas. Certifique-se de que os logs sejam capturados no formato .txt ou .gz/.tar. Atualmente, o arquivoshow tech-supportoushow tech-support detailscapturado nos formatos de texto ASCII e UTF-8 é suportado.

Abra uma solicitação de serviço TAC regular no Cisco Support Case Manager com o seguinte conjunto de palavras-chave (Tecnologia / Subtecnologia / Código do problema):

Tecnologia: Data center e rede de armazenamento

Subtecnologia: (escolha uma plataforma apropriada)
Nexus 3000 (somente série N3000) - Verificação de integridade e configuração (AUTOMATIZADA)
Nexus 3000 (série N3100-N3600) - Verificação de integridade e configuração (AUTOMATIZADA)
Switch Nexus 7000 Series - Verificação de integridade e configuração (AUTOMATIZADA)
Nexus 9200 - Verificação de integridade e configuração (AUTOMATIZADO)
Nexus 9300 (não EX/FX/R Series) - Verificação de integridade e configuração (AUTOMATIZADA)
Nexus 9300 (EX/FX/R Series) - Verificação de integridade e configuração (AUTOMATIZADA)

Switches Nexus 9400 Series - Verificação de integridade e configuração (AUTOMATIZADA)
Nexus 9500 (não EX/FX/R Series) - Verificação de integridade e configuração (AUTOMATIZADA)
Nexus 9500 (EX/FX/R Series) - Verificação de integridade e configuração (AUTOMATIZADA)

Switches Nexus 9800 Series - Verificação de integridade e configuração (AUTOMATIZADA)

Código do problema: verificação de integridade e configuração

Depois que o SR é aberto, um Cisco Guided Workflow o orienta nas etapas para carregar os logs show tech-support detailsoushow tech-support.

Após o upload da saída necessária, a Cisco analisa os logs e fornece um relatório de verificação de integridade (em formato PDF), que é anexado a um e-mail enviado ao usuário. O relatório contém uma lista de problemas detectados, etapas relevantes para solucionar os problemas e plano de ações recomendado.

Se houver dúvidas em relação às falhas de verificação de integridade reportadas, os usuários são aconselhados a abrir uma solicitação de serviço separada com palavras-chave apropriadas para

obter assistência especializada adicional. É altamente recomendável consultar o número da Solicitação de Serviço (SR) aberto para a Verificação Automatizada de Integridade e Configuração junto com o relatório gerado para agilizar a investigação.

Módulos de verificação de integridade e configuração

Automated Nexus Health and Configuration Check Version 1, versão de agosto de 2022, executa as verificações listadas na Tabela 1.

Tabela 1: Módulos de verificação de integridade e CLIs associadas usados pelos módulos

Índice	Módulo de verificação de integridade	Breve descrição do módulo	CLI(s) usada(s) para executar a verificação de integridade
1.	Verificação da versão do NX-OS	Verifica se o dispositivo executa uma versão do software NX-OS recomendada pela Cisco	show version
2.	Verificação de produto Nexus EoS/EoL	Verifica se algum dos componentes (hardware/software) chegou ao fim da vida útil (EOL) ou ao fim das vendas (EOS)	**show version show module show inventory**
3.	Verificação de notificação de campo	Verifica se o dispositivo é potencialmente afetado por um PSIRT/CVE ou Field Notice conhecidos.	show version show module show inventory show running-config e qualquer comando necessário para verificar o arquivo em relação a um determinado FN/PSIRT.
4.	Verificação de integridade da CPU do NX-OS	Verifica os sintomas para a utilização elevada da CPU. É relatado quando o uso atual/histórico da CPU é >60%.	show processes cpu show processes cpu sort show processes cpu history show system resources
5.	Verificação de integridade da memória do NX-OS	Verifica se o uso de memória no dispositivo está acima dos limites de memória do sistema (valores padrão ou configurados pelo usuário).	show version show processes memory show system resources
6.	Verificação de	Verifica se qualquer uma das interfaces	show interface show interface brief show queuing

	interfaces do NX-OS	relatadas cai na direção RX ou TX. O módulo imprime 5 interfaces com as taxas de erro mais altas em cada direção.	
7.	Verificação de integridade de CoPP	Verifica se o CoPP está desabilitado ou configurado incorretamente (por exemplo, todo o tráfego vinculado à CPU que atinge a classe padrão), ou tem uma política de CoPP desatualizada (por exemplo, transportada de versões mais antigas), ou >1000 quedas relatadas em classes não padrão.	**show copp status show policy-map interface control-plane show running-config**
8.	Verificação de Integridade da Comunicação Interprocessos (MTS)	Detecta se há alguma mensagem de comunicação entre processos (conhecida como MTS) travada por mais de 1 dia.	**show system internal mts buffer summary show system internal mts buffer details**
9.	Verificação de integridade do módulo Nexus	Verifica se algum dos módulos (placa de linha, estrutura e assim por diante) reportou falhas de diagnóstico ou está desligado/com falha	show moduleshow inventory show diagnostic result module all detail
10.	Verificação de integridade de PSU e FAN	Detecta se alguma fonte de alimentação não está em estado operacional.	show inventoryshow environment show logging log show logging nvram
11.	Verificação de Práticas Recomendadas do vPC	Valida se a configuração do dispositivo atende às práticas recomendadas do vPC, como configurações de roteador ponto, switch ponto a ponto e gateway ponto a ponto.	Roteador par da camada 3: show running-config (para verificar se as adjacências OSPF, EIGRP e BGP foram formadas) Gateway de mesmo nível/switch de mesmo nível: show running-config show spanning-tree show vpc brief show interface brief

12.	Verificação de MTU	Detecta configurações de MTU inconsistentes, como a interface da camada 2 e a SVI da camada 3 têm configurações de MTU incompatíveis, MTU incorreto em interfaces de junção OTV ou MTU Jumbo não habilitado em interfaces onde é necessário e assim por diante.	show running-configshow interface show ip arp show mac address-table show ip route detail show ip eigrp neighbors show ip ospf neighbors show bgp
13.	Verificação de Integridade da Configuração do recurso de Camada 2	Verifica se algum recurso L2 está habilitado, mas não foi usado	show running-config
14.	Verificação de compatibilidade do vPC do NX-OS	Verifica se foram relatados erros de incompatibilidade tipo 1/tipo 2 de Canais de Porta Virtual (vPC).	show running-config show vpc
15.	Verificação de Integridade do Protocolo Spanning Tree	Verifica as saídas anexadas para obter uma indicação de instabilidades do Spanning Tree Protocol ou em um estado inesperado. O módulo relata vlans onde ocorreram as alterações de topologia mais recentes juntamente com algumas informações adicionais: carimbos de data/hora, interface e ID da bridge raiz. Atualmente, este módulo de verificação de integridade suporta apenas RSTP; o suporte para MST está planejado para as versões futuras.	show spanning-tree detail show spanning-tree internal errors show spanning-tree internal event-history show spanning-tree active show logging log show mac address-table notification mac-move show system internal

16.	Verificação de integridade do PortChannel	Detecta se algum dos membros configurados do canal de porta está em estado não íntegro: (I), (s) (D) ou (H)	show port-channel summary
17.	Verificação de validação de SFP	Detecta todos os transceptores que relataram o erro "Falha na validação do SFP"	**show interface brief**
18.	Verificação de Integridade da Configuração do Recurso de Camada 3	Verifica se algum recurso L3 está habilitado, mas não foi usado	show running-config
19.	Rota padrão via verificação de VRF de gerenciamento	Verifica se o dispositivo tem uma rota padrão configurada no VRF padrão apontando através do VRF de gerenciamento.	show running-config show accounting log
20.	Verificação de Roteamento Multicast sobre vPC sem Suporte	Verifica a adjacência de PIM não suportada sobre vPC	**show running-config show ip pim interface vrf all internal show ip pim neighbor vrf all detail**
21.	Verificação de integridade do OSPF	Verifica possíveis problemas de adjacência observados no dispositivo.Por exemplo: • vários vizinhos detectados na interface configurada como P2P • ID do roteador não configurada manualmente ou que usou um IP de loopback • adjacências fora do estado FULL • adjacências que alcançaram o estado FULL recentemente e indicam instabilidade potencial	show running-config show ip interface brief vrf all show ip ospf neighbors detail vrf all private show ip ospf interface vrf all private show logging log
22.	Verificação de Integridade do EIGRP	Verifica possíveis problemas de adjacência observados no dispositivo. Por exemplo:	show running-config show logging log show ip eigrp neighbors detail vrf all show ip eigrp detail vrf all

		• Número AS não configurado • Nenhum vizinho ativo detectado • Valores altos de SRTT, RTO ou Q Cnt detectados • Alto número de pacotes EIGRP descartados detectados • Menos de 15 minutos de tempo de atividade de adjacência e indica possível instabilidade • A adjacência caiu nos últimos 7 dias	
23.	Verificação de Integridade de Pares BGP	Verifica a adjacência BGP no estado IDLE.	show running-config show bgp vrf all all summary
24.	FHRP (First-Hop Redundancy Protocol, protocolo de redundância de primeiro salto)	Verifica as configurações de timer não padrão, pois essas configurações podem resultar em um desempenho abaixo do ideal. Este módulo de verificação de integridade abrange SOMENTE o protocolo de roteamento de hot-standby (HSRP)	show running-config
25.	Verificador de Consistência de Configuração de VXLAN EVPN	Verifica as saídas anexadas para a configuração de acordo com o Guia de configuração de VXLAN do NX-OS. Por exemplo, verifique se: • A Interface de Loopback usada como a origem da NVE e a Interface de Loopback usada como as atualizações de BGP de origem não são as mesmas • A interface de loopback usada como origem do NVE está no VRF padrão • Os uplinks L3 de tráfego encapsulado em VXLAN estão no VRF padrão e não são configurados como SVI ou como subinterfaces.	show running-config show version show module show inventory show vpc show port-channel summary show vlan all-ports

		• Os uplinks L3 têm uma única entrada ARP (isto é, sem multiacesso). • O recurso vPC está habilitado e há um domínio vPC • A SVI de backup está no VRF padrão, permitida no vPC Peer-Link e definida como uma infra-vlan. • O status administrativo do estado NVE é UP para os dois pares vPC (parâmetros de consistência vPC) • "ingress-Replication" ou "mcast-group" é configurado para cada VNI L2, ou "global mcast-group" é definido sob o NVE • O modo PIM escasso é ativado nos uplinks L3. Se o multicast for usado como modo de replicação para o tráfego BUM • PIM Sparse-mode está ativado nos uplinks L3, sem "vpn multisite dci-tracking" • "suppress-arp" é configurado somente em L2VNIs onde o SVI da VLAN estendida é configurado com "modo de encaminhamento de estrutura anycast-gateway" • "advertise l2vpn vpn" é configurado nas versões do NX-OS anteriores à 9.2 • multisite' é configurado somente no Nexus 9000 com ASICs em nuvem • "vpn multisite dci-tracking" é configurado em links DCI e "fabric-tracking" é configurado em Uplinks L3 e a interface não é uma SVI • "peer-type fabric-external" é configurado nas sessões L2VPN entre os BGWs • A Interface de Loopback usada como origem para Multisite é definida no NVE • "peer-gateway", "peer-switch'", "ip arp synchronize'", "ipv6 nd synchronize" estão configurados	

		no domínio vPC • 'associate-vrf' é configurado para o L3VNI e o SVI do L3VNI tem um segmento VN • A adjacência L2VPN EVPN para BGWs remotos tem "peer-type fabric-external" e "rewrite-evpn-rt-asn"	

Relatórios e avisos

- O SR de verificação de integridade e configuração é automatizado e tratado pelo engenheiro do TAC virtual.
- O relatório (em formato PDF) geralmente é gerado dentro de 24 horas úteis após todos os logs necessários anexados ao SR.
- O relatório é compartilhado automaticamente por e-mail (fornecido em jhwatson@cisco.com) com todos os contatos (principais e secundários) associados à solicitação de serviço.
- O relatório também é anexado à Solicitação de Serviço para permitir sua disponibilidade em qualquer momento posterior.
- Lembre-se de que os problemas listados no relatório se baseiam nos registros fornecidos e estão dentro do escopo dos módulos de verificação de integridade listados anteriormente na Tabela 1.
- A lista de verificações de integridade e configuração executadas não é exaustiva e os usuários são aconselhados a executar outras verificações de integridade conforme necessário.
- Para o Nexus 7000 com vários Virtual Device Context (VDC), é necessário um arquivo de detalhes show tech-support de cada VDC para obter os melhores resultados.
- Para VxLAN EVPN, as próximas verificações não são executadas:
  - Escala para números de VNIs L2, L3, VRFs de Locatários, número de endereços Mac de Sobreposição ou Grupos Multicast.
  - Configuração de Tenant Routed Multicast (TRM), vPC Fabric Peering, Downstream VNI (DSVNI), novos L3VNI, Q-in-VNI ou Q-in-Q-in-VNI, vPC Peer reserved-vlan miss-match ou preferência de caminho onde o caminho para outros sites é através da SVI de backup em vez das interconexões DCI.
- Para configurações de VxLAN EVPN, em relação ao SVI de backup entre vPC Leaf Switches:
  - Configurações feitas usando DCNM ou NDFC : presume-se que o valor padrão de "3600" foi selecionado como a VLAN para que a Interface Vlan 3600 seja considerada como a SVI de Backup.
  - O IGP configurado no SVI é OSPF ou ISIS. As configurações em que uma sessão unicast iBGP IPv4 é estabelecida entre os pares vPC na subjacência e não há IGP configurado na SVI são relatadas como ausentes na SVI de backup.

Perguntas freqüentes

P1: Posso carregar show tech-support details mais de um switch no mesmo SR para obter o relatório de verificação de integridade de todos os switches?

R1: Este é um tratamento de caso automatizado e as verificações de integridade são realizadas pelo Engenheiro do TAC Virtual. A verificação de integridade é feita apenas para o primeiroshow tech-support detailscarregado.

P2: Posso carregar mais de umshow tech-support details para o mesmo dispositivo, digamos, com poucas horas de intervalo, para fazer uma verificação de integridade para ambos?

R2: Este é um tratamento de caso automatizado e stateless realizado pelo Engenheiro do TAC Virtual e a verificação de integridade e configuração é feita para o primeiroshow tech-support detailsarquivo carregado no SR, independentemente de os arquivos carregados serem do mesmo switch ou de switches diferentes.

P3: Posso fazer verificações de integridade para os switches cujos show tech-support details arquivos são compactados como um único arquivo rar/gz e carregados no SR?

R3: Não. se váriosshow tech-support detailsarquivos forem carregados como um único arquivo rar/zip/gz, somente o primeiro arquivo no arquivo será processado para verificações de integridade.

P4: Não vejo a verificação de integridade e configuração que cobre as plataformas Nexus 5000/6000. Isso será abordado posteriormente?

R4: Não. A partir de agora, não há planos para cobrir as plataformas Nexus5000/6000 em um futuro próximo.

P5: O que posso fazer se tiver dúvidas sobre uma das falhas de verificação de integridade reportadas?

R5:Abra uma solicitação de serviço do TAC separada para obter mais assistência sobre o resultado específico da verificação de integridade. É altamente recomendável anexar o relatório de verificação de integridade e consultar o número do caso de solicitação de serviço (SR) aberto para a verificação automática de integridade e configuração.

P6: Posso usar o mesmo SR aberto para a verificação automatizada de integridade e configuração para solucionar os problemas encontrados?

R6: Não. Como a verificação de integridade proativa é automatizada, abra uma nova solicitação de serviço para solucionar os problemas relatados. Informamos que a SR aberta para verificação de integridade é fechada em 24 horas após a publicação do relatório de integridade.

P7: A verificação automatizada de integridade e configuração é executada em relação ao show tech-support details arquivo do switch que executa versões mais antigas do que a mencionada anteriormente?

R7: A verificação automatizada de integridade e configuração foi criada para as plataformas e versões de software mencionadas abaixo. Para dispositivos que executam versões mais antigas, é o melhor esforço e não há garantia da precisão do relatório.

- Switches Nexus 3x00 Series que executam imagem de software unificada do NX-OS: 7.0(3)Ix ou mais recente
- Switches Nexus 7000/7700 Series com software NX-OS versão 7.x ou mais recente
- Switches Nexus 9x00 Series que executam a imagem do software NX-OS unificado: 7.0(3)Ix ou mais recente

P8: Como fechar o SR aberto para verificação de integridade?

R8: O SR é fechado dentro de 24 horas após o envio do primeiro relatório de Verificação de Integridade. Nenhuma ação necessária do usuário em direção ao fechamento de SR.

P9: Como compartilhar comentários ou comentários sobre a verificação proativa de integridade e configuração?

A9: Compartilhe-os por e-mail para Nexus-HealthCheck-Feedback@cisco.com

P10. Qual é o método recomendado para capturar `show tech-support` ou `show tech-support details` de um switch?

R10: É altamente recomendável capturar a saída do comando`show tech-support`ou`show tech-support details`direcionando-a para`bootflash:`(como mostrado no próximo exemplo) em vez de capturá-la para um arquivo de log no aplicativo de terminal (por exemplo, SecureCRT, PuTTY). Lembre-se de que o arquivo de log capturado pelo aplicativo de terminal pode estar no formato UTF-8-BOM (ou similar), que NÃO é suportado pela verificação de integridade automatizada. A verificação de integridade e configuração automatizada suporta arquivos somente nos formatos ASCII ou UTF-8.

Exemplo de CLIs para redirecionar a saída para`bootflash:`e compactar o arquivo:

```
Nexus1# show tech-support details >> bootflash:showtechdetails_Nexus1.txt
Nexus1# gzip bootflash:showtechdetails_Nexus1.txt
```

Feedback

Qualquer feedback sobre as operações dessas ferramentas é altamente apreciado. Se você tiver observações ou sugestões (por exemplo, sobre a facilidade de uso, escopo e qualidade dos relatórios gerados), compartilhe-as conosco em Nexus-HealthCheck-Feedback@cisco.com.

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.