Monitoramento de integridade

ONTAP 9

NetApp
January 17, 2025

Índice

Monitoramento de integridade

Monitore a integridade da visão geral do sistema

Os monitores de integridade monitoram proativamente certas condições críticas no cluster e emitem alertas se detetarem uma falha ou risco. Se existirem alertas ativos, o estado de funcionamento do sistema comunica um estado degradado para o cluster. Os alertas incluem as informações de que você precisa para responder à integridade degradada do sistema.

Se o estado estiver degradado, pode visualizar detalhes sobre o problema, incluindo a causa provável e as ações de recuperação recomendadas. Depois de resolver o problema, o estado de funcionamento do sistema regressa automaticamente a OK.

O status de integridade do sistema reflete vários monitores de integridade separados. Um status degradado em um monitor de integridade individual causa um status degradado para a integridade geral do sistema.

Para obter detalhes sobre como o ONTAP suporta switches de cluster para monitoramento de integridade do sistema em seu cluster, consulte *Hardware Universe*.

"Switches suportados no Hardware Universe"

Para obter detalhes sobre as causas das mensagens do AutoSupport do Monitor de integridade do comutador de cluster (CSHM) e as ações necessárias para resolver esses alertas, consulte o artigo da base de conhecimento.

"Mensagem do AutoSupport: Processo do monitor de saúde CSHM"

Como funciona o monitoramento de saúde

Os monitores de saúde individuais têm um conjunto de políticas que acionam alertas quando ocorrem determinadas condições. Entender como funciona o monitoramento de saúde pode ajudá-lo a responder a problemas e controlar futuros alertas.

O monitoramento de integridade consiste nos seguintes componentes:

- Monitores de saúde individuais para subsistemas específicos, cada um dos quais tem seu próprio estado de saúde

  Por exemplo, o subsistema Storage tem um monitor de integridade da conetividade de nó.

- Um monitor geral de integridade do sistema que consolida o estado de saúde dos monitores de saúde individuais

  Um status degradado em qualquer subsistema resulta em um status degradado para todo o sistema. Se nenhum subsistema tiver alertas, o status geral do sistema é OK.

Cada monitor de saúde é composto pelos seguintes elementos-chave:

- Alerta de que o monitor de integridade pode potencialmente aumentar

Cada alerta tem uma definição, que inclui detalhes como a gravidade do alerta e sua causa provável.

- Políticas de saúde que identificam quando cada alerta é acionado

  Cada política de saúde tem uma expressão de regra, que é a condição ou mudança exata que aciona o alerta.

Um monitor de integridade monitora e valida continuamente os recursos em seu subsistema para mudanças de condição ou estado. Quando uma condição ou mudança de estado corresponde a uma expressão de regra em uma política de saúde, o monitor de integridade gera um alerta. Um alerta faz com que o estado de funcionamento do subsistema e o estado geral do estado do sistema se degradem.

Maneiras de responder a alertas de integridade do sistema

Quando um alerta de integridade do sistema ocorre, você pode reconhecê-lo, saber mais sobre ele, reparar a condição subjacente e impedir que ele ocorra novamente.

Quando um monitor de saúde gera um alerta, você pode responder de qualquer uma das seguintes maneiras:

- Obtenha informações sobre o alerta, que inclui o recurso afetado, a gravidade do alerta, a causa provável, o possível efeito e as ações corretivas.
- Obtenha informações detalhadas sobre o alerta, como a hora em que o alerta foi gerado e se alguém já reconheceu o alerta.
- Obtenha informações relacionadas à integridade sobre o estado do recurso ou subsistema afetado, como um compartimento ou disco específico.
- Reconheça o alerta para indicar que alguém está trabalhando no problema e identifique-se como o ""reconhecimento"".
- Resolva o problema tomando as ações corretivas fornecidas no alerta, como a fixação de cabeamento para resolver um problema de conetividade.
- Exclua o alerta, se o sistema não o apagou automaticamente.
- Suprimir um alerta para impedir que ele afete o status de integridade de um subsistema.

  Suprimir é útil quando você entende um problema. Depois de suprimir um alerta, ele ainda pode ocorrer, mas a integridade do subsistema é exibida como "'ok-with-suppressed.'" quando o alerta suprimido ocorre.

Personalização do alerta de integridade do sistema

Você pode controlar quais alertas um monitor de integridade gera ativando e desativando as políticas de integridade do sistema que definem quando os alertas são acionados. Isso permite que você personalize o sistema de monitoramento de integridade para seu ambiente específico.

Você pode aprender o nome de uma política exibindo informações detalhadas sobre um alerta gerado ou exibindo definições de política para um monitor de integridade específico, nó ou ID de alerta.

Desativar políticas de saúde é diferente de suprimir alertas. Quando você suprime um alerta, ele não afeta o status de integridade do subsistema, mas o alerta ainda pode ocorrer.

Se você desabilitar uma política, a condição ou estado definido em sua expressão de regra de política não

acionará mais um alerta.

Exemplo de um alerta que você deseja desativar

Por exemplo, suponha que ocorra um alerta que não seja útil para você. Você usa o `system health alert show -instance` comando para obter o ID da política para o alerta. Você usa o ID da política no `system health policy definition show` comando para exibir informações sobre a política. Depois de analisar a expressão da regra e outras informações sobre a política, você decide desativar a política. Você usa o `system health policy definition modify` comando para desativar a política.

Como os alertas de saúde acionam mensagens e eventos do AutoSupport

Os alertas de integridade do sistema acionam mensagens e eventos AutoSupport no sistema de Gestão de Eventos (EMS), permitindo-lhe monitorizar a integridade do sistema utilizando mensagens AutoSupport e o EMS, além de utilizar diretamente o sistema de monitorização de integridade.

O sistema envia uma mensagem AutoSupport dentro de cinco minutos após um alerta. A mensagem AutoSupport inclui todos os alertas gerados desde a mensagem AutoSupport anterior, exceto para alertas que duplicam um alerta para o mesmo recurso e causa provável na semana anterior.

Alguns alertas não acionam mensagens AutoSupport. Um alerta não aciona uma mensagem AutoSupport se a sua política de integridade desativar o envio de mensagens AutoSupport. Por exemplo, uma política de integridade pode desativar as mensagens do AutoSupport por padrão porque o AutoSupport já gera uma mensagem quando o problema ocorre. Você pode configurar políticas para não acionar mensagens AutoSupport usando o `system health policy definition modify` comando.

Você pode ver uma lista de todas as mensagens AutoSupport acionadas por alerta enviadas na semana anterior usando o `system health autosupport trigger history show` comando.

Os alertas também acionam a geração de eventos para o EMS. Um evento é gerado cada vez que um alerta é criado e cada vez que um alerta é apagado.

Monitores de integridade do cluster disponíveis

Existem vários monitores de integridade que monitorizam diferentes partes de um cluster. Os monitores de integridade ajudam você a se recuperar de erros nos sistemas ONTAP detetando eventos, enviando alertas para você e excluindo eventos conforme eles forem claros.

Nome do monitor de integridade (identificador)	Nome do subsistema (identificador)	Finalidade
Interrutor do cluster (interrutor do cluster)	Interrutor (estado do interrutor)	Monitora os switches de rede de cluster e os switches de rede de gerenciamento para temperatura, utilização, configuração de interface, redundância (somente switches de rede de cluster) e operação de ventilador e fonte de alimentação. O monitor de integridade do comutador de cluster comunica com os comutadores através do SNMP. SNMPv2c é a configuração padrão. A partir do ONTAP 9.2, este monitor pode detetar e reportar quando uma central de cluster foi reinicializada desde o último período de polling.
MetroCluster Fabric	Interrutor	Monitora a topologia da malha de back-end de configuração do MetroCluster e deteta configurações incorretas, como cabeamento e zoneamento incorretos e falhas de ISL.
MetroCluster Saúde	Interconexão, RAID e armazenamento	Monitora os adaptadores FC-VI, os adaptadores iniciador FC, os discos e agregados esquerdos e as portas entre clusters
Conetividade do nó (nó-conexão)	Operações ininterruptas de CIFS (CIFS-NDO)	Monitora conexões SMB para operações ininterruptas com aplicações Hyper-V.
Storage (conexão SAS)	Monitora compartimentos, discos e adaptadores no nível do nó para ver os caminhos e as conexões apropriados.	Sistema
não aplicável	Agrega informações de outros monitores de saúde.	Conetividade do sistema (conexão do sistema)

Receba alertas de integridade do sistema automaticamente

Você pode visualizar manualmente os alertas de integridade do sistema usando o `system health alert show` comando. No entanto, você deve assinar mensagens específicas do sistema de Gerenciamento de Eventos (EMS) para receber notificações automaticamente quando um monitor de integridade gera um alerta.

Sobre esta tarefa

O procedimento a seguir mostra como configurar notificações para todas as mensagens hm.alert.raised e todas as mensagens hm.alert.cleared.

Todas as mensagens hm.alert.raised e todas as mensagens hm.alert.cleared incluem um trap SNMP. Os nomes dos traps SNMP são `HealthMonitorAlertRaised` e `HealthMonitorAlertCleared`. Para obter informações sobre traps SNMP, consulte o *Network Management Guide*.

Passos

1. Utilize o `event destination create` comando para definir o destino para o qual pretende enviar as mensagens EMS.

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

2. Utilize o `event route add-destinations` comando para encaminhar a `hm.alert.raised` mensagem e a `hm.alert.cleared` mensagem para um destino.

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

Informações relacionadas

"Gerenciamento de rede"

Responder à integridade do sistema degradado

Quando o estado de funcionamento do sistema estiver degradado, pode apresentar alertas, ler sobre a causa provável e as acões correctivas, apresentar informações sobre o subsistema degradado e resolver o problema. Alertas suprimidos também são mostrados para que você possa modificá-los e ver se eles foram reconhecidos.

Sobre esta tarefa

Você pode descobrir que um alerta foi gerado visualizando uma mensagem AutoSupport ou um evento EMS, ou usando os `system health` comandos.

Passos

1. Use o `system health alert show` comando para visualizar os alertas que estão comprometendo a integridade do sistema.

2. Leia a causa provável, o possível efeito e as ações corretivas do alerta para determinar se você pode resolver o problema ou precisa de mais informações.
3. Se você precisar de mais informações, use o `system health alert show -instance` comando para exibir informações adicionais disponíveis para o alerta.
4. Use o `system health alert modify` comando com o `-acknowledge` parâmetro para indicar que você está trabalhando em um alerta específico.
5. Tome medidas corretivas para resolver o problema conforme descrito pelo `Corrective Actions` campo no alerta.

   As ações corretivas podem incluir a reinicialização do sistema.

   Quando o problema é resolvido, o alerta é automaticamente apagado. Se o subsistema não tiver outros alertas, a integridade do subsistema será alterada para `OK`. Se a integridade de todos os subsistemas estiver OK, o estado geral do sistema muda para `OK`.

6. Utilize o `system health status show` comando para confirmar se o estado de funcionamento do sistema é `OK`.

   Se o estado de funcionamento do sistema não for `OK` , repita este procedimento.

Exemplo de resposta à integridade do sistema degradado

Ao analisar um exemplo específico de integridade do sistema degradado causado por um compartimento que não tem dois caminhos para um nó, você pode ver o que a CLI exibe quando você responde a um alerta.

Depois de iniciar o ONTAP, você verifica a integridade do sistema e descobre que o status está degradado:

```
cluster1::>system health status show
  Status
  ---------------
  degraded
```

Você mostra alertas para descobrir onde está o problema e vê que o compartimento 2 não tem dois caminhos para o node1:

```
      cluster1::>system health alert show
                 Node: node1
             Resource: Shelf ID 2
             Severity: Major
       Indication Time: Mon Nov 10 16:48:12 2013
     Probable Cause: Disk shelf 2 does not have two paths to controller
                     node1.
    Possible Effect: Access to disk shelf 2 via controller node1 will be
                     lost with a single hardware component failure (e.g.
                     cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached
to disk shelf 2.
                     2. Connect disk shelf 2 to controller node1 via two
paths following the rules in the Universal SAS and ACP Cabling Guide.
                     3. Reboot the halted controllers.
                     4. Contact support personnel if the alert persists.
```

Você exibe detalhes sobre o alerta para obter mais informações, incluindo o ID de alerta:

```
      cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
                  Node: node1
               Monitor: node-connect
              Alert ID: DualPathToDiskShelf_Alert
     Alerting Resource: 50:05:0c:c1:02:00:0f:02
             Subsystem: SAS-connect
       Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
        Probable Cause: Connection_establishment_error
           Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
       Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
          Acknowledge: false
             Suppress: false
               Policy: DualPathToDiskShelf_Policy
         Acknowledger: -
           Suppressor: -
Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
Alerting Resource Name: Shelf ID 2
```

Você reconhece o alerta para indicar que está trabalhando nele.

```
      cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true
```

Você conserta o cabeamento entre as prateleiras 2 e node1 e reinicializa o sistema. Em seguida, você verifica novamente a integridade do sistema e vê se o status é `OK`:

```
cluster1::>system health status show
  Status
  ---------------
  OK
```

Configurar a descoberta de switches de rede de gerenciamento e cluster

O monitor de integridade do switch de cluster tenta automaticamente descobrir os switches de rede de gerenciamento e cluster usando o Protocolo de detecção de Cisco (CDP). Você deve configurar o monitor de integridade se ele não conseguir descobrir automaticamente um switch ou se você não quiser usar o CDP para deteção automática.

Sobre esta tarefa

O `system cluster-switch show` comando lista os switches que o monitor de integridade descobriu. Se você não vir um switch que você esperava ver nessa lista, o monitor de integridade não poderá descobri-lo automaticamente.

Passos

1. Se você quiser usar o CDP para deteção automática, faça o seguinte:

   a. Certifique-se de que o Protocolo de detecção de Cisco (CDP) está ativado nos seus comutadores.

      Consulte a documentação do switch para obter instruções.

   b. Execute o seguinte comando em cada nó no cluster para verificar se o CDP está ativado ou desativado:

      `run -node *node_name* -command options cdpd.enable`

      Se o CDP estiver ativado, passe à operação d. se o CDP estiver desativado, passe à operação c.

   c. Execute o seguinte comando para ativar o CDP:

      `run -node *node_name* -command options cdpd.enable on`

   Aguarde cinco minutos antes de ir para o próximo passo.

   a. Use o `system cluster-switch show` comando para verificar se o ONTAP agora pode descobrir automaticamente os switches.

2. Se o monitor de integridade não conseguir descobrir automaticamente um switch, use o `system cluster-switch create` comando para configurar a descoberta do switch:

```
cluster1::> system cluster-switch create -device switch1 -address
192.0.2.250 -snmp-version SNMPv2c -community cshm1! -model NX5020 -type
cluster-network
```

Aguarde cinco minutos antes de ir para o próximo passo.

3. Use o `system cluster-switch show` comando para verificar se o ONTAP pode descobrir o switch para o qual você adicionou informações.

Depois de terminar

Verifique se o monitor de integridade pode monitorar seus switches.

Verifique o monitoramento dos switches de rede de gerenciamento e cluster

O monitor de integridade do switch de cluster tenta monitorar automaticamente os switches que ele descobre; no entanto, o monitoramento pode não acontecer automaticamente se os switches não estiverem configurados corretamente. Você deve verificar se o monitor de integridade está configurado corretamente para monitorar seus switches.

Passos

1. Para identificar os switches detetados pelo monitor de integridade do switch de cluster, digite o seguinte comando:

   ONTAP 9 F.8 e mais tarde

   `system switch ethernet show`

   ONTAP 9 F.7 e anteriores

   `system cluster-switch show`

   Se a `Model` coluna exibir o valor `OTHER`, o ONTAP não poderá monitorar o switch. O ONTAP define o valor para `OTHER` se um switch que ele descobre automaticamente não for suportado para monitoramento de integridade.

   Se um switch não for exibido na saída do comando, você deverá configurar a descoberta do switch.

2. Atualize para o software de switch suportado mais recente e consulte o arquivo de configuração (RCF) no site de suporte da NetApp.

   "Página de transferências do suporte da NetApp"

   A cadeia de carateres da comunidade no RCF do switch deve corresponder à cadeia de carateres da comunidade que o monitor de integridade está configurado para usar. Por padrão, o monitor de integridade usa a cadeia de carateres da comunidade `cshm1!` .

   Neste momento, o monitor de integridade só suporta SNMPv2.

   Se você precisar alterar informações sobre um switch que o cluster monitora, você poderá modificar a cadeia de carateres da comunidade usada pelo monitor de integridade usando o seguinte comando:

ONTAP 9 F.8 e mais tarde

```
system switch ethernet modify
```

ONTAP 9 F.7 e anteriores

```
system cluster-switch modify
```

3. Verifique se a porta de gerenciamento do switch está conetada à rede de gerenciamento.

   Esta conexão é necessária para executar consultas SNMP.

Comandos para monitorar a integridade do seu sistema

Você pode usar os `system health` comandos para exibir informações sobre a integridade dos recursos do sistema, responder a alertas e configurar alertas futuros. O uso dos comandos CLI permite exibir informações detalhadas sobre como o monitoramento de integridade é configurado. As páginas man para os comandos contêm mais informações.

Apresentar o estado da integridade do sistema

Se você quiser…	Use este comando…
Apresentar o estado de funcionamento do sistema, que reflete o estado geral dos monitores de saúde individuais	`system health status show`
Apresentar o estado de funcionamento dos subsistemas para os quais a monitorização de integridade está disponível	`system health subsystem show`

Exibir o status da conetividade do nó

Se você quiser…	Use este comando…
Exiba detalhes sobre a conectividade do nó para o compartimento de storage, incluindo informações de porta, velocidade da porta HBA, taxa de transferência de e/S e taxa de operações de e/S por segundo	`storage shelf show -connectivity` Use o `-instance` parâmetro para exibir informações detalhadas sobre cada prateleira.
Exiba informações sobre unidades e LUNs de storage, incluindo o espaço utilizável, os números de compartimento e compartimento e o nome do nó proprietário	`storage disk show` Use o `-instance` parâmetro para exibir informações detalhadas sobre cada unidade.

Se você quiser…	Use este comando…
Exiba informações detalhadas sobre as portas do compartimento de armazenamento, incluindo o tipo, a velocidade e o status da porta	`storage port show` Use o `-instance` parâmetro para exibir informações detalhadas sobre cada adaptador.

Gerenciar a descoberta de switches de rede de cluster, armazenamento e gerenciamento

Se você quiser…	Use este comando. (ONTAP 9.8 e posterior)	Use este comando. (ONTAP 9 .7 e anteriores)
Apresentar os interrutores que o grupo de instrumentos monitoriza	`system switch ethernet show`	`system cluster-switch show`
Exiba os switches que o cluster monitora atualmente, incluindo os switches que você excluiu (mostrados na coluna motivo na saída do comando) e as informações de configuração necessárias para acesso à rede ao cluster e aos switches de rede de gerenciamento. Este comando está disponível no nível de privilégio avançado.	`system switch ethernet show-all`	`system cluster-switch show-all`
Configurar a descoberta de um switch não descoberto	`system switch ethernet create`	`system cluster-switch create`
Modificar informações sobre um switch que o cluster monitora (por exemplo, nome do dispositivo, endereço IP, versão SNMP e cadeia de carateres da comunidade)	`system switch ethernet modify`	`system cluster-switch modify`
Desativar a monitorização de um interrutor	`system switch ethernet modify -disable-monitoring`	`system cluster-switch modify -disable-monitoring`
Desative a descoberta e o monitoramento de um switch e exclua as informações de configuração do switch	`system switch ethernet delete`	`system cluster-switch delete`

Se você quiser…	Use este comando. (ONTAP 9.8 e posterior)	Use este comando. (ONTAP 9 .7 e anteriores)
Remover permanentemente as informações de configuração do switch que são armazenadas no banco de dados (isso rehabilita a descoberta automática do switch)	`system switch ethernet delete -force`	`system cluster-switch delete -force`
Ative o registo automático para enviar com mensagens AutoSupport.	`system switch ethernet log`	`system cluster-switch log`

Responder a alertas gerados

Se você quiser…	Use este comando…
Exiba informações sobre alertas gerados, como o recurso e o nó em que o alerta foi acionado, e a gravidade e a causa provável do alerta	`system health alert show`
Exibir informações sobre cada alerta gerado	`system health alert show -instance`
Indique que alguém está trabalhando em um alerta	`system health alert modify`
Confirme um alerta	`system health alert modify -acknowledge`
Suprimir um alerta subsequente para que não afete o estado de funcionamento de um subsistema	`system health alert modify -suppress`
Exclua um alerta que não foi apagado automaticamente	`system health alert delete`
Exiba informações sobre as mensagens do AutoSupport que alertas dispararam na última semana, por exemplo, para determinar se um alerta acionou uma mensagem do AutoSupport	`system health autosupport trigger history show`

Configurar alertas futuros

Se você quiser…	Use este comando…
Ative ou desative a política que controla se um estado de recurso específico gera um alerta específico	`system health policy definition modify`

Exiba informações sobre como o monitoramento de integridade é configurado

Se você quiser…	Use este comando…
Exibir informações sobre monitores de integridade, como seus nós, nomes, subsistemas e status	`system health config show` Use o `-instance` parâmetro para exibir informações detalhadas sobre cada monitor de integridade.
Exiba informações sobre os alertas que um monitor de integridade pode gerar	`system health alert definition show` Use o `-instance` parâmetro para exibir informações detalhadas sobre cada definição de alerta.
Exiba informações sobre as políticas do monitor de integridade, que determinam quando os alertas são gerados	`system health policy definition show` Use o `-instance` parâmetro para exibir informações detalhadas sobre cada política. Use outros parâmetros para filtrar a lista de alertas - por exemplo, por status da política (habilitado ou não), monitor de integridade, alerta e assim por diante.

Apresentar informações ambientais

Os sensores ajudam a monitorar os componentes ambientais do seu sistema. As informações que você pode exibir sobre os sensores ambientais incluem seus avisos de tipo, nome, estado, valor e limite.

Passo

1. Para exibir informações sobre sensores ambientais, use o `system node environment sensors show` comando.

Informações sobre direitos autorais

Informações sobre marcas comerciais