Esegui controllo stato e configurazione Nexus

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Convenzioni](#)
[Procedura di verifica dello stato e della configurazione](#)
[Moduli di verifica dello stato e della configurazione](#)
[Rapporti e avvertenze](#)
[Wireless LAN Controller serie 9800](#)
[Feedback](#)

Introduzione

Questo documento descrive la procedura e i requisiti per eseguire controlli automatici di stato e configurazione per le piattaforme Nexus 3000/9000 e 7000.

Prerequisiti

Requisiti

Il controllo automatico dello stato e della configurazione è supportato solo per le piattaforme Nexus che eseguono il software NX-OS standalone e non per gli switch con software ACI.

Sono supportate le seguenti piattaforme hardware:

- Switch Nexus serie 3000/9000 con software NX-OS unificato: 7.0(3)Ix o versione successiva
- Switch Nexus serie 7000/7700 con software NX-OS versione 7.x o successive

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Procedura di verifica dello stato e della configurazione

Raccogliere **show tech-support details** (o **show tech-support** logs) dallo switch Nexus per il quale si desidera eseguire il controllo dello stato e della configurazione. **show tech-support details** è l'opzione preferibile, in quanto fornisce un valore superiore con un numero maggiore di controlli eseguiti. Verificare che i registri siano stati acquisiti in formato .txt o .gz/.tar.

Aprire una normale richiesta di servizio TAC in Cisco Support Case Manager con queste parole chiave (tecnologia/sottotecnologia/codice problema):

Tech: Reti di storage e data center

Tecnologia secondaria: (scegliere una piattaforma appropriata)
Nexus 3000 (solo serie N3000) - Controllo stato e configurazione (AUTOMATIZZATO)
Nexus 3000 (serie N3100-N3600) - Controllo stato e configurazione (AUTOMATIZZATO)
Nexus serie 7000 Switch - Controllo stato e configurazione (AUTOMATIZZATO)
Nexus 9200 - Controllo stato e configurazione (AUTOMATICO)
Nexus 9300 (non serie EX/FX/R) - Controllo stato e configurazione (AUTOMATIZZATO)
Nexus 9300 (serie EX/FX/R) - Controllo stato e configurazione (AUTOMATIZZATO)

Switch Nexus serie 9400 - Controllo stato e configurazione (AUTOMATIZZATO)
Nexus 9500 (non serie EX/FX/R) - Controllo stato e configurazione (AUTOMATIZZATO)
Nexus 9500 (serie EX/FX/R) - Controllo stato e configurazione (AUTOMATIZZATO)

Switch Nexus serie 9800 - Controllo stato e configurazione (AUTOMATIZZATO)

Codice problema: verifica dello stato e della configurazione

Una volta aperta la SR, un flusso di lavoro guidato da Cisco può guidarti fino al caricamento **dei dettagli di supporto tecnico** (o) **mostrare** i log di supporto tecnico.

Dopo aver caricato l'output richiesto, Cisco analizza i log e fornisce un report (in formato PDF) allegato a un'e-mail inviata all'utente. Il report contiene un elenco dei problemi rilevati, le operazioni da eseguire per risolverli e il piano di azioni consigliato.

In caso di domande relative ai guasti del controllo dello stato segnalati, si consiglia agli utenti di aprire una o più richieste di assistenza separate con parole chiave appropriate per ottenere ulteriore assistenza da parte di esperti. Si consiglia di fare riferimento al numero della richiesta di servizio (SR) aperto per il controllo automatico dello stato e della configurazione insieme al report generato per accelerare l'analisi.

Moduli di verifica dello stato e della configurazione

Controllo automatico dello stato e della configurazione di Nexus **versione 1**, agosto 2022, esegue i controlli elencati nella tabella 1.

Tabella 1: moduli di controllo dello stato e CLI associati utilizzati dai moduli

Indice	Modulo di verifica dello stato	Breve descrizione del modulo	CLI utilizzati per eseguire il controllo dello stato
1.	Controllo del rilascio di NX-OS	Controlla se il dispositivo esegue una versione del software NX-OS consigliata	show version

		da Cisco	
2.	Controllo dei prodotti Nexus EoS/EoL	Verifica se uno dei componenti (hardware/software) ha raggiunto la fine del ciclo di vita (EOL) o di vendita (EOS)	show version show module mostra inventario
3.	Controllo delle notifiche	Controlla se il dispositivo è potenzialmente interessato da un PSIRT/CVE noto o da una notifica sul campo.	show version show module mostra inventario show running-config e qualsiasi comando necessario per controllare il file rispetto a un FN/PSIRT specificato.
4.	Controllo dello stato della CPU NX-OS	Controlla i sintomi per verificare l'utilizzo elevato della CPU. Viene segnalato quando l'utilizzo corrente/storico della CPU è >60%.	show processes cpu show processes cpu sort mostra cronologia cpu processi mostra risorse di sistema
5.	Verifica dello stato della memoria NX-OS	Controlla se l'utilizzo di memoria sul dispositivo è superiore alle soglie della memoria di sistema (valori predefiniti o configurati dall'utente).	show version mostra memoria dei processi mostra risorse di sistema
6.	Verifica interfacce NX-OS	Controlla se una delle interfacce segnalate subisce cadute in direzione RX o TX. Il modulo stampa 5 interfacce con la frequenza di errore più alta in ciascuna direzione.	show interface show interface brief mostra coda
7.	Controllo di prevenzione sullo stato del protocollo CoPP	Controlla se CoPP è disabilitato o configurato in modo non corretto (ad esempio, tutto il traffico basato sulla CPU che raggiunge la classe predefinita), se i criteri CoPP sono obsoleti (ad esempio, riportati da versioni precedenti) o se nelle classi non predefinite sono segnalati intervalli superiori a 1000.	mostra stato copp show policy-map interface control plane show running-config
8.	Verifica dello stato della comunicazione interprocesso (MTS)	Rileva la presenza di messaggi di comunicazione tra processi (denominati MTS) bloccati per più di 1 giorno.	mostra riepilogo buffer mts interno del sistema mostra dettagli buffer mts interno del sistema

9.	Verifica dello stato del modulo Nexus	Controlla se uno dei moduli (linecard, fabric e così via) ha riportato errori di diagnostica o è spento/guasto	mostrare modulicome fare l'inventario mostra tutti i dettagli del modulo risultati diagnostica
10.	Controllo dello stato di PSU e VENTOLE	Rileva se uno degli alimentatori non è in stato operativo.	show inventoryshow environment <opzioni> mostra log di log show logging nvram
11.	Verifica delle best practice di vPC	Verifica che la configurazione del dispositivo soddisfi le best practice vPC, come le configurazioni di router peer, switch peer e gateway peer.	<u>Router peer di layer 3:</u> show running-config (per verificare se sono presenti adiacenze OSPF, EIGRP e BGP) <u>Peer-Gateway/Peer-Switch:</u> show running-config show spanning-tree show vpc brief show interface brief
12.	Controllo MTU	Rileva configurazioni MTU incoerenti, come l'interfaccia di layer 2 e la SVI di layer 3 che non corrispondono alle configurazioni MTU, MTU errata sulle interfacce di join OTV o MTU jumbo non abilitata sulle interfacce dove è richiesta e così via.	show running-configshow interface show ip arp <opzioni> show mac address-table show ip route detail <opzioni> show ip eigrp neighbors <opzioni> show ip ospf neighbors <opzioni> show bgp <opzioni>
13.	Controllo stato configurazione funzionalità Layer2	Controlla se sono abilitate funzionalità L2 ma non vengono utilizzate	show running-config
14.	Verifica compatibilità vPC	Controlla se sono stati segnalati errori di incompatibilità di tipo 1/tipo 2 dei canali	show running-config

	NX-OS	porte virtuali (vPC).	show vpc <opzioni>
15.	Controllo stato Spanning Tree Protocol	Controlla gli output collegati per individuare eventuali instabilità del protocollo Spanning Tree o uno stato imprevisto. Il modulo segnala le vlan in cui sono state apportate le modifiche più recenti alla topologia, oltre ad alcune informazioni aggiuntive: timestamp, interfaccia e ID bridge radice. Attualmente, questo modulo di verifica dello stato supporta solo RSTP; il supporto per MST è previsto per le versioni future.	mostra dettagli spanning-tree mostra errori interni spanning-tree show spanning-tree internal event-history <opzioni> show spanning-tree active mostra log di log show mac address-table notification show system internal <L2FM, MTM, L2DBG opzioni>
16.	Verifica dello stato di PortChannel	Rileva se uno dei membri del canale della porta configurati è in stato non integro: (I), (s) (D) o (H)	show port-channel summary
17.	Controllo convalida SFP	Rileva eventuali ricetrasmettitori che hanno segnalato un errore di "Convalida SFP non riuscita"	show interface brief
18.	Controllo dello stato della configurazione della funzionalità di layer 3	Controlla se sono attivate funzionalità L3 ma non utilizzate	show running-config
19.	Route predefinita tramite controllo VRF di gestione	Controlla se il dispositivo dispone di un percorso predefinito configurato nel file vrf predefinito che punta tramite il file vrf di gestione.	show running-config mostra registro di accounting
20.	Controllo routing multicast su vPC non supportato	Verifica l'adiacenza PIM non supportata su vPC	show running-config show ip pim interface vrf all internal show ip pim neighbors vrf all detail
21.	Controllo di prevenzione e risoluzione problemi OSPF	Verifica la presenza di eventuali problemi di adiacenza rilevati sul dispositivo. Ad esempio: • rilevati più vicini sull'interfaccia configurata come P2P	show running-config show ip interface brief vrf all show ip ospf neighbors detail vrf all private

		• ID router non configurato manualmente o che ha utilizzato un IP di loopback • adiacenze non in stato FULL • adiacenze che hanno raggiunto lo stato FULL di recente e che indicano una potenziale instabilità	show ip ospf interface vrf all private mostra log di log
22.	Controllo dello stato di EIGRP	Verifica la presenza di eventuali problemi di adiacenza rilevati sul dispositivo. Ad esempio: • Numero AS non configurato • Nessun vicino attivo rilevato • Rilevati valori elevati di SRTT, RTO o Q Cnt • Rilevato numero elevato di pacchetti EIGRP ignorati • Inferiore al tempo di attività di 15 minuti dell'adiacenza e indica instabilità potenziale • Adiacente è sceso negli ultimi 7 giorni	show running-config mostra log di log show ip eigrp neighbors detail vrf all show ip eigrp detail vrf all
23.	Controllo stato peer BGP	Verifica l'adiacenza BGP nello stato IDLE.	show running-config mostra riepilogo tutto vrf bgp
24.	Protocollo FHRP (First-Hop Redundancy Protocol)	Controlla la presenza di configurazioni del timer non predefinite, in quanto tali configurazioni possono determinare prestazioni non ottimali. Questo modulo di verifica dello stato copre SOLO il protocollo HSRP (Hot-Standby Routing Protocol)	show running-config

Rapporti e avvertenze

- Il servizio di verifica dello stato e della configurazione SR è automatizzato e gestito dal tecnico TAC virtuale.
- Il report (in formato PDF) viene in genere generato entro 24 ore lavorative dopo che tutti i registri necessari sono stati allegati alla SR.
- Il report viene automaticamente condiviso tramite e-mail (disponibile all'indirizzo jhwatson@cisco.com) con tutti i contatti (principali e secondari) associati alla richiesta di servizio.
- Il report viene inoltre allegato alla richiesta di assistenza per consentirne la disponibilità in un momento successivo.
- Si tenga presente che i problemi elencati nel rapporto si basano sui registri forniti e rientrano nell'ambito dei moduli di controllo dello stato elencati in precedenza nella tabella 1.

- L'elenco dei controlli dello stato e della configurazione eseguiti non è esaustivo e si consiglia agli utenti di eseguire ulteriori controlli, se necessario.

Wireless LAN Controller serie 9800

D1: È possibile caricare i *dettagli del supporto tecnico* per più switch nella stessa SR per ottenere un rapporto di verifica dello stato per tutti gli switch?

R1: Si tratta di una gestione automatizzata dei casi e i controlli di integrità vengono eseguiti dal tecnico TAC virtuale. Il controllo dello stato viene eseguito solo per la prima *visualizzazione dei dettagli del supporto tecnico* caricati.

D2: Posso caricare più di un *show tech-support dettagli* per lo stesso dispositivo diciamo, catturato a poche ore di distanza, per ottenere il controllo dello stato fatto per entrambi?

A2: Si tratta di una gestione automatizzata e senza conservazione dello stato eseguita dal Virtual TAC Engineer. Il controllo dello stato e della configurazione viene eseguito per la prima volta sul file *show tech-support details* caricato nella SR, a prescindere dal fatto che i file caricati provengano dallo stesso switch o da switch diversi.

D3: È possibile eseguire controlli di prevenzione sullo stato degli switch i cui file con *i dettagli del supporto tecnico* vengono compressi come un singolo file rar/gz e caricati nella SR?

R3: No. Se vengono caricati più *dettagli di visualizzazione del supporto tecnico* come un unico file rar/zip/gz, per i controlli di integrità viene elaborato solo il primo file dell'archivio.

D4: Non è possibile verificare lo stato e la configurazione delle piattaforme Nexus 5000/6000. Viene trattato in un secondo momento?

R4: No. Al momento non è prevista la copertura delle piattaforme Nexus 5000/6000 nel prossimo futuro.

Q5: Cosa posso fare se ho domande su uno dei guasti del controllo dello stato segnalati?

R5: Aprire una richiesta di assistenza TAC separata per ottenere ulteriore assistenza sui risultati specifici del controllo dello stato. Si consiglia di allegare il rapporto di controllo dello stato e fare riferimento al numero di richiesta di servizio (SR) aperto per il controllo automatico dello stato e della configurazione.

D6: È possibile utilizzare la stessa SR aperta per il controllo automatico dello stato e della configurazione per risolvere i problemi rilevati?

R6: No. Poiché il controllo proattivo dello stato è automatizzato, aprire una nuova richiesta di assistenza per risolvere i problemi segnalati. Si tenga presente che la SR aperta per il controllo dello stato viene chiusa entro 24 ore dalla pubblicazione del rapporto di stato.

D7: Il controllo automatico dello stato e della configurazione viene eseguito in base al file *show tech-support details* per lo switch con versioni precedenti a quella menzionata sopra?

R7: Il controllo automatico dello stato e della configurazione è progettato per le piattaforme e le versioni software indicate di seguito. Per i dispositivi che eseguono versioni precedenti, è consigliabile e non vi è alcuna garanzia sull'accuratezza del report.

- Switch Nexus serie 3x00 con software NX-OS unificato: 7.0(3)Ix o versione successiva
- Switch Nexus serie 7000/7700 con software NX-OS versione 7.x o successive
- Switch Nexus serie 9x00 con software NX-OS unificato: 7.0(3)Ix o versione successiva

D8: Come è possibile chiudere la SR aperta per la verifica dello stato?

A8: la SR viene chiusa entro 24 ore dall'invio del primo rapporto di verifica dello stato. Non è necessaria alcuna azione da parte dell'utente verso la chiusura della SR.

D9: Come posso condividere commenti o feedback sul controllo proattivo dello stato e della configurazione?

R9: Inviale un'e-mail a Nexus-HealthCheck-Feedback@cisco.com

Feedback

Qualsiasi commento sul funzionamento di questi strumenti è molto apprezzato. Per eventuali osservazioni o suggerimenti (ad esempio sulla facilità d'uso, l'ambito di applicazione e la qualità delle segnalazioni generate), contattateci all'indirizzo Nexus-HealthCheck-Feedback@cisco.com.

Informazioni su questa traduzione

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