Executar Verificação de Integridade e Configuração do MDS

Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Conventions
Procedimento de verificação de integridade e configuração
<u>Níveis de severidade</u>
Módulos de verificação de integridade e configuração
Relatórios e avisos
Perguntas freqüentes
Realizar verificação de integridade e configuração do Nexus
Feedback

Introdução

Este documento descreve o procedimento e os requisitos para executar verificações automáticas de integridade e configuração para as plataformas MDS 9000.

Pré-requisitos

Requisitos

A Verificação Automatizada de Integridade e Configuração é suportada apenas para plataformas MDS que executam uma versão suportada do software NX-OS®.

Estas plataformas de hardware são suportadas:

 Todos os switches MDS 9000 Series que ainda não alcançaram a última data de suporte: HW. Consulte os Avisos de Fim da Vida Útil e Fim das Vendas do MDS aqui:

Avisos de fim da vida útil e fim das vendas

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 <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

Procedimento de verificação de integridade e configuração

Para executar uma verificação automatizada de integridade e configuração em switches MDS, abra uma solicitação de serviço TAC regular no Cisco <u>Support Case Manager</u> com o seguinte conjunto de palavras-chave:

Técnico: Data Center e rede de armazenamento

Sub-Tech: MDS9000 - Verificação de integridade e configuração (AUTOMATIZADA)

Código do problema: verificação de integridade e configuração

Para o TAC SR aberto, carregue a saída do comando "show tech-support details" capturado do switch, no formato .txt ou .gz/.tar. Atualmente, o arquivo de detalhes show tech-support capturado nos formatos de texto ASCII e UTF-8 é suportado. Para obter instruções de carregamento, consulte <u>Carregamentos de arquivos do cliente TAC</u>.

Começando com o NX-OS 8.4(2d) e 9.2(1), o comando MDS tac-pac foi aprimorado para criar rapidamente um arquivo no bootflash que contém um show tech-support details com um show logging onboard anexado. Esse é o método preferido de criar o arquivo de entrada para qualquer Solicitação de Serviço (SR) do TAC que exija detalhes de show tech-support, incluindo um caso de verificação automatizada de integridade e configuração.

Depois que a saída necessária é anexada ao SR, a automação da Cisco analisa os logs e fornece um relatório (em formato PDF) anexado a um e-mail enviado a você. O relatório contém uma lista de problemas detectados, etapas relevantes para solucionar os problemas e um plano de ação 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 mais assistência. 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.

Níveis de severidade

Na tabela estão os próximos níveis de gravidade padrão do NX-OS e suas definições são usadas.

Nível de severidade	Descrição	
Emergência(0)	O sistema está inutilizável.	
Alerta(1)	Condições críticas, atenção imediata necessária.	
Crítico(2)	Condições principais.	
Erro(3)	Condições menores.	
Aviso(4)	Condições de aviso.	
Aviso(5)	Notificação básica e mensagens informativas. Possivelmente independentemente insignificante.	
Informações(6)	Evento normal significando retorno ao estado normal.	

Módulos de verificação de integridade e configuração

Automated MDS Health and Configuration Check Versão 1, de maio de 2023, 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 do transceptor MDS para EOL/EOS	Verifica se algum transceptor está no fim da vida útil (EOL) ou no fim das vendas (EOS).	show version show clock show hardware
3	Utilização da taxa de dados para interfaces FC no switch MDS	Verifica as taxas de entrada e saída da interface. Lista as 10 principais interfaces e alertas em interfaces que estão acima de 80% de utilização.	show version show interface brief show interface
4	Informações detalhadas do	Verifica os valores de temperatura,	show version

	transceptor para o switch MDS	voltagem, corrente, potência de transmissão ou potência rx da interface para obter valores nominais. Sugere as próximas etapas se forem detectadas falhas.	show hardware show interface transceiver details
5	Verificar se há defeitos de PSIRT com base na versão do NX-OS em execução	Combina com uma variedade de PSIRTs de acordo com o HW/SW e a configuração. Isto não é exaustivo.	show version show running-config
6	Verificação de MDS para Informações de Relógio	Verifica a configuração de relógio recomendada e fornece exemplos de configurações de relógio recomendadas.	show running-config show clock
7	Verificação de hardware MDS para EOL/EOS	Identifica as datas de EOL (End-of- Life, fim da vida útil) e EOS (End-of- Support, fim do suporte) para módulos e chassis MDS.	show version show module show hardware show inventory
8	Verificação do software MDS para EOL/EOS	Identifica as datas de EOL (End-of- Life, fim da vida útil) e EOS (End-of- Support, fim do suporte) das versões do MDS NX-OS.	show version show module
9	Verificação de consistência do banco de dados MDS FCNS e do banco de dados FLOGI	Verifique a consistência entre as saídas de show FCNS database e show FLOGI database.	show version show hardware show flogi database show fcns database local vsan 1-4093
10	Verificação de MDS para todas as VSANs ativas em todas as portas TF	Verifique para garantir que todas as portas TF tenham todas as VSANs permitidas no estado ativo, sem VSANs em estados isolados ou de inicialização.	show version show hardware show interface

			show interface brief show port-channel database
11	Verificação de MDS para todas as VSANs ativas em todas as portas TE	Verifique se todas as portas TE permitiram VSANs no estado ativo, sem VSANs nos estados isolado ou de inicialização.	show version show module show interface show interface brief show port-channel database
12	Dispositivos Remotos de Verificação de OUI do MDS	Certifique-se de que o MDS reconheça o OUI de conexões conectadas através de conexões de tronco e de canal de porta.	show flogi internal event- history errors show port internal event- history errors show system internal fcfwd idxmap interface show flogi internal event- history debugs show accounting log
13	Verificação de Bloqueio MDS CFS	Verifique se há bloqueios de CFS e etapas sugeridas para limpar os bloqueios.	show version show module show hardware show cfs lock show logging log show cfs internal session- history show cfs peers show fcdomain domain-list show cfs internal event- history errors

			show clock
14	Link MDS Check do supervisor ativo mgmt0	Verifique se o status do link ativo ou somente do supervisor mgmt0 mostra 'ativado'.	show version show interface mgmt0
15	MDS 9700 Verificar link mgmt0 do supervisor em standby	Verifique se o status do link do supervisor mgmt0 standby mostra "ativado". Válido somente para diretors MDS 9700 que executam o NX-OS 9.2(1) e versões posteriores.	show version show interface mgmt0 standby
16	Verificação de Alocação de Membro de PC Subótimo do MDS	Os canais de porta são importantes para a resiliência em SANs Fibre Channel de vários switches. A configuração de canais de porta para tolerância máxima a falhas e utilização de recursos de hardware contribui para a resiliência da SAN. Este módulo verifica cada canal de porta Fibre Channel encontrado para garantir que suas interfaces membro sejam distribuídas da maneira mais uniforme possível pelos módulos e mecanismos de fwd disponíveis no switch.	show version show interface brief
17	Verificação de consistência do MDS FSPF	Verifica os custos do FSPF em cada ISL para garantir que os switches adjacentes tenham os mesmos custos/consistentes. Se os custos forem diferentes em cada lado do ISL, poderá ocorrer roteamento inesperado ou assimétrico. Essa verificação não é aplicável a switches no modo NPV, pois não há nenhum banco de dados FSPF nesses switches.	show switchname show fspf database show fcs ie show npv internal info
18	Verificação de Alta Utilização da CPU do MDS	Verifique se a utilização atual da CPU está dentro do limite predeterminado, verificando várias	show processes cpu show processes cpu

		saídas de comando. Notificar o usuário se o uso exceder 60%, informar o usuário se o uso exceder 80% e avisar o usuário se o uso exceder 90%.	history show logging log
19	Verificação de Utilização de Memória Alta do MDS	Verifique algumas saídas de comando diferentes para determinar se o uso de memória atual é menor que os limites configurados ou se qualquer um dos processos está sendo executado dentro do limite de memória designado. Se o uso exceder 90%, notifique os usuários.	show version show processes memory show running-config
20	Configuração de Taxa de Dados Tx do Monitor de Porta de Verificação do MDS para Detectar a Utilização Excedente	Verifique a(s) política(s) ativa(s) do monitor de porta para determinar se os contadores tx-datarate e/ou tx- datarate-burst estão configurados para detectar corretamente a subutilização.	show version show interface brief show running-config

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 (originado do Cisco TAC Automated Emails <no-reply@cisco.com>) com todos os contatos (primários e secundários) associados à solicitação de serviço.
- O relatório também é anexado à Solicitação de Serviço para permitir sua disponibilidade em qualquer momento posterior.
- Informamos que os problemas listados no relatório se baseiam nos logs fornecidos e estão dentro do escopo dos módulos de verificação de integridade listados na Tabela 1 (mostrada anteriormente).
- 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.
- Novas verificações de integridade e configuração podem ser adicionadas ao longo do tempo.

Perguntas freqüentes

P1: Posso carregar detalhes do show tech-support para mais de um switch no mesmo SR para obter o relatório de verificação de integridade para 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 somente para os primeiros detalhes show tech-support carregados.

P2: Posso carregar mais de um detalhe show tech-support para o mesmo dispositivo, por exemplo, capturado com poucas horas de intervalo, para fazer uma verificação de integridade para ambos?

R2: Este é um tratamento de caso automatizado e stateless executado pelo Engenheiro TAC Virtual, e a verificação de integridade e configuração é feita para o primeiro arquivo show techsupport details carregado para o SR, independentemente de os arquivos carregados serem do mesmo switch ou de switches diferentes.

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

R3: Não. se vários detalhes do show tech support forem carregados como um único arquivo rar/zip/gz, somente o primeiro arquivo do arquivo será processado para verificações de integridade.

P4: O que posso fazer se tiver dúvidas sobre uma das falhas de verificação de integridade reportadas?

R4: 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.

P5: Posso usar o mesmo SR aberto para a verificação automatizada de integridade e configuração para solucionar os problemas encontrados?

R5: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 dentro de 24 horas após a publicação do relatório de integridade.

P6: A verificação automatizada de integridade e configuração é executada no arquivo show techsupport details para o switch que executa versões mais antigas do que a mencionada anteriormente?

R6: A verificação automatizada de integridade e configuração foi criada para as plataformas e versões de software mencionadas anteriormente. Para dispositivos que executam versões mais antigas, é o melhor esforço e não há garantia da precisão do relatório.

P7: Como posso fechar o SR aberto para verificação de integridade?

R7: 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.

P8: Como compartilhar comentários ou comentários sobre a verificação proativa de integridade e configuração?

R8: Compartilhe-os por e-mail para MDS-HealthCheck-Feedback@cisco.com

P9. Qual é o método recomendado para capturar "show tech-support" ou "show tech-support details" de um switch?

R9:Como mencionado anteriormente neste documento, começando com o NX-OS 8.4(2d) e 9.2(1), o comando MDS tac-pac foi aprimorado para criar rapidamente um arquivo no bootflash que contém um show tech-support details com um show logging onboard anexado . Esse é o método preferido de criação do arquivo de entrada para qualquer Solicitação de Serviço (SR) do TAC que exija detalhes de show tech-support, incluindo uma verificação automatizada de integridade e configuração. A saída CLI capturada em um arquivo de registro no aplicativo de terminal (por exemplo, SecureCRT, PuTTY) 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.

Realizar verificação de integridade e configuração do Nexus

Consulte Executar verificação de integridade e configuração do Nexus .

Feedback

Qualquer comentário sobre o funcionamento dessas ferramentas é muito apreciado. Se você tiver observações ou sugestões (por exemplo, sobre a facilidade de uso, escopo, qualidade dos relatórios gerados e assim por diante), compartilhe-as aqui <u>MDS-HealthCheck-</u> <u>Feedback@cisco.com.</u>

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.