Vérification de l'intégrité et de la configuration Nexus

Table des matières

Introduction

Ce document décrit la procédure et la configuration requise pour effectuer des vérifications automatiques de l'intégrité et de la configuration pour les plates-formes Nexus 3000/9000 et 7000.

Conditions préalables

Exigences

Le contrôle automatique de l'intégrité et de la configuration est pris en charge uniquement pour les plates-formes Nexus qui exécutent le logiciel NX-OS autonome, et non pour les commutateurs qui exécutent le logiciel ACI.

Les plates-formes matérielles suivantes sont prises en charge :

- Commutateurs de la gamme Nexus 3000/9000 qui exécutent une image logicielle NX-OS unifiée : 7.0(3)Ix ou ultérieure
- Commutateurs de la gamme Nexus 7000/7700 qui exécutent le logiciel NX-OS version 7.x ou ultérieure

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Procédure de vérification du fonctionnement et de la configuration

Veuillez collecter show tech-support detailsoushow tech-support des journaux à partir du commutateur Nexus pour lequel vous souhaitez effectuer une vérification de l'état et de la configuration. Leshow tech-support detailsest fortement recommandé, car il offre une valeur supérieure avec davantage de vérifications effectuées. Assurez-vous que les journaux sont capturés au format .txt ou .gz/.tar. Actuellement, les fichiersshow tech-supportoushow tech-support detailscapturés dans les formats de texte ASCII et UTF-8 sont pris en charge.

Ouvrez une demande de service TAC régulière auprès du gestionnaire de cas d'assistance Cisco avec les mots clés suivants (technologie / sous-technologie / code de problème) :

Tech : Data center et réseau de stockage

Sous-technologie : (choisissez une plate-forme appropriée)
Nexus 3000 (série N3000 uniquement) - Contrôle de l'intégrité et de la configuration (AUTOMATISÉ)
Nexus 3000 (série N3100-N3600) - Contrôle de l'intégrité et de la configuration (AUTOMATISÉ)
Commutateur de la gamme Nexus 7000 - Contrôle de l'intégrité et de la configuration (AUTOMATISÉ)
Nexus 9200 - Contrôle de l'intégrité et de la configuration (AUTOMATISÉ)
Nexus 9300 (Non EX/FX/R Series) - Contrôle de l'intégrité et de la configuration (AUTOMATISÉ)
Nexus 9300 (série EX/FX/R) - Contrôle de l'intégrité et de la configuration (AUTOMATISÉ)

Commutateurs de la gamme Nexus 9400 - Contrôle de l'intégrité et de la configuration (AUTOMATISÉ)
Nexus 9500 (Non EX/FX/R Series) - Contrôle de l'intégrité et de la configuration (AUTOMATISÉ)
Nexus 9500 (série EX/FX/R) - Contrôle de l'intégrité et de la configuration (AUTOMATISÉ)

Commutateurs de la gamme Nexus 9800 - Contrôle de l'intégrité et de la configuration (AUTOMATISÉ)

Code du problème : Contrôle d'intégrité et de configuration

Une fois la demande de service ouverte, un workflow guidé Cisco vous guide tout au long des étapes de téléchargement des show tech-support detailsou des journauxshow tech-support.

Une fois le résultat requis téléchargé, Cisco analyse les journaux et fournit un rapport de

vérification de l'intégrité (au format PDF), qui est joint à un e-mail envoyé à l'utilisateur. Le rapport contient une liste des problèmes détectés, les étapes appropriées pour résoudre les problèmes et le plan d'actions recommandé.

Si vous avez des questions concernant les échecs de vérification de l'intégrité signalés, nous conseillons aux utilisateurs d'ouvrir une ou plusieurs demandes de service séparées avec les mots-clés appropriés pour obtenir une assistance spécialisée supplémentaire. Il est vivement recommandé de renvoyer le numéro de demande de service (SR) ouvert pour la vérification automatisée de l'intégrité et de la configuration avec le rapport généré pour accélérer l'enquête.

Modules de vérification de l'intégrité et de configuration

La vérification automatique de l'intégrité et de la configuration de Nexus, version 1, version d'août 2022, effectue les vérifications répertoriées dans le tableau 1.

Tableau 1 : Modules de vérification du fonctionnement et CLI associées utilisés par les modules

Indice	Module de contrôle de santé	Brève description du module	CLI(s) utilisée(s) pour effectuer la vérification du fonctionnement
1.	Vérification de la version de NX-OS	Vérifie si le périphérique exécute une version du logiciel NX-OS recommandée par Cisco	show version
2.	Vérification du produit Nexus EoS/EoL	Vérifie si l'un des composants (matériel/logiciel) a atteint la fin de vie (EOL) ou la fin de commercialisation (EOS)	**show version show module show inventory**
3.	Vérification des notices de terrain	Vérifie si le périphérique est potentiellement affecté par un PSIRT/CVE ou un avis de champ connu.	show version show module show inventory show running-config et toute commande nécessaire pour vérifier le fichier par rapport à un FN/PSIRT donné.
4.	Vérification de l'intégrité du processeur NX-OS	Vérifie les symptômes de l'utilisation élevée du CPU. Il est signalé lorsque l'utilisation actuelle/historique du CPU est supérieure à 60 %.	show processes cpu show processes cpu sort show processes cpu history show system resources

5.	Vérification de l'intégrité de la mémoire NX-OS	Vérifie si l'utilisation de la mémoire sur le périphérique dépasse les seuils de mémoire système (valeurs par défaut ou configurées par l'utilisateur).	show version show processes memory show system resources
6.	Vérification des interfaces NX-OS	Vérifie si l'une des interfaces signalées tombe dans la direction RX ou TX. Le module imprime 5 interfaces avec les taux d'erreur les plus élevés dans chaque direction.	show interface show interface brief show queuing
7.	bilan de santé de la CoPP	Vérifie si le protocole CoPP est désactivé ou mal configuré (par exemple, tout le trafic lié au CPU qui atteint la classe par défaut), ou si la stratégie CoPP est obsolète (par exemple, reportée à partir de versions antérieures) ou si plus de 1 000 abandons sont signalés dans des classes autres que les classes par défaut.	**show copp status show policy-map interface control-plane show running-config**
8.	Vérification du fonctionnement de la communication interprocessus (MTS)	Détecte si des messages de communication entre processus (appelés MTS) sont bloqués pendant plus d'un jour.	**show system internal mts buffer summary show system internal mts buffer details**
9.	Vérification du fonctionnement du module Nexus	Vérifie si l'un des modules (carte de ligne, fabric, etc.) a signalé des défaillances de diagnostic ou s'il est hors tension/en panne	show moduleshow inventory show diagnostic result module all detail
10.	Contrôle de l'état des PSU et FAN	Détecte si l'une des alimentations n'est pas en état de fonctionnement.	show inventoryshow environment show logging log show logging nvram
11.	Vérification des meilleures pratiques vPC	Valide la configuration du périphérique conformément aux meilleures pratiques vPC, telles que les configurations peer-	Routeur homologue de couche 3 : show running-config (pour vérifier

		router, peer-switch et peer-gateway.	si des contiguïtés OSPF, EIGRP et BGP sont formées) Passerelle d'homologue / Commutateur d'homologue : show running-config show spanning-tree show vpc brief show interface brief
12.	Contrôle MTU	Détecte les configurations de MTU incohérentes, comme l'interface de couche 2 et l'interface SVI de couche 3 ont des configurations de MTU incompatibles, MTU incorrect sur les interfaces de jointure OTV ou MTU jumbo non activé sur les interfaces où il est nécessaire, etc.	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.	Vérification de l'intégrité de la configuration des fonctionnalités de couche 2	Vérifie si une fonctionnalité L2 est activée mais pas utilisée	show running-config
14.	Vérification de la compatibilité NX-OS vPC	Vérifie si des erreurs d'incompatibilité de type 1/type 2 ont été signalées pour Virtual Port-Channels (vPC).	show running-config show vpc
15.	Vérification du fonctionnement du protocole Spanning Tree	Recherche dans les sorties jointes une indication d'instabilités du protocole Spanning Tree ou d'un état inattendu. Le module signale les VLAN où les modifications topologiques les plus récentes ont eu lieu, ainsi que des informations supplémentaires :	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-

		les horodatages, l’interface et l’ID du pont racine. Actuellement, ce module de contrôle d'intégrité prend uniquement en charge le protocole RSTP ; la prise en charge de MST est prévue pour les versions futures.	move show system internal
16.	Contrôle d'intégrité PortChannel	Détecte si l'un des membres Port Channel configurés est dans un état non sain : (I), (s) (D) ou (H)	show port-channel summary
17.	Contrôle de validation SFP	Détecte les émetteurs ayant signalé l'erreur « Échec de la validation SFP »	**show interface brief**
18.	Vérification du fonctionnement de la configuration des fonctionnalités de couche 3	Vérifie si une fonctionnalité L3 est activée mais pas utilisée	show running-config
19.	Route par défaut via la vérification VRF de gestion	Vérifie si le périphérique dispose d'une route par défaut configurée dans le VRF par défaut pointant vers le VRF de gestion.	show running-config show accounting log
20.	Vérification du routage multidiffusion sur vPC non pris en charge	Recherche des contiguïtés PIM non prises en charge sur vPC	**show running-config show ip pim interface vrf all internal show ip pim neighbor vrf all detail**
21.	Contrôle de santé OSPF	Recherche les éventuels problèmes de contiguïté observés sur le périphérique.Par exemple : • plusieurs voisins détectés sur l'interface configurée comme P2P • ID de routeur non configuré manuellement ou utilisant une adresse IP de bouclage	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

		• contiguïtés non à l'état FULL • contiguïtés qui ont récemment atteint l'état FULL et qui indiquent une instabilité potentielle	
22.	Vérification du fonctionnement EIGRP	Recherche les éventuels problèmes de contiguïté observés sur le périphérique. Exemple : • Numéro AS non configuré • Aucun voisin actif détecté • Valeurs élevées de SRTT, RTO ou Q Cnt détectées • Nombre élevé de paquets EIGRP abandonnés détectés • Temps de disponibilité de la contiguïté inférieur à 15 minutes et indique une instabilité potentielle • La contiguïté a diminué au cours des 7 derniers jours	show running-config show logging log show ip eigrp neighbors detail vrf all show ip eigrp detail vrf all
23.	Vérification du fonctionnement des homologues BGP	Vérifie la contiguïté BGP en état IDLE.	show running-config show bgp vrf all all summary
24.	Protocole FHRP (First-Hop Redundancy Protocol)	Vérifie les configurations de minuteurs autres que les configurations par défaut, car ces configurations peuvent entraîner des performances sous-optimales. Ce module de contrôle d'intégrité couvre UNIQUEMENT le protocole HSRP (Hot-Standby Routing Protocol)	show running-config
25.	Vérificateur de cohérence de configuration EVPN VXLAN	Vérifie la configuration des sorties jointes conformément au Guide de configuration du VXLAN de NX-OS. Par exemple, vérifiez que : • L'interface de bouclage utilisée comme source du NVE et l'interface de bouclage utilisée comme source des mises à jour BGP ne sont pas identiques	show running-config show version show module show inventory show vpc show port-channel summary

		• L’interface de bouclage utilisée comme source du NVE se trouve dans le VRF par défaut • Les liaisons ascendantes de couche 3 du trafic encapsulé par VXLAN se trouvent dans le VRF par défaut et ne sont pas configurées en tant que SVI ou sous-interfaces. • Les liaisons ascendantes de couche 3 ont une seule entrée ARP (c'est-à-dire, pas d'accès multiple). • La fonctionnalité vPC est activée et il existe un domaine vPC • L'interface SVI de sauvegarde est dans le VRF par défaut, autorisée sur le Peer-Link vPC et définie comme un infra-VLAN. • L'état d'administration de NVE est UP pour les deux homologues vPC (paramètres de cohérence vPC) • "ingress-Replication" ou "mcast-group" est configuré pour chaque VNI L2, ou "global mcast-group" est défini sous le NVE • PIM Sparse-mode est activé sur les liaisons ascendantes de couche 3 Si la multidiffusion est utilisée comme mode de réplication pour le trafic BUM • PIM Sparse-mode est activé sur les liaisons ascendantes L3, sans « evpn multisite dci-tracking » • « suppress-arp » est configuré uniquement sur les L2VNI où l'interface SVI du VLAN étendu est configurée avec « mode de transfert de fabric anycast-gateway » • « advertise l2vpn evpn » est configuré sur les versions de NX-OS antérieures à 9.2 • multisite est configuré uniquement sur Nexus 9000 avec des ASIC à	show vlan all-ports

		l'échelle du cloud • « evpn multisite dci-tracking » est configuré sur les liaisons DCI et « fabric-tracking » est configuré sur les liaisons ascendantes L3 et l'interface n'est pas une interface SVI • « peer-type fabric-external » est configuré sur les sessions L2VPN entre les BGW • Interface de bouclage utilisée comme source pour Multisite définie sur le NVE • "peer-gateway", "peer-switch'" "ip arp synchronize'" , "ipv6 nd synchronize" sont configurés sous le domaine vPC • 'associate-vrf' est configuré pour L3VNI et l'interface SVI de L3VNI possède un segment VN • La contiguïté EVPN L2VPN aux BGW distants a « peer-type fabric-external » et « rewrite-evpn-rt-asn »	

Rapports et avertissements

- La vérification de l'intégrité et de la configuration est automatisée et gérée par l'ingénieur du centre d'assistance technique virtuel.
- Le rapport (en format PDF) est généralement généré dans les 24 heures ouvrables suivant l'ajout de tous les journaux nécessaires à la demande de service.
- Le rapport est automatiquement partagé par e-mail (provenant de jhwatson@cisco.com) avec tous les contacts (principaux et secondaires) associés à la demande de service.
- Le rapport est également joint à la demande de service pour permettre sa disponibilité à tout moment ultérieur.
- Notez que les problèmes répertoriés dans le rapport sont basés sur les journaux fournis et entrent dans le cadre des modules de vérification de l'état de santé répertoriés précédemment dans le tableau 1.
- La liste des contrôles d'intégrité et de configuration effectués n'est pas exhaustive et il est conseillé aux utilisateurs d'effectuer d'autres contrôles d'intégrité si nécessaire.
- Pour Nexus 7000 avec plusieurs VDC (Virtual Device Context), un fichier de détails show tech-support est nécessaire pour chaque VDC afin d'obtenir les meilleurs résultats.
- Pour VxLAN EVPN, les vérifications suivantes ne sont pas effectuées :
    - Évolutivité pour les nombres de VNI de couche 2, 3, VRF de locataire, le nombre

d'adresses Mac de superposition ou de groupes de multidiffusion.
    - Configuration de la multidiffusion routée par le locataire (TRM), de l'appairage de fabric vPC, du VNI en aval (DSVNI), du nouveau L3VNI, du nouveau Q-in-VNI ou du nouveau Q-in-Q-in-VNI, de la non-correspondance de VLAN réservé de l'homologue vPC ou de la préférence de chemin lorsque le chemin vers d'autres sites passe par l'interface SVI de secours au lieu des interconnexions DCI.
- Pour les configurations EVPN VxLAN, en ce qui concerne l'interface SVI de secours entre les commutateurs leaf vPC :
    - Configurations effectuées à l'aide de DCNM ou NDFC : on suppose que la valeur par défaut de "3600" a été sélectionnée comme VLAN de sorte que l'interface VLAN 3600 est considérée comme SVI de sauvegarde.
    - Le protocole IGP configuré sur l'interface SVI est OSPF ou ISIS. Les configurations dans lesquelles une session de monodiffusion IPv4 iBGP est établie entre les homologues vPC dans le sous-réseau et qu'il n'y a pas d'IGP configuré sur l'interface SVI sont signalées comme manquant l'interface SVI de sauvegarde.

FAQ

Q1 : Puis-je effectuer un téléchargement show tech-support details pour plusieurs commutateurs dans le même SR afin d'obtenir un rapport de vérification de l'état de tous les commutateurs ?

R1 : Il s'agit d'un traitement automatisé des dossiers et les contrôles d'intégrité sont effectués par l'ingénieur du centre d'assistance technique virtuel. Le contrôle d'intégrité est effectué uniquement pour le premier show tech-support details téléchargement.

Q2 : Puis-je télécharger plus d'un fichier show tech-support details pour le même périphérique, par exemple, capturé à quelques heures d'intervalle, afin de vérifier l'état de santé des deux périphériques ?

R2 : Il s'agit d'un traitement de cas automatisé et sans état effectué par l'ingénieur du centre d'assistance technique virtuel. La vérification de l'état et de la configuration est effectuée pour le premier show tech-support details fichier téléchargé sur le routeur de service, que les fichiers téléchargés proviennent du même commutateur ou de commutateurs différents.

Q3 : Puis-je effectuer des contrôles d'intégrité pour les commutateurs dont les show tech-support details fichiers sont compressés en tant que fichier rar/gz unique et téléchargés sur le routeur de service ?

R3 : Non. Si plusieurs show tech-support details fichiers sont téléchargés en tant que fichier unique rar/zip/gz, seul le premier fichier de l'archive est traité pour les vérifications de l'intégrité.

Q4 : Je ne vois pas le contrôle d'intégrité et de configuration qui couvre les plates-formes Nexus 5000/6000. Est-il couvert à un moment ultérieur ?

R4 : Non. Pour l'instant, il n'est pas prévu de couvrir les plates-formes Nexus5000/6000 dans un avenir proche.

Q5 : Que puis-je faire si j'ai des questions sur l'un des échecs de vérification de l'intégrité signalés

?

R5 : Veuillez ouvrir une demande de service TAC distincte pour obtenir de l'aide sur le résultat spécifique du bilan de santé. Il est vivement recommandé de joindre le rapport de contrôle d'intégrité et de renvoyer le numéro de dossier de demande de service ouvert pour le contrôle d'intégrité et de configuration automatisé.

Q6 : Puis-je utiliser la même demande de service ouverte pour la vérification automatisée de l'intégrité et de la configuration afin de résoudre les problèmes détectés ?

R6 : Non. La vérification proactive de l'état étant automatisée, ouvrez une nouvelle demande de service pour résoudre les problèmes signalés. Veuillez noter que le SR ouvert pour vérification de santé est fermé dans les 24 heures suivant la publication du rapport de santé.

Q7 : La vérification automatique de l'intégrité et de la configuration s'exécute-t-elle par rapport au `show tech-support details` fichier du commutateur qui exécute les versions antérieures à celle mentionnée précédemment ?

R7 : La vérification automatisée de l'intégrité et de la configuration est conçue pour les plates-formes et les versions logicielles mentionnées ci-dessous. Pour les périphériques qui exécutent des versions plus anciennes, il est préférable et il n'y a aucune garantie sur l'exactitude du rapport.

- Commutateurs de la gamme Nexus 3x00 qui exécutent une image logicielle NX-OS unifiée : 7.0(3)Ix ou ultérieure
- Commutateurs de la gamme Nexus 7000/7700 qui exécutent le logiciel NX-OS version 7.x ou ultérieure
- Commutateurs de la gamme Nexus 9x00 qui exécutent une image logicielle NX-OS unifiée : 7.0(3)Ix ou ultérieure

Q8 : Comment puis-je fermer la demande de service ouverte pour la vérification du fonctionnement ?

R8 : Le SR est fermé dans les 24 heures suivant l'envoi du premier rapport de vérification de l'état de santé. Aucune action requise de la part de l'utilisateur vers la fermeture du SR.

Q9 : Comment puis-je partager des commentaires ou des commentaires sur la vérification proactive de l'intégrité et de la configuration ?

A9 : Veuillez les partager par e-mail à l'adresse Nexus-HealthCheck-Feedback@cisco.com

Q10. Quelle est la méthode recommandée pour capturer `show tech-support` ou extraire `show tech-support details` d'un commutateur ?

R10 : Il est fortement recommandé de capturer le résultat de la commande`show tech-support`ou`show tech-support details`en le dirigeant vers`bootflash:`(comme indiqué dans l'exemple suivant) plutôt que de le capturer dans un fichier journal dans l'application de terminal (par exemple, SecureCRT, PuTTY). N'oubliez pas que le fichier journal capturé par l'application de terminal peut être au format UTF-8-BOM (ou similaire), ce qui n'est PAS pris en charge par le contrôle d'intégrité automatisé. Le

contrôle d'intégrité et de configuration automatisé prend uniquement en charge les fichiers au format ASCII ou UTF-8.

Exemples d'interfaces de ligne de commande pour rediriger le résultat vers`bootflash:`le fichier et le compresser :

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

Commentaires

Toute rétroaction sur le fonctionnement de ces outils est très appréciée. Si vous avez des observations ou des suggestions (par exemple, sur la facilité d'utilisation, la portée, la qualité des rapports générés), veuillez les partager avec nous à l'adresse Nexus-HealthCheck-Feedback@cisco.com.

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

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