



# Monitoramento de eventos, desempenho e integridade

ONTAP 9

NetApp  
January 17, 2025

# Índice

- Monitoramento de eventos, desempenho e integridade ..... 1
  - Monitore o desempenho do cluster com o System Manager ..... 1
  - Monitore e gerencie a performance do cluster usando a CLI ..... 13
  - Monitore o desempenho do cluster com o Unified Manager ..... 52
  - Monitore o desempenho do cluster com o Cloud Insights ..... 52
  - Log de auditoria ..... 53
  - AutoSupport ..... 59
  - Monitoramento de integridade ..... 91
  - Análise do sistema de arquivos ..... 105
  - Configuração EMS ..... 120

# Monitoramento de eventos, desempenho e integridade

## Monitore o desempenho do cluster com o System Manager

### Monitore o desempenho do cluster usando o System Manager

Os tópicos nesta seção mostram como gerenciar a integridade e o desempenho do cluster com o System Manager no ONTAP 9.7 e versões posteriores.

#### Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "[estes passos](#)" para monitorar o desempenho do cluster. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

Você pode monitorar o desempenho do cluster exibindo informações sobre o sistema no Painel do System Manager. O Dashboard exibe informações sobre alertas e notificações importantes, a eficiência e a capacidade das camadas e volumes de storage, os nós disponíveis em um cluster, o status dos nós em um par de HA, as aplicações e objetos mais ativos e as métricas de performance de um cluster ou nó.

O Dashboard permite determinar as seguintes informações:

- **Saúde:** Quão saudável é o cluster?
- **Capacidade:** Que capacidade está disponível no cluster?
- **Desempenho:** O desempenho do cluster com base na latência, IOPS e taxa de transferência?
- **Rede:** Como a rede é configurada com hosts e objetos de armazenamento, como portas, interfaces e VMs de armazenamento?

Nas visões gerais de integridade e capacidade, você pode clicar [→](#) para exibir informações adicionais e executar tarefas.

Na Visão geral de desempenho, você pode visualizar as métricas com base na hora, no dia, na semana, no mês ou no ano.

Na visão geral da rede, o número de cada objeto na rede é exibido (por exemplo, "8 portas NVMe/FC"). Você pode clicar nos números para exibir detalhes sobre cada objeto de rede.

### Veja a visão geral do cluster no painel do System Manager

O dashboard do System Manager oferece uma visualização rápida e abrangente do cluster do ONTAP em um único local.

Com o dashboard do System Manager, você pode visualizar informações gerais sobre alertas e notificações importantes, a eficiência e a capacidade das camadas e volumes de storage, os nós disponíveis em um cluster, o status dos nós em um par de alta disponibilidade (HA), as aplicações e objetos mais ativos e as métricas de performance de um cluster ou nó.

O painel de instrumentos inclui quatro painéis descritos da seguinte forma:

## Saúde

O modo de exibição integridade exibe informações sobre a integridade geral de todos os nós detetáveis no cluster.

A visualização Saúde também exibe os erros e avisos no nível do cluster, como detalhes do nó não configurados, indicando as características que podem ser modificadas para melhorar o desempenho do cluster.

Clique → para expandir a visualização Saúde para obter uma visão geral do cluster, como o nome do cluster, a versão, a data e hora de criação do cluster e muito mais. Você também pode monitorar as estatísticas relacionadas à integridade dos nós associados a um cluster. Você pode gerenciar tags que permitem agrupar e identificar recursos em seu ambiente. A seção Insights ajuda a otimizar a capacidade, a conformidade de segurança e a configuração do seu sistema.

## Capacidade

A exibição capacidade exibe o espaço de armazenamento de um cluster. Você pode visualizar o espaço lógico total usado, o espaço físico total usado e o espaço em disco disponível.

Você pode optar por se Registrar no ActiveIQ para visualizar os dados históricos do cluster. Clique → para expandir a visualização capacidade para ver uma visão geral dos níveis associados a um cluster. É possível exibir informações de capacidade sobre cada uma das camadas: O espaço total, o espaço usado e o espaço disponível. Os detalhes são exibidos para taxa de transferência, IOPS e latência. ["Saiba mais sobre essas medições de capacidade no System Manager"](#).

Você pode optar por adicionar uma categoria local ou uma categoria de nuvem usando a visualização de capacidade. Para obter mais informações sobre a exibição capacidade, ["Exibir a capacidade de um cluster"](#) consulte .

## Rede

O modo de exibição rede exibe as portas físicas, as interfaces de rede e as VMs de armazenamento que fazem parte da rede.

O modo de exibição rede exibe o tipo de clientes conectados à rede. Cada um desses clientes conectados à rede é representado por um número (por exemplo, "NVMe/FC 16"). Selecione o número para visualizar detalhes específicos em cada um desses elementos de rede.

Clique → para ver uma visualização expansiva de página inteira da rede que engloba portas, interfaces de rede, VMs de armazenamento e hosts na rede.

## Desempenho


A visualização desempenho exibe estatísticas de desempenho para ajudar a monitorar a integridade e a eficiência do cluster do ONTAP. As estatísticas incluem os principais indicadores de desempenho do cluster, como latência, taxa de transferência e IOPS, representados como gráficos.

A visualização desempenho apresenta estatísticas de desempenho em diferentes intervalos de tempo por dia, hora, semana ou ano. Você pode analisar rapidamente o desempenho do cluster usando os vários gráficos e identificar as características que podem exigir otimização. Essa análise rápida ajuda você a decidir como adicionar ou mover cargas de trabalho. Você também pode olhar para os horários de pico de uso para Planejar possíveis mudanças.

A visualização de performance exibe as métricas totais de performance relacionadas à latência, taxa de transferência e IOPS.

A partir de 9.15.1, a visualização de desempenho é aprimorada para exibir gráficos para métricas de desempenho de leitura, gravação, outras e totais relacionadas à latência, taxa de transferência e IOPS. Outras métricas incluem quaisquer operações que não sejam lidas ou gravadas.

Os valores de performance são atualizados a cada 3 segundos e o gráfico de performance é atualizado a cada 15 segundos. Um gráfico não será exibido se as informações sobre o desempenho do cluster não estiverem disponíveis.

Clique  para ver uma visualização de página inteira das métricas de desempenho por hora, dia, semana, mês e ano. Você também pode baixar um relatório das métricas de desempenho em seu sistema local.

## Identificar volumes ativos e outros objetos

Acelere a performance do cluster identificando os volumes (hot volumes) e dados acessados com frequência (hot objetos).



A partir do ONTAP 9.10,1, você pode usar o recurso Rastreamento de atividades no sistema de arquivos Analytics para monitorar objetos ativos em um volume.

### Passos

1. Clique em **armazenamento > volumes**.
2. Filtre as colunas IOPS, latência e taxa de transferência para visualizar os volumes e dados acessados com frequência.

## Modificar QoS

A partir do ONTAP 9.8, quando você provisiona o storage, **Qualidade do serviço (QoS)** é habilitado por padrão. Você pode desativar o QoS ou escolher uma política de QoS personalizada durante o processo de provisionamento. Também é possível modificar a QoS depois que o storage tiver sido provisionado.

### Passos

1. No System Manager, selecione **Storage** e depois **volumes**.
2. Ao lado do volume para o qual você deseja modificar QoS, selecione **⋮ Editar**.

## Monitorar riscos

A partir do ONTAP 9.10,0, você pode usar o Gerenciador do sistema para monitorar os riscos relatados pelo consultor digital da Active IQ (também conhecido como consultor digital). A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para reconhecer os riscos.

O consultor digital da NetApp relata oportunidades para reduzir riscos e melhorar a performance e a eficiência do seu ambiente de storage. Com o System Manager, você pode aprender sobre os riscos relatados pelo Digital Advisor e receber inteligência acionável que ajuda a administrar o storage e a obter maior disponibilidade, maior segurança e melhor desempenho de storage.

## Link para sua conta do Digital Advisor

Para receber informações sobre riscos do Digital Advisor, primeiro você deve vincular a sua conta do Digital Advisor do System Manager.

### Passos

1. No System Manager, clique em **Cluster > Settings**.
2. Em **Registo Active IQ**, clique em **Registo**.
3. Introduza as suas credenciais para o Digital Advisor.
4. Depois que suas credenciais forem autenticadas, clique em **Confirm (confirmar) para vincular o Active IQ ao Gerenciador do sistema**.

## Veja o número de riscos

A partir do ONTAP 9.10,0, você pode visualizar no painel do Gerenciador de sistemas o número de riscos relatados pelo Consultor Digital.

### Antes de começar

Você deve estabelecer uma conexão do System Manager com sua conta do Digital Advisor. [Link para sua conta do Digital Advisor](#)Consulte a .

### Passos

1. No System Manager, clique em **Dashboard**.
2. Na seção **Saúde**, veja o número de riscos relatados.



Você pode ver informações mais detalhadas sobre cada risco clicando na mensagem mostrando o número de riscos. [Ver detalhes dos riscos](#)Consulte .

## Ver detalhes dos riscos

A partir do ONTAP 9.10,0, você pode ver no Gerenciador de sistemas como os riscos relatados pelo Consultor Digital são categorizados por áreas de impactos. Você também pode exibir informações detalhadas sobre cada risco relatado, seu potencial impactos no seu sistema e ações corretivas que você pode tomar.

### Antes de começar

Você deve estabelecer uma conexão do System Manager com sua conta do Digital Advisor. [Link para sua conta do Digital Advisor](#)Consulte a .

### Passos

1. Clique em **Eventos > todos os eventos**.
2. Na seção **Visão geral**, em **sugestões de Active IQ**, veja o número de riscos em cada categoria de área de impactos. As categorias de risco incluem:
  - Desempenho e eficiência
  - Disponibilidade e proteção
  - Capacidade
  - Configuração
  - Segurança

3. Clique na guia **sugestões de Active IQ** para visualizar informações sobre cada risco, incluindo o seguinte:
  - Nível de impactos no seu sistema
  - Categoria do risco
  - Nós afetados
  - Tipo de mitigação necessária
  - Ações corretivas que você pode tomar

### Reconheça os riscos

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para reconhecer qualquer um dos riscos abertos.

#### Passos

1. No System Manager, exiba a lista de riscos executando o procedimento [Ver detalhes dos riscos](#) em .
2. Clique no nome de risco de um risco aberto que você deseja reconhecer.
3. Insira as informações nos seguintes campos:
  - Lembrete (data)
  - Justificação
  - Comentários
4. Clique em **confirmar**.



Depois de reconhecer um risco, leva alguns minutos para que a alteração seja refletida na lista de sugestões do Digital Advisor.

### Não reconhecer riscos

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para desreconhecer qualquer risco que tenha sido reconhecido anteriormente.

#### Passos

1. No System Manager, exiba a lista de riscos executando o procedimento [Ver detalhes dos riscos](#) em .
2. Clique no nome de risco de um risco reconhecido que você deseja desreconhecer.
3. Insira as informações nos seguintes campos:
  - Justificação
  - Comentários
4. Clique em **Cancelar reconhecimento**.



Depois de desreconhecer um risco, leva alguns minutos para que a alteração seja refletida na lista de sugestões do Digital Advisor.

### Insights do System Manager

A partir do ONTAP 9.11,1, o Gerenciador de sistema exibe *insights* que ajudam a otimizar o desempenho e a segurança do seu sistema.



Para visualizar, personalizar e responder a insights, consulte "[Obtenha insights para ajudar a otimizar seu sistema](#)"

## Insights de capacidade

O System Manager pode exibir os seguintes insights em resposta às condições de capacidade do seu sistema:

Insight	Gravidade	Condição	Correções
As camadas locais não têm espaço	Remediar riscos	Um ou mais níveis locais estão mais de 95% cheios e crescendo rapidamente. Os workloads existentes podem não ser capazes de crescer ou, em casos extremos, os workloads existentes podem ficar sem espaço e falhar.	<b>Correção recomendada:</b> Execute uma das seguintes opções. <ul style="list-style-type: none"><li>• Limpe a fila de recuperação de volume.</li><li>• Habilite o provisionamento de thin Provisioning em volumes provisionados espessos para liberar o storage preso.</li><li>• Mova volumes para outro nível local.</li><li>• Excluir cópias snapshot desnecessárias.</li><li>• Exclua diretórios desnecessários ou arquivos nos volumes.</li><li>• Habilite o Fabric Pool para categorizar os dados na nuvem.</li></ul>
As aplicações não têm espaço	Precisa de atenção	Um ou mais volumes estão mais de 95% cheios, mas não têm o crescimento automático ativado.	<b>Recomendado:</b> Ative o crescimento até 150% da capacidade atual. <b>Outras opções:</b> <ul style="list-style-type: none"><li>• Recupere espaço com a exclusão de cópias Snapshot.</li><li>• Redimensione os volumes.</li><li>• Excluir diretórios ou arquivos.</li></ul>
A capacidade do volume FlexGroup é desequilibrada	Otimizar o armazenamento	O tamanho dos volumes constituintes de um ou mais volumes do FlexGroup cresceu de forma desigual ao longo do tempo, levando a um desequilíbrio no uso da capacidade. Se os volumes constituintes ficarem cheios, podem ocorrer falhas de gravação.	<b>Recomendado:</b> Rebalanceamento dos volumes FlexGroup.



As VMs de storage estão ficando sem capacidade	Otimizar o armazenamento	Uma ou mais VMs de storage estão perto da capacidade máxima. Você não poderá provisionar mais espaço para volumes novos ou existentes se as VMs de storage alcançarem a capacidade máxima.	<b>Recomendado:</b> Se possível, aumente o limite máximo de capacidade da VM de armazenamento.
--	--------------------------	--	--

## Insights de segurança

O System Manager pode exibir os seguintes insights em resposta a condições que podem comprometer a segurança de seus dados ou do sistema.

Insight	Gravidade	Condição	Correções
Os volumes ainda estão no modo de aprendizado Autonomous ransomware Protection	Precisa de atenção	Um ou mais volumes estão no modo de aprendizado anti-ransomware por 90 dias.	<b>Recomendado:</b> Ative o modo ativo Autonomous ransomware Protection para esses volumes.
A exclusão automática de cópias Snapshot está habilitada nos volumes	Precisa de atenção	A eliminação automática de instantâneos está ativada num ou mais volumes.	<b>Recomendado:</b> Desative a exclusão automática de cópias Snapshot. Caso contrário, em caso de ataque de ransomware, a recuperação de dados para esses volumes pode não ser possível.
Os volumes não têm políticas Snapshot	Precisa de atenção	Um ou mais volumes não têm uma política de snapshot adequada anexada a eles.	<b>Recomendado:</b> Anexe uma política Snapshot a volumes que não tenham um. Caso contrário, em caso de ataque de ransomware, a recuperação de dados para esses volumes pode não ser possível.
FPolicy nativo não está configurado	Prática recomendada	O FPolicy nativo não está configurado em uma ou mais VMs de armazenamento nas.	<b>Recomendado: IMPORTANTE:</b> Bloquear extensões pode levar a resultados inesperados. A partir de 9.11.1, é possível habilitar o FPolicy nativo para VMs de armazenamento, o que bloqueia mais de 3000 extensões de arquivo conhecidas por serem usadas para ataques de ransomware. " <a href="#">Configurar FPolicy nativo</a> " Nas VMs de armazenamento nas para controlar as extensões de arquivo permitidas ou não permitidas para serem gravadas em volumes em seu ambiente.

O Telnet está ativado	Prática recomendada	O Secure Shell (SSH) deve ser usado para acesso remoto seguro.	<b>Recomendado:</b> Desative o Telnet e use SSH para acesso remoto seguro.
Poucos servidores NTP estão configurados	Prática recomendada	O número de servidores configurados para NTP é inferior a 3.	<b>Recomendado:</b> Associe pelo menos três servidores NTP ao cluster. Caso contrário, podem ocorrer problemas com a sincronização da hora do cluster.
O Remote Shell (RSH) está ativado	Prática recomendada	O Secure Shell (SSH) deve ser usado para acesso remoto seguro.	<b>Recomendado:</b> Desative o RSH e use SSH para acesso remoto seguro.
O banner de login não está configurado	Prática recomendada	As mensagens de login não são configuradas para o cluster, para a VM de armazenamento ou para ambos.	<b>Recomendado:</b> Configure os banners de login para o cluster e a VM de armazenamento e habilite seu uso.
O AutoSupport está usando um protocolo não seguro	Prática recomendada	O AutoSupport não está configurado para se comunicar via HTTPS.	<b>Recomendado:</b> É altamente recomendável usar HTTPS como protocolo de transporte padrão para enviar mensagens AutoSupport para suporte técnico.
O utilizador de administrador predefinido não está bloqueado	Prática recomendada	Ninguém fez login usando uma conta administrativa padrão (admin ou diag), e essas contas não estão bloqueadas.	<b>Recomendado:</b> Bloqueie contas administrativas padrão quando elas não estiverem sendo usadas.
O Secure Shell (SSH) está usando cifras não seguras	Prática recomendada	A configuração atual usa cifras CBC não seguras.	<b>Recomendado:</b> Você deve permitir apenas cifras seguras em seu servidor web para proteger a comunicação segura com seus visitantes. Remover cifras que tenham nomes contendo "cbc", como "ais128-cbc", "aes192-cbc", "AES256-cbc" e "3DES-cbc".
A conformidade com o FIPS 140-2 global está desativada	Prática recomendada	A conformidade com o FIPS 140-2 global é desativada no cluster.	<b>Recomendado:</b> Por motivos de segurança, você deve habilitar a criptografia compatível com FIPS global 140-2 para garantir que o ONTAP possa se comunicar com segurança com clientes externos ou clientes de servidor.

Os volumes não estão sendo monitorados para ataques de ransomware	Precisa de atenção	A proteção autônoma contra ransomware é desativada em um ou mais volumes.	<b>Recomendado:</b> Ative a proteção Autonomous ransomware nos volumes. Caso contrário, você pode não notar quando os volumes estão sendo ameaçados ou sob ataque.
As VMs de armazenamento não estão configuradas para o Autonomous ransomware Protection	Prática recomendada	Uma ou mais VMs de storage não estão configuradas para o Autonomous ransomware Protection.	<b>Recomendado:</b> Ative a proteção Autonomous ransomware nas VMs de armazenamento. Caso contrário, você pode não notar quando as VMs de armazenamento estão sendo ameaçadas ou sob ataque.

### Insights de configuração

O System Manager pode exibir os seguintes insights em resposta a preocupações sobre a configuração do seu sistema.

Insight	Gravidade	Condição	Correções
O cluster não está configurado para notificações	Prática recomendada	E-mail, webhooks ou um trapshot SNMP não está configurado para permitir que você receba notificações sobre problemas com o cluster.	<b>Recomendado:</b> Configure notificações para o cluster.
O cluster não está configurado para atualizações automáticas.	Prática recomendada	O cluster não foi configurado para receber atualizações automáticas para o pacote de qualificação de disco mais recente, firmware de disco, firmware de gaveta, firmware de SP/BMC ou arquivos de segurança quando estiverem disponíveis.	<b>Recomendado:</b> Ative este recurso.

O firmware do cluster não está atualizado	Prática recomendada	O seu sistema não tem a atualização mais recente do firmware, que pode ter melhorias, patches de segurança ou novos recursos que ajudam a proteger o cluster para um melhor desempenho.	<b>Recomendado:</b> Atualize o firmware do ONTAP.
---	---------------------	---	---

## Obtenha insights para ajudar a otimizar seu sistema

Com o System Manager, você pode visualizar insights que ajudam a otimizar seu sistema.

### Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga ["estes passos"](#) para ver os insights que o ajudam a otimizar seu sistema. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

A partir do ONTAP 9.11,0, você pode visualizar insights no Gerenciador de sistemas que ajudam a otimizar a conformidade de capacidade e segurança do seu sistema.

A partir do ONTAP 9.11,1, você pode visualizar insights adicionais que ajudam a otimizar a capacidade, a conformidade de segurança e a configuração do seu sistema.

**Bloquear extensões pode levar a resultados inesperados.** A partir do ONTAP 9.11,1, você pode habilitar o FPolicy nativo para VMs de armazenamento usando o Gerenciador do sistema. Você pode receber uma mensagem do System Manager Insight recomendando que ["Configurar FPolicy nativo"](#) você seja uma VM de storage.



Com o FPolicy Native Mode, você pode permitir ou desativar extensões de arquivo específicas. O System Manager recomenda mais de 3000 extensões de arquivos não permitidas que foram usadas em ataques de ransomware anteriores. Algumas dessas extensões podem ser usadas por arquivos legítimos em seu ambiente e bloqueá-las pode levar a problemas inesperados.

Portanto, é altamente recomendável que você modifique a lista de extensões para atender às necessidades do seu ambiente. Consulte a ["Como remover uma extensão de arquivo de uma configuração FPolicy nativa criada pelo System Manager usando o System Manager para recriar a diretiva"](#).

Para saber mais sobre FPolicy nativo, ["Tipos de configuração Fpolicy"](#) consulte .

Com base nas práticas recomendadas, esses insights são exibidos em uma página a partir da qual você pode iniciar ações imediatas para otimizar seu sistema. Para obter mais detalhes sobre cada insight, ["Insights do System Manager"](#) consulte .

## Ver insights de otimização





### Passos

1. No System Manager, clique em **Insights** na coluna de navegação à esquerda.

A página **Insights** mostra grupos de insights. Cada grupo de insights pode conter um ou mais insights. São apresentados os seguintes grupos:

- Precisa de sua atenção
- Remediar riscos
- Otimizar seu storage

2. (Opcional) filtre os insights exibidos clicando nesses botões no canto superior direito da página:

-  Exibe os insights relacionados à segurança.
-  Exibe os insights relacionados à capacidade.
-  Exibe os insights relacionados à configuração.
-  Exibe todos os insights.

## Responda a insights para otimizar seu sistema

No System Manager, você pode responder a insights descartando-os, explorando diferentes maneiras de corrigir os problemas ou iniciando o processo para corrigir os problemas.

### Passos

1. No System Manager, clique em **Insights** na coluna de navegação à esquerda.
2. Passe o Mouse sobre um insight para revelar os botões para executar as seguintes ações:
  - **Dismiss:** Remova o insight da visualização. Para "não descartar" a percepção, [[customize-settings-insights](#)]consulte .
  - **Explore:** Descubra várias maneiras de remediar o problema mencionado no insight. Este botão aparece apenas se houver mais de um método de correção.
  - **Fix:** Inicie o processo de correção do problema mencionado no insight. Você será solicitado a confirmar se deseja executar a ação necessária para aplicar a correção.




Algumas dessas ações podem ser iniciadas de outras páginas no System Manager, mas a página **Insights** ajuda você a simplificar suas tarefas diárias, permitindo que você inicie essa ação a partir desta página.

## Personalize as configurações para insights

Você pode personalizar quais insights serão notificados no System Manager.

### Passos


1. No System Manager, clique em **Insights** na coluna de navegação à esquerda.
2. No canto superior direito da página, clique  em e selecione **Configurações**.

3. Na página **Configurações**, verifique se há uma seleção nas caixas de seleção ao lado dos insights sobre os quais você deseja ser notificado. Se você descartou anteriormente um insight, você pode "cancelar o insight", garantindo que uma verificação esteja em sua caixa de seleção.
4. Clique em **Salvar**.

## Exporte os insights como um arquivo PDF

Você pode exportar todos os insights aplicáveis como um arquivo PDF.

### Passos

1. No System Manager, clique em **Insights** na coluna de navegação à esquerda.
2. No canto superior direito da página, clique  em e selecione **Exportar**.

## Configurar FPolicy nativo

A partir do ONTAP 9.11,1, quando você recebe um Insight do System Manager que sugere a implementação de FPolicy nativo, você pode configurá-lo em suas VMs e volumes de storage.

### Antes de começar

Quando você acessa o System Manager Insights, em **aplicar práticas recomendadas**, você pode receber uma mensagem dizendo que o FPolicy nativo não está configurado.

Para saber mais sobre os tipos de configuração FPolicy, "[Tipos de configuração FPolicy](#)" consulte .

### Passos

1. No System Manager, clique em **Insights** na coluna de navegação à esquerda.
2. Em **aplicar as melhores práticas**, localize **Native FPolicy não está configurado**.
3. Leia a seguinte mensagem antes de tomar medidas:



**Bloquear extensões pode levar a resultados inesperados.** A partir do ONTAP 9.11,1, você pode habilitar o FPolicy nativo para VMs de armazenamento usando o Gerenciador do sistema. Com o FPolicy Native Mode, você pode permitir ou desativar extensões de arquivo específicas. O System Manager recomenda mais de 3000 extensões de arquivos não permitidas que foram usadas em ataques de ransomware anteriores. Algumas dessas extensões podem ser usadas por arquivos legítimos em seu ambiente e bloqueá-las pode levar a problemas inesperados.

Portanto, é altamente recomendável que você modifique a lista de extensões para atender às necessidades do seu ambiente. Consulte a "[Como remover uma extensão de arquivo de uma configuração FPolicy nativa criada pelo System Manager usando o System Manager para recriar a diretiva](#)".

4. Clique em **Fix**.
5. Selecione as VMs de armazenamento às quais você deseja aplicar o FPolicy nativo.
6. Para cada VM de armazenamento, selecione os volumes que receberão o FPolicy nativo.
7. Clique em **Configurar**.

# Monitore e gerencie a performance do cluster usando a CLI

## Visão geral do gerenciamento e monitoramento de desempenho

Você pode configurar tarefas básicas de monitoramento e gerenciamento de desempenho e identificar e resolver problemas comuns de desempenho.

Você pode usar esses procedimentos para monitorar e gerenciar o desempenho do cluster se as seguintes suposições se aplicarem à sua situação:

- Você quer usar as práticas recomendadas, não explorar todas as opções disponíveis.
- Você deseja exibir o status e os alertas do sistema, monitorar o desempenho do cluster e realizar análises de causa-raiz usando o Active IQ Unified Manager (antigo Gerenciador Unificado de OnCommand), além da interface de linha de comando do ONTAP.
- Você está usando a interface de linha de comando ONTAP para configurar a qualidade do serviço (QoS) de storage. QoS também está disponível através do seguinte:
  - System Manager
  - API REST do ONTAP
  - Ferramentas do ONTAP para VMware vSphere
  - Gerenciador de nível de Serviço (NetApp)
  - OnCommand Workflow Automation (WFA)
- Você deseja instalar o Unified Manager usando um dispositivo virtual, em vez de uma instalação baseada no Linux ou no Windows.
- Você está disposto a usar uma configuração estática em vez de DHCP para instalar o software.
- Pode acessar aos comandos ONTAP no nível avançado de privilégios.
- Você é um administrador de cluster com a função "admin".

### Informações relacionadas

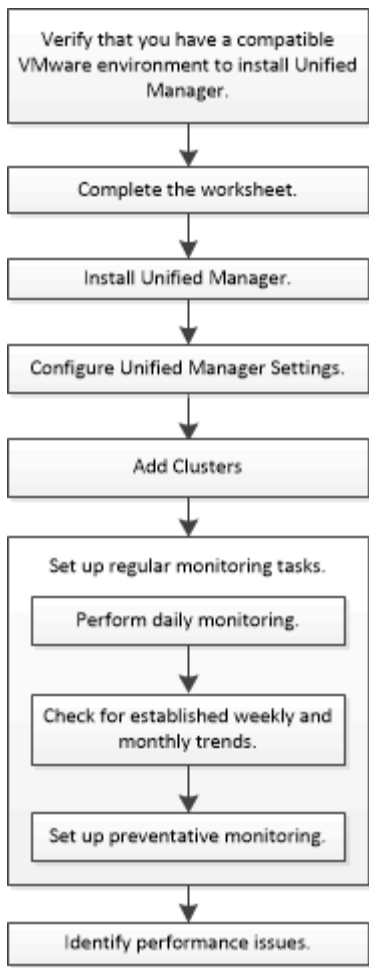
Se essas suposições não estiverem corretas para sua situação, você deverá ver os seguintes recursos:

- ["Instalação do Active IQ Unified Manager 9,8"](#)
- ["Administração do sistema"](#)

## Monitorar o desempenho

### Visão geral do fluxo de trabalho de manutenção e monitoramento de desempenho

O monitoramento e a manutenção do desempenho do cluster envolvem a instalação do software Active IQ Unified Manager, a configuração de tarefas básicas de monitoramento, a identificação de problemas de desempenho e a realização de ajustes conforme necessário.



### Verifique se seu ambiente VMware é compatível

Para instalar o Active IQ Unified Manager com êxito, você deve verificar se o ambiente VMware atende aos requisitos necessários.

#### Passos

1. Verifique se sua infraestrutura VMware atende aos requisitos de dimensionamento para a instalação do Unified Manager.
2. Vá para a "[Matriz de interoperabilidade](#)" para verificar se você tem uma combinação suportada dos seguintes componentes:
  - Versão de ONTAP
  - Versão do sistema operacional ESXi
  - Versão do VMware vCenter Server
  - Versão do VMware Tools
  - Tipo e versão do navegador



A Matriz de interoperabilidade lista as configurações suportadas do Unified Manager.

3. Clique no nome da configuração selecionada.

Os detalhes dessa configuração são exibidos na janela Detalhes da configuração.



#### 4. Revise as informações nas guias a seguir:

- Notas

Lista alertas importantes e informações específicas à sua configuração.

- Políticas e Diretrizes

Fornece diretrizes gerais para todas as configurações.

### Folha de cálculo do Active IQ Unified Manager

Antes de instalar, configurar e conectar o Active IQ Unified Manager, você deve ter informações específicas sobre seu ambiente prontamente disponíveis. Pode registrar as informações na folha de trabalho.

#### Informações de instalação do Unified Manager

Máquina virtual na qual o software é implantado	O seu valor
Endereço IP do servidor ESXi	
Host nome de domínio totalmente qualificado	
Endereço IP do host	
Máscara de rede	
Endereço IP do gateway	
Endereço DNS primário	
Endereço DNS secundário	
Pesquisar domínios	
Nome de utilizador de manutenção	
Palavra-passe do utilizador de manutenção	


#### Informações de configuração do Unified Manager

Definição	O seu valor
Endereço de e-mail do usuário de manutenção	
Servidor NTP	

Nome do host do servidor SMTP ou endereço IP	
Nome de utilizador SMTP	
Palavra-passe SMTP	
Porta padrão SMTP	25 (valor padrão)
E-mail a partir do qual as notificações de alerta são enviadas	
Nome distinto de ligação LDAP	
Palavra-passe LDAP BIND	
Nome de administrador do ativo Directory	
Palavra-passe do ativo Directory	
Nome distinto da base do servidor de autenticação	
Nome do host ou endereço IP do servidor de autenticação	

### Informações do cluster

Capture as informações a seguir para cada cluster no Unified Manager.

Cluster 1 de N	O seu valor
Nome do host ou endereço IP de gerenciamento de cluster	
Nome de usuário do administrador do ONTAP   O administrador deve ter sido atribuído a função "admin".	
Senha do administrador do ONTAP	
Protocolo (HTTP ou HTTPS)	

### Informações relacionadas

["Autenticação de administrador e RBAC"](#)

## Instale o Active IQ Unified Manager

### Baixe e implante o Active IQ Unified Manager

Para instalar o software, você deve baixar o arquivo de instalação do dispositivo virtual (VA) e usar um cliente VMware vSphere para implantar o arquivo em um servidor VMware ESXi. O VA está disponível num ficheiro OVA.

#### Passos

1. Vá para a página **Download de software do site de suporte da NetApp** e localize o Active IQ Unified Manager.

<https://mysupport.netapp.com/products/index.html>

2. Selecione **VMware vSphere** no menu suspenso **Select Platform** e clique em **Go!**
3. Salve o arquivo "OVA" em um local local ou de rede acessível ao cliente VMware vSphere.
4. No VMware vSphere Client, clique em **File > Deploy OVF Template**.
5. Localize o arquivo "OVA" e use o assistente para implantar o dispositivo virtual no servidor ESXi.

Você pode usar a guia **Propriedades** no assistente para inserir suas informações de configuração estática.

6. Ligue a VM.
7. Clique na guia **Console** para exibir o processo de inicialização inicial.
8. Siga o prompt para instalar o VMware Tools na VM.
9. Configure o fuso horário.
10. Introduza um nome de utilizador e uma palavra-passe de manutenção.
11. Vá para o URL exibido pelo console da VM.

### Configure as definições iniciais do Active IQ Unified Manager

A caixa de diálogo Configuração inicial do Active IQ Unified Manager é exibida quando você acessa pela primeira vez a IU da Web, o que permite configurar algumas configurações iniciais e adicionar clusters.

#### Passos

1. Aceite a configuração padrão AutoSupport Enabled.
2. Insira os detalhes do servidor NTP, o endereço de e-mail do usuário de manutenção, o nome do host do servidor SMTP e opções SMTP adicionais e clique em **Salvar**.

#### Depois de terminar

Quando a configuração inicial estiver concluída, a página fontes de dados do cluster é exibida onde você pode adicionar os detalhes do cluster.

### Especifique os clusters a serem monitorados

Você deve adicionar um cluster a um servidor Active IQ Unified Manager para monitorar o cluster, exibir o status de descoberta do cluster e monitorar seu desempenho.

## O que você vai precisar

- Você deve ter as seguintes informações:
  - Nome do host ou endereço IP de gerenciamento de cluster

O nome do host é o nome de domínio totalmente qualificado (FQDN) ou o nome abreviado que o Unified Manager usa para se conectar ao cluster. Esse nome de host deve ser resolvido para o endereço IP de gerenciamento de cluster.

O endereço IP de gerenciamento de cluster deve ser o LIF de gerenciamento de cluster da máquina virtual de storage administrativo (SVM). Se você usar um LIF de gerenciamento de nós, a operação falhará.

- Nome de usuário e senha do administrador do ONTAP
  - Tipo de protocolo (HTTP ou HTTPS) que pode ser configurado no cluster e o número da porta do cluster
- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
  - O administrador do ONTAP deve ter as funções de administrador ONTAPI e SSH.
  - O FQDN do Gerenciador Unificado deve ser capaz de fazer ping no ONTAP.

Você pode verificar isso usando o comando ONTAP `ping -node node_name -destination Unified_Manager_FQDN`.

## Sobre esta tarefa

Para uma configuração do MetroCluster, você deve adicionar clusters locais e remotos, e os clusters devem estar configurados corretamente.

## Passos

1. Clique em **Configuration > Cluster Data Sources**.
2. Na página clusters, clique em **Add**.
3. Na caixa de diálogo **Adicionar cluster**, especifique os valores necessários, como o nome do host ou o endereço IP (IPv4 ou IPv6) do cluster, nome de usuário, senha, protocolo de comunicação e número da porta.

Por predefinição, o protocolo HTTPS é selecionado.

Você pode alterar o endereço IP de gerenciamento de cluster de IPv6 para IPv4 ou de IPv4 para IPv6. O novo endereço IP é refletido na grade do cluster e na página de configuração do cluster após o próximo ciclo de monitoramento terminar.

4. Clique em **Add**.
5. Se o HTTPS estiver selecionado, execute as seguintes etapas:
  - a. Na caixa de diálogo **autorizar Host**, clique em **Exibir certificado** para exibir as informações do certificado sobre o cluster.
  - b. Clique em **Sim**.

O Unified Manager verifica o certificado somente quando o cluster é adicionado inicialmente, mas não o verifica para cada chamada de API para o ONTAP.

Se o certificado expirou, não é possível adicionar o cluster. Você deve renovar o certificado SSL e, em

seguida, adicionar o cluster.

6. **Opcional:** Veja o status de descoberta do cluster:

- a. Revise o status de detecção de cluster na página **Configuração de cluster**.

O cluster é adicionado ao banco de dados do Unified Manager após o intervalo de monitoramento padrão de aproximadamente 15 minutos.

## Configure tarefas básicas de monitoramento

### Realize a monitorização diária

Você pode executar o monitoramento diário para garantir que não tenha problemas imediatos de desempenho que exijam atenção.

#### Passos

1. Na IU do Active IQ Unified Manager, vá para a página **Inventário de Eventos** para ver todos os eventos atuais e obsoletos.
2. Na opção **View**, `Active Performance Events` selecione e determine qual ação é necessária.

### Use tendências de desempenho semanais e mensais para identificar problemas de desempenho

Identificar tendências de desempenho pode ajudá-lo a identificar se o cluster está sendo usado em excesso ou subusado analisando a latência do volume. Você pode usar etapas semelhantes para identificar gargalos de CPU, rede ou outros sistemas.

#### Passos

1. Localize o volume que você suspeita estar sendo subutilizado ou sobreusado.
2. Na guia **Detalhes do volume**, clique em **30 d** para exibir os dados históricos.
3. No menu suspenso "dividir dados por", selecione **latência** e clique em **Enviar**.
4. Desmarque **Aggregate** no gráfico de comparação de componentes de cluster e compare a latência do cluster com o gráfico de latência de volume.
5. Selecione **agregar** e desmarque todos os outros componentes no gráfico de comparação de componentes de cluster e, em seguida, compare a latência agregada com o gráfico de latência de volume.
6. Compare o gráfico de latência de leitura/gravação com o gráfico de latência de volume.
7. Determinar se os workloads de aplicações cliente causaram uma contenção de workload e rebalancear os workloads conforme necessário.
8. Determine se o agregado é usado demais e cause contenção e rebalancear os workloads conforme necessário.

### Use limites de performance para gerar notificações de eventos

Eventos são notificações que o Active IQ Unified Manager gera automaticamente quando ocorre uma condição predefinida ou quando um valor de contador de desempenho cruza um limite. Os eventos ajudam a identificar problemas de desempenho nos clusters que você está monitorando. Você pode configurar alertas para enviar notificações por e-mail automaticamente quando ocorrerem eventos de determinados tipos de gravidade.

## Definir limites de desempenho

Você pode definir limites de desempenho para monitorar problemas críticos de performance. Os limites definidos pelo usuário acionam um aviso ou uma notificação de evento crítico quando o sistema se aproxima ou excede o limite definido.

### Passos

1. Crie os limites de aviso e evento crítico:
  - a. Selecione **Configuração > limites de desempenho**.
  - b. Clique em **criar**.
  - c. Selecione o tipo de objeto e especifique um nome e uma descrição da política.
  - d. Selecione a condição do contador de objetos e especifique os valores limite que definem eventos de aviso e crítico.
  - e. Selecione a duração do tempo em que os valores-limite devem ser violados para que um evento seja enviado e clique em **Salvar**.
2. Atribua a política de limite ao objeto de storage.
  - a. Vá para a página Inventário para o mesmo tipo de objeto de cluster que você selecionou anteriormente e escolha **desempenho** na opção Exibir.
  - b. Selecione o objeto ao qual você deseja atribuir a política de limite e clique em **Assign Threshold Policy**.
  - c. Selecione a política criada anteriormente e clique em **Assign Policy**.

### Exemplo

Você pode definir limites definidos pelo usuário para saber mais sobre problemas críticos de desempenho. Por exemplo, se você tem um Microsoft Exchange Server e sabe que ele falha se a latência do volume exceder 20 milissegundos, você pode definir um limite de aviso em 12 milissegundos e um limite crítico em 15 milissegundos. Com essa configuração de limite, você pode receber notificações quando a latência do volume exceder o limite.



Object Counter Condition\* Warning Critical

Average Latency ms/op 12 ms/op 15 ms/op

### Adicionar alertas

Você pode configurar alertas para notificá-lo quando um evento específico é gerado. Você pode configurar alertas para um único recurso, para um grupo de recursos ou para eventos de um tipo de gravidade específico. Você pode especificar a frequência com que deseja ser notificado e associar um script ao alerta.

### O que você vai precisar

- Você deve ter configurado configurações de notificação, como endereço de e-mail do usuário, servidor SMTP e host de intercetação SNMP, para permitir que o servidor Active IQ Unified Manager use essas configurações para enviar notificações aos usuários quando um evento é gerado.
- Você deve saber os recursos e eventos para os quais deseja acionar o alerta e os nomes de usuário ou endereços de e-mail dos usuários que deseja notificar.
- Se você quiser que um script seja executado com base no evento, você deve ter adicionado o script ao

Unified Manager usando a página Scripts.

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.

### Sobre esta tarefa

Você pode criar um alerta diretamente da página de detalhes do evento depois de receber um evento, além de criar um alerta na página Configuração de Alerta, conforme descrito aqui.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de alerta**.
2. Na página **Configuração de alerta**, clique em **Adicionar**.
3. Na caixa de diálogo **Adicionar alerta**, clique em **Nome** e insira um nome e uma descrição para o alerta.
4. Clique em **recursos** e selecione os recursos a serem incluídos ou excluídos do alerta.

Você pode definir um filtro especificando uma cadeia de texto no campo **Name contains** para selecionar um grupo de recursos. Com base na cadeia de texto especificada, a lista de recursos disponíveis exibe apenas os recursos que correspondem à regra de filtro. A cadeia de texto especificada é sensível a maiúsculas e minúsculas.

Se um recurso estiver em conformidade com as regras incluir e excluir que você especificou, a regra excluir terá precedência sobre a regra incluir e o alerta não será gerado para eventos relacionados ao recurso excluído.

5. Clique em **Eventos** e selecione os eventos com base no nome do evento ou no tipo de gravidade do evento para os quais deseja acionar um alerta.



Para selecionar mais de um evento, pressione a tecla Ctrl enquanto você faz suas seleções.

6. Clique em **ações** e selecione os usuários que você deseja notificar, escolha a frequência de notificação, escolha se uma trap SNMP será enviada ao recetor de trap e atribua um script a ser executado quando um alerta for gerado.



Se você modificar o endereço de e-mail especificado para o usuário e reabrir o alerta para edição, o campo Nome será exibido em branco porque o endereço de e-mail modificado não será mais mapeado para o usuário selecionado anteriormente. Além disso, se você modificou o endereço de e-mail do usuário selecionado na página usuários, o endereço de e-mail modificado não será atualizado para o usuário selecionado.

Você também pode optar por notificar os usuários através de traps SNMP.

7. Clique em **Salvar**.

### Exemplo de adição de um alerta

Este exemplo mostra como criar um alerta que atenda aos seguintes requisitos:

- Nome do alerta: HealthTest
- Recursos: Inclui todos os volumes cujo nome contém "abc" e exclui todos os volumes cujo nome contém "xyz"
- Eventos: Inclui todos os eventos críticos de saúde

- Ações: Inclui "sample@domain.com", um script "Test", e o usuário deve ser notificado a cada 15 minutos

Execute as seguintes etapas na caixa de diálogo Adicionar alerta:

1. Clique em **Nome** e insira HealthTest no campo **Nome** do alerta.
2. Clique em **recursos** e, na guia incluir, selecione **volumes** na lista suspensa.
  - a. Digite abc o campo **Name contains** para exibir os volumes cujo nome contém "abc".
  - b. Selecione \*[All Volumes whose name contains 'abc'] na área recursos disponíveis e mova-o para a área recursos selecionados.
  - c. Clique em **Excluir**, digite xyz o campo **Nome contém** e clique em **Adicionar**.
3. Clique em **Eventos** e selecione **Crítica** no campo gravidade do evento.
4. Selecione **todos os Eventos críticos** na área Eventos correspondentes e mova-os para a área Eventos selecionados.
5. Clique em **ações** e insira sample@domain.com no campo alertar esses usuários.
6. Selecione **lembrar a cada 15 minutos** para notificar o usuário a cada 15 minutos.

Você pode configurar um alerta para enviar repetidamente notificações aos destinatários por um tempo especificado. Você deve determinar a hora a partir da qual a notificação de evento está ativa para o alerta.

7. No menu Selecionar Script para execução, selecione **Test** script.
8. Clique em **Salvar**.

#### Configure as definições de alerta

Você pode especificar quais eventos do Active IQ Unified Manager acionam alertas, os destinatários de e-mail desses alertas e a frequência dos alertas.

#### O que você vai precisar

Tem de ter a função Administrador de aplicações.

#### Sobre esta tarefa

Você pode configurar configurações de alerta exclusivas para os seguintes tipos de eventos de desempenho:

- Eventos críticos desencadeados por violações de limites definidos pelo usuário
- Eventos de aviso acionados por violações de limites definidos pelo usuário, limites definidos pelo sistema ou limites dinâmicos

Por padrão, os alertas de e-mail são enviados aos usuários administrativos do Unified Manager para todos os novos eventos. Você pode enviar alertas por e-mail para outros usuários adicionando os endereços de e-mail desses usuários.



Para desativar o envio de alertas para determinados tipos de eventos, você deve desmarcar todas as caixas de seleção de uma categoria de evento. Esta ação não impede que os eventos apareçam na interface do utilizador.

#### Passos

1. No painel de navegação esquerdo, selecione **Gerenciamento de armazenamento > Configuração de alerta**.



É apresentada a página Configuração de alerta.

2. Clique em **Add** e configure as configurações apropriadas para cada um dos tipos de evento.

Para enviar alertas de e-mail para vários usuários, insira uma vírgula entre cada endereço de e-mail.

3. Clique em **Salvar**.

### Identificar problemas de desempenho no Active IQ Unified Manager

Se ocorrer um evento de desempenho, você poderá localizar a origem do problema no Active IQ Unified Manager e usar outras ferramentas para corrigi-lo. Você pode receber uma notificação por e-mail de um evento ou notar o evento durante o monitoramento diário.

#### Passos

1. Clique no link na notificação por e-mail, que o leva diretamente ao objeto de armazenamento com um evento de desempenho.

Se você...	Então...
Receba uma notificação por e-mail de um evento	Clique no link para ir diretamente para a página de detalhes do evento.
Observe o evento enquanto analisa a página Inventário de Eventos	Selecione o evento para ir diretamente para a página de detalhes do evento.

2. Se o evento tiver cruzado um limite definido pelo sistema, siga as ações sugeridas na IU para solucionar o problema.
3. Se o evento tiver atravessado um limite definido pelo usuário, analise o evento para determinar se você precisa agir.
4. Se o problema persistir, verifique as seguintes definições:
  - Definições de protocolo no sistema de armazenamento
  - Configurações de rede em qualquer Ethernet ou switch de malha
  - Definições de rede no sistema de armazenamento
  - Layout de disco e métricas agregadas no sistema de storage
5. Se o problema persistir, contacte o suporte técnico para obter assistência.

### Use o Digital Advisor para visualizar o desempenho do sistema

Para qualquer sistema ONTAP que envie telemetria de AutoSupport para o NetApp, é possível visualizar dados abrangentes de desempenho e capacidade. O Digital Advisor mostra o desempenho do sistema por um período mais longo do que você pode ver no System Manager.

Você pode visualizar gráficos de utilização da CPU, latência, IOPS, IOPS por protocolo e taxa de transferência de rede. Você também pode baixar esses dados no formato .csv para análise em outras ferramentas.

Além desses dados de performance, o Digital Advisor mostra a eficiência de storage por workload e compara essa eficiência com a eficiência esperada para esse tipo de workload. Você pode ver as tendências de capacidade e ver uma estimativa de quanto storage adicional você pode precisar adicionar em um determinado período de tempo.



- A eficiência de storage está disponível no nível do cliente, do cluster e do nó, no lado esquerdo do painel principal.
- O desempenho está disponível no nível do cluster e do nó no lado esquerdo do painel principal.

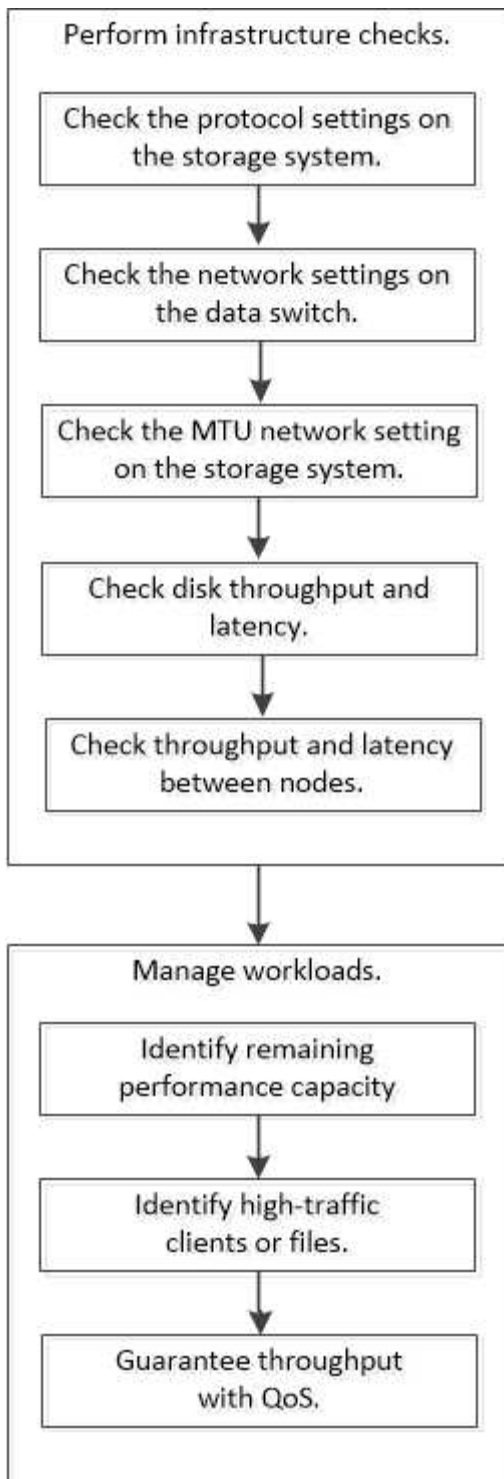
#### Informações relacionadas

- ["Documentação do Digital Advisor"](#)
- ["Lista de reprodução de vídeo do Digital Advisor"](#)
- ["Portal Web do Digital Advisor"](#)

## Gerenciar problemas de performance

### Fluxo de trabalho de gerenciamento de desempenho

Depois de identificar um problema de desempenho, você poderá realizar algumas verificações básicas de diagnóstico de sua infraestrutura para descartar erros óbvios de configuração. Se eles não identificarem o problema, você pode começar a analisar problemas de gerenciamento de workload.



### Realizar verificações básicas de infraestrutura

Verifique as definições do protocolo no sistema de armazenamento

### Verifique o tamanho máximo de transferência TCP NFS

Para NFS, você pode verificar se o tamanho máximo de transferência TCP para leituras e gravações pode estar causando um problema de desempenho. Se você acha que o tamanho está diminuindo o desempenho, você pode aumentá-lo.

### O que você vai precisar

- Você deve ter o administrador de cluster Privileges para executar esta tarefa.
- Tem de utilizar comandos avançados de nível de privilégio para esta tarefa.

### Passos

1. Mude para o nível de privilégio avançado:

```
set -privilege advanced
```

2. Verifique o tamanho máximo de transferência TCP:

```
vserver nfs show -vserver vserver_name -instance
```

3. Se o tamanho máximo de transferência TCP for muito pequeno, aumente o tamanho:

```
vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer
```

4. Voltar ao nível de privilégio administrativo:

```
set -privilege admin
```

### Exemplo

O exemplo a seguir altera o tamanho máximo de transferência TCP de SVM1 para 1048576:

```
cluster1::*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size 1048576
```

### Verifique o tamanho de leitura/gravação iSCSI TCP

Para iSCSI, você pode verificar o tamanho de leitura/gravação TCP para determinar se a configuração de tamanho está criando um problema de desempenho. Se o tamanho for a origem de um problema, você pode corrigi-lo.

### O que você vai precisar

São necessários comandos avançados de nível de privilégio para esta tarefa.

### Passos

1. Alterar para nível de privilégio avançado:

```
set -privilege advanced
```

2. Verifique a configuração de tamanho da janela TCP:

```
vserver iscsi show -vserver vserver_name -instance
```

3. Modifique a configuração de tamanho da janela TCP:

```
vserver iscsi modify -vserver vserver_name -tcp-window-size integer
```

4. Retornar ao privilégio administrativo:

```
set -privilege admin
```

### Exemplo

O exemplo a seguir altera o tamanho da janela TCP SVM1 para 131.400 bytes:

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

### Verificar as definições multiplexadas CIFS

Se o desempenho lento da rede CIFS causar um problema de desempenho, pode modificar as definições multiplexadas para melhorá-las e corrigi-las.

#### Passos

1. Verificar a definição multiplexada CIFS:

```
vserver cifs options show -vserver -vserver_name -instance
```

2. Modificar a definição multiplexada CIFS:

```
vserver cifs options modify -vserver -vserver_name -max-mpx integer
```

### Exemplo

O exemplo seguinte altera a contagem multiplexada máxima SVM1 para 255:

```
cluster1:::> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

### Verifique a velocidade da porta do adaptador FC

A velocidade da porta de destino do adaptador deve corresponder à velocidade do dispositivo ao qual se conecta, para otimizar o desempenho. Se a porta estiver definida para negociação automática, pode demorar mais tempo para se reconectar após uma tomada de posse e giveback ou outra interrupção.

#### O que você vai precisar

Todos os LIFs que usam esse adaptador como porta inicial devem estar offline.

#### Passos

1. Coloque o adaptador offline:

```
network fcp adapter modify -node nodename -adapter adapter -state down
```

2. Verifique a velocidade máxima do adaptador de porta:

```
fcp adapter show -instance
```

3. Altere a velocidade da porta, se necessário:

```
network fcp adapter modify -node nodename -adapter adapter -speed
{1|2|4|8|10|16|auto}
```

4. Coloque o adaptador online:

```
network fcp adapter modify -node nodename -adapter adapter -state up
```

5. Coloque todos os LIFs no adaptador online:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port e0c }
-status-admin up
```

## Exemplo

O exemplo a seguir altera a velocidade da porta do adaptador 0d node1 para 2 Gbps:

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -speed 2
```

## Verifique as definições de rede nos interruptores de dados

Embora seja necessário manter as mesmas configurações de MTU em seus clientes, servidores e sistemas de armazenamento (ou seja, endpoints de rede), os dispositivos de rede intermediários, como NICs e switches, devem ser definidos para seus valores máximos de MTU para garantir que o desempenho não seja afetado.

Para obter o melhor desempenho, todos os componentes da rede devem poder encaminhar quadros jumbo (9000 bytes IP, 9022 bytes incluindo Ethernet). Os switches de dados devem ser definidos para pelo menos 9022 bytes, mas um valor típico de 9216 é possível com a maioria dos switches.

## Procedimento

Para centrais de dados, verifique se o tamanho da MTU está definido para 9022 ou superior.

Para obter mais informações, consulte a documentação do fornecedor do switch.

## Verifique a configuração de rede MTU no sistema de armazenamento

Você pode alterar as configurações de rede no sistema de armazenamento se elas não forem as mesmas do cliente ou de outros endpoints de rede. Enquanto a configuração MTU da rede de gerenciamento está definida como 1500, o tamanho da MTU da rede de dados deve ser 9000.

## Sobre esta tarefa

Todas as portas dentro de um domínio de broadcast têm o mesmo tamanho MTU, com exceção do tráfego de gerenciamento de portas e0M. Se a porta for parte de um domínio de broadcast, use o `broadcast-domain modify` comando para alterar a MTU para todas as portas dentro do domínio de broadcast modificado.

Observe que os dispositivos de rede intermediários, como NICs e switches de dados, podem ser definidos para tamanhos de MTU mais altos do que os endpoints de rede. Para obter mais informações, ["Verifique as definições de rede nos interruptores de dados"](#) consulte .

## Passos

1. Verifique a configuração da porta MTU no sistema de armazenamento:

```
network port show -instance
```

2. Altere a MTU no domínio de broadcast usado pelas portas:

```
network port broadcast-domain modify -ip-space ip-space -broadcast-domain  
broadcast_domain -mtu new_mtu
```

## Exemplo

O exemplo a seguir altera a configuração da porta MTU para 9000:

```
network port broadcast-domain modify -ip-space Cluster -broadcast-domain  
Cluster -mtu 9000
```

## Verifique a taxa de transferência e a latência do disco

Você pode verificar a taxa de transferência de disco e as métricas de latência dos nós de cluster para ajudá-lo na solução de problemas.

## Sobre esta tarefa

São necessários comandos avançados de nível de privilégio para esta tarefa.

## Passos

1. Alterar para nível de privilégio avançado:

```
set -privilege advanced
```

2. Verifique as métricas de taxa de transferência e latência do disco:

```
statistics disk show -sort-key latency
```

## Exemplo

O exemplo a seguir exibe os totais em cada operação de leitura ou gravação do usuário para `node2` em `cluster1`:

```

::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15

```

Disk	Node	Busy (%)	Total Ops	Read Ops	Write Ops	Read (Bps)	Write (Bps)	*Latency (us)
1.10.20	node2	4	5	3	2	95232	367616	23806
1.10.8	node2	4	5	3	2	138240	386048	22113
1.10.6	node2	3	4	2	2	48128	371712	19113
1.10.19	node2	4	6	3	2	102400	443392	19106
1.10.11	node2	4	4	2	2	122880	408576	17713

### Verifique a taxa de transferência e a latência entre nós

Você pode usar o `network test-path` comando para identificar gargalos de rede ou para pré-qualificar caminhos de rede entre nós. Você pode executar o comando entre nós ou nós entre clusters.

#### Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- São necessários comandos avançados de nível de privilégio para esta tarefa.
- Para um caminho entre clusters, os clusters de origem e destino devem ser peered.

#### Sobre esta tarefa

Ocasionalmente, o desempenho da rede entre nós pode não atender às expectativa de configuração do caminho. Uma taxa de transmissão de 1 Gbps para o tipo de grandes transferências de dados vistas nas operações de replicação do SnapMirror, por exemplo, não seria consistente com um link de 10 GbE entre os clusters de origem e destino.

Você pode usar o `network test-path` comando para medir a taxa de transferência e a latência entre nós. Você pode executar o comando entre nós ou nós entre clusters.



O teste satura o caminho da rede com dados, então você deve executar o comando quando o sistema não estiver ocupado e quando o tráfego de rede entre nós não for excessivo. O teste expira após dez segundos. O comando só pode ser executado entre nós ONTAP 9.

A `session-type` opção identifica o tipo de operação que você está executando sobre o caminho da rede - por exemplo, "AsyncMirrorRemote" para replicação do SnapMirror para um destino remoto. O tipo determina a quantidade de dados utilizados no teste. A tabela a seguir define os tipos de sessão:

Tipo de sessão	Descrição
AsyncMirrorLocal	Configurações usadas pelo SnapMirror entre nós no mesmo cluster



AsyncMirrorRemote	Configurações usadas pelo SnapMirror entre nós em clusters diferentes (tipo padrão)
RemoteDataTransfer	Configurações usadas pelo ONTAP para acesso remoto a dados entre nós no mesmo cluster (por exemplo, uma solicitação NFS para um nó para um arquivo armazenado em um volume em um nó diferente)

## Passos

1. Alterar para nível de privilégio avançado:

```
set -privilege advanced
```

2. Meça a taxa de transferência e a latência entre nós:

```
network test-path -source-node source_nodename |local -destination-cluster
destination_clustername -destination-node destination_nodename -session-type
Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTransfer
```

O nó de origem deve estar no cluster local. O nó de destino pode estar no cluster local ou em um cluster com peering. Um valor de "local" para `-source-node` especifica o nó no qual você está executando o comando.

O comando a seguir mede a taxa de transferência e a latência para operações de replicação do tipo SnapMirror entre `node1` no cluster local e `node3` no `cluster2`:

```
cluster1::> network test-path -source-node node1 -destination-cluster
cluster2 -destination-node node3 -session-type AsyncMirrorRemote
```

Saída de amostra (os detalhes de saída podem variar dependendo da sua versão do ONTAP):

```
Test Duration:      10.88 secs
Send Throughput:   18.23 MB/sec
Receive Throughput: 18.23 MB/sec
MB sent:           198.31
MB received:       198.31
Avg latency in ms: 2301.47
```

3. Retornar ao privilégio administrativo:

```
set -privilege admin
```

## Depois de terminar

Se o desempenho não atender às expectativas de configuração do caminho, você deve verificar as estatísticas de desempenho do nó, usar as ferramentas disponíveis para isolar o problema na rede, verificar as configurações do switch e assim por diante.

## Gerenciar workloads

### Identificar a capacidade de performance restante

A capacidade de desempenho, ou *headroom*, mede quanto trabalho você pode colocar em um nó ou agregado antes que o desempenho das cargas de trabalho no recurso comece a ser afetado pela latência. Conhecer a capacidade de performance disponível no cluster ajuda você a provisionar e equilibrar workloads.

### O que você vai precisar

São necessários comandos avançados de nível de privilégio para esta tarefa.

### Sobre esta tarefa

Você pode usar os seguintes valores para a `-object` opção de coletar e exibir estatísticas de headroom:

- Para CPUs, `resource_headroom_cpu`.
- Para agregados `resource_headroom_aggr`, .

Você também pode concluir esta tarefa usando o Gerenciador de sistema e o Active IQ Unified Manager.

### Passos

1. Alterar para nível de privilégio avançado:

```
set -privilege advanced
```

2. Iniciar a coleção de estatísticas de headroom em tempo real:

```
statistics start -object resource_headroom_cpu|aggr
```

Para obter a sintaxe completa do comando, consulte a página `man`.

3. Apresentar informações estatísticas em tempo real do espaço livre:

```
statistics show -object resource_headroom_cpu|aggr
```

Para obter a sintaxe completa do comando, consulte a página `man`.

4. Retornar ao privilégio administrativo:

```
set -privilege admin
```

### Exemplo

O exemplo a seguir exibe as estatísticas médias horárias do espaço livre para nós de cluster.

Você pode calcular a capacidade de desempenho disponível para um nó subtraindo o `current_utilization` contador do `optimal_point_utilization` contador. Neste exemplo, a capacidade de utilização para `CPU_sti2520-213` é de -14% (72%-86%), o que sugere que a CPU foi superutilizada em média na última hora.

Pode ter especificado `ewma_daily`, `ewma_weekly` ou `ewma_monthly` obter a mesma média das informações durante períodos de tempo mais longos.

```
sti2520-2131454963690::*> statistics show -object resource_headroom_cpu
-raw -counter ewma_hourly
(statistics show)
```

```
Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213
```

Counter	Value
-----	-----
ewma_hourly	-
current_ops	4376
current_latency	37719
current_utilization	86
optimal_point_ops	2573
optimal_point_latency	3589
optimal_point_utilization	72
optimal_point_confidence_factor	1

```
Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214
```

Counter	Value
-----	-----
ewma_hourly	-
current_ops	0
current_latency	0
current_utilization	0
optimal_point_ops	0
optimal_point_latency	0
optimal_point_utilization	71
optimal_point_confidence_factor	1

2 entries were displayed.

### Identificar clientes ou arquivos de alto tráfego

Você pode usar a tecnologia ONTAP active Objects para identificar clientes ou arquivos responsáveis por uma quantidade desproporcionalmente grande de tráfego de cluster. Depois de identificar esses "principais" clientes ou arquivos, você pode reequilibrar as cargas de trabalho do cluster ou tomar outras medidas para resolver o problema.

## O que você vai precisar

Você deve ser um administrador de cluster para executar esta tarefa.

### Passos

1. Veja os principais clientes que acessam o cluster:

```
statistics top client show -node node_name -sort-key sort_column -interval  
seconds_between_updates -iterations iterations -max number_of_instances
```

Para obter a sintaxe completa do comando, consulte a página `man`.

O comando a seguir exibe os principais clientes acessando `cluster1`:

```
cluster1::> statistics top client show  
  
cluster1 : 3/23/2016 17:59:10  
  
                *Total  
      Client Vserver          Node Protocol    Ops  
-----
```

172.17.180.170	vs4	siderop1-vs4	nfs	668
172.17.180.169	vs3	siderop1-vs3	nfs	337
172.17.180.171	vs3	siderop1-vs3	nfs	142
172.17.180.170	vs3	siderop1-vs3	nfs	137
172.17.180.123	vs3	siderop1-vs3	nfs	137
172.17.180.171	vs4	siderop1-vs4	nfs	95
172.17.180.169	vs4	siderop1-vs4	nfs	92
172.17.180.123	vs4	siderop1-vs4	nfs	92
172.17.180.153	vs3	siderop1-vs3	nfs	0

2. Veja os principais arquivos acessados no cluster:

```
statistics top file show -node node_name -sort-key sort_column -interval  
seconds_between_updates -iterations iterations -max number_of_instances
```

Para obter a sintaxe completa do comando, consulte a página `man`.

O comando a seguir exibe os principais arquivos acessados no `cluster1`:

```
cluster1::> statistics top file show
```

```
cluster1 : 3/23/2016 17:59:10
```

```

                                *Total
      File Volume Vserver      Node      Ops
-----
/vol/vol1/vm170-read.dat  vol1      vs4 siderop1-vs4      22
/vol/vol1/vm69-write.dat  vol1      vs3 siderop1-vs3       6
  /vol/vol2/vm171.dat     vol2      vs3 siderop1-vs3       2
/vol/vol2/vm169.dat      vol2      vs3 siderop1-vs3       2
  /vol/vol2/p123.dat      vol2      vs4 siderop1-vs4       2
  /vol/vol2/p123.dat      vol2      vs3 siderop1-vs3       2
/vol/vol1/vm171.dat      vol1      vs4 siderop1-vs4       2
/vol/vol1/vm169.dat      vol1      vs4 siderop1-vs4       2
/vol/vol1/vm169.dat      vol1      vs4 siderop1-vs3       2
  /vol/vol1/p123.dat      vol1      vs4 siderop1-vs4       2
```

#### Garantir taxa de transferência com QoS

#### Garanta a taxa de transferência com uma visão geral de QoS

Use a qualidade do serviço (QoS) de storage para garantir que a performance de workloads essenciais não seja degradada pelos workloads da concorrência. Você pode definir um throughput *ceiling* em uma carga de trabalho concorrente para limitar seu impacto nos recursos do sistema ou definir um throughput *floor* para uma carga de trabalho crítica, garantindo que ele atenda aos objetivos mínimos de taxa de transferência, independentemente da demanda por cargas de trabalho concorrentes. Você pode até mesmo definir um teto e piso para a mesma carga de trabalho.

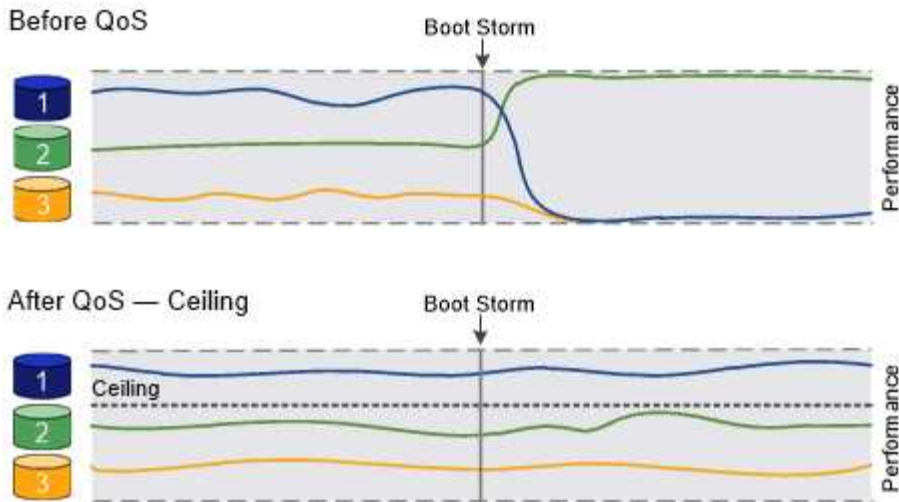
#### Sobre limites máximos de taxa de transferência (QoS Max)

Um limite máximo de taxa de transferência limita a taxa de transferência de um workload a um número máximo de IOPS ou Mbps, ou IOPS e Mbps. Na figura abaixo, o limite de taxa de transferência para a carga de trabalho 2 garante que não "bully" as cargas de trabalho 1 e 3.

Um *grupo de políticas* define o limite máximo de taxa de transferência para uma ou mais cargas de trabalho. Um workload representa as operações de e/S de um *objeto de storage*: um volume, arquivo, qtree ou LUN, ou todos os volumes, arquivos, qtrees ou LUNs em um SVM. Você pode especificar o limite máximo ao criar o grupo de políticas ou esperar até que você monitore cargas de trabalho para especificá-lo.



A taxa de transferência para workloads pode exceder o limite máximo especificado em até 10%, especialmente se um workload sofrer mudanças rápidas na taxa de transferência. O teto pode ser excedido em até 50% para lidar com explosões. As explosões ocorrem em nós únicos quando os tokens acumulam até 150%



### Sobre os andares de taxa de transferência (QoS min)

Um piso de taxa de transferência garante que a taxa de transferência para um workload não fique abaixo de um número mínimo de IOPS ou Mbps, ou IOPS e Mbps. Na figura abaixo, os andares de taxa de transferência para o workload 1 e o workload 3 garantem que eles atendam aos destinos mínimos de taxa de transferência, independentemente da demanda por workload 2.



Como os exemplos sugerem, um teto de throughput limita a taxa de transferência diretamente. Um piso de taxa de transferência mantém a taxa de transferência indiretamente, dando prioridade às cargas de trabalho para as quais o piso foi definido.

Você pode especificar o piso ao criar o grupo de políticas ou esperar até que você monitore cargas de trabalho para especificá-lo.

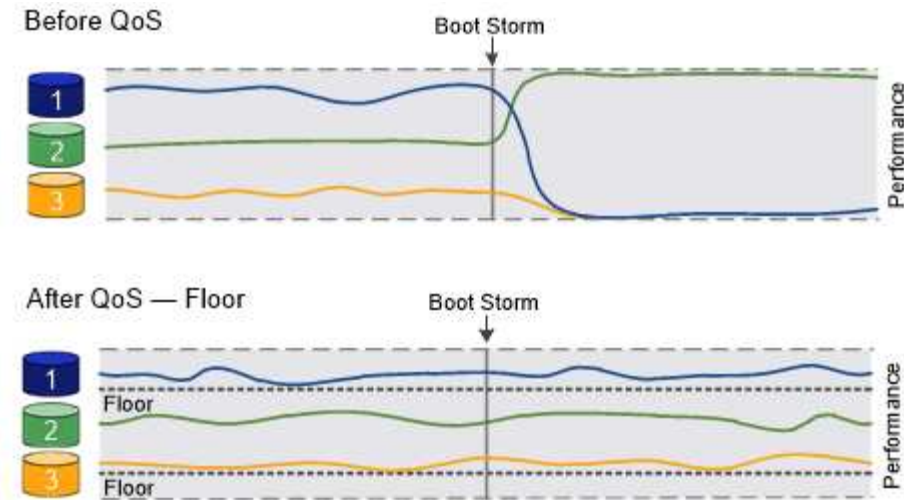
A partir do ONTAP 9.13.1, é possível definir os andares de taxa de transferência no escopo da SVM com [\[adaptive-qos-templates\]](#). Nas versões do ONTAP anteriores a 9.13.1, um grupo de políticas que define uma área de taxa de transferência não pode ser aplicado a um SVM.

Nos lançamentos anteriores ao ONTAP 9.7, os pisos de taxa de transferência são garantidos quando há capacidade de desempenho suficiente disponível.

No ONTAP 9.7 e posterior, os andares de throughput podem ser garantidos mesmo quando há capacidade de desempenho insuficiente disponível. Este novo comportamento do piso é chamado de pisos v2. Para atender às garantias, o piso v2 pode resultar em maior latência em cargas de trabalho sem uma taxa de transferência ou no trabalho que exceda as configurações básicas. Os pisos v2 aplicam-se a QoS e QoS adaptável.



A opção de ativar/desativar o novo comportamento dos pisos v2 está disponível no ONTAP 9.7P6 e posterior. Uma carga de trabalho pode ficar abaixo do nível especificado durante operações críticas como `volume move trigger-cutover`. Mesmo quando a capacidade suficiente está disponível e as operações críticas não estão ocorrendo, a taxa de transferência para uma carga de trabalho pode ficar abaixo do piso especificado em até 5%. Se os andares forem superprovisionados e não houver capacidade de performance, alguns workloads podem ficar abaixo do andar especificado.



### Sobre grupos de políticas de QoS compartilhados e não compartilhados

A partir do ONTAP 9.4, você pode usar um grupo de políticas de QoS *não compartilhado* para especificar que o limite ou o piso da taxa de transferência definido se aplica a cada workload de membro individualmente. O comportamento dos grupos de políticas *shared* depende do tipo de política:

- Para limites máximos de taxa de transferência, a taxa de transferência total para as cargas de trabalho atribuídas ao grupo de políticas partilhadas não pode exceder o limite máximo especificado.
- Para andares de taxa de transferência, o grupo de políticas compartilhadas pode ser aplicado somente a um único workload.

### Sobre a QoS adaptável

Normalmente, o valor do grupo de políticas que você atribui a um objeto de storage é fixo. Você precisa alterar o valor manualmente quando o tamanho do objeto de armazenamento muda. Um aumento na quantidade de espaço usado em um volume, por exemplo, geralmente requer um aumento correspondente no limite de produtividade especificado para o volume.

O *Adaptive QoS* dimensiona automaticamente o valor do grupo de políticas para o tamanho do workload, mantendo a taxa de IOPS para TBs|GBs conforme o tamanho do workload muda. Essa é uma vantagem significativa quando você gerencia centenas ou milhares de workloads em uma implantação grande.

Normalmente, você usa QoS adaptável para ajustar limites máximos de taxa de transferência, mas também pode usá-la para gerenciar andares de taxa de transferência (quando o tamanho do workload aumenta). O tamanho do workload é expresso como o espaço alocado para o objeto de storage ou o espaço usado pelo objeto de storage.



O espaço usado está disponível para pisos de throughput no ONTAP 9.5 e posterior. Não é suportado para pisos de rendimento no ONTAP 9.4 e anteriores.

- Uma política *allocated space* mantém a relação IOPS/TB|GB de acordo com o tamanho nominal do objeto de armazenamento. Se a taxa for de 100 IOPS/GB, um volume de 150 GB terá um limite máximo de taxa de transferência de 15.000 IOPS enquanto o volume permanecer nesse tamanho. Se o volume for redimensionado para 300 GB, a QoS adaptável ajusta o limite da taxa de transferência para 30.000 IOPS.
- Uma política *used space* (o padrão) mantém a taxa IOPS/TB|GB de acordo com a quantidade de dados reais armazenados antes da eficiência de armazenamento. Se a taxa for de 100 IOPS/GB, um volume de 150 GB que tenha 100 GB de dados armazenados teria um limite máximo de taxa de transferência de 10.000 IOPS. À medida que a quantidade de espaço usado muda, a QoS adaptável ajusta o teto de taxa

de transferência de acordo com a taxa.

A partir do ONTAP 9.5, você pode especificar um tamanho de bloco de e/S para o aplicativo que permite que um limite de taxa de transferência seja expresso em IOPS e Mbps. O limite de Mbps é calculado a partir do tamanho do bloco multiplicado pelo limite de IOPS. Por exemplo, um tamanho de bloco de e/S de 32K MB para um limite de IOPS de 6144IOPS GB/TB produz um limite de Mbps de 192MBps GB.

Você pode esperar o seguinte comportamento para tetos e pisos de rendimento:

- Quando um workload é atribuído a um grupo de políticas de QoS adaptável, o teto ou o piso é atualizado imediatamente.
- Quando um workload em um grupo de políticas de QoS adaptável é redimensionado, o teto ou o piso é atualizado em aproximadamente cinco minutos.

A taxa de transferência deve aumentar em pelo menos 10 IOPS antes que as atualizações ocorram.

Grupos de políticas de QoS adaptáveis sempre não são compartilhados: O limite ou o piso da taxa de transferência definida se aplica a cada workload de membro individualmente.

A partir do ONTAP 9.6, os andares de taxa de transferência são suportados no ONTAP Select premium com SSD.

### Modelo de grupo de políticas adaptável

A partir do ONTAP 9.13,1, você pode definir um modelo de QoS adaptável em um SVM. Os modelos de grupo de políticas adaptáveis permitem definir andares e tetos de taxa de transferência para todos os volumes em uma SVM.

Os modelos de grupo de políticas adaptáveis só podem ser definidos após a criação do SVM. Use o `vserver modify` comando com o `-qos-adaptive-policy-group-template` parâmetro para definir a política.

Quando você define um modelo de grupo de políticas adaptativas, os volumes criados ou migrados após a configuração da diretiva herdam automaticamente a política. Quaisquer volumes existentes no SVM não serão afetados quando você atribuir o modelo de política. Se você desativar a política no SVM, qualquer volume posteriormente migrado ou criado no SVM não receberá a política. A desativação do modelo de grupo de políticas adaptativas não afeta os volumes que herdaram o modelo de política à medida que retêm o modelo de política.

Para obter mais informações, [Defina um modelo de grupo de políticas adaptável](#) consulte .

### Suporte geral

A tabela a seguir mostra as diferenças no suporte para limites máximos de taxa de transferência, andares de taxa de transferência e QoS adaptável.

Recurso ou recurso	Teto com taxa de transferência	Piso de taxa de transferência	Piso de taxa de transferência v2	QoS adaptável
Versão ONTAP 9	Tudo	9,2 e mais tarde	9,7 e mais tarde	9,3 e mais tarde



Recurso ou recurso	Teto com taxa de transferência	Piso de taxa de transferência	Piso de taxa de transferência v2	QoS adaptável
Plataformas	Tudo	<ul style="list-style-type: none"> <li>• AFF</li> <li>• C190 *</li> <li>• ONTAP Select premium com SSD *</li> </ul>	<ul style="list-style-type: none"> <li>• AFF</li> <li>• C190</li> <li>• ONTAP Select premium com SSD</li> </ul>	Tudo
Protocolos	Tudo	Tudo	Tudo	Tudo
FabricPool	Sim	Sim, se a política de disposição em categorias estiver definida como "nenhum" e não houver blocos na nuvem.	Sim, se a política de disposição em categorias estiver definida como "nenhum" e não houver blocos na nuvem.	Não
SnapMirror síncrono	Sim	Não	Não	Sim

O suporte ao C190 e ao ONTAP Select começou com o lançamento do ONTAP 9.6.

### Workloads compatíveis com limites máximos de taxa de transferência

A tabela a seguir mostra o suporte do workload para limites máximos de taxa de transferência pela versão do ONTAP 9. Volumes raiz, espelhos de compartilhamento de carga e espelhos de proteção de dados não são compatíveis.

Suporte à carga de trabalho - limite máximo	ONTAP 9,0	ONTAP 9,1	ONTAP 9,2	ONTAP 9,3	ONTAP 9.4 - 9,7	ONTAP 9 F.8 e mais tarde
Volume	sim	sim	sim	sim	sim	sim
Ficheiro	sim	sim	sim	sim	sim	sim
LUN	sim	sim	sim	sim	sim	sim
SVM	sim	sim	sim	sim	sim	sim
Volume FlexGroup	não	não	não	sim	sim	sim
qtrees*	não	não	não	não	não	sim

<b>Suporte à carga de trabalho - limite máximo</b>	<b>ONTAP 9,0</b>	<b>ONTAP 9,1</b>	<b>ONTAP 9,2</b>	<b>ONTAP 9,3</b>	<b>ONTAP 9.4 - 9,7</b>	<b>ONTAP 9 F.8 e mais tarde</b>
Vários workloads por grupo de políticas	sim	sim	sim	sim	sim	sim
Grupos de políticas não compartilhados	não	não	não	não	sim	sim

A partir do ONTAP 9.8, o acesso NFS é compatível com qtrees nos volumes FlexVol e FlexGroup com NFS habilitado. A partir do ONTAP 9.9,1, o acesso SMB também é suportado em qtrees nos volumes FlexVol e FlexGroup com SMB ativado.

### **Workloads compatíveis em pisos de taxa de transferência**

A tabela a seguir mostra o suporte do workload para andares de taxa de transferência pela versão do ONTAP 9. Volumes raiz, espelhos de compartilhamento de carga e espelhos de proteção de dados não são compatíveis.

<b>Suporte de carga de trabalho - básico</b>	<b>ONTAP 9,2</b>	<b>ONTAP 9,3</b>	<b>ONTAP 9.4 - 9,7</b>	<b>ONTAP 9.8 - 9.13.0</b>	<b>ONTAP 9.13,1 e posterior</b>
Volume	sim	sim	sim	sim	sim
Ficheiro	não	sim	sim	sim	sim
LUN	sim	sim	sim	sim	sim
SVM	não	não	não	não	sim
Volume FlexGroup	não	não	sim	sim	sim
qtrees *	não	não	não	sim	sim
Vários workloads por grupo de políticas	não	não	sim	sim	sim
Grupos de políticas não compartilhados	não	não	sim	sim	sim

A partir do ONTAP 9.8, o acesso NFS é suportado em qtrees nos volumes FlexVol e FlexGroup com NFS ativado. A partir do ONTAP 9.9,1, o acesso SMB também é suportado em qtrees nos volumes FlexVol e FlexGroup com SMB ativado.

## Workloads compatíveis com QoS adaptável

A tabela a seguir mostra o suporte do workload para QoS adaptável pela versão do ONTAP 9. Volumes raiz, espelhos de compartilhamento de carga e espelhos de proteção de dados não são compatíveis.

Suporte a workload - QoS adaptável	ONTAP 9,3	ONTAP 9.4 - 9.13.0	ONTAP 9.13,1 e posterior
Volume	sim	sim	sim
Ficheiro	não	sim	sim
LUN	não	sim	sim
SVM	não	não	sim
Volume FlexGroup	não	sim	sim
Vários workloads por grupo de políticas	sim	sim	sim
Grupos de políticas não compartilhados	sim	sim	sim

## Número máximo de cargas de trabalho e grupos de políticas

A tabela a seguir mostra o número máximo de cargas de trabalho e grupos de políticas por versão do ONTAP 9.

Suporte a workload	ONTAP 9 .3 e anteriores	ONTAP 9 .4 e mais tarde
Máximo de workloads por cluster	12.000	40.000
Máximo de workloads por nó	12.000	40.000
Máximo de grupos de políticas	12.000	12.000

## Ativar ou desativar os pisos de rendimento v2

Você pode ativar ou desativar os andares de taxa de transferência v2 no AFF. A predefinição é Enabled (activado). Com os andares v2 ativados, os andares de taxa de transferência podem ser atendidos quando os controladores são muito usados em detrimento da latência mais alta em outros workloads. Os pisos v2 aplicam-se a QoS e QoS adaptável.

### Passos

1. Alterar para nível de privilégio avançado:

```
set -privilege advanced
```

2. Introduza um dos seguintes comandos:

Se você quiser...	Use este comando:
Desativar pisos v2	<code>qos settings throughput-floors-v2 -enable false</code>
Ativar os pisos v2	<code>qos settings throughput-floors-v2 -enable true</code>



Para desativar os pisos de taxa de transferência v2 num cluster MetroCluster, tem de executar o.

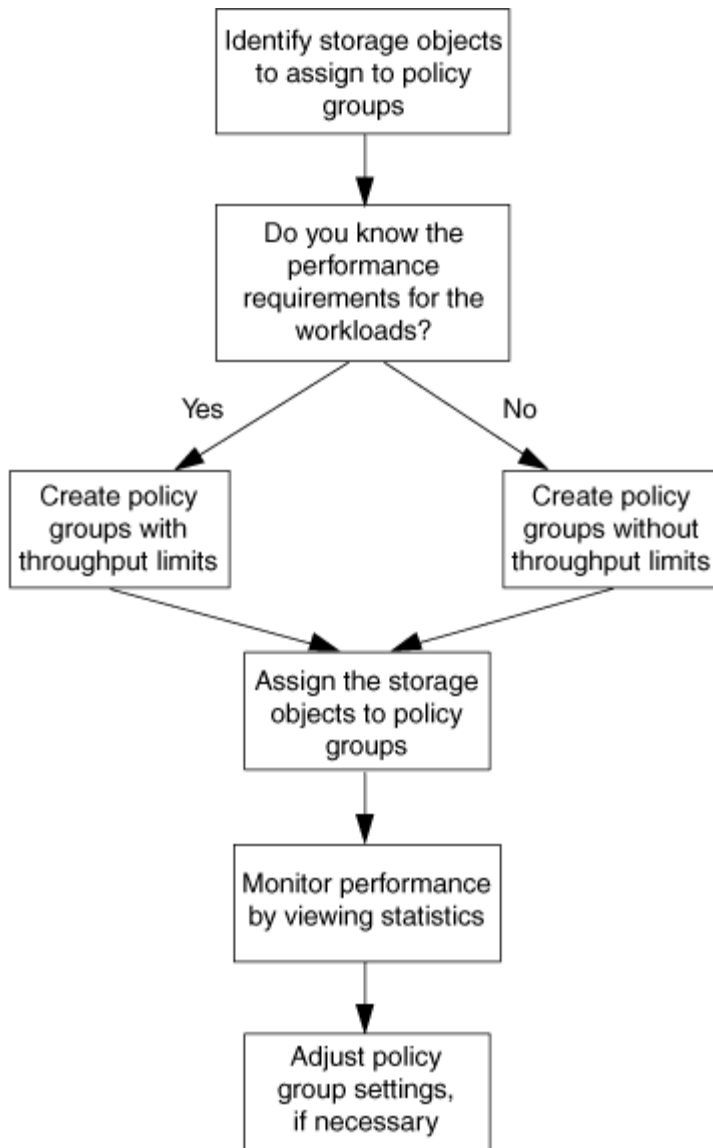
```
qos settings throughput-floors-v2 -enable false
```

comando nos clusters de origem e destino.

```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

### Fluxo de trabalho de QoS do storage

Se você já conhece os requisitos de desempenho para os workloads que deseja gerenciar com QoS, poderá especificar o limite de taxa de transferência ao criar o grupo de políticas. Caso contrário, você pode esperar até que você monitore as cargas de trabalho para especificar o limite.



### Defina um limite de taxa de transferência com QoS

Você pode usar o `max-throughput` campo de um grupo de políticas para definir um limite máximo de taxa de transferência para workloads de objetos de storage (QoS Max). Você pode aplicar o grupo de políticas ao criar ou modificar o objeto de armazenamento.

#### O que você vai precisar

- Você deve ser um administrador de cluster para criar um grupo de políticas.
- Você deve ser um administrador de cluster para aplicar um grupo de políticas a um SVM.

#### Sobre esta tarefa

- A partir do ONTAP 9.4, você pode usar um grupo de políticas de QoS *não compartilhado* para especificar que o limite de taxa de transferência definido se aplica a cada workload de membro individualmente. Caso contrário, o grupo de políticas é *compartilhado*: a taxa de transferência total para as cargas de trabalho atribuídas ao grupo de políticas não pode exceder o limite máximo especificado.

Defina `-is-shared=false` para que o `qos policy-group create` comando especifique um grupo de políticas não compartilhado.

- Você pode especificar o limite de taxa de transferência para o limite máximo em IOPS, MB/s ou IOPS, MB/s. Se você especificar IOPS e MB/s, qualquer limite atingido primeiro será aplicado.



Se você definir um teto e um piso para a mesma carga de trabalho, poderá especificar o limite de taxa de transferência para o limite máximo apenas em IOPS.

- Um objeto de storage que esteja sujeito a um limite de QoS precisa estar contido pelo SVM a que o grupo de políticas pertence. Vários grupos de políticas podem pertencer ao mesmo SVM.
- Não é possível atribuir um objeto de armazenamento a um grupo de políticas se o objeto que contém ou os objetos filho pertencerem ao grupo de políticas.
- É uma prática recomendada de QoS aplicar um grupo de políticas ao mesmo tipo de objetos de storage.

## Passos

### 1. Criar um grupo de políticas:

```
qos policy-group create -policy-group policy_group -vserver SVM -max
-throughput number_of_iops|Mb/S|iops,Mb/S -is-shared true|false
```

Para obter a sintaxe completa do comando, consulte a página man. Você pode usar o `qos policy-group modify` comando para ajustar os tetos de taxa de transferência.

O comando a seguir cria o grupo de políticas compartilhadas `pg-vs1` com uma taxa de transferência máxima de 5.000 IOPS:

```
cluster1::> qos policy-group create -policy-group pg-vs1 -vserver vs1
-max-throughput 5000iops -is-shared true
```

O comando a seguir cria o grupo de políticas não compartilhadas `pg-vs3` com uma taxa de transferência máxima de 100 IOPS e 400 Kb/S:

```
cluster1::> qos policy-group create -policy-group pg-vs3 -vserver vs3
-max-throughput 100iops,400KB/s -is-shared false
```

O comando a seguir cria o grupo de políticas não compartilhadas `pg-vs4` sem um limite de taxa de transferência:

```
cluster1::> qos policy-group create -policy-group pg-vs4 -vserver vs4
-is-shared false
```

### 2. Aplique um grupo de políticas a um SVM, arquivo, volume ou LUN:

```
storage_object create -vserver SVM -qos-policy-group policy_group
```

Para obter a sintaxe completa do comando, consulte as páginas man. Você pode usar o `storage_object modify` comando para aplicar um grupo de políticas diferente ao objeto de armazenamento.

O comando a seguir aplica o grupo de políticas `pg-vs1` ao SVM `vs1`:

```
cluster1::> vserver create -vserver vs1 -qos-policy-group pg-vs1
```

Os comandos a seguir aplicam o grupo de políticas `pg-app` aos volumes `app1` e `app2`:

```
cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1  
-qos-policy-group pg-app
```

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1  
-qos-policy-group pg-app
```

### 3. Monitorar o desempenho do grupo de políticas:

```
qos statistics performance show
```

Para obter a sintaxe completa do comando, consulte a página `man`.



Monitore o desempenho do cluster. Não use uma ferramenta no host para monitorar o desempenho.

O comando a seguir mostra o desempenho do grupo de políticas:

```
cluster1::> qos statistics performance show
```

Policy Group	IOPS	Throughput	Latency
-total-	12316	47.76MB/s	1264.00us
pg_vs1	5008	19.56MB/s	2.45ms
_System-Best-Effort	62	13.36KB/s	4.13ms
_System-Background	30	0KB/s	0ms

### 4. Monitorar a performance do workload:

```
qos statistics workload performance show
```

Para obter a sintaxe completa do comando, consulte a página `man`.



Monitore o desempenho do cluster. Não use uma ferramenta no host para monitorar o desempenho.

O comando a seguir mostra o desempenho da carga de trabalho:

```
cluster1::> qos statistics workload performance show
Workload          ID      IOPS      Throughput      Latency
-----
-total-          -      12320      47.84MB/s      1215.00us
app1-wid7967     7967      7219      28.20MB/s      319.00us
vs1-wid12279     12279      5026      19.63MB/s      2.52ms
_USERSPACE_APPS  14        55        10.92KB/s      236.00us
_Scan_Backgro... 5688      20        0KB/s          0ms
```



Use o `qos statistics workload latency show` comando para visualizar estatísticas detalhadas de latência para workloads de QoS.

## Defina um piso de taxa de transferência com QoS

Você pode usar o `min-throughput` campo de um grupo de políticas para definir um piso de taxa de transferência para workloads de objetos de storage (QoS min). Você pode aplicar o grupo de políticas ao criar ou modificar o objeto de armazenamento. A partir do ONTAP 9.8, você pode especificar o piso da taxa de transferência em IOPS ou Mbps, ou IOPS e Mbps.

### Antes de começar

- Você deve estar executando o ONTAP 9.2 ou posterior. Os pisos de taxa de transferência estão disponíveis a partir do ONTAP 9.2.
- Você deve ser um administrador de cluster para criar um grupo de políticas.
- A partir do ONTAP 9.13,1, você pode aplicar pisos de taxa de transferência no nível SVM usando um [modelo de grupo de políticas adaptável](#). Não é possível definir um modelo de grupo de políticas adaptável em um SVM com um grupo de políticas de QoS.

### Sobre esta tarefa

- A partir do ONTAP 9.4, você pode usar um grupo de políticas de QoS *não compartilhado* para especificar que o piso da taxa de transferência definido seja aplicado individualmente a cada workload de membro. Essa é a única condição em que um grupo de políticas para uma área de transferência pode ser aplicado a várias cargas de trabalho.

Defina `-is-shared=false` para que o `qos policy-group create` comando especifique um grupo de políticas não compartilhado.

- A taxa de transferência para uma carga de trabalho pode ficar abaixo do nível especificado se houver capacidade de desempenho (espaço livre) insuficiente no nó ou no agregado.
- Um objeto de storage que esteja sujeito a um limite de QoS precisa estar contido pelo SVM a que o grupo de políticas pertence. Vários grupos de políticas podem pertencer ao mesmo SVM.
- É uma prática recomendada de QoS aplicar um grupo de políticas ao mesmo tipo de objetos de storage.
- Um grupo de políticas que define um piso de taxa de transferência não pode ser aplicado a um SVM.

### Passos

1. Verifique se há capacidade de desempenho adequada no nó ou no agregado, conforme descrito



"Identificação da capacidade de performance restante" em .

## 2. Criar um grupo de políticas:

```
qos policy-group create -policy group policy_group -vserver SVM -min  
-throughput qos_target -is-shared true|false
```

Para obter a sintaxe de comando completa, consulte a página man para sua versão do ONTAP. Você pode usar o `qos policy-group modify` comando para ajustar os andares de taxa de transferência.

O comando a seguir cria o grupo de políticas compartilhadas `pg-vs2` com uma taxa de transferência mínima de 1.000 IOPS:

```
cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2  
-min-throughput 1000iops -is-shared true
```

O comando a seguir cria o grupo de políticas não compartilhadas `pg-vs4` sem um limite de taxa de transferência:

```
cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4  
-is-shared false
```

## 3. Aplicar um grupo de políticas a um volume ou LUN:

```
storage_object create -vserver SVM -qos-policy-group policy_group
```

Para obter a sintaxe completa do comando, consulte as páginas man. Você pode usar o `_storage_object_modify` comando para aplicar um grupo de políticas diferente ao objeto de armazenamento.

O comando a seguir aplica o grupo de políticas `pg-app2` ao volume `app2`:

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1  
-qos-policy-group pg-app2
```

## 4. Monitorar o desempenho do grupo de políticas:

```
qos statistics performance show
```

Para obter a sintaxe completa do comando, consulte a página man.



Monitore o desempenho do cluster. Não use uma ferramenta no host para monitorar o desempenho.

O comando a seguir mostra o desempenho do grupo de políticas:

```
cluster1::> qos statistics performance show
Policy Group          IOPS          Throughput    Latency
-----
-total-              12316         47.76MB/s    1264.00us
pg_app2              7216          28.19MB/s    420.00us
_System-Best-Effort   62            13.36KB/s    4.13ms
_System-Background   30            0KB/s        0ms
```

## 5. Monitorar a performance do workload:

```
qos statistics workload performance show
```

Para obter a sintaxe completa do comando, consulte a página `man`.



Monitore o desempenho do cluster. Não use uma ferramenta no host para monitorar o desempenho.

O comando a seguir mostra o desempenho da carga de trabalho:

```
cluster1::> qos statistics workload performance show
Workload             ID          IOPS          Throughput    Latency
-----
-total-              -           12320         47.84MB/s    1215.00us
app2-wid7967         7967        7219          28.20MB/s    319.00us
vs1-wid12279         12279       5026          19.63MB/s    2.52ms
_USERSPACE_APPS      14          55            10.92KB/s    236.00us
_Scan_Backgro...    5688        20            0KB/s        0ms
```



Use o `qos statistics workload latency show` comando para visualizar estatísticas detalhadas de latência para workloads de QoS.

## Use grupos de políticas de QoS adaptáveis

Você pode usar um grupo de políticas *Adaptive QoS* para escalar automaticamente um limite de taxa de transferência ou um tamanho de chão para volume, mantendo a taxa de IOPS para TBs|GBs conforme o tamanho do volume muda. Essa é uma vantagem significativa quando você gerencia centenas ou milhares de workloads em uma implantação grande.

### Antes de começar

- Você deve estar executando o ONTAP 9.3 ou posterior. Os grupos de políticas de QoS adaptáveis estão disponíveis a partir do ONTAP 9.3.
- Você deve ser um administrador de cluster para criar um grupo de políticas.

### Sobre esta tarefa

Um objeto de storage pode ser membro de um grupo de políticas adaptáveis ou de um grupo de políticas não adaptáveis, mas não ambos. O SVM do objeto de storage e a política devem ser os mesmos. O objeto de storage deve estar on-line.

Grupos de políticas de QoS adaptáveis sempre não são compartilhados: O limite ou o piso da taxa de transferência definida se aplica a cada workload de membro individualmente.

A proporção de limites de taxa de transferência para o tamanho do objeto de armazenamento é determinada pela interação dos seguintes campos:

- `expected-iops` É o mínimo esperado de IOPS por TB|GB alocado.



`expected-iops` É garantido apenas nas plataformas AFF.  
`expected-iops` Será garantido para o FabricPool somente se a política de disposição em categorias estiver definida como "nenhuma" e não houver blocos na nuvem. `expected-iops` É garantido para volumes que não estão em uma relação síncrona SnapMirror.

- `peak-iops` É o máximo de IOPS possível por TB|GB alocado ou usado.
- `expected-iops-allocation` especifica se o espaço alocado (o padrão) ou o espaço usado é usado para iops-esperado.



`expected-iops-allocation` Está disponível no ONTAP 9.5 e posterior. Ele não é suportado no ONTAP 9.4 e anterior.

- `peak-iops-allocation` especifica se o espaço alocado ou o espaço usado (o padrão) é usado para `peak-iops`.
- `absolute-min-iops` É o número mínimo absoluto de IOPS. Você pode usar este campo com objetos de armazenamento muito pequenos. Substitui ambos `peak-iops` e `expected-iops` ou quando `absolute-min-iops` é maior do que o `expected-iops` calculado.

Por exemplo, se você definir `expected-iops` como 1.000 IOPS/TB e o tamanho do volume for inferior a 1 GB, o calculado `expected-iops` será uma IOP fracionária. O calculado `peak-iops` será uma fração ainda menor. Você pode evitar isso definindo `absolute-min-iops` um valor realista.

- `block-size` Especifica o tamanho do bloco de e/S da aplicação. A predefinição é 32K. Os valores válidos são 8K, 16K, 32K, 64K, QUALQUER. QUALQUER significa que o tamanho do bloco não é imposto.

Três grupos de políticas de QoS adaptáveis padrão estão disponíveis, como mostrado na tabela a seguir. Você pode aplicar esses grupos de políticas diretamente a um volume.

Grupo de políticas padrão	IOPS/TB esperados	IOPS/TB de pico	IOPS mín. Absoluto
extreme	6.144	12.288	1000

performance	2.048	4.096	500
value	128	512	75

Não é possível atribuir um objeto de armazenamento a um grupo de políticas se o objeto que contém ou os objetos filho pertencerem a um grupo de políticas. A tabela a seguir lista as restrições.

Se você atribuir...	Então você não pode atribuir...
SVM em um grupo de políticas	Quaisquer objetos de storage contidos pelo SVM em um grupo de políticas
Volume para um grupo de políticas	Volume contendo SVM ou LUNs filho, em um grupo de políticas
LUN para um grupo de políticas	LUN que contém volume ou SVM em um grupo de políticas
Arquivo para um grupo de políticas	Os arquivos contêm volume ou SVM em um grupo de políticas

## Passos

1. Criar um grupo de políticas de QoS adaptável:

```
qos adaptive-policy-group create -policy group policy_group -vserver SVM
-expected-iops number_of_iops/TB|GB -peak-iops number_of_iops/TB|GB -expected
-iops-allocation-space|used-space -peak-iops-allocation allocated-space|used-
space -absolute-min-iops number_of_iops -block-size 8K|16K|32K|64K|ANY
```

Para obter a sintaxe completa do comando, consulte a página man.



-expected-iops-allocation E -block-size está disponível em ONTAP 9.5 e posterior. Essas opções não são suportadas no ONTAP 9.4 e versões anteriores.

O comando a seguir cria um grupo de políticas de QoS adaptável `adpg-app1` -expected-iops definido como 300 IOPS/TB, -peak-iops definido como 1.000 IOPS/TB, -peak-iops-allocation definido como used-space e -absolute-min-iops definido como 50 IOPS:

```
cluster1::> qos adaptive-policy-group create -policy group adpg-app1
-vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak-iops
-allocation used-space -absolute-min-iops 50iops
```

2. Aplicar um grupo de políticas de QoS adaptável a um volume:

```
volume create -vserver SVM -volume volume -aggregate aggregate -size number_of
TB|GB -qos-adaptive-policy-group policy_group
```

Para obter a sintaxe completa do comando, consulte as páginas man.

O comando a seguir aplica o grupo de políticas de QoS adaptável `adpg-app1` ao volume `app1`:

```
cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1
-size 2TB -qos-adaptive-policy-group adpg-app1
```

Os comandos a seguir aplicam o grupo de políticas de QoS adaptável padrão `extreme` ao novo volume `app4` e ao volume existente `app5`. O limite máximo de taxa de transferência definido para o grupo de políticas aplica-se a volumes `app4` e `app5` individualmente:

```
cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4
-size 2TB -qos-adaptive-policy-group extreme
```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy
-group extreme
```

## Defina um modelo de grupo de políticas adaptável

A partir do ONTAP 9.13.1, você pode aplicar pisos e tetos de taxa de transferência no nível SVM usando um modelo de grupo de políticas adaptável.

### Sobre esta tarefa

- O modelo de grupo de políticas adaptativas é uma política `apg1` padrão. A política pode ser modificada a qualquer momento. Ela só pode ser definida com a API REST CLI ou ONTAP e só pode ser aplicada a SVMs existentes.
- O modelo de grupo de políticas adaptável afeta apenas os volumes criados ou migrados para o SVM após você definir a política. Os volumes existentes no SVM mantêm seu status atual.

Se você desabilitar o modelo de grupo de políticas adaptáveis, os volumes no SVM manterão suas políticas existentes. Somente os volumes posteriormente criados ou migrados para o SVM serão afetados pelo desfalecimento.

- Não é possível definir um modelo de grupo de políticas adaptável em um SVM com um grupo de políticas de QoS.
- Os modelos de grupo de políticas adaptáveis são projetados para plataformas AFF. Um modelo de grupo de políticas adaptável pode ser definido em outras plataformas, mas a política pode não impor uma taxa de transferência mínima. Da mesma forma, você pode adicionar um modelo de grupo de políticas adaptável a um SVM em um agregado do FabricPool ou em um agregado que não ofereça suporte a taxa de transferência mínima. No entanto, o nível de taxa de transferência não será imposto.
- Se o SVM estiver em uma configuração do MetroCluster ou em uma relação do SnapMirror, o modelo de grupo de políticas adaptável será aplicado no SVM espelhado.

### Passos

1. Modifique o SVM para aplicar o modelo de grupo de políticas adaptável:  
`vserver modify -qos-adaptive-policy-group-template apg1`

2. Confirme se a política foi definida:

```
vserver show -fields qos-adaptive-policy-group
```

## Monitore o desempenho do cluster com o Unified Manager

Com o Active IQ Unified Manager, você pode maximizar a disponibilidade e manter o controle da infraestrutura de storage NetApp AFF e FAS para aumentar a escalabilidade, a capacidade de suporte, a performance e a segurança.

O Active IQ Unified Manager monitora continuamente a integridade do sistema e envia alertas para que sua organização possa liberar recursos da equipe DE TI. Você pode visualizar instantaneamente o status do storage em um único painel e solucionar problemas rapidamente por meio das ações recomendadas.

O gerenciamento de dados é simplificado porque é possível descobrir, monitorar e receber notificações para gerenciar proativamente o storage e resolver problemas com rapidez. A eficiência dos administradores é aprimorada porque é possível monitorar petabytes de dados em um único dashboard e gerenciar os dados em escala.

Com o Active IQ Unified Manager, você pode acompanhar as flutuações das demandas de negócios, otimizando o desempenho usando dados de desempenho e análises avançadas. Os recursos de relatórios permitem que você acesse relatórios padrão ou crie relatórios operacionais personalizados para atender às necessidades específicas de sua empresa.

Links relacionados:

- ["Saiba mais sobre o Active IQ Unified Manager"](#)
- ["Comece a usar o Active IQ Unified Manager para VMware"](#)
- ["Comece a usar o Active IQ Unified Manager para Linux"](#)
- ["Comece a usar o Active IQ Unified Manager para Windows"](#)

## Monitore o desempenho do cluster com o Cloud Insights

O NetApp Cloud Insights é uma ferramenta de monitoramento que oferece visibilidade de toda a sua infraestrutura. Com o Cloud Insights, você pode monitorar, solucionar problemas e otimizar todos os recursos, incluindo suas nuvens públicas e seus data centers privados.

### Cloud Insights vem em duas edições

A edição básica do Cloud Insights foi projetada especificamente para monitorar e otimizar seus ativos do NetApp Data Fabric. Ele fornece análises avançadas para conexões entre todos os recursos do NetApp, incluindo HCI e All Flash FAS (AFF) no ambiente gratuitamente.

O Cloud Insights Standard Edition se concentra não apenas em componentes de infraestrutura habilitados para NetApp Data Fabric, mas também em ambientes de vários fornecedores e multicloud. Com seus recursos enriquecidos, você pode acessar o suporte para mais de 100 serviços e recursos.

No mundo de hoje, com recursos em jogo de seus data centers no local para várias nuvens públicas, é crucial ter a visão completa, desde a própria aplicação até o disco de back-end do storage array. O suporte adicional para monitoramento de aplicativos (como Kafka, MongoDB e nginx) fornece as informações e o conhecimento

que você precisa para operar no nível ideal de utilização, bem como com o buffer de risco perfeito.

Ambas as edições (Basic e Standard) podem se integrar ao NetApp Active IQ Unified Manager. Os clientes que usam o Active IQ Unified Manager podem ver as informações de associação dentro da interface de usuário do Cloud Insights. As notificações postadas no Active IQ Unified Manager não são negligenciadas e podem ser correlacionadas a eventos no Cloud Insights. Em outras palavras, você obtém o melhor dos dois mundos.

## **Monitore, solucione problemas e otimize todos os seus recursos**

O Cloud Insights ajuda você a reduzir significativamente o tempo para resolver problemas e evitar que eles afetem os usuários finais. Ele também ajuda a reduzir os custos de infraestrutura de nuvem. Sua exposição a ameaças internas é reduzida ao proteger seus dados com inteligência acionável.

O Cloud Insights oferece visibilidade de toda a sua infraestrutura híbrida em um só lugar, da nuvem pública ao data center. Você pode criar instantaneamente painéis relevantes que podem ser personalizados de acordo com suas necessidades específicas. Você também pode criar alertas direcionados e condicionais que sejam específicos e relevantes para as necessidades da sua organização.

A detecção avançada de anomalias ajuda a corrigir problemas de forma proativa, antes que eles ocorram. Você pode visualizar a contenção e a degradação de recursos automaticamente para restaurar os workloads afetados com rapidez. A solução de problemas vai mais rapidamente com a hierarquia de relações criada automaticamente entre os diferentes componentes da pilha.

Você pode identificar recursos não utilizados ou abandonados em todo o seu ambiente, o que ajuda a descobrir oportunidades de dimensionar corretamente a infraestrutura e otimizar todo o seu gasto.

O Cloud Insights visualiza a topologia do sistema para entender a arquitetura do Kubernetes. Você pode monitorar a integridade dos clusters do Kubernetes, incluindo os nós com problemas, e aumentar o zoom quando encontrar um problema.

O Cloud Insights ajuda você a proteger os dados organizacionais contra a utilização indevida por usuários mal-intencionados ou comprometidos por meio de aprendizado de máquina avançado e detecção de anomalias. Isso proporciona informações úteis sobre ameaças internas.

O Cloud Insights ajuda você a visualizar métricas do Kubernetes para que você possa entender completamente as relações entre seus pods, nós e clusters. Você pode avaliar a integridade de um cluster ou um pod de trabalho, bem como a carga que ele está processando atualmente, permitindo que você assuma o comando do cluster K8S e controle a integridade e o custo da implantação.

### **Links relacionados**

- ["Saiba mais sobre o Cloud Insights"](#)
- ["Comece a usar o Cloud Insights"](#)

## **Log de auditoria**

### **Como o ONTAP implementa o log de auditoria**

As atividades de gerenciamento registradas no log de auditoria são incluídas nos relatórios padrão do AutoSupport e certas atividades de Registro são incluídas nas mensagens do EMS. Você também pode encaminhar o log de auditoria para destinos especificados e exibir arquivos de log de auditoria usando a CLI ou um navegador da

## Web.

A partir do ONTAP 9.11,1, você pode exibir o conteúdo do log de auditoria usando o Gerenciador do sistema.

A partir do ONTAP 9.12,1, o ONTAP fornece alertas de adulteração para logs de auditoria. O ONTAP executa um trabalho de segundo plano diário para verificar se há adulteração de arquivos `audit.log` e envia um alerta EMS se ele encontrar arquivos de log que foram alterados ou adulterados.

O ONTAP Registra as atividades de gerenciamento que são executadas no cluster, por exemplo, qual solicitação foi emitida, o usuário que acionou a solicitação, o método de acesso do usuário e a hora da solicitação.

As atividades de gestão podem ser um dos seguintes tipos:

- Definir solicitações, que normalmente se aplicam a comandos ou operações que não sejam exibidas:
  - Essas solicitações são emitidas quando você executa um `create` comando, `modify`, ou `delete`, por exemplo.
  - As solicitações de conjunto são registradas por padrão.
- OBTENHA solicitações, que recuperam informações e exibem na interface de gerenciamento:
  - Essas solicitações são emitidas quando você executa um `show` comando, por exemplo.
  - As SOLICITAÇÕES GET não são registradas por padrão, mas você pode controlar se as solicitações GET enviadas da CLI do ONTAP (`-cliget`), da API do ONTAP (`-ontapiget`) ou da API REST (`-httpget`) estão registradas no arquivo.

O ONTAP Registra atividades de gerenciamento `/mroot/etc/log/mlog/audit.log` no arquivo de um nó. Comandos dos três shells para comandos CLI - o `clustershell`, o `nodeshell` e o `systemshell` não interativo (comandos do `systemshell` interativo não são registrados) - assim como os comandos API são registrados aqui. Os logs de auditoria incluem carimbos de data/hora para mostrar se todos os nós de um cluster estão sincronizados com a hora.

O `audit.log` arquivo é enviado pela ferramenta AutoSupport para os destinatários especificados. Você também pode encaminhar o conteúdo de forma segura para destinos externos especificados por você; por exemplo, um Splunk ou um servidor syslog.

O `audit.log` arquivo é girado diariamente. A rotação também ocorre quando atinge 100 MB de tamanho, e as 48 cópias anteriores são preservadas (com um total máximo de 49 arquivos). Quando o arquivo de auditoria executa sua rotação diária, nenhuma mensagem EMS é gerada. Se o arquivo de auditoria girar porque seu limite de tamanho de arquivo é excedido, uma mensagem EMS é gerada.

## Alterações ao registo de auditoria no ONTAP 9

A partir do ONTAP 9, o `command-history.log` arquivo é substituído pelo `audit.log`, e o `mgwd.log` arquivo não contém mais informações de auditoria. Se você estiver atualizando para o ONTAP 9, revise todos os scripts ou ferramentas que se referem aos arquivos legados e seus conteúdos.

Após a atualização para o ONTAP 9, os arquivos existentes `command-history.log` são preservados. Eles são girados para fora (excluídos) à medida que novos `audit.log` arquivos são girados em (criados).

Ferramentas e scripts que verificam o `command-history.log` arquivo podem continuar funcionando, porque



um link de software de `command-history.log` para `audit.log` é criado na atualização. No entanto, ferramentas e scripts que verificam o `mgwd.log` arquivo falharão, porque esse arquivo não contém mais informações de auditoria.

Além disso, os logs de auditoria no ONTAP 9 e posterior não incluem mais as seguintes entradas porque não são consideradas úteis e causam atividade de Registro desnecessária:

- Comandos internos executados pelo ONTAP (ou seja, onde o nome de usuário é root)
- Aliases de comando (separadamente do comando para o qual eles apontam)

A partir do ONTAP 9, você pode transmitir os logs de auditoria de forma segura para destinos externos usando os protocolos TCP e TLS.

## Exibir conteúdo do log de auditoria

Você pode exibir o conteúdo dos arquivos do cluster `/mroot/etc/log/mlog/audit.log` usando a CLI do ONTAP, o Gerenciador de sistema ou um navegador da Web.

As entradas do arquivo de log do cluster incluem o seguinte:

### Tempo

O carimbo de data/hora da entrada de registro.

### Aplicação

A aplicação utilizada para ligar ao cluster. Exemplos de valores possíveis são `internal`, `console`, `ssh`, `http`, `ontapi`, `snmp rsh`, `telnet` e `service-processor`.

### Utilizador

O nome de utilizador do utilizador remoto.

### Estado

O estado atual da solicitação de auditoria, que pode ser `success`, `pending` ou `error`.

### Mensagem

Um campo opcional que pode conter erro ou informações adicionais sobre o status de um comando.

### Session ID

O Session ID no qual o pedido é recebido. Cada SSH *session* recebe um Session ID, enquanto cada HTTP, ONTAPI ou SNMP *Request* recebe um Session ID exclusivo.

### Armazenamento VM

O SVM por meio do qual o usuário se conectou.

### Âmbito de aplicação

É exibido `svm` quando a solicitação está em uma VM de armazenamento de dados; caso contrário, exibe `cluster`.

### ID do comando

O ID de cada comando recebido em uma sessão CLI. Isso permite correlacionar uma solicitação e uma resposta. As solicitações ZAPI, HTTP e SNMP não têm IDs de comando.

Você pode exibir as entradas de log do cluster a partir da CLI do ONTAP, de um navegador da Web e, começando com ONTAP 9.11.1, do Gerenciador do sistema.

### System Manager

- Para exibir o inventário, selecione **Eventos e trabalhos > Logs de auditoria**. Cada coluna tem controles para filtrar, classificar, pesquisar, mostrar e categorias de inventário. Os detalhes do inventário podem ser baixados como uma pasta de trabalho do Excel.
- Para definir filtros, clique no botão **filtro** no canto superior direito e selecione os campos desejados. Você também pode visualizar todos os comandos executados na sessão em que ocorreu uma falha clicando no link Session ID.

### CLI

Para exibir entradas de auditoria mescladas de vários nós no cluster, digite `security audit log show <[parameters]>`

Você pode usar o `security audit log show` comando para exibir entradas de auditoria para nós individuais ou mesclados de vários nós no cluster. Você também pode exibir o conteúdo do `/mroot/etc/log/mlog` diretório em um único nó usando um navegador da Web. Consulte a página de manual para obter detalhes.

### Navegador da Web


Você pode exibir o conteúdo do `/mroot/etc/log/mlog` diretório em um único nó usando um navegador da Web. ["Saiba mais sobre como acessar os arquivos de log, despejo de memória e MIB de um nó usando um navegador da Web"](#).

## Gerenciar as configurações de solicitação DE auditoria

Embora as SOLICITAÇÕES DE CONJUNTO sejam registradas por padrão, as SOLICITAÇÕES DE OBTENÇÃO não são. No entanto, você pode controlar se as solicitações GET enviadas do ONTAP HTML (`-httpget`), da CLI do ONTAP (`-cliget`) ou das APIs do ONTAP (`-ontapiget`) estão registradas no arquivo.

Você pode modificar as configurações de log de auditoria a partir da CLI do ONTAP e, a partir do ONTAP 9.11.1, do Gerenciador do sistema.

## System Manager

1. Selecione **Eventos e trabalhos > Registos de auditoria**.
2. Clique  no canto superior direito e escolha as solicitações a serem adicionadas ou removidas.

## CLI

- Para especificar que AS SOLICITAÇÕES GET da CLI ou APIs do ONTAP devem ser registradas no log de auditoria (o arquivo audit.log), além das solicitações de conjunto padrão, digite `security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]`
- Para visualizar as definições atuais, introduza `security audit show`

Consulte as páginas de manual para obter detalhes.

## Gerenciar destinos de log de auditoria

Você pode encaminhar o log de auditoria para um máximo de 10 destinos. Por exemplo, você pode encaminhar o log para um servidor Splunk ou syslog para fins de monitoramento, análise ou backup.

### Sobre esta tarefa

Para configurar o encaminhamento, você deve fornecer o endereço IP do host syslog ou Splunk, seu número de porta, um protocolo de transmissão e a facilidade syslog para usar nos logs encaminhados. ["Saiba mais sobre as instalações do syslog"](#).

Pode selecionar um dos seguintes valores de transmissão utilizando o `-protocol` parâmetro:

### UDP não encriptado

Protocolo de datagrama de usuário sem segurança (padrão)

### TCP não criptografado

Protocolo de controlo da transmissão sem segurança

### TCP criptografado

Protocolo de controle de transmissão com TLS (Transport Layer Security) e opção **Verify Server** está disponível quando o protocolo criptografado TCP é selecionado.

A porta padrão é 514 para UDP e 6514 para TCP, mas você pode designar qualquer porta que atenda às necessidades de sua rede.

Você pode selecionar um dos seguintes formatos de mensagem usando o `-message-format` comando:

### legacy-NetApp

Uma variação do formato RFC-3164 Syslog (formato: <PRIVAL>)




### rfc-5424

Formato syslog de acordo com RFC-5424 (formato: <PRIVAL>)

Você pode encaminhar logs de auditoria da CLI do ONTAP e, a partir do ONTAP 9.11.1, do Gerenciador de

sistemas.

## System Manager

- Para exibir destinos de log de auditoria, selecione **Cluster >Settings**. Uma contagem de destinos de log é mostrada no bloco **Notification Management**. Clique  para mostrar detalhes.
- Para adicionar, modificar ou eliminar destinos de registro de auditoria, selecione **Eventos e trabalhos > Registros de auditoria** e, em seguida, clique em **gerir destinos de auditoria** no canto superior direito do ecrã. Clique  **Add** em ou clique  na coluna **Endereço do host** para editar ou excluir entradas.

## CLI

1. Para cada destino para o qual você deseja encaminhar o log de auditoria, especifique o endereço IP de destino ou o nome do host e quaisquer opções de segurança.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 6514 -protocol tcp-encrypted -facility user
```

- Se o `cluster log-forwarding create` comando não puder fazer ping no host de destino para verificar a conectividade, o comando falhará com um erro. Embora não seja recomendado, usar o `-force` parâmetro com o comando ignora a verificação de conectividade.
  - Quando você define o `-verify-server` parâmetro como `true`, a identidade do destino de encaminhamento de log é verificada validando seu certificado. Pode definir o valor `true` apenas quando selecionar o `tcp-encrypted` valor no `-protocol` campo.
2. Verifique se os Registros de destino estão corretos usando o `cluster log-forwarding show` comando.

```
cluster1::> cluster log-forwarding show

Destination Host          Port    Protocol          Verify Syslog
-----
192.168.123.96           514    udp-unencrypted  false  user
192.168.123.98           6514   tcp-encrypted   true   user
2 entries were displayed.
```

Consulte a `cluster log-forwarding create` página de manual para obter detalhes.

# AutoSupport

## Saiba mais sobre o AutoSupport

### Sobre o AutoSupport

O AutoSupport é um mecanismo que monitora proativamente a integridade do sistema e envia mensagens automaticamente para o suporte técnico da NetApp, sua organização de suporte interno e um parceiro de suporte. Embora as mensagens do AutoSupport para suporte técnico estejam habilitadas por padrão, você deve definir as opções corretas e ter um host de e-mail válido para que as mensagens sejam enviadas para sua organização interna de suporte.

Somente o administrador do cluster pode executar o gerenciamento do AutoSupport. O administrador da máquina virtual de storage (SVM) não tem acesso ao AutoSupport.

O AutoSupport é ativado por padrão quando você configura o sistema de storage pela primeira vez. O AutoSupport começa a enviar mensagens para o suporte técnico 24 horas após a ativação do AutoSupport. Você pode encurtar o período de 24 horas atualizando ou revertendo o sistema, modificando a configuração do AutoSupport ou alterando o tempo do sistema para ser algo diferente de um período de 24 horas.



Você pode desativar o AutoSupport a qualquer momento, mas deve deixá-lo habilitado. A ativação do AutoSupport pode ajudar a acelerar significativamente a determinação e a resolução de problemas em caso de problema no sistema de storage. Por padrão, o sistema coleta informações do AutoSupport e as armazena localmente, mesmo que você desative o AutoSupport.

Para obter mais informações sobre o AutoSupport, consulte o site de suporte da NetApp.

### Informações relacionadas

- ["Suporte à NetApp"](#)
- ["Referência do comando ONTAP"](#)

### Sobre o consultor digital e o AutoSupport

O componente AutoSupport do ONTAP coleta telemetria e envia-a para análise. O consultor digital analisa os dados do AutoSupport e fornece cuidado e otimização proativos. Usando inteligência artificial, o Digital Advisor pode identificar possíveis problemas e ajudá-lo a resolvê-los antes que eles afetem seu negócio.

O Digital Advisor permite otimizar sua infraestrutura de dados em toda a nuvem híbrida global, fornecendo análises preditivas práticas e suporte proativo por meio de um portal baseado na nuvem e aplicativo móvel. Insights e recomendações orientados por dados do consultor digital estão disponíveis para todos os clientes da NetApp com um contrato de SupportEdge ativo (os recursos variam de acordo com o produto e a camada de suporte).

Aqui estão algumas coisas que você pode fazer com o Digital Advisor:

- Planejar atualizações. O consultor digital identifica problemas no seu ambiente que podem ser resolvidos ao atualizar para uma versão mais recente do ONTAP e o componente do consultor de atualização ajuda

você a Planejar uma atualização bem-sucedida.

- Veja o bem-estar do sistema. Seu painel do Digital Advisor relata quaisquer problemas de bem-estar e ajuda você a corrigir esses problemas. Monitore a capacidade do sistema para garantir que você nunca fique sem espaço de armazenamento. Veja casos de suporte para o seu sistema.
- Gerenciar a performance. O Digital Advisor mostra o desempenho do sistema por um período mais longo do que você pode ver no System Manager. Identifique problemas de configuração e sistema que estejam afetando a performance.
- Maximizar a eficiência: Visualize as métricas de eficiência de storage e identifique maneiras de armazenar mais dados em menos espaço.
- Ver inventário e configuração. O Digital Advisor exibe o inventário completo e as informações de configuração de software e hardware. Veja quando os contratos de serviço estão expirando e renove-os para garantir que você permaneça suportado.

### Informações relacionadas

["Documentação do NetApp: Consultor digital"](#)

["Inicie o Digital Advisor"](#)

["Serviços da SupportEdge"](#)

### Quando e onde as mensagens AutoSupport são enviadas

O AutoSupport envia mensagens para diferentes destinatários, dependendo do tipo de mensagem. Aprender quando e onde o AutoSupport envia mensagens pode ajudá-lo a entender as mensagens que você recebe por e-mail ou exibição no site do consultor digital.

Salvo especificação em contrário, as configurações nas tabelas a seguir são parâmetros do `system node autosupport modify` comando.

#### Mensagens acionadas por eventos

Quando ocorrem eventos no sistema que exigem ação corretiva, o AutoSupport envia automaticamente uma mensagem acionada por evento.

Quando a mensagem é enviada	Onde a mensagem é enviada
O AutoSupport responde a um evento de ativação no EMS	Endereços especificados em <code>-to</code> e <code>-noteto</code> . (Apenas eventos críticos que afetam o serviço são enviados.)  Endereços especificados em <code>-partner-address</code>  Suporte técnico, se <code>-support</code> estiver definido como <code>enable</code>

#### Mensagens agendadas

O AutoSupport envia automaticamente várias mensagens em um horário regular.

<b>Quando a mensagem é enviada</b>	<b>Onde a mensagem é enviada</b>
Diariamente (por padrão, enviado entre as 12:00h e as 1:00h como uma mensagem de log)	Endereços especificados em <code>-partner-address</code>  Suporte técnico, se <code>-support</code> estiver definido como <code>enable</code>
Diariamente (por padrão, enviado entre 12:00 e 1:00 como uma mensagem de desempenho), se o <code>-perf</code> parâmetro estiver definido como <code>true</code>	Endereços especificados no endereço <code>-parceiro»</code>  Suporte técnico, se <code>-support</code> estiver definido como <code>enable</code>
Semanal (por padrão, enviado domingo entre as 12:00h e as 1:00h)	Endereços especificados em <code>-partner-address</code>  Suporte técnico, se <code>-support</code> estiver definido como <code>enable</code>

### Mensagens acionadas manualmente

Você pode iniciar ou reenviar manualmente uma mensagem do AutoSupport.

<b>Quando a mensagem é enviada</b>	<b>Onde a mensagem é enviada</b>
Você inicia manualmente uma mensagem usando o <code>system node autosupport invoke</code> comando	Se um URI for especificado usando o <code>-uri</code> parâmetro no <code>system node autosupport invoke</code> comando, a mensagem será enviada para esse URI.  Se <code>-uri</code> for omitido, a mensagem é enviada para os endereços especificados em <code>-to</code> e <code>-partner-address</code> . A mensagem também é enviada para o suporte técnico se <code>-support</code> estiver definido como <code>enable</code> .

Quando a mensagem é enviada	Onde a mensagem é enviada
<p>Você inicia manualmente uma mensagem usando o <code>system node autosupport invoke-core-upload</code> comando</p>	<p>Se um URI é especificado usando o <code>-uri</code> parâmetro no <code>system node autosupport invoke-core-upload</code> comando, a mensagem é enviada para esse URI, e o arquivo de despejo do núcleo é carregado para o URI.</p> <p>Se <code>-uri</code> for omitido <code>system node autosupport invoke-core-upload</code> no comando, a mensagem é enviada para o suporte técnico e o arquivo de despejo do núcleo é enviado para o site de suporte técnico.</p> <p>Ambos os cenários requerem que <code>-support</code> esteja definido como <code>enable</code> e <code>-transport</code> definido como <code>https</code> ou <code>http</code>.</p> <p>Devido ao grande tamanho dos arquivos de despejo de núcleo, a mensagem não é enviada para os endereços especificados nos <code>-to</code> parâmetros e <code>-partner-addresses</code></p>
<p>Você inicia manualmente uma mensagem usando o <code>system node autosupport invoke-performance-archive</code> comando</p>	<p>Se um URI for especificado usando o <code>-uri</code> parâmetro no <code>system node autosupport invoke-performance-archive</code> comando, a mensagem será enviada para esse URI e o arquivo de desempenho será carregado para o URI.</p> <p>Se <code>-uri</code> for omitido <code>system node autosupport invoke-performance-archive</code> no , a mensagem será enviada para o suporte técnico e o arquivo de desempenho será carregado no site de suporte técnico.</p> <p>Ambos os cenários requerem que <code>-support</code> esteja definido como <code>enable</code> e <code>-transport</code> definido como <code>https</code> ou <code>http</code>.</p> <p>Devido ao grande tamanho dos arquivos de arquivamento de desempenho, a mensagem não é enviada para os endereços especificados nos <code>-to</code> parâmetros e <code>-partner-addresses</code></p>
<p>Você reenvia manualmente uma mensagem passada usando o <code>system node autosupport history retransmit</code> comando</p>	<p>Apenas para o URI que você especificar no <code>-uri</code> parâmetro do <code>system node autosupport history retransmit</code> comando</p>



## Mensagens acionadas pelo suporte técnico

O suporte técnico pode solicitar mensagens do AutoSupport usando o recurso AutoSupport OnDemand.

Quando a mensagem é enviada	Onde a mensagem é enviada
Quando o AutoSupport obtém instruções de entrega para gerar novas mensagens AutoSupport	Endereços especificados em <code>-partner-address</code>  Suporte técnico, se <code>-support</code> estiver definido como <code>enable</code> e <code>-transport</code> estiver definido como <code>https</code>
Quando o AutoSupport obtém instruções de entrega para reenviar mensagens passadas do AutoSupport	Suporte técnico, se <code>-support</code> estiver definido como <code>enable</code> e <code>-transport</code> estiver definido como <code>https</code>
Quando o AutoSupport obtém instruções de entrega para gerar novas mensagens AutoSupport que carregam arquivos de despejo de memória ou arquivo de desempenho	Suporte técnico, se <code>-support</code> estiver definido como <code>enable</code> e <code>-transport</code> estiver definido como <code>https</code> . O despejo de memória ou arquivo de desempenho é carregado para o site de suporte técnico.

## Como o AutoSupport cria e envia mensagens acionadas por eventos

O AutoSupport cria mensagens AutoSupport acionadas por eventos quando o EMS processa um evento de acionamento. Uma mensagem do AutoSupport acionada por evento alerta os destinatários para problemas que exigem ação corretiva e contém apenas informações relevantes para o problema. Você pode personalizar o conteúdo a incluir e quem recebe as mensagens.

O AutoSupport usa o seguinte processo para criar e enviar mensagens AutoSupport acionadas por eventos:

1. Quando o EMS processa um evento de ativação, o EMS envia um pedido ao AutoSupport.

Um evento de gatilho é um evento EMS com um destino AutoSupport e um nome que começa com um `callhome.` prefixo.

2. O AutoSupport cria uma mensagem AutoSupport acionada por evento.

O AutoSupport coleta informações básicas e de solução de problemas de subsistemas associados ao gatilho para criar uma mensagem que inclua apenas informações relevantes para o evento de acionamento.

Um conjunto padrão de subsistemas é associado a cada gatilho. No entanto, você pode optar por associar subsistemas adicionais a um gatilho usando o `system node autosupport trigger modify` comando.

3. O AutoSupport envia a mensagem AutoSupport acionada por evento aos destinatários definidos pelo `system node autosupport modify` comando com os `-to` parâmetros, `-noteto`, `-partner-address` e `-support`

Você pode ativar e desativar a entrega de mensagens do AutoSupport para gatilhos específicos usando o `system node autosupport trigger modify` comando com os `-to` parâmetros e `-noteto`

### Exemplo de dados enviados para um evento específico

O `storage shelf PSU failed` evento EMS aciona uma mensagem que contém dados básicos dos subsistemas obrigatório, arquivos de log, armazenamento, RAID, HA, Plataforma e rede e dados de solução de problemas dos subsistemas obrigatório, arquivos de log e armazenamento.

Você decide que deseja incluir dados sobre NFS em qualquer mensagem do AutoSupport enviada em resposta a um evento futuro `storage shelf PSU failed`. Digite o seguinte comando para habilitar dados em nível de solução de problemas para NFS para `callhome.shlf.ps.fault` o evento:

```
cluster1::\>
system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

Observe que o `callhome.` prefixo é descartado do `callhome.shlf.ps.fault` evento quando você usa os `system node autosupport trigger` comandos, ou quando referenciado por eventos AutoSupport e EMS na CLI.

### Tipos de mensagens AutoSupport e seu conteúdo

As mensagens AutoSupport contêm informações de status sobre subsistemas suportados. Aprender o que as mensagens do AutoSupport contêm pode ajudá-lo a interpretar ou responder às mensagens que você recebe em e-mail ou exibição no site do consultor digital.

Tipo de mensagem	Tipo de dados que a mensagem contém
Acionado por evento	Arquivos contendo dados sensíveis ao contexto sobre o subsistema específico em que o evento ocorreu
Diariamente	Ficheiros de registo
Desempenho	Dados de desempenho amostrados durante as 24 horas anteriores
Semanalmente	Dados de configuração e status

Tipo de mensagem	Tipo de dados que a mensagem contém
<p>Acionado pelo <code>system node autosupport invoke</code> comando</p>	<p>Depende do valor especificado no <code>-type</code> parâmetro:</p> <ul style="list-style-type: none"> <li>• <code>test</code> envia uma mensagem acionada pelo usuário com alguns dados básicos.</li> </ul> <p>Essa mensagem também aciona uma resposta automática de e-mail do suporte técnico para qualquer endereço de e-mail especificado, usando a <code>-to</code> opção, para que você possa confirmar que as mensagens do AutoSupport estão sendo recebidas.</p> <ul style="list-style-type: none"> <li>• <code>performance</code> envia dados de desempenho.</li> <li>• <code>all</code> envia uma mensagem acionada pelo usuário com um conjunto completo de dados semelhante à mensagem semanal, incluindo dados de solução de problemas de cada subsistema.</li> </ul> <p>O suporte técnico normalmente solicita essa mensagem.</p>
<p>Acionado pelo <code>system node autosupport invoke-core-upload</code> comando</p>	<p>Arquivos de despejo de núcleo para um nó</p>
<p>Acionado pelo <code>system node autosupport invoke-performance-archive</code> comando</p>	<p>Arquivos de arquivamento de desempenho por um período de tempo especificado</p>
<p>Acionado por AutoSupport OnDemand</p>	<p>O AutoSupport OnDemand pode solicitar novas mensagens ou mensagens anteriores:</p> <ul style="list-style-type: none"> <li>• As novas mensagens, dependendo do tipo de coleção AutoSupport, podem ser <code>test</code>, <code>all</code> ou <code>performance</code>.</li> <li>• As mensagens anteriores dependem do tipo de mensagem que é reenviada.</li> </ul> <p>O AutoSupport OnDemand pode solicitar novas mensagens que carreguem os seguintes arquivos para o site de suporte da NetApp em "<a href="https://mysupport.netapp.com">mysupport.NetApp.com</a>":</p> <ul style="list-style-type: none"> <li>• Despejo de memória</li> <li>• Arquivamento de performance</li> </ul>

### Ver subsistemas AutoSupport

Cada subsistema fornece informações básicas e de solução de problemas que o

AutoSupport usa para suas mensagens. Cada subsistema também está associado a eventos de gatilho que permitem que o AutoSupport colete apenas informações relevantes para o evento de acionamento.

O AutoSupport coleta conteúdo sensível ao contexto.

### Passos

1. Exibir informações sobre subsistemas e eventos de acionamento:

```
system node autosupport trigger show
```

### Orçamentos de tamanho e tempo da AutoSupport

O AutoSupport coleta informações, organizadas por subsistema, e impõe um orçamento de tamanho e tempo para o conteúdo de cada subsistema. À medida que os sistemas de storage crescem, os orçamentos da AutoSupport fornecem controle sobre a carga útil da AutoSupport, que por sua vez fornece entrega dimensionável de dados da AutoSupport.

O AutoSupport pára de coletar informações e trunca o conteúdo do AutoSupport se o conteúdo do subsistema exceder seu tamanho ou orçamento de tempo. Se o conteúdo não puder ser truncado facilmente (por exemplo, arquivos binários), o AutoSupport omite o conteúdo.

Você deve modificar o tamanho padrão e os orçamentos de tempo somente se solicitado pelo suporte da NetApp. Você também pode revisar o tamanho padrão e os orçamentos de tempo dos subsistemas usando o `autosupport manifest show` comando.

### Arquivos enviados em mensagens AutoSupport acionadas por evento

As mensagens AutoSupport acionadas por evento contêm apenas informações básicas e de solução de problemas de subsistemas associados ao evento que fez com que o AutoSupport gerasse a mensagem. Os dados específicos ajudam os parceiros de suporte e suporte da NetApp a solucionar o problema.

O AutoSupport usa os seguintes critérios para controlar o conteúdo em mensagens AutoSupport acionadas por evento:

- Quais subsistemas estão incluídos

Os dados são agrupados em subsistemas, incluindo subsistemas comuns, como arquivos de log e subsistemas específicos, como RAID. Cada evento aciona uma mensagem que contém apenas os dados de subsistemas específicos.

- O nível de detalhe de cada subsistema incluído

Os dados para cada subsistema incluído são fornecidos em um nível básico ou de solução de problemas.

Você pode visualizar todos os eventos possíveis e determinar quais subsistemas estão incluídos nas mensagens sobre cada evento usando o `system node autosupport trigger show` comando com o `-instance` parâmetro.

Além dos subsistemas que são incluídos por padrão para cada evento, você pode adicionar subsistemas adicionais em um nível básico ou de solução de problemas usando o `system node autosupport trigger modify` comando.

### Arquivos de log enviados em mensagens do AutoSupport

As mensagens do AutoSupport podem conter vários arquivos de log-chave que permitem que a equipe de suporte técnico analise a atividade recente do sistema.

Todos os tipos de mensagens do AutoSupport podem incluir os seguintes arquivos de log quando o subsistema arquivos de log está habilitado:

Ficheiro de registo	Quantidade de dados incluídos no arquivo
<ul style="list-style-type: none"><li>• Arquivos de log do <code>/mroot/etc/log/mlog/</code> diretório</li><li>• O ficheiro de registo DE MENSAGENS</li></ul>	<p>Somente novas linhas adicionadas aos logs desde a última mensagem AutoSupport até um máximo especificado. Isso garante que as mensagens do AutoSupport tenham dados exclusivos e relevantes, não sobrepostos.</p> <p>(Os arquivos de log de parceiros são a exceção; para parceiros, os dados máximos permitidos são incluídos.)</p>
<ul style="list-style-type: none"><li>• Arquivos de log do <code>/mroot/etc/log/shelflog/</code> diretório</li><li>• Arquivos de log do <code>/mroot/etc/log/acp/</code> diretório</li><li>• Dados de registo do sistema de gestão de eventos (EMS)</li></ul>	<p>As linhas de dados mais recentes até um máximo especificado.</p>

O conteúdo das mensagens do AutoSupport pode mudar entre as versões do ONTAP.

### Arquivos enviados em mensagens AutoSupport semanais

As mensagens AutoSupport semanais contêm dados adicionais de configuração e status que são úteis para rastrear alterações no seu sistema ao longo do tempo.

As seguintes informações são enviadas em mensagens AutoSupport semanais:

- Informações básicas sobre cada subsistema
- Conteúdo de arquivos de diretório selecionados `/mroot/etc`
- Ficheiros de registo
- Saída de comandos que fornecem informações do sistema
- Informações adicionais, incluindo informações de banco de dados replicado (RDB), estatísticas de serviço e muito mais

## Como o AutoSupport OnDemand obtém instruções de entrega do suporte técnico

O AutoSupport OnDemand se comunica periodicamente com o suporte técnico para obter instruções de entrega para enviar, reenviar e recusar mensagens AutoSupport, bem como carregar arquivos grandes para o site de suporte da NetApp. O AutoSupport OnDemand permite que as mensagens do AutoSupport sejam enviadas sob demanda em vez de esperar que a tarefa AutoSupport semanal seja executada.

O AutoSupport OnDemand consiste nos seguintes componentes:

- Cliente AutoSupport OnDemand que é executado em cada nó
- Serviço do AutoSupport OnDemand que reside no suporte técnico

O cliente do AutoSupport OnDemand faz periodicamente pesquisas no serviço do AutoSupport OnDemand para obter instruções de entrega do suporte técnico. Por exemplo, o suporte técnico pode usar o serviço OnDemand do AutoSupport para solicitar que uma nova mensagem do AutoSupport seja gerada. Quando o cliente AutoSupport OnDemand executa o serviço AutoSupport OnDemand, o cliente obtém as instruções de entrega e envia a nova mensagem AutoSupport sob demanda conforme solicitado.

O AutoSupport OnDemand está ativado por padrão. No entanto, o AutoSupport OnDemand depende de algumas configurações do AutoSupport para continuar se comunicando com o suporte técnico. O AutoSupport OnDemand se comunica automaticamente com o suporte técnico quando os seguintes requisitos são atendidos:

- O AutoSupport está ativado.
- O AutoSupport está configurado para enviar mensagens ao suporte técnico.
- O AutoSupport está configurado para utilizar o protocolo de transporte HTTPS.

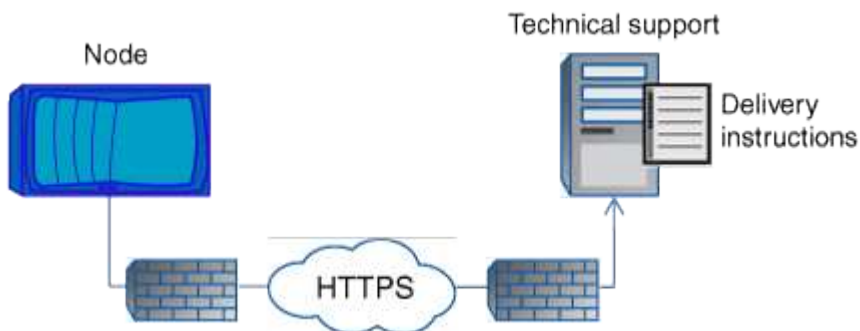
O cliente AutoSupport OnDemand envia solicitações HTTPS para o mesmo local de suporte técnico para o qual as mensagens AutoSupport são enviadas. O cliente AutoSupport OnDemand não aceita conexões de entrada.



O AutoSupport OnDemand usa a conta de usuário "AutoSupport" para se comunicar com o suporte técnico. O ONTAP impede que você exclua essa conta.

Se você quiser desativar o AutoSupport OnDemand, mas manter o AutoSupport habilitado, use o comando `system node autosupport modify -ondemand-state disable`. Saiba mais sobre `system node autosupport modify -ondemand-state disable` no ["Referência do comando ONTAP"](#).

A ilustração a seguir mostra como o AutoSupport OnDemand envia solicitações HTTPS para o suporte técnico para obter instruções de entrega.



As instruções de entrega podem incluir pedidos para que a AutoSupport faça o seguinte:

- Gerar novas mensagens AutoSupport.

O suporte técnico pode solicitar novas mensagens do AutoSupport para ajudar a triagem de problemas.

- Gere novas mensagens do AutoSupport que carregam arquivos de despejo de memória ou arquivos de arquivo de desempenho para o site de suporte do NetApp.

O suporte técnico pode solicitar arquivos de despejo de núcleo ou arquivamento de desempenho para ajudar a triagem de problemas.

- Retransmita mensagens AutoSupport geradas anteriormente.

Esta solicitação acontece automaticamente se uma mensagem não for recebida devido a uma falha de entrega.

- Desative a entrega de mensagens AutoSupport para eventos de gatilho específicos.

O suporte técnico pode desativar a entrega de dados que não são usados.

2024 dez 19, ONTAPDOC-2569

## Estrutura das mensagens AutoSupport enviadas por e-mail

Quando uma mensagem AutoSupport é enviada por e-mail, a mensagem tem um assunto padrão, um corpo breve e um anexo grande em formato de arquivo 7z que contém os dados.



Se o AutoSupport estiver configurado para ocultar dados privados, certas informações, como o nome do host, serão omitidas ou mascaradas no cabeçalho, assunto, corpo e anexos.

### Assunto

A linha de assunto das mensagens enviadas pelo mecanismo AutoSupport contém uma cadeia de texto que identifica o motivo da notificação. O formato da linha de assunto é o seguinte:

Notificação de Grupo HA de *Nome\_do\_sistema (mensagem) gravidade*

- *Nome\_do\_sistema* é o nome do host ou o ID do sistema, dependendo da configuração do AutoSupport

### Corpo

O corpo da mensagem AutoSupport contém as seguintes informações:

- Data e carimbo de data/hora da mensagem
- Versão do ONTAP no nó que gerou a mensagem
- ID do sistema, número de série e nome do host do nó que gerou a mensagem
- Número de sequência AutoSupport
- Nome e localização do contacto SNMP, se especificado
- ID do sistema e nome do host do partnernode HA

## Ficheiros anexados

As informações-chave de uma mensagem AutoSupport estão contidas em arquivos compactados em um arquivo 7z chamado `body.7z` e anexado à mensagem.

Os arquivos contidos no anexo são específicos para o tipo de mensagem AutoSupport.

## Tipos de gravidade do AutoSupport

As mensagens do AutoSupport têm tipos de gravidade que ajudam a entender o propósito de cada mensagem - por exemplo, chamar a atenção imediata para um problema de emergência ou apenas para fornecer informações.

As mensagens têm uma das seguintes gravidades:

- **Alerta:** As mensagens de alerta indicam que um evento de nível superior próximo pode ocorrer se você não tomar alguma ação.

Você deve tomar uma ação contra mensagens de alerta dentro de 24 horas.

- **Emergência:** As mensagens de emergência são exibidas quando ocorre uma interrupção.

Você deve tomar uma ação contra mensagens de emergência imediatamente.

- **Erro:** As condições de erro indicam o que pode acontecer se você ignorar.
- **Aviso:** Condição normal, mas significativa.
- **Info:** A mensagem informativa fornece detalhes sobre o problema, que você pode ignorar.
- **Debug:** Mensagens no nível de depuração fornecem instruções que você deve executar.

Se a organização de suporte interno receber mensagens do AutoSupport por e-mail, a gravidade será exibida na linha de assunto da mensagem de e-mail.

## Obter descrições de mensagens do AutoSupport

As descrições das mensagens do AutoSupport que você recebe estão disponíveis através do Tradutor Syslog do ONTAP.

### Passos

1. Vá para "[Syslog Translator](#)".
2. No campo **Liberção**, insira a versão do ONTAP que você está usando. No campo **Search String**, digite "callhome". Selecione **Traduzir**.
3. O Syslog Translator listará alfabeticamente todos os eventos que correspondem à cadeia de caracteres da mensagem que você inseriu.

## Comandos para gerenciar o AutoSupport

Você usa os `system node autosupport` comandos para alterar ou exibir a configuração do AutoSupport, exibir informações sobre mensagens AutoSupport anteriores e enviar, reenviar ou cancelar uma mensagem do AutoSupport.



## Configurar o AutoSupport

Se você quiser...	Use este comando...
Controle se quaisquer mensagens AutoSupport são enviadas	<code>system node autosupport modify</code> com o <code>-state</code> parâmetro
Controlar se as mensagens AutoSupport são enviadas para o suporte técnico	<code>system node autosupport modify</code> com o <code>-support</code> parâmetro
Configure o AutoSupport ou modifique a configuração do AutoSupport	<code>system node autosupport modify</code>
Ative e desative as mensagens do AutoSupport para sua organização de suporte interno para eventos de acionamento individuais e especifique relatórios de subsistema adicionais a serem incluídos nas mensagens enviadas em resposta a eventos de acionamento individuais	<code>system node autosupport trigger modify</code>

## Exibir informações sobre a configuração do AutoSupport



Se você quiser...	Use este comando...
Apresentar a configuração do AutoSupport	<code>system node autosupport show</code> com o <code>-node</code> parâmetro
Veja um resumo de todos os endereços e URLs que recebem mensagens do AutoSupport	<code>system node autosupport destinations show</code>
Exiba quais mensagens do AutoSupport são enviadas para sua organização interna de suporte para eventos de acionamento individuais	<code>system node autosupport trigger show</code>
Apresentar o estado da configuração do AutoSupport, bem como a entrega para vários destinos	<code>system node autosupport check show</code>
Apresentar o estado detalhado da configuração do AutoSupport, bem como a entrega para vários destinos	<code>system node autosupport check show-details</code>

## Exibir informações sobre mensagens anteriores do AutoSupport

Se você quiser...	Use este comando...
Exiba informações sobre uma ou mais das 50 mensagens AutoSupport mais recentes	<code>system node autosupport history show</code>

Se você quiser...	Use este comando...
Exiba informações sobre mensagens recentes do AutoSupport geradas para carregar arquivos de despejo de memória ou arquivamento de desempenho para o site de suporte técnico ou um URI especificado	<code>system node autosupport history show-upload-details</code>
Visualize as informações nas mensagens do AutoSupport, incluindo o nome e o tamanho de cada arquivo coletado para a mensagem, juntamente com quaisquer erros	<code>system node autosupport manifest show</code>

### Enviar, reenviar ou cancelar mensagens AutoSupport

Se você quiser...	Use este comando...
<p>Retransmita uma mensagem AutoSupport armazenada localmente, identificada pelo seu número de sequência AutoSupport</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  <p>Se você retransmitir uma mensagem do AutoSupport e se o suporte já recebeu essa mensagem, o sistema de suporte não criará um caso duplicado. Se, por outro lado, o suporte não recebeu essa mensagem, o sistema AutoSupport analisará a mensagem e criará um caso, se necessário.</p> </div>	<pre>system node autosupport history retransmit</pre>
<p>Gerar e enviar uma mensagem AutoSupport - por exemplo, para fins de teste</p>	<pre>system node autosupport invoke</pre> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  <p>Use o <code>-force</code> parâmetro para enviar uma mensagem mesmo que o AutoSupport esteja desativado. Use o <code>-uri</code> parâmetro para enviar a mensagem para o destino especificado em vez do destino configurado.</p> </div>
<p>Cancelar uma mensagem AutoSupport</p>	<pre>system node autosupport history cancel</pre>

### Informações relacionadas

["Referência do comando ONTAP"](#)

### Informações incluídas no manifesto AutoSupport

O manifesto do AutoSupport fornece uma visualização detalhada dos arquivos coletados para cada mensagem do AutoSupport. O manifesto AutoSupport também inclui informações sobre erros de coleta quando o AutoSupport não consegue coletar os

arquivos de que ele precisa.

O manifesto AutoSupport inclui as seguintes informações:

- Número de sequência da mensagem AutoSupport
- Quais arquivos AutoSupport incluídos na mensagem AutoSupport
- Tamanho de cada arquivo, em bytes
- Status da coleção de manifesto do AutoSupport
- Descrição do erro, se o AutoSupport não conseguir recolher um ou mais ficheiros

Você pode exibir o manifesto do AutoSupport usando o `system node autosupport manifest show` comando.

O manifesto do AutoSupport é incluído com todas as mensagens do AutoSupport e apresentado em formato XML, o que significa que você pode usar um visualizador XML genérico para lê-lo ou visualizá-lo usando o portal do Consultor Digital.

## Plano

### Prepare-se para usar o AutoSupport

Você pode configurar um cluster do ONTAP para entregar mensagens do AutoSupport ao NetApp. Como parte disso, você também pode enviar uma cópia das mensagens para endereços de e-mail locais, normalmente dentro da sua organização. Você deve se preparar para configurar o AutoSupport revisando as opções disponíveis.

### Entregar mensagens AutoSupport ao NetApp

As mensagens AutoSupport podem ser entregues ao NetApp usando protocolos HTTPS ou SMTP. Começando com ONTAP 9.15,1, você também pode usar TLS com SMTP.



Use HTTPS sempre que possível para comunicação com o AutoSupport OnDemand e upload de arquivos grandes.

Observe também o seguinte:

- Apenas um canal de entrega ao NetApp pode ser configurado para as mensagens AutoSupport. Não é possível usar dois protocolos para entregar mensagens AutoSupport ao NetApp.
- O AutoSupport limita o tamanho máximo do arquivo para cada protocolo. Se o tamanho de uma mensagem AutoSupport exceder o limite configurado, o AutoSupport entrega o máximo possível da mensagem, mas ocorrerá truncamento.
- Você pode alterar o tamanho máximo do arquivo, se necessário. Saiba mais sobre o `system node autosupport modify` comando ONTAP na referência de comando.
- Ambos os protocolos podem ser transportados em IPv4 ou IPv6 com base na família de endereços para a qual o nome resolve.
- A conexão TCP estabelecida pelo ONTAP para enviar mensagens AutoSupport é temporária e de curta duração.

## HTTPS

Isso fornece os recursos mais robustos. Observe o seguinte:

- O AutoSupport OnDemand e a transferência de arquivos grandes são suportados.
- Uma solicitação HTTPS PUT é tentada primeiro. Se a solicitação falhar durante a transmissão, a solicitação será reiniciada onde ela parou.
- Se o servidor não suportar PUT, o método HTTPS POST é usado.
- O limite padrão para transferências HTTPS é de 50 MB.
- O protocolo HTTPS utiliza a porta 443.

## SMTP

Como regra geral, você deve usar SMTP somente se HTTPS não for permitido ou não for suportado. Observe o seguinte:

- O AutoSupport OnDemand e as transferências de arquivos grandes não são suportadas.
- Se as credenciais de login SMTP estiverem configuradas, elas serão enviadas sem criptografia e na opção Limpar.
- O limite padrão para transferências é de 5 MB.
- O protocolo SMTP não protegido usa a porta 25.

### Melhore a segurança SMTP com TLS

Ao usar SMTP, todo o tráfego é descriptografado e pode ser facilmente interceptado e lido. Começando com ONTAP 9.15,1 você também pode usar TLS com SMTP (SMTPS). Neste caso, *explícito TLS* é usado que ativa o canal seguro após a conexão TCP ser estabelecida.

A seguinte porta é normalmente utilizada para SMTPS: Porta 587

### Considerações de configuração adicionais

Há algumas considerações adicionais ao configurar o AutoSupport.

Para obter mais informações sobre os comandos relevantes para estas considerações, "[Configure o AutoSupport](#)" consulte .

### Envie uma cópia local usando e-mail

Independentemente do protocolo usado para entregar mensagens AutoSupport ao NetApp, você também pode enviar uma cópia de cada mensagem para um ou mais endereços de e-mail locais. Por exemplo, você pode enviar mensagens para sua organização interna de suporte ou uma organização parceira.



Se você entregar mensagens para o NetApp usando SMTP (ou SMTPS) e enviar cópias de e-mail locais dessas mensagens, a mesma configuração do servidor de e-mail será usada.

### Proxy HTTP

Dependendo da configuração da rede, o protocolo HTTPS pode exigir configuração adicional de um URL de proxy. Se o HTTPS for usado para enviar mensagens do AutoSupport para o suporte técnico e você tiver um proxy, você deverá identificar o URL do proxy. Se o proxy usar uma porta diferente da padrão (porta 3128), você poderá especificar a porta para esse proxy. Você também pode especificar opcionalmente um nome de

usuário e senha para autenticação de proxy.

### **Instale o certificado do servidor**

Com TLS (HTTPS ou SMTPS), o certificado baixado do servidor é validado pelo ONTAP com base no certificado CA raiz. Antes de usar HTTPS ou SMTPS, você precisa garantir que o certificado raiz esteja instalado no ONTAP e que o ONTAP possa validar o certificado do servidor. Essa validação é realizada com base na CA que assinou o certificado do servidor.

O ONTAP inclui um grande número de certificados de CA raiz pré-instalados. Em muitos casos, o certificado para o seu servidor será imediatamente reconhecido pelo ONTAP sem configuração adicional. Dependendo de como o certificado do servidor foi assinado, talvez seja necessário instalar um certificado de CA raiz e quaisquer certificados intermediários.

Use o procedimento a seguir para instalar o certificado, se necessário. Você deve instalar todos os certificados necessários no nível do cluster.

## Exemplo 1. Passos

### System Manager

1. No System Manager, selecione **Cluster > Settings**.
2. Role para baixo até a seção **Segurança**.
3. Selecione **→** ao lado de **certificados**.
4. Na guia **autoridades de certificação confiáveis**, clique em **Adicionar**.
5. Clique em **Importar** e selecione o arquivo de certificado.
6. Complete os parâmetros de configuração para o seu ambiente.
7. Clique em **Add**.

### CLI

1. Inicie a instalação:

```
security certificate install -type server-ca
```

2. Procure a seguinte mensagem do console:

```
Please enter Certificate: Press <Enter> when done
```

3. Abra o arquivo de certificado com um editor de texto.
4. Copie o certificado inteiro, incluindo as seguintes linhas:

```
-----BEGIN CERTIFICATE-----
```

```
-----END CERTIFICATE-----
```

5. Cole o certificado no terminal após o prompt de comando.
6. Pressione **Enter** para concluir a instalação.
7. Confirme se o certificado está instalado executando um dos seguintes comandos:

```
security certificate show-user-installed
```

```
security certificate show
```

### Informações relacionadas

- ["Configure o AutoSupport"](#)

## Configure o AutoSupport

Você pode configurar um cluster do ONTAP para entregar mensagens do AutoSupport ao suporte técnico da NetApp e enviar cópias de e-mail para sua organização de suporte interno. Como parte disso, você também pode testar a configuração antes de usá-la em um ambiente de produção.

### Sobre esta tarefa

A partir do ONTAP 9.5, você ativa e configura o AutoSupport para todos os nós de um cluster simultaneamente. Quando um novo nó entra no cluster, o nó herda automaticamente a mesma configuração do AutoSupport. Para dar suporte a isso, o escopo do comando CLI `system node autosupport modify` é no nível do cluster. A `-node` opção de comando é mantida para compatibilidade com versões anteriores, mas é ignorada.



No ONTAP 9.4 e versões anteriores, o comando `system node autosupport modify` é específico para cada nó. Se o cluster estiver executando o ONTAP 9.4 ou anterior, será necessário habilitar e configurar o AutoSupport em cada nó do cluster.

### Antes de começar

A configuração de transporte recomendada para entregar mensagens AutoSupport para o NetApp é HTTPS (HTTP com TLS). Esta opção fornece os recursos mais robustos e a melhor segurança.

Consulte "[Prepare-se para usar o AutoSupport](#)" para obter mais informações antes de configurar o cluster do ONTAP.

### Passos

1. Certifique-se de que o AutoSupport está ativado:

```
system node autosupport modify -state enable
```

2. Se você quiser que o suporte técnico da NetApp receba mensagens do AutoSupport, use o seguinte comando:

```
system node autosupport modify -support enable
```

Você deve habilitar essa opção se quiser habilitar o AutoSupport para trabalhar com o AutoSupport OnDemand ou se quiser fazer upload de arquivos grandes, como arquivos de despejo de núcleo e arquivamento de desempenho, para suporte técnico ou um URL especificado.



O AutoSupport OnDemand é ativado por padrão e funcional quando configurado para enviar mensagens para suporte técnico usando o protocolo de transporte HTTPS.

3. Se você tiver habilitado o suporte técnico do NetApp para receber mensagens do AutoSupport, especifique qual protocolo de transporte usar para essas mensagens.

Você pode escolher entre as seguintes opções:

Se você quiser...	Em seguida, defina os seguintes parâmetros <code>system node autosupport modify</code> do comando...
Utilize o protocolo HTTPS predefinido	<p>a. Defina <code>-transport</code> para <code>https</code>.</p> <p>b. Se você usar um proxy, defina <code>-proxy-url</code> o URL do seu proxy. Esta configuração suporta a comunicação com o AutoSupport OnDemand e carregamentos de ficheiros grandes.</p>
Utilize SMTP	<p>Defina <code>-transport</code> para <code>smtp</code>.</p> <p>Esta configuração não suporta o AutoSupport OnDemand ou carregamentos de ficheiros grandes.</p>

4. Se você quiser que sua organização de suporte interna ou um parceiro de suporte recebam mensagens do AutoSupport, execute as seguintes ações:

a. Identifique os destinatários em sua organização definindo os seguintes parâmetros `system node autosupport modify` do comando:

Definir este parâmetro...	Para isso...
<code>-to</code>	Até cinco endereços de e-mail individuais separados por vírgulas ou listas de distribuição em sua organização de suporte interno que receberão as principais mensagens do AutoSupport
<code>-noteto</code>	Até cinco endereços de e-mail individuais separados por vírgulas ou listas de distribuição em sua organização de suporte interno que receberão uma versão abreviada das principais mensagens AutoSupport projetadas para telefones celulares e outros dispositivos móveis
<code>-partner-address</code>	Até cinco endereços de e-mail individuais separados por vírgulas ou listas de distribuição na sua organização de parceiros de suporte que receberão todas as mensagens do AutoSupport

b. Verifique se os endereços estão corretamente configurados listando os destinos usando o `system node autosupport destinations show` comando.

5. Se você configurou os endereços de destinatário para sua organização de suporte interno na etapa anterior ou escolheu o transporte SMTP para mensagens para suporte técnico, configure o SMTP definindo os seguintes parâmetros `system node autosupport modify` do comando:

◦ Defina `-mail-hosts` como um ou mais hosts de e-mail, separados por vírgulas.

Você pode definir um máximo de cinco.



Você pode configurar um valor de porta para cada host de e-mail especificando dois pontos e um número de porta após o nome do host de e-mail: Por exemplo, `mymailhost.example.com:5678`, onde 5678 é a porta para o host de e-mail.

- Defina `-from` para o endereço de e-mail que envia a mensagem AutoSupport.

6. Configure o DNS.

7. Opcionalmente, adicione opções de comando se você quiser alterar configurações específicas:

Se você quiser fazer isso...	Em seguida, defina os seguintes parâmetros <code>system node autosupport modify</code> do comando...
Oculte dados privados removendo, mascarando ou codificando dados confidenciais nas mensagens	Defina <code>-remove-private-data</code> para <code>true</code> . Se você mudar de <code>false</code> para <code>true</code> , todo o histórico do AutoSupport e todos os arquivos associados serão excluídos.
Pare de enviar dados de desempenho em mensagens AutoSupport periódicas	Defina <code>-perf</code> para <code>false</code> .

8. Se você estiver usando SMTP para entregar mensagens do AutoSupport ao NetApp, você pode opcionalmente ativar o TLS para maior segurança.

a. Apresentar os valores disponíveis para o novo parâmetro:

```
cluster1::> system node autosupport modify -smtp-encryption ?
```

b. Ativar TLS para envio de mensagens SMTP:

```
cluster1::> system node autosupport modify -smtp-encryption start_tls
```

c. Apresentar a configuração atual:

```
cluster1::> system node autosupport show -fields smtp-encryption
```

9. Verificar a configuração geral utilizando o `system node autosupport show` comando com o `-node` parâmetro.

10. Verifique a operação do AutoSupport usando o `system node autosupport check show` comando.

Se algum problema for relatado, use o `system node autosupport check show-details` comando para exibir mais informações.

11. Teste se as mensagens AutoSupport estão sendo enviadas e recebidas:

a. Utilize o `system node autosupport invoke` comando com o `-type` parâmetro definido para `test`:

```
cluster1::> system node autosupport invoke -type test -node node1
```

b. Confirme se o NetApp está recebendo suas mensagens do AutoSupport:

```
system node autosupport history show -node local
```

O estado da mensagem AutoSupport de saída mais recente deverá eventualmente mudar para para `sent-successful` todos os destinos de protocolo apropriados.

c. Opcionalmente, confirme se as mensagens do AutoSupport estão sendo enviadas para sua organização de suporte interna ou para seu parceiro de suporte verificando o e-mail de qualquer endereço configurado para os `-to` parâmetros, `-noteto` ou `-partner-address` do `system node autosupport modify` comando.

### Informações relacionadas

- ["Prepare-se para usar o AutoSupport"](#)

## Configurar

### Gerir as definições do AutoSupport

Pode utilizar o Gestor do sistema para gerir as definições da sua conta AutoSupport.

Para obter mais informações sobre as opções de configuração do AutoSupport, incluindo as configurações que não estão disponíveis no Gerenciador do sistema, consulte `system-node-autosupport-modify` no ["Referência do comando ONTAP"](#).

### Ver definições do AutoSupport

Você pode usar o Gerenciador do sistema para exibir as configurações da sua conta do AutoSupport.

### Passos

1. No System Manager, clique em **Cluster > Settings**.

Na seção **AutoSupport**, as seguintes informações são exibidas:

- Estado
- Protocolo de transporte
- Servidor proxy
- Do endereço de e-mail


2. Na seção **AutoSupport**,  selecione e, em seguida, selecione **mais opções**.

São apresentadas informações adicionais sobre a ligação à AutoSupport e as definições de correio eletrônico. Além disso, o histórico de transferência de mensagens é listado.

## Gerar e enviar dados AutoSupport

No Gerenciador de sistema, você pode iniciar a geração de mensagens do AutoSupport e escolher de qual nó ou nós de cluster os dados são coletados.


### Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Na seção **AutoSupport**,  selecione e, em seguida, selecione **Generate and Send**.
3. Introduza um assunto.
4. Marque a caixa de seleção em **coletar dados de** para especificar os nós dos quais coletar os dados.

### Teste a conexão com o AutoSupport

No Gerenciador de sistema, você pode enviar uma mensagem de teste para verificar a conexão com o AutoSupport.

### Passos

1. No System Manager, clique em **Cluster > Settings**.
2. Na seção **AutoSupport**,  selecione e, em seguida, **testar conectividade**.
3. Introduza um assunto para a mensagem.

### Ative ou desative o AutoSupport


O AutoSupport oferece benefícios de negócios comprovados para clientes da NetApp, incluindo identificação proativa de possíveis problemas de configuração e resolução acelerada de casos de suporte. O AutoSupport é ativado por padrão em novos sistemas. Se necessário, você pode usar o Gerenciador do sistema para desativar a capacidade do AutoSupport de monitorar a integridade do sistema de storage e enviar mensagens de notificação. Você pode ativar o AutoSupport novamente depois que ele tiver sido desativado.


### Sobre esta tarefa

Antes de desativar o AutoSupport, você deve estar ciente de que você está desligando o sistema call-home do NetApp e você perderá os seguintes benefícios:

- **Monitoramento de integridade:** O AutoSupport monitora a integridade do seu sistema de storage e envia notificações ao suporte técnico e à sua organização de suporte interno.
- **Automação:** O AutoSupport automatiza a geração de relatórios de casos de suporte. A maioria dos casos de suporte são abertos automaticamente antes que os clientes percebam que há um problema.
- **\* Resolução mais rápida\*:** Os sistemas que enviam dados AutoSupport têm seus casos de suporte resolvidos pela metade do tempo em comparação aos casos para sistemas que não enviam dados AutoSupport.
- **Atualizações mais rápidas:** O AutoSupport capacita fluxos de trabalho de autoatendimento do cliente, como atualizações de versão, complementos, renovações e automação de atualizações de firmware no System Manager.
- **Mais funções:** Certas funções em outras ferramentas funcionam somente quando o AutoSupport está habilitado, por exemplo, alguns fluxos de trabalho no BlueXP .

### Passos

1. Selecione **Cluster > Settings**.
2. Na seção **AutoSupport**,  selecione e, em seguida, selecione **Desativar**.

3. Se quiser ativar o AutoSupport novamente, na seção **AutoSupport**,  selecione e, em seguida, selecione **Enable**.

### Suprimir a geração de casos de suporte


A partir do ONTAP 9.10.1, você pode usar o Gerenciador do sistema para enviar uma solicitação ao AutoSupport para suprimir a geração de casos de suporte.

#### Sobre esta tarefa

Para suprimir a geração de casos de suporte, especifique os nós e o número de horas para os quais deseja que a supressão ocorra.

Suprimir casos de suporte pode ser especialmente útil se você não quiser que o AutoSupport crie casos automatizados enquanto estiver realizando manutenção em seus sistemas.


#### Passos

1. Selecione **Cluster > Settings**.
2. Na seção **AutoSupport**,  selecione e, em seguida, **suprimir geração de casos de suporte**.
3. Introduza o número de horas que pretende que a supressão ocorra.
4. Selecione os nós para os quais você deseja que a supressão ocorra.

### Retomar a geração de casos de suporte

A partir do ONTAP 9.10.1, você pode usar o Gerenciador do sistema para retomar a geração de casos de suporte do AutoSupport se ele tiver sido suprimido.



#### Passos

1. Selecione **Cluster > Settings**.
2. Na seção **AutoSupport**,  selecione e, em seguida, **Resume Support Case Generation**.
3. Selecione os nós para os quais deseja que a geração seja retomada.

### Edite as definições do AutoSupport

Você pode usar o Gerenciador do sistema para modificar as configurações de conexão e e-mail da sua conta do AutoSupport.

#### Passos

1. Selecione **Cluster > Settings**.
2. Na seção **AutoSupport**,  selecione e, em seguida, selecione **mais opções**.
3. Na seção **conexões** ou na seção **Email**,  **Edit** selecione para modificar as configurações de qualquer seção.

#### Informações relacionadas

- ["Prepare-se para usar o AutoSupport"](#)
- ["Configure o AutoSupport"](#)

### Suprimir a criação de casos AutoSupport durante as janelas de manutenção programada no ONTAP

A supressão de casos AutoSupport permite que você impeça que casos desnecessários sejam criados por mensagens AutoSupport que são acionadas durante janelas de

manutenção programada.

### Passos

1. Invoque manualmente uma mensagem AutoSupport com a cadeia de texto `MAINT=xh`, onde `x` é a duração da janela de manutenção em horas. Substitua o `<node>` pelo nome do nó a partir do qual enviar a mensagem AutoSupport:

```
system node autosupport invoke -node <node> -message MAINT=xh
```

### Informações relacionadas

- ["Referência do comando ONTAP"](#)
- ["Como suprimir a criação automática de casos durante as janelas de manutenção programada"](#)

## Carregue ficheiros utilizando o AutoSupport

### Carregue arquivos de despejo de memória

Quando um arquivo de despejo de memória é salvo, uma mensagem de evento é gerada. Se o serviço AutoSupport estiver ativado e configurado para enviar mensagens ao suporte do NetApp, uma mensagem AutoSupport será transmitida e uma confirmação automática por e-mail será enviada para você.

### O que você vai precisar

- Você deve ter configurado o AutoSupport com as seguintes configurações:
  - O AutoSupport está ativado no nó.
  - O AutoSupport está configurado para enviar mensagens ao suporte técnico.
  - O AutoSupport está configurado para usar o protocolo de transporte HTTP ou HTTPS.

O protocolo de transporte SMTP não é suportado ao enviar mensagens que incluam arquivos grandes, como arquivos de despejo de memória.

### Sobre esta tarefa

Você também pode fazer o upload do arquivo de despejo do núcleo através do serviço AutoSupport em HTTPS usando o `system node autosupport invoke-core-upload` comando, se solicitado pelo suporte do NetApp.

### ["Como fazer upload de um arquivo para o NetApp"](#)

### Passos

1. Veja os arquivos de despejo de núcleo para um nó usando o `system node coredump show` comando.

No exemplo a seguir, os arquivos de despejo do núcleo são exibidos para o nó local:

```
cluster1::> system node coredump show -node local
Node:Type Core Name Saved Panic Time
-----
node:kernel
core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
```

2. Gere uma mensagem AutoSupport e carregue um arquivo de despejo de memória usando o `system node autosupport invoke-core-upload` comando.

No exemplo a seguir, uma mensagem do AutoSupport é gerada e enviada para o local padrão, que é suporte técnico, e o arquivo de despejo de núcleo é carregado para o local padrão, que é o site de suporte do NetApp:

```
cluster1::> system node autosupport invoke-core-upload -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

No exemplo a seguir, uma mensagem do AutoSupport é gerada e enviada para o local especificado no URI, e o arquivo de despejo do núcleo é carregado para o URI:

```
cluster1::> system node autosupport invoke-core-upload -uri
https://files.company.com -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

## Carregue ficheiros de arquivo de desempenho

Você pode gerar e enviar uma mensagem do AutoSupport que contenha um arquivo de desempenho. Por padrão, o suporte técnico da NetApp recebe a mensagem AutoSupport e o arquivo de desempenho é carregado no site de suporte da NetApp. Você pode especificar um destino alternativo para a mensagem e upload.

### O que você vai precisar

- Você deve ter configurado o AutoSupport com as seguintes configurações:
  - O AutoSupport está ativado no nó.
  - O AutoSupport está configurado para enviar mensagens ao suporte técnico.
  - O AutoSupport está configurado para usar o protocolo de transporte HTTP ou HTTPS.

O protocolo de transporte SMTP não é suportado ao enviar mensagens que incluam arquivos grandes, como arquivos de desempenho.

### Sobre esta tarefa

Tem de especificar uma data de início para os dados de arquivo de desempenho que pretende carregar. A maioria dos sistemas de storage mantém arquivos de performance por duas semanas, permitindo que você especifique uma data de início há até duas semanas. Por exemplo, se hoje é 15 de janeiro, você pode

especificar uma data de início de 2 de janeiro.

## Passo

1. Gere uma mensagem AutoSupport e carregue o arquivo de desempenho usando o `system node autosupport invoke-performance-archive` comando.

No exemplo a seguir, 4 horas de arquivos de arquivamento de desempenho de 12 de janeiro de 2015 são adicionados a uma mensagem do AutoSupport e carregados para o local padrão, que é o site de suporte do NetApp:

```
cluster1::> system node autosupport invoke-performance-archive -node
local -start-date 1/12/2015 13:42:09 -duration 4h
```

No exemplo a seguir, 4 horas de arquivos de arquivo de desempenho a partir de 12 de janeiro de 2015 são adicionados a uma mensagem AutoSupport e carregados para o local especificado pelo URI:

```
cluster1::> system node autosupport invoke-performance-archive -node
local -start-date 1/12/2015 13:42:09 -duration 4h -uri
https://files.company.com
```

## Solucionar problemas

### Solucionar problemas do AutoSupport quando as mensagens não forem recebidas

Se o sistema não enviar a mensagem AutoSupport, você pode determinar se isso ocorre porque o AutoSupport não pode gerar a mensagem ou não pode entregar a mensagem.

#### Passos

1. Verifique o status de entrega das mensagens usando o `system node autosupport history show` comando.
2. Leia o estado.

Este estado	Meios
a inicializar	O processo de coleta está começando. Se este estado é temporário, tudo está bem. No entanto, se este estado persistir, há um problema.
falha na recolha	O AutoSupport não pode criar o conteúdo AutoSupport no diretório spool. Você pode ver o que o AutoSupport está tentando coletar digitando o <code>system node autosupport history show -detail</code> comando.
colecção em andamento	O AutoSupport está coletando conteúdo do AutoSupport. Você pode ver o que o AutoSupport está coletando digitando o <code>system node autosupport manifest show</code> comando.

<b>Este estado</b>	<b>Meios</b>
em fila de espera	As mensagens AutoSupport estão na fila para entrega, mas ainda não entregues.
transmissão	O AutoSupport está atualmente entregando mensagens.
enviado com sucesso	O AutoSupport entregou a mensagem com êxito. Você pode descobrir onde o AutoSupport entregou a mensagem digitando o <code>system node autosupport history show -delivery</code> comando.
ignorar	O AutoSupport não tem destinos para a mensagem. Você pode visualizar os detalhes da entrega inserindo o <code>system node autosupport history show -delivery</code> comando.
re-enfileirada	O AutoSupport tentou entregar mensagens, mas a tentativa falhou. Como resultado, o AutoSupport colocou as mensagens de volta na fila de entrega para outra tentativa. Você pode ver o erro digitando o <code>system node autosupport history show</code> comando.
falha na transmissão	O AutoSupport não conseguiu entregar a mensagem o número especificado de vezes e parou de tentar entregar a mensagem. Você pode ver o erro digitando o <code>system node autosupport history show</code> comando.
ondemand-ignore	A mensagem AutoSupport foi processada com sucesso, mas o serviço AutoSupport OnDemand optou por ignorá-la.

3. Execute uma das seguintes ações:

<b>Para este estado</b>	<b>Faça isso</b>
inicialização ou falha de coleta	Entre em Contato com o suporte da NetApp porque o AutoSupport não pode gerar a mensagem. Mencione o seguinte artigo da base de dados de Conhecimento:  <a href="#">"O AutoSupport não consegue entregar: O estado está preso na inicialização"</a>
ignorar, recolocar em fila ou falha na transmissão	Verifique se os destinos estão configurados corretamente para SMTP, HTTP ou HTTPS porque o AutoSupport não consegue entregar a mensagem.

### Solucionar problemas de entrega de mensagens do AutoSupport através de HTTPS

Se o sistema não enviar a mensagem AutoSupport esperada e você estiver usando HTTPS ou o recurso Atualização automática não estiver funcionando, você poderá



verificar várias configurações para resolver o problema.

### Antes de começar

Você deve ter confirmado a conectividade básica de rede e a pesquisa de DNS:

- Seu LIF de gerenciamento de nós precisa estar pronto para o status operacional e administrativo.
- Você deve ser capaz de fazer ping a um host em funcionamento na mesma sub-rede a partir do LIF de gerenciamento de cluster (não um LIF em nenhum dos nós).
- Você deve ser capaz de fazer ping a um host em funcionamento fora da sub-rede a partir do LIF de gerenciamento de cluster.
- Você deve ser capaz de fazer ping a um host em funcionamento fora da sub-rede a partir do LIF de gerenciamento de cluster usando o nome do host (não o endereço IP).

### Sobre esta tarefa

Essas etapas são para casos em que você determinou que o AutoSupport pode gerar a mensagem, mas não pode entregar a mensagem por HTTPS.

Se você encontrar erros ou não conseguir concluir uma etapa neste procedimento, determine e solucione o problema antes de prosseguir para a próxima etapa.

### Passos

1. Apresentar o estado detalhado do subsistema AutoSupport:

```
system node autosupport check show-details
```

Isso inclui verificar a conectividade com destinos do AutoSupport enviando mensagens de teste e fornecendo uma lista de possíveis erros nas configurações do AutoSupport.

2. Verifique o status do LIF de gerenciamento de nós:

```
network interface show -home-node local -role node-mgmt -fields  
vserver,lif,status-oper,status-admin,address,role
```

Os `status-oper` campos e `status-admin` devem retornar `up`.

3. Registre o nome da SVM, o nome LIF e o endereço IP LIF para uso posterior.
4. Certifique-se de que o DNS está ativado e configurado corretamente:

```
vserver services name-service dns show
```

5. Solucione quaisquer erros retornados pela mensagem AutoSupport:

```
system node autosupport history show -node * -fields node,seq-  
num,destination,last-update,status,error
```

Para obter assistência para solucionar quaisquer erros retornados, consulte o ["Guia de resolução ONTAP"](#)

AutoSupport (HTTPS de transporte e HTTP)".

6. Confirme se o cluster pode acessar aos servidores de que necessita e à Internet com sucesso:

- a. `network traceroute -lif node-management_LIF -destination DNS server`
- b. `network traceroute -lif node_management_LIF -destination support.netapp.com`



O endereço `support.netapp.com` em si não responde ao ping/traceroute, mas as informações por salto são valiosas.

- c. `system node autosupport show -fields proxy-url`
- d. `network traceroute -node node_management_LIF -destination proxy_url`

Se alguma dessas rotas não estiver funcionando, tente a mesma rota de um host em funcionamento na mesma sub-rede que o cluster, usando o `traceroute` utilitário ou `tracert` encontrado na maioria dos clientes de rede de terceiros. Em seguida, você pode determinar se o problema está na configuração da rede ou na configuração do cluster.

7. Se estiver a utilizar HTTPS para o protocolo de transporte AutoSupport, certifique-se de que o tráfego HTTPS pode sair da rede:

- a. Configure um cliente Web na mesma sub-rede que o LIF de gerenciamento de cluster.

Certifique-se de que todos os parâmetros de configuração sejam os mesmos valores que para a configuração do AutoSupport, incluindo o uso do mesmo servidor proxy, nome de usuário, senha e porta.

- b. Acesso `https://support.netapp.com` com o cliente web.

O acesso deve ser bem-sucedido. Caso contrário, verifique se todos os firewalls estão configurados corretamente para permitir tráfego HTTPS e DNS e se o servidor proxy está configurado corretamente. Para obter mais informações sobre como configurar a resolução de nomes estáticos para `support.NetApp.com`, consulte o artigo da base de dados de Conhecimento "[Como uma ENTRADA DE HOST seria adicionada no ONTAP para support.NetApp.com?](#)"

8. A partir do ONTAP 9.10.1 se você ativou o recurso Atualização automática, verifique se você tem conectividade HTTPS com os seguintes URLs adicionais:

- <https://support-sg-emea.NetApp.com>
- <https://support-sg-naeast.NetApp.com>
- <https://support-sg-nawest.NetApp.com>

## Solucionar problemas de entrega de mensagens do AutoSupport através de SMTP

Se o sistema não puder entregar mensagens AutoSupport por SMTP, você poderá verificar várias configurações para resolver o problema.

### O que você vai precisar

Você deve ter confirmado a conectividade básica de rede e a pesquisa de DNS:

- Seu LIF de gerenciamento de nós precisa estar pronto para o status operacional e administrativo.
- Você deve ser capaz de fazer ping a um host em funcionamento na mesma sub-rede a partir do LIF de

gerenciamento de cluster (não um LIF em nenhum dos nós).

- Você deve ser capaz de fazer ping a um host em funcionamento fora da sub-rede a partir do LIF de gerenciamento de cluster.
- Você deve ser capaz de fazer ping a um host em funcionamento fora da sub-rede a partir do LIF de gerenciamento de cluster usando o nome do host (não o endereço IP).

### Sobre esta tarefa

Essas etapas são para casos em que você determinou que o AutoSupport pode gerar a mensagem, mas não pode entregar a mensagem por SMTP.

Se você encontrar erros ou não conseguir concluir uma etapa neste procedimento, determine e solucione o problema antes de prosseguir para a próxima etapa.

Todos os comandos são inseridos na interface de linha de comando do ONTAP, a menos que especificado de outra forma.

### Passos

1. Verifique o status do LIF de gerenciamento de nós:

```
network interface show -home-node local -role node-mgmt -fields  
vserver,lif,status-oper,status-admin,address,role
```

Os `status-oper` campos e `status-admin` devem retornar `up`.

2. Registre o nome da SVM, o nome LIF e o endereço IP LIF para uso posterior.
3. Certifique-se de que o DNS está ativado e configurado corretamente:

```
vserver services name-service dns show
```

4. Exibir todos os servidores configurados para serem usados pelo AutoSupport:

```
system node autosupport show -fields mail-hosts
```

Gravar todos os nomes de servidor exibidos.

5. Para cada servidor exibido pela etapa anterior, e `support.netapp.com`, certifique-se de que o servidor ou URL pode ser alcançado pelo nó:

```
network traceroute -node local -destination server_name
```

Se alguma dessas rotas não estiver funcionando, tente a mesma rota de um host em funcionamento na mesma sub-rede que o cluster, usando o utilitário "traceroute" ou "tracert" encontrado na maioria dos clientes de rede de terceiros. Isso ajuda você a determinar se o problema está na configuração da rede ou na configuração do cluster.

6. Faça login no host designado como host de e-mail e certifique-se de que ele possa atender solicitações SMTP:

```
netstat -aAn|grep 25
```

25 É o número da porta SMTP do ouvinte.

É apresentada uma mensagem semelhante ao seguinte texto:

```
ff64878c tcp          0          0 *.25      *.*      LISTEN.
```

7. De algum outro host, abra uma sessão Telnet com a porta SMTP do host de e-mail:

```
telnet mailhost 25
```

É apresentada uma mensagem semelhante ao seguinte texto:

```
220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
10:49:04 PST
```

8. No prompt do telnet, verifique se uma mensagem pode ser retransmitida do host de e-mail:

```
HELO domain_name
```

```
MAIL FROM: your_email_address
```

```
RCPT TO: autosupport@netapp.com
```

domain\_name é o nome de domínio da sua rede.

Se um erro for retornado dizendo que a retransmissão é negada, a retransmissão não será ativada no host de e-mail. Contacte o administrador do sistema.

9. No prompt do telnet, envie uma mensagem de teste:

```
DATA
```

```
SUBJECT: TESTING
```

```
THIS IS A TEST
```

```
.
```



Certifique-se de inserir o último período (.) em uma linha por si só. O período indica ao host de e-mail que a mensagem está concluída.

Se um erro for retornado, seu host de e-mail não será configurado corretamente. Contacte o administrador do sistema.

10. Na interface de linha de comando do ONTAP, envie uma mensagem de teste do AutoSupport para um endereço de e-mail confiável ao qual você tenha acesso:

```
system node autosupport invoke -node local -type test
```

11. Localize o número de sequência da tentativa:

```
system node autosupport history show -node local -destination smtp
```

Encontre o número da sequência para a sua tentativa com base no carimbo de data/hora. É provavelmente a tentativa mais recente.

12. Exibir o erro para a tentativa de mensagem de teste:

```
system node autosupport history show -node local -seq-num seq_num -fields error
```

Se o erro exibido for `Login denied`, o servidor SMTP não aceita solicitações de envio do LIF de gerenciamento de cluster. Se não pretender alterar para utilizar HTTPS como protocolo de transporte, contacte o administrador de rede do site para configurar os gateways SMTP para resolver este problema.

Se este teste for bem-sucedido, mas a mesma mensagem enviada para `mailto:AutoSupport` em `NetApp.com` não, certifique-se de que o reencaminhamento SMTP esteja ativado em todos os seus hosts de email SMTP ou use HTTPS como um protocolo de transporte.

Se mesmo a mensagem para a conta de e-mail administrada localmente não for bem-sucedida, confirme se seus servidores SMTP estão configurados para encaminhar anexos com ambas as características:

- O sufixo `"7z"`
- O tipo MIME `"application/x-7x-Compressed"`.

## Solucionar problemas do subsistema AutoSupport

Os `system node check show` comandos podem ser usados para verificar e solucionar problemas relacionados à configuração e entrega do AutoSupport.

### Passo

1. Use os comandos a seguir para exibir o status do subsistema AutoSupport.

Use este comando...	Para fazer isso...
<code>system node autosupport check show</code>	Exiba o status geral do subsistema AutoSupport, como o status do destino HTTP ou HTTPS do AutoSupport, destinos SMTP do AutoSupport, servidor OnDemand do AutoSupport e configuração do AutoSupport
<code>system node autosupport check show-details</code>	Exibir o status detalhado do subsistema AutoSupport, como descrições detalhadas de erros e ações corretivas

## 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 detectarem 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 conectividade 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 conectividade.
- 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)	<p>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.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>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.</p> </div>
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 ações 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 detecção 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 detecção 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 cshml! -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 caracteres da comunidade no RCF do switch deve corresponder à cadeia de caracteres da comunidade que o monitor de integridade está configurado para usar. Por padrão, o monitor de integridade usa a cadeia de caracteres da comunidade `cshml!`.



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 caracteres 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 conectada 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	<code>system health status show</code>
Apresentar o estado de funcionamento dos subsistemas para os quais a monitorização de integridade está disponível	<code>system health subsystem show</code>

### Exibir o status da conectividade 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	<code>storage shelf show -connectivity</code>  Use o <code>-instance</code> 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	<code>storage disk show</code>  Use o <code>-instance</code> 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	<pre>storage port show</pre> <p>Use o <code>-instance</code> parâmetro para exibir informações detalhadas sobre cada adaptador.</p>

### 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 interruptores que o grupo de instrumentos monitoriza	<pre>system switch ethernet show</pre>	<pre>system cluster-switch show</pre>
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 de cluster e aos switches de rede de gerenciamento.  Este comando está disponível no nível de privilégio avançado.	<pre>system switch ethernet show-all</pre>	<pre>system cluster-switch show-all</pre>
Configurar a descoberta de um switch não descoberto	<pre>system switch ethernet create</pre>	<pre>system cluster-switch create</pre>
Modificar informações sobre um switch que o cluster monitora (por exemplo, nome do dispositivo, endereço IP, versão SNMP e cadeia de caracteres da comunidade)	<pre>system switch ethernet modify</pre>	<pre>system cluster-switch modify</pre>
Desativar a monitorização de um interruptor	<pre>system switch ethernet modify -disable-monitoring</pre>	<pre>system cluster-switch modify -disable-monitoring</pre>
Desative a descoberta e o monitoramento de um switch e exclua as informações de configuração do switch	<pre>system switch ethernet delete</pre>	<pre>system cluster-switch delete</pre>

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 reabilita a descoberta automática do switch)	<code>system switch ethernet delete -force</code>	<code>system cluster-switch delete -force</code>
Ative o registo automático para enviar com mensagens AutoSupport.	<code>system switch ethernet log</code>	<code>system cluster-switch log</code>




### 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	<code>system health alert show</code>
Exibir informações sobre cada alerta gerado	<code>system health alert show -instance</code>
Indique que alguém está trabalhando em um alerta	<code>system health alert modify</code>
Confirme um alerta	<code>system health alert modify -acknowledge</code>
Suprimir um alerta subsequente para que não afete o estado de funcionamento de um subsistema	<code>system health alert modify -suppress</code>
Exclua um alerta que não foi apagado automaticamente	<code>system health alert delete</code>
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	<code>system health autosupport trigger history show</code>

### 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	<code>system health policy definition modify</code>

### 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	<pre>system health config show</pre> <p> Use o <code>-instance</code> parâmetro para exibir informações detalhadas sobre cada monitor de integridade.</p>
Exiba informações sobre os alertas que um monitor de integridade pode gerar	<pre>system health alert definition show</pre> <p> Use o <code>-instance</code> parâmetro para exibir informações detalhadas sobre cada definição de alerta.</p>
Exiba informações sobre as políticas do monitor de integridade, que determinam quando os alertas são gerados	<pre>system health policy definition show</pre> <p> Use o <code>-instance</code> 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.</p>

## 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.

## Análise do sistema de arquivos

### Visão geral do File System Analytics

A análise do sistema de arquivos (FSA) foi apresentada pela primeira vez no ONTAP 9.8 para fornecer visibilidade em tempo real sobre as tendências de utilização de arquivos e capacidade de storage nos volumes ONTAP FlexGroup ou FlexVol. Essa funcionalidade nativa elimina a necessidade de ferramentas externas e fornece insights importantes sobre como seu storage é utilizado e se há oportunidades de otimizar o storage para suas necessidades empresariais.

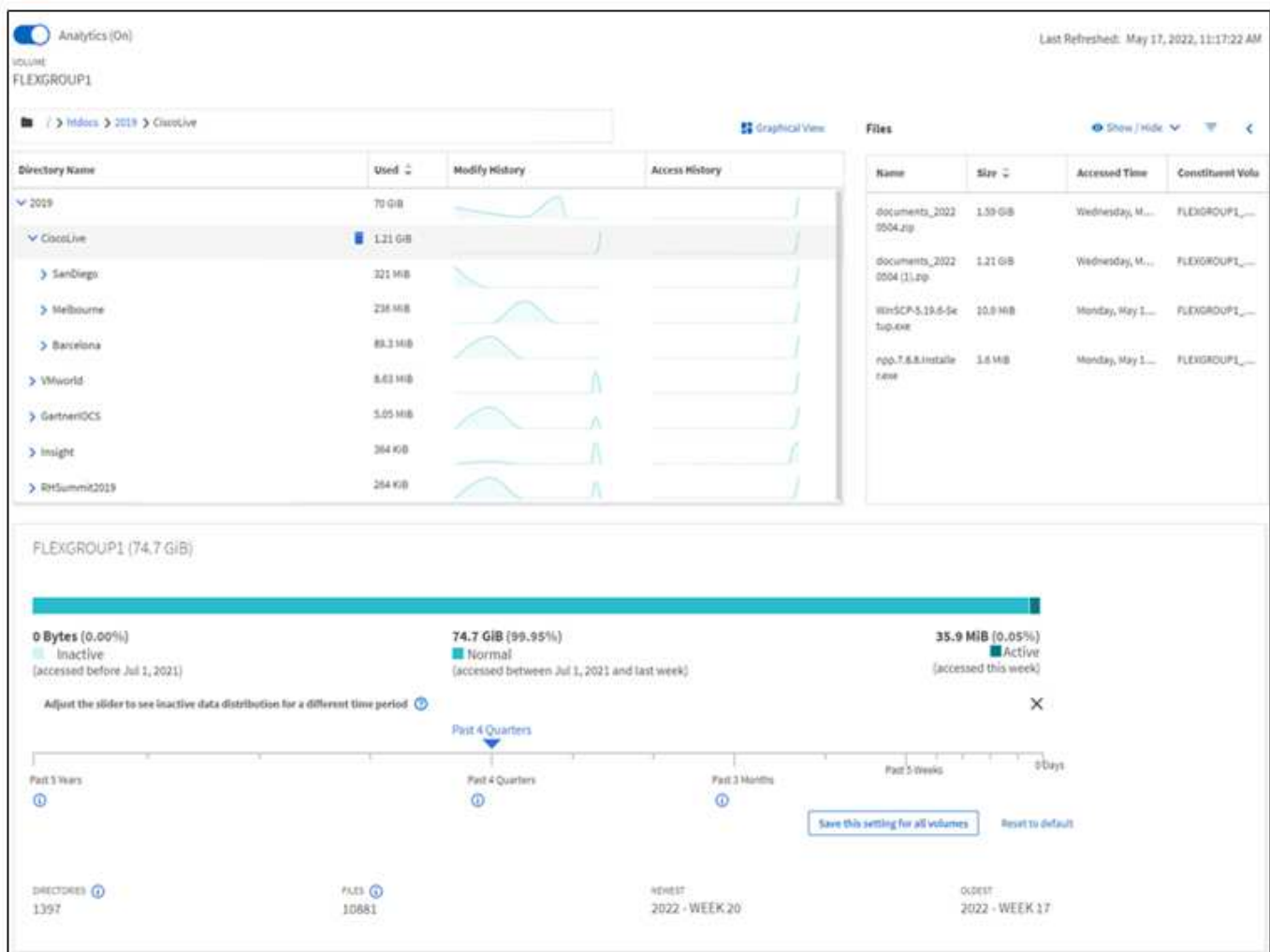
Com o FSA, você tem visibilidade em todos os níveis da hierarquia do sistema de arquivos de um volume no nas. Por exemplo, você pode obter insights de uso e capacidade nos níveis de VM de storage (SVM), volume,

diretório e arquivo. Você pode usar o FSA para responder perguntas como:

- O que está preenchendo meu armazenamento e há arquivos grandes que eu possa mover para outro local de armazenamento?
- Quais são meus volumes, diretórios e arquivos mais ativos? A performance do meu storage é otimizada para as necessidades dos meus usuários?
- Quantos dados foram adicionados no último mês?
- Quem são meus usuários de storage mais ativos ou menos ativos?
- Quantos dados inativos ou inativos estão no meu storage primário? Posso migrar esses dados para uma camada pouco econômica?
- Minhas alterações planejadas de qualidade do serviço afetarão negativamente o acesso a arquivos críticos e acessados com frequência?

A análise do sistema de arquivos está integrada ao ONTAP System Manager. As visualizações no System Manager fornecem:

- Visibilidade em tempo real para gerenciamento e operação de dados eficazes
- Coleta e agregação de dados em tempo real
- Subdiretório e tamanhos de arquivo e contagens, juntamente com perfis de desempenho associados
- Histogramas de idade de arquivo para modificar e histórico de acesso



## Tipos de volume suportados

A análise do sistema de arquivos foi projetada para fornecer visibilidade em volumes com dados nas ativos, com exceção dos caches do FlexCache e dos volumes de destino do SnapMirror.

## Disponibilidade do recurso análise do sistema de arquivos

Cada versão do ONTAP expande o escopo da análise do sistema de arquivos.

	ONTAP 9.15,1	ONTAP 9.14,1	ONTAP 9.13,1	ONTAP 9.12,1	ONTAP 9.11,1	ONTAP 9.10,1	ONTAP 9.9,1	ONTAP 9,8
Visualização no System Manager	✓	✓	✓	✓	✓	✓	✓	✓
Análise de capacidade	✓	✓	✓	✓	✓	✓	✓	✓
Informações de dados inativos	✓	✓	✓	✓	✓	✓	✓	✓
Suporte para volumes transferidos do modo Data ONTAP 7	✓	✓	✓	✓	✓	✓	✓	
Capacidade de personalizar o período inativo no System Manager	✓	✓	✓	✓	✓	✓	✓	
Monitorização de atividade em nível de volume	✓	✓	✓	✓	✓	✓		
Faça o download dos dados de acompanhamento da atividade para CSV	✓	✓	✓	✓	✓	✓		
Monitoramento de atividades no nível da SVM	✓	✓	✓	✓	✓			
Linha do tempo	✓	✓	✓	✓	✓			
Análise de utilização	✓	✓	✓	✓				
Opção para ativar a análise do sistema de ficheiros por predefinição	✓	✓	✓					
Inicialização do monitor de progresso da digitalização	✓	✓						

## Saiba mais sobre o File System Analytics

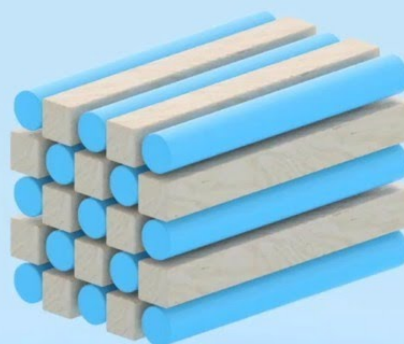
# ONTAP File System Analytics



Daniel Tennant  
Director of Software Engineering  
December 13, 2020



© 2020 NetApp, Inc. All rights reserved. — NETAPP CONFIDENTIAL —



## Leitura adicional

- ["TR 4687: Diretrizes de práticas recomendadas para análise do sistema de arquivos do ONTAP"](#)
- ["Base de Conhecimento: Latência alta ou flutuante após ativar a análise do sistema de arquivos do NetApp ONTAP"](#)

## Ative a análise do sistema de ficheiros

Para coletar e exibir dados de uso, como análise de capacidade, você precisa ativar o File System Analytics em um volume.

### Sobre esta tarefa

- A partir do ONTAP 9.8, você pode ativar a análise do sistema de arquivos em um volume novo ou existente. Se você atualizar um sistema para o ONTAP 9.8 ou posterior, certifique-se de que todos os processos de atualização foram concluídos antes de ativar a análise do sistema de arquivos.
- O tempo necessário para habilitar a análise depende do tamanho e do conteúdo do volume. O System Manager exibe o progresso e apresenta dados analíticos quando concluído. Se precisar de informações mais precisas sobre o progresso da digitalização de inicialização, você pode usar o comando ONTAP CLI `volume analytics show`.
  - A partir do ONTAP 9.14,1, o ONTAP fornece o acompanhamento do progresso para a verificação de inicialização, além de notificações sobre eventos de limitação que afetam o progresso da digitalização.
  - A partir do ONTAP 9.15,1, você pode realizar apenas quatro verificações de inicialização simultaneamente em um nó. Tem de esperar que uma digitalização seja concluída antes de iniciar uma nova digitalização. O ONTAP também impõe que haja espaço disponível suficiente no volume e apresenta uma mensagem de erro se não houver. Certifique-se de que pelo menos 5 a 8% do espaço disponível do volume esteja livre. Se o volume tiver o dimensionamento automático ativado, calcule o tamanho disponível com base no tamanho máximo do crescimento automático.
  - Para mais considerações relacionadas com a digitalização de inicialização, [Considereções de](#)

## Ative a análise do sistema de arquivos em um volume existente

Você pode ativar a análise do sistema de arquivos com o ONTAP System Manager ou a CLI.

### Exemplo 2. Passo

#### System Manager

Em ONTAP 9 .8 e 9.9.1	Começando em ONTAP 9.10,1
<ol style="list-style-type: none"><li>1. Selecione <b>armazenamento &gt; volumes</b>.</li><li>2. Selecione o volume desejado e, em seguida, selecione <b>Explorer</b>.</li><li>3. Selecione <b>Ativar o Analytics</b> ou <b>Desativar o Analytics</b>.</li></ol>	<ol style="list-style-type: none"><li>1. Selecione <b>armazenamento &gt; volumes</b>.</li><li>2. Selecione o volume pretendido. No menu volume individual, selecione <b>sistema de arquivos &gt; Explorador</b>.</li><li>3. Selecione <b>Ativar o Analytics</b> ou <b>Desativar o Analytics</b>.</li></ol>

#### CLI

##### Ative a análise do sistema de arquivos com a CLI

1. Execute o seguinte comando:

```
volume analytics on -vserver svm_name -volume volume_name [-foreground {true|false}]
```

Por padrão, o comando é executado em primeiro plano; o ONTAP exibe o progresso e apresenta dados analíticos quando concluído. Se você precisar de informações mais precisas, você pode executar o comando em segundo plano usando a `-foreground false` opção e, em seguida, usar o `volume analytics show` comando para exibir o progresso de inicialização na CLI.

2. Depois de habilitar com êxito a análise do sistema de arquivos, use o Gerenciador do sistema ou a API REST do ONTAP para exibir os dados analíticos.

## Modifique as configurações padrão de análise do sistema de arquivos


A partir do ONTAP 9.13,1, é possível modificar as configurações de SVM ou clusters para habilitar a análise do sistema de arquivos por padrão em novos volumes.

### Exemplo 3. Passos

#### System Manager

Se você estiver usando o System Manager, poderá modificar as configurações de VM ou cluster de armazenamento para habilitar a análise de capacidade e o acompanhamento de atividades na criação de volume por padrão. A habilitação padrão se aplica somente a volumes criados após a modificação das configurações, não a volumes existentes.

#### Modificar as configurações de análise do sistema de arquivos em um cluster

1. No System Manager, navegue até **Configurações de cluster**.
2. Em **Configurações de cluster**, consulte a guia Configurações do sistema de arquivos. Para modificar as definições, selecione o  ícone.
3. No campo **Rastreamento de atividade**, insira os nomes dos SVMs para habilitar o Rastreamento de atividades por padrão. Deixar o campo em branco deixará o acompanhamento de atividades desativado em todos os SVMs.

Desmarque a caixa **Ativar em novas VMs de armazenamento** para desativar o acompanhamento de atividades por padrão em novas VMs de armazenamento.

4. No campo **Analytics**, insira os nomes das VMs de armazenamento para as quais você deseja que a análise de capacidade esteja habilitada por padrão. Deixar o campo em branco deixará a análise de capacidade desativada em todos os SVMs.

Desmarque a caixa **Ativar em novas VMs de armazenamento** para desativar a análise de capacidade por padrão em novas VMs de armazenamento.

5. Selecione **Guardar**.

#### Modificar as configurações de análise do sistema de arquivos em uma SVM

1. Selecione o SVM que você deseja modificar e, em seguida, **Storage VM settings**.
2. No cartão **File System Analytics**, use as alternâncias para ativar ou desativar o acompanhamento de atividades e a análise de capacidade para todos os novos volumes na VM de armazenamento.

#### CLI

Você pode configurar a VM de storage para habilitar a análise do sistema de arquivos por padrão em novos volumes usando a CLI do ONTAP.

#### Por padrão, ative a análise do sistema de arquivos em uma SVM

1. Modifique o SVM para habilitar a análise de capacidade e o acompanhamento de atividades por padrão em todos os volumes recém-criados:

```
vserver modify -vserver svm_name -auto-enable-activity-tracking true -auto-enable-analytics true
```

### Exibir atividade do sistema de arquivos

Depois que o File System Analytics (FSA) estiver ativado, você poderá visualizar o conteúdo do diretório raiz de um volume selecionado, classificado pelo espaço usado em cada subárvore.

Selecione qualquer objeto de sistema de arquivos para navegar no sistema de arquivos e exibir informações



detalhadas sobre cada objeto em um diretório. Informações sobre diretórios também podem ser exibidas graficamente. Ao longo do tempo, os dados históricos são exibidos para cada subárvore. O espaço usado não é classificado se houver mais de 3000 diretórios.

## Explorador

A tela File System Analytics **Explorer** consiste em três áreas:

- Exibição em árvore de diretórios e subdiretórios; lista expansível mostrando nome, tamanho, histórico de modificação e histórico de acesso.
- Arquivos; mostrando nome, tamanho e tempo acessado para o objeto selecionado na lista de diretórios.
- Comparação de dados ativos e inativos para o objeto selecionado na lista de diretórios.

Começando com ONTAP 9.9,1, você pode personalizar o intervalo a ser relatado. O valor padrão é um ano. Com base nessas personalizações, você pode tomar medidas corretivas, como mover volumes e modificar a política de disposição em categorias.

A hora acessada é mostrada por padrão. No entanto, se o padrão de volume tiver sido alterado a partir da CLI (definindo a `-atime-update` opção como `false` com o `volume modify` comando), então somente o último tempo modificado será mostrado. Por exemplo:

- A exibição em árvore não exibirá o **histórico de acesso**.
- A vista de ficheiros será alterada.
- A vista de dados ativo/inativo será baseada no tempo modificado (`mtime`).

Usando esses monitores, você pode examinar o seguinte:

- Localizações do sistema de arquivos que consomem mais espaço
- Informações detalhadas sobre uma árvore de diretórios, incluindo contagem de arquivos e subdiretórios dentro de diretórios e subdiretórios
- Locais do sistema de arquivos que contêm dados antigos (por exemplo, árvores de arranhão, temperatura ou log)

Tenha em mente os seguintes pontos ao interpretar a saída FSA:

- A FSA mostra onde e quando seus dados estão em uso, não quantos dados estão sendo processados. Por exemplo, o grande consumo de espaço por arquivos recentemente acessados ou modificados não indica necessariamente altas cargas de processamento do sistema.
- A forma como o separador **Explorador de volumes** calcula o consumo de espaço para o FSA pode ser diferente de outras ferramentas. Em particular, pode haver diferenças significativas em comparação com o consumo relatado no **volume Overview** se o volume tiver recursos de eficiência de armazenamento ativados. Isso ocorre porque a guia **Explorador de volumes** não inclui economia de eficiência.
- Devido às limitações de espaço na exibição do diretório, não é possível visualizar uma profundidade de diretório superior a 8 níveis na *Vista de lista*. Para visualizar diretórios com mais de 8 níveis de profundidade, você deve alternar para *Vista gráfica*, localizar o diretório desejado e, em seguida, voltar para *Vista de lista*. Isto permitirá espaço adicional no ecrã.

## Passos

1. Exibir o conteúdo do diretório raiz de um volume selecionado:

Em ONTAP 9 .8 e 9.9.1	Começando em ONTAP 9.10,1
Clique em <b>armazenamento &gt; volumes</b> , selecione o volume desejado e clique em <b>Explorer</b> .	Selecione <b>armazenamento &gt; volumes</b> e selecione o volume desejado. No menu volume individual, selecione <b>sistema de ficheiros &gt; Explorador</b> .

## Ative o acompanhamento de atividades

A partir do ONTAP 9.10,1, a análise do sistema de arquivos inclui um recurso de acompanhamento de atividades que permite identificar objetos ativos e fazer o download dos dados como um arquivo CSV. A partir do ONTAP 9.11,1, o acompanhamento de atividades é expandido para o escopo da SVM. Também começando no ONTAP 9.11,1, o Gerenciador de sistema apresenta uma linha do tempo para o acompanhamento de atividades, permitindo que você analise até cinco minutos de dados de acompanhamento de atividades.

O acompanhamento de atividades permite a monitorização em quatro categorias:

- Diretórios
- Ficheiros
- Clientes
- Usuários

Para cada categoria monitorada, o acompanhamento de atividades exibirá IOPs de leitura, escrita IOPs, leitura de throughput e gravação de throughput. As consultas sobre o acompanhamento de atividades são atualizadas a cada 10 a 15 segundos referentes aos pontos quentes vistos no sistema em relação ao intervalo de cinco segundos anterior.

As informações de rastreamento de atividade são aproximadas e a precisão dos dados depende da distribuição do tráfego de e/S de entrada.

Ao visualizar o acompanhamento de atividades no System Manager no nível do volume, apenas o menu do volume expandido será atualizado ativamente. Se a visualização de quaisquer volumes estiver colapsada, eles não serão atualizados até que a exibição do volume seja expandida. Você pode parar as atualizações com o botão **Pausa Atualizar**. Os dados de atividade podem ser baixados em um formato CSV que exibirá todos os dados pontuais capturados para o volume selecionado.

Com o recurso de linha do tempo disponível a partir do ONTAP 9.11,1, você pode manter um Registro da atividade de hotspot em um volume ou SVM, atualizando continuamente aproximadamente a cada cinco segundos e mantendo os cinco minutos de dados anteriores. Os dados da linha do tempo são retidos apenas para campos que são área visível da página. Se você recolher uma categoria de rastreamento ou rolar para que a linha do tempo esteja fora de exibição, a linha do tempo deixará de coletar dados. Por padrão, os cronogramas são desativados e serão automaticamente desativados quando você navegar para fora da guia atividade.

## Ative o acompanhamento de atividades para um único volume

Você pode ativar o acompanhamento de atividades com o Gerenciador de sistema do ONTAP ou com a CLI.

### Sobre esta tarefa

Se você usar o RBAC com a API REST do ONTAP ou o Gerenciador de sistemas, precisará criar funções

personalizadas para gerenciar o acesso ao acompanhamento de atividades. Consulte [Controles de acesso baseados em função](#) para obter este processo.

## System Manager

### Passos

1. Selecione **armazenamento > volumes**. Selecione o volume pretendido. No menu volume individual, selecione sistema de arquivos e, em seguida, selecione a guia atividade.
2. Certifique-se de que **Activity Tracking** esteja ativado para visualizar relatórios individuais em diretórios, arquivos, clientes e usuários superiores.
3. Para analisar dados em maior profundidade sem atualizações, selecione **Pausa Atualizar**. Você pode baixar os dados para ter um Registro CSV do relatório também.

## CLI

### Passos

1. Ativar monitorização de atividade:

```
volume activity-tracking on -vserver svm_name -volume volume_name
```

2. Verifique se o estado de monitorização de atividade para um volume está ligado ou desligado com o comando:

```
volume activity-tracking show -vserver svm_name -volume volume_name -state
```

3. Uma vez ativado, use o Gerenciador de sistema do ONTAP ou a API REST do ONTAP para exibir dados de acompanhamento de atividades.

## Ative o acompanhamento de atividades para vários volumes

Você pode ativar o acompanhamento de atividades para vários volumes com o System Manager ou a CLI.

### Sobre esta tarefa

Se você usar o RBAC com a API REST do ONTAP ou o Gerenciador de sistemas, precisará criar funções personalizadas para gerenciar o acesso ao acompanhamento de atividades. Consulte [Controles de acesso baseados em função](#) para obter este processo.

## System Manager

### Ativar para volumes específicos

1. Selecione **armazenamento > volumes**. Selecione o volume pretendido. No menu volume individual, selecione sistema de arquivos e, em seguida, selecione a guia atividade.
2. Selecione os volumes em que pretende ativar o acompanhamento de atividades. Na parte superior da lista de volume, selecione o botão **mais Opções**. Selecione **Ativar monitorização de atividade**.
3. Para exibir o acompanhamento de atividades no nível SVM, selecione o SVM específico que você gostaria de exibir em **Storage > volumes**. Navegue até a guia sistema de arquivos e, em seguida, Activity e você verá os dados dos volumes que têm o acompanhamento de atividades ativado.

### Ativar para todos os volumes

1. Selecione **armazenamento > volumes**. Selecione uma SVM no menu.
2. Navegue até a guia **sistema de arquivos**, escolha a guia **mais** para ativar o acompanhamento de atividades em todos os volumes no SVM.

## CLI

A partir do ONTAP 9.13,1, você pode ativar o acompanhamento de atividades para vários volumes usando a CLI do ONTAP.

### Passos

1. Ativar monitorização de atividade:

```
volume activity-tracking on -vserver svm_name -volume [*|!volume_names]
```

``\*``Use para ativar o acompanhamento de atividades para todos os volumes na VM de armazenamento especificada.

Use ! seguido por nomes de volume para ativar o acompanhamento de atividades para todos os volumes na SVM, exceto os volumes nomeados.

2. Confirme se a operação foi bem-sucedida:

```
volume show -fields activity-tracking-state
```

3. Uma vez ativado, use o Gerenciador de sistema do ONTAP ou a API REST do ONTAP para exibir dados de acompanhamento de atividades.

## Habilite a análise de uso

A partir do ONTAP 9.12,1, você pode habilitar a análise de uso para ver quais diretórios dentro de um volume estão usando mais espaço. Você pode exibir o número total de diretórios em um volume ou o número total de arquivos em um volume. Os relatórios são limitados aos diretórios 25 que usam mais espaço.

As análises para grandes diretórios são atualizadas a cada 15 minutos. Você pode monitorar a atualização mais recente verificando o carimbo de data/hora da última atualização na parte superior da página. Você também pode clicar no botão Download para baixar dados para uma pasta de trabalho do Excel. A operação

de download é executada em segundo plano e apresenta as informações mais recentes relatadas para o volume selecionado. Se a digitalização voltar sem resultados, certifique-se de que o volume está online. Eventos como o SnapRestore farão com que a análise do sistema de arquivos reconstrua sua lista de grandes diretórios.

### Passos

1. Selecione **armazenamento > volumes**. Selecione o volume pretendido.
2. No menu volume individual, selecione **sistema de ficheiros**. Em seguida, selecione a guia **Usage**.
3. Alterne a opção **Analytics** para ativar a análise de uso.
4. O System Manager exibirá um gráfico de barras identificando os diretórios com o maior tamanho em ordem decrescente.



O ONTAP pode exibir dados parciais ou nenhum dado enquanto a lista de diretórios superiores está sendo coletada. O progresso da digitalização pode estar no separador **Usage** (utilização) que é apresentado durante a digitalização.

Para obter mais informações sobre um diretório específico, você pode [exibir atividade em um sistema de arquivos](#).

### Tome medidas corretivas com base em análises

A partir do ONTAP 9.9,1, você pode tomar ações corretivas com base nos dados atuais e nos resultados desejados diretamente a partir das telas de análise do sistema de arquivos.

### Excluir diretórios e arquivos

No visor do Explorer, pode selecionar diretórios ou ficheiros individuais para eliminar. Os diretórios são excluídos com a funcionalidade de exclusão assíncrona de diretório de baixa latência. (A exclusão assíncrona de diretório também está disponível a partir do ONTAP 9.9,1 sem a análise ativada.)

### Passos

1. Clique em **Storage > volumes** e, em seguida, clique em **Explorer**.

Quando você passa o Mouse sobre um arquivo ou pasta, a opção para excluir é exibida. Você só pode excluir um objeto de cada vez.



Quando diretórios e arquivos são excluídos, os novos valores de capacidade de armazenamento não são exibidos imediatamente.

### Atribua custo de Mídia em camadas de storage para comparar custos de locais de storage de dados inativos

O custo de Mídia é um valor que você atribui com base em sua avaliação dos custos de armazenamento, representado como sua moeda escolhida por GB. Quando definido, o System Manager usa o custo de Mídia atribuído para projetar economias estimadas ao mover volumes.

O custo de Mídia definido não é persistente; ele só pode ser definido para uma única sessão do navegador.

### Passos

1. Clique em **armazenamento > camadas** e, em seguida, clique em **Definir custo de Mídia** nos blocos de nível local desejado (agregado).

Certifique-se de selecionar níveis ativos e inativos para permitir a comparação.

2. Introduza um tipo de moeda e um montante.


Quando introduz ou altera o custo do material, a alteração é efetuada em todos os tipos de material.

### **Mova volumes para reduzir custos de storage**

Com base em exibições de análise e comparações de custo de Mídia, você pode migrar volumes para um storage mais barato em camadas locais.

Apenas um volume de cada vez pode ser comparado e movido.

#### **Passos**

1. Depois de ativar a exibição de custo de Mídia, clique em **armazenamento > camadas** e, em seguida, clique em **volumes**.
2. Para comparar as opções de destino de um volume, clique  em para o volume e, em seguida, clique em **mover**.
3. No visor **Select Destination local Tier** (Selecionar nível local de destino), selecione Destination Tiers (níveis de destino) para apresentar a diferença de custo estimada.
4. Depois de comparar as opções, selecione o nível desejado e clique em **mover**.

### **Controles de acesso baseados em função com File System Analytics**

A partir do ONTAP 9.12,1, o ONTAP inclui uma função pré-definida de controle de acesso baseado em função (RBAC) `admin-no-fsa` chamada `.A admin-no-fsa` função concede Privileges de nível de administrador, mas impede que o usuário execute operações relacionadas ao `files` endpoint (ou seja, análise do sistema de arquivos) na CLI do ONTAP, API REST e no Gerenciador de sistema.



Para obter mais informações sobre a `admin-no-fsa` função, [Funções predefinidas para administradores de cluster](#) consulte .

Se você estiver usando uma versão do ONTAP lançada antes do ONTAP 9.12,1, será necessário criar uma função dedicada para controlar o acesso à análise do sistema de arquivos. Nas versões do ONTAP anteriores ao ONTAP 9.12,1, é necessário configurar permissões RBAC por meio da CLI do ONTAP ou da API REST do ONTAP.

## System Manager

A partir do ONTAP 9.12,1, você pode configurar permissões RBAC para análise do sistema de arquivos usando o Gerenciador de sistema.

### Passos

1. Selecione **Cluster > Settings**. Em **Segurança**, navegue até **usuários e funções** e selecione .
2. Em **funções**,  **Add** selecione .
3. Forneça um nome para a função. Em atributos de função, configure o acesso ou as restrições para a função de usuário fornecendo o "**Pontos de extremidade API**" apropriado . Consulte a tabela abaixo para ver os caminhos primários e os caminhos secundários para configurar as restrições ou o acesso ao File System Analytics.

Restrição	Caminho primário	Caminho secundário
Monitorização de atividade em volumes	/api/storage/volumes	<ul style="list-style-type: none"><li>• /:uuid/top-metrics/directories</li><li>• /:uuid/top-metrics/files</li><li>• /:uuid/top-metrics/clients</li><li>• /:uuid/top-metrics/users</li></ul>
Monitorização de atividades em SVMs	/api/svm/svms	<ul style="list-style-type: none"><li>• /:uuid/top-metrics/directories</li><li>• /:uuid/top-metrics/files</li><li>• /:uuid/top-metrics/clients</li><li>• /:uuid/top-metrics/users</li></ul>
Todas as operações de análise do sistema de arquivos	/api/storage/volumes	/:uuid/files

Você pode usar `/*` em vez de um UUID para definir a política para todos os volumes ou SVMs no endpoint.

Escolha o Access Privileges para cada endpoint.

4. Selecione **Guardar**.
5. Para atribuir a função a um utilizador ou utilizadores, [Controle o acesso do administrador](#) consulte .

### CLI

Se você estiver usando uma versão do ONTAP lançada antes do ONTAP 9.12,1, use a CLI do ONTAP para criar uma função personalizada.

## Passos

1. Crie uma função padrão para ter acesso a todos os recursos.

Isso precisa ser feito antes de criar a função restritiva para garantir que a função seja apenas restritiva no acompanhamento de atividades:

```
security login role create -cmddirname DEFAULT -access all -role storageAdmin
```

2. Crie a função restritiva:

```
security login role create -cmddirname "volume file show-disk-usage" -access none -role storageAdmin
```

3. Autorize funções para acessar os serviços da Web do SVM:

- `rest` Para chamadas de API REST
- `security` para proteção por senha
- `sysmgr` Para acesso ao System Manager

```
vserver services web access create -vserver svm-name -name_ -name rest -role storageAdmin
```

```
vserver services web access create -vserver svm-name -name security -role storageAdmin
```

```
vserver services web access create -vserver svm-name -name sysmgr -role storageAdmin
```

4. Crie um usuário.

Você deve emitir um comando criar distinto para cada aplicativo que deseja aplicar ao usuário. Chamadas criar várias vezes no mesmo usuário simplesmente aplica todos os aplicativos a esse usuário e não cria um novo usuário a cada vez. O `http` parâmetro para o tipo de aplicativo se aplica à API REST do ONTAP e ao Gerenciador de sistema.

```
security login create -user-or-group-name storageUser -authentication -method password -application http -role storageAdmin
```

5. Com as novas credenciais de usuário, agora você pode fazer login no Gerenciador de sistemas ou usar a API REST do ONTAP para acessar os dados de análise de sistemas de arquivos.

## Mais informações

- [Funções predefinidas para administradores de cluster](#)
- [Controle o acesso do administrador com o System Manager](#)
- ["Saiba mais sobre as funções RBAC e a API REST do ONTAP"](#)

## Considerações para análise do sistema de arquivos

Você deve estar ciente de certos limites de uso e possíveis impactos no desempenho



associados à implementação do File System Analytics.

## Relacionamentos protegidos por SVM

Se você tiver habilitado a análise do sistema de arquivos em volumes com SVM em um relacionamento de proteção, os dados de análise não serão replicados para o SVM de destino. Se o SVM de origem precisar ser ressincronizado em uma operação de recuperação, será necessário reabilitar manualmente as análises dos volumes desejados após a recuperação.

## Considerações de desempenho

Em alguns casos, a ativação do File System Analytics pode afetar negativamente o desempenho durante a coleta inicial de metadados. Isso geralmente é visto em sistemas que estão na utilização máxima. Para evitar a ativação de análises em tais sistemas, você pode usar as ferramentas de monitoramento de desempenho do Gerenciador do sistema do ONTAP.

Se você tiver um aumento notável na latência, consulte o artigo da base de dados de Conhecimento ["Latência alta ou flutuante após ativar a análise do sistema de arquivos do NetApp ONTAP"](#).

## Considerações de digitalização

Quando você ativa o análise de capacidade, o ONTAP realiza uma verificação de inicialização para análise de capacidade. A verificação acessa metadados para todos os arquivos em volumes para os quais a análise de capacidade está ativada. Nenhum dado de arquivo é lido durante a digitalização. A partir do ONTAP 9.14,1, você pode acompanhar o andamento da verificação com a API REST, na guia **Explorer** do Gerenciador de sistema ou com o `volume analytics show` comando CLI. Se houver um evento de limitação, o ONTAP fornecerá uma notificação.

Ao ativar a análise do sistema de arquivos em um volume, certifique-se de que pelo menos 5 a 8% do espaço disponível do volume esteja livre. Se o volume tiver o dimensionamento automático ativado, calcule o tamanho disponível com base no tamanho máximo do crescimento automático. A partir do ONTAP 9.15,1, o ONTAP apresenta uma mensagem de erro se não houver espaço suficiente disponível quando você ativar a análise do sistema de arquivos em um volume.

Após a conclusão da verificação, o File System Analytics é atualizado continuamente em tempo real à medida que o sistema de arquivos muda.

O tempo necessário para a digitalização é proporcional ao número de diretórios e arquivos no volume. Como a digitalização coleta metadados, o tamanho do arquivo não afeta o tempo de digitalização.

Para obter mais informações sobre a digitalização de inicialização, ["TR-4867: Diretrizes de melhores práticas para análise de sistemas de arquivos"](#) consulte .

## Práticas recomendadas

Você deve iniciar a verificação em volumes que não compartilham agregados. Você pode ver quais agregados estão hospedando atualmente quais volumes usando o comando:

```
volume show -volume comma-separated-list_of_volumes -fields aggr-list
```

Enquanto a verificação é executada, os volumes continuam a servir o tráfego do cliente. Recomenda-se que inicie a verificação durante períodos em que antecipe um menor tráfego de clientes.

Se o tráfego do cliente aumentar, ele irá consumir recursos do sistema e fazer com que a varredura leve mais tempo.

A partir do ONTAP 9.12,1, você pode pausar a coleta de dados no Gerenciador do sistema e com a CLI do ONTAP.

- Se você estiver usando a CLI do ONTAP:
  - Você pode pausar a coleta de dados com o comando: `volume analytics initialization pause -vserver svm_name -volume volume_name`
  - Uma vez que o tráfego do cliente abrandou, você pode retomar a coleta de dados com o comando: `volume analytics initialization resume -vserver svm_name -volume volume_name`
- Se você estiver usando o System Manager, na exibição **Explorer** do menu de volume, use os botões **Pausa coleta de dados** e **Resume coleta de dados** para gerenciar a digitalização.

## Configuração EMS

### Visão geral da configuração EMS

Você pode configurar o ONTAP 9 para enviar notificações de eventos importantes do EMS (sistema de gerenciamento de eventos) diretamente para um endereço de e-mail, servidor syslog, traphost de protocolo de rede de gerenciamento simples (SNMP) ou aplicativo webhook para que você seja imediatamente notificado sobre problemas do sistema que exigem atenção imediata.

Como as notificações de eventos importantes não estão habilitadas por padrão, você precisa configurar o EMS para enviar notificações para um endereço de e-mail, um servidor syslog, um traphost SNMP ou um aplicativo webhook.

Reveja as versões específicas da versão do ["Referência EMS da ONTAP 9"](#).

Se o mapeamento de eventos do EMS usar conjuntos de comandos ONTAP obsoletos (como destino de eventos, rota de eventos), é recomendável atualizar o mapeamento. ["Saiba como atualizar seu mapeamento EMS a partir de comandos ONTAP obsoletos"](#).

### Configurar notificações e filtros de eventos EMS com o System Manager

Você pode usar o System Manager para configurar como o sistema de gerenciamento de eventos (EMS) entrega notificações de eventos para que você possa ser notificado sobre problemas do sistema que exigem sua atenção imediata.

Versão de ONTAP	Com o System Manager, você pode...
ONTAP 9.12,1 e posterior	Especifique o protocolo TLS (Transport Layer Security) ao enviar eventos para servidores syslog remotos.
ONTAP 9.10,1 e posterior	Configure endereços de e-mail, servidores syslog e aplicativos de webhook, bem como hosts SNMP.
ONTAP 9 F.7 a 9.10.0	Configurar apenas os hosts SNMP. Você pode configurar outro destino EMS com a CLI do ONTAP. <a href="#">"Visão geral da configuração EMS"</a> Consulte .

Você pode executar os seguintes procedimentos:

- [\[add-ems-destination\]](#)
- [\[create-ems-filter\]](#)
- [\[edit-ems-destination\]](#)
- [\[edit-ems-filter\]](#)
- [\[delete-ems-destination\]](#)
- [\[delete-ems-filter\]](#)

### Informações relacionadas



- ["Referência EMS da ONTAP"](#)
- ["Usando a CLI para configurar hosts SNMP para receber notificações de eventos"](#)

### Adicionar um destino de notificação de evento EMS

Você pode usar o System Manager para especificar para onde deseja que as mensagens EMS sejam enviadas.

A partir do ONTAP 9.12.1, os eventos EMS podem ser enviados para uma porta designada em um servidor syslog remoto através do protocolo TLS (Transport Layer Security). Para obter detalhes, consulte a `event notification destination create` página de manual.

### Passos

1. Clique em **Cluster > Settings**.
2. Na seção **Gerenciamento de notificações**, clique  em **Exibir destinos de eventos**.
3. Na página **Gerenciamento de notificações**, selecione a guia **Destinos de eventos**.
4. Clique  **Add** em .
5. Especifique um nome, um tipo de destino EMS e filtros.



Se necessário, você pode adicionar um novo filtro. Clique em **Adicionar um novo filtro de evento**.

6. Dependendo do tipo de destino EMS selecionado, especifique o seguinte:



Para configurar...	Especificar ou selecionar...
SNMP traphost	<ul style="list-style-type: none"><li>• Nome do Traphost</li></ul>
E-mail (Começando com 9.10.1)	<ul style="list-style-type: none"><li>• Endereço de e-mail de destino</li><li>• Servidor de correio</li><li>• Do endereço de e-mail</li></ul>


<p>Servidor syslog</p> <p>(Começando com 9.10.1)</p>	<ul style="list-style-type: none"> <li>• Nome do host ou endereço IP do servidor</li> <li>• Porta syslog (começando com 9.12.1)</li> <li>• Transporte syslog (começando com 9.12.1)</li> </ul> <p>Selecionar <b>TCP Encrypted</b> ativa o protocolo TLS (Transport Layer Security). Se nenhum valor for inserido para <b>Syslog port</b>, um padrão será usado com base na seleção <b>Syslog transport</b>.</p>
<p>Webhook</p> <p>(Começando com 9.10.1)</p>	<ul style="list-style-type: none"> <li>• URL do webhook</li> <li>• Autenticação de cliente (selecione esta opção para especificar um certificado de cliente)</li> </ul>

### Crie um novo filtro de notificação de eventos EMS

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para definir novos filtros personalizados que especificam as regras para o tratamento de notificações EMS.

#### Passos


1. Clique em **Cluster > Settings**.
2. Na seção **Gerenciamento de notificações**, clique  em **Exibir destinos de eventos**.
3. Na página **Gerenciamento de notificações**, selecione a guia **filtros de eventos**.
4. Clique  **Add** em .
5. Especifique um nome e selecione se deseja copiar regras de um filtro de evento existente ou adicionar novas regras.
6. Dependendo da sua escolha, execute as seguintes etapas:


Se você escolher...	Em seguida, execute estes passos...
<p><b>Copiar regras do filtro de eventos existente</b></p>	<ol style="list-style-type: none"> <li>1. Selecione um filtro de eventos existente.</li> <li>2. Modifique as regras existentes.</li> <li>3. Adicione outras regras, se necessário, clicando  <b>Add</b> em .</li> </ol>
<p><b>Adicione novas regras</b></p>	<p>Especifique o tipo, o padrão de nome, as severidades e o tipo de trap SNMP para cada nova regra.</p>

### Editar um destino de notificação de evento EMS

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para alterar as informações de destino da notificação de eventos.

#### Passos

1. Clique em **Cluster > Settings**.
2. Na seção **Gerenciamento de notificações**, clique  em **Exibir destinos de eventos**.
3. Na página **Gerenciamento de notificações**, selecione a guia **Destinos de eventos**.

4. Ao lado do nome do destino do evento, clique  em e, em seguida, clique em **Editar**.
5. Modifique as informações de destino do evento e clique em **Salvar**.



### Editar um filtro de notificação de eventos EMS

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para modificar filtros personalizados para alterar a forma como as notificações de eventos são tratadas.



Não é possível modificar filtros definidos pelo sistema.

#### Passos

1. Clique em **Cluster > Settings**.
2. Na seção **Gerenciamento de notificações**, clique  em **Exibir destinos de eventos**.
3. Na página **Gerenciamento de notificações**, selecione a guia **filtros de eventos**.
4. Ao lado do nome do filtro de evento, clique  em e, em seguida, clique em **Editar**.
5. Modifique as informações do filtro de eventos e clique em **Salvar**.



### Eliminar um destino de notificação de evento EMS

A partir do ONTAP 9.10,1, pode utilizar o Gestor do sistema para eliminar um destino de notificação de eventos EMS.



Não é possível eliminar destinos SNMP.

#### Passos

1. Clique em **Cluster > Settings**.
2. Na seção **Gerenciamento de notificações**, clique  em **Exibir destinos de eventos**.
3. Na página **Gerenciamento de notificações**, selecione a guia **Destinos de eventos**.
4. Ao lado do nome do destino do evento, clique  em e, em seguida, clique em **Excluir**.



### Eliminar um filtro de notificação de eventos EMS

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para excluir filtros personalizados.



Não é possível eliminar filtros definidos pelo sistema.

#### Passos

1. Clique em **Cluster > Settings**.
2. Na seção **Gerenciamento de notificações**, clique  em **Exibir destinos de eventos**.
3. Na página **Gerenciamento de notificações**, selecione a guia **filtros de eventos**.
4. Ao lado do nome do filtro de evento, clique  em e, em seguida, clique em **Eliminar**.

## Configure as notificações de eventos EMS com a CLI

## Fluxo de trabalho de configuração do EMS

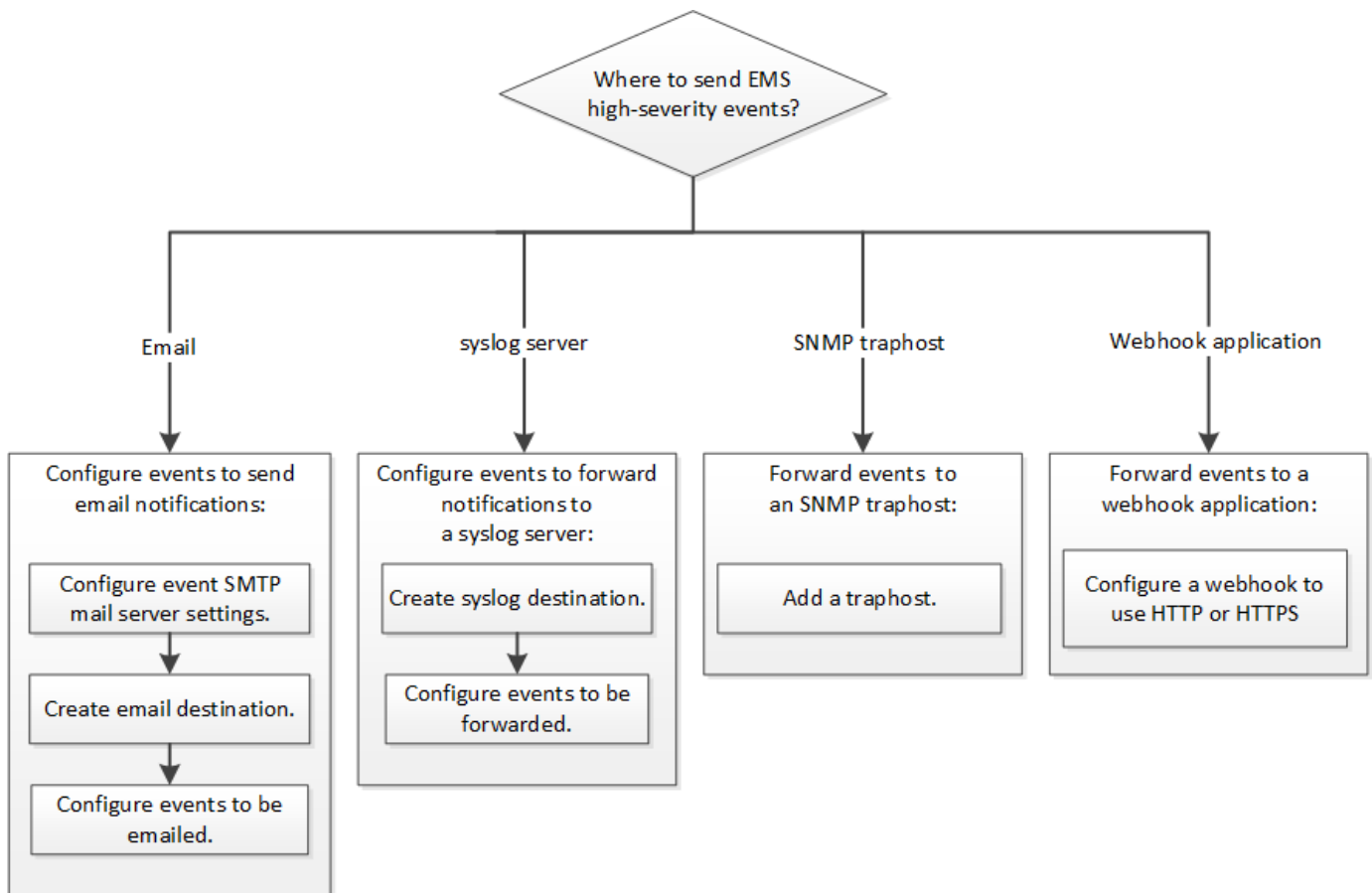
Você deve configurar notificações importantes de eventos EMS para serem enviadas como e-mail, encaminhadas para um servidor syslog, encaminhadas para um traphost SNMP ou encaminhadas para um aplicativo webhook. Isso ajuda você a evitar interrupções no sistema, tomando ações corretivas em tempo hábil.

### Sobre esta tarefa

Se o seu ambiente já contém um servidor syslog para agregar os eventos registrados de outros sistemas, como servidores e aplicativos, então é mais fácil usar esse servidor syslog também para notificações de eventos importantes de sistemas de armazenamento.

Se o seu ambiente ainda não contém um servidor syslog, é mais fácil usar e-mail para notificações de eventos importantes.

Se você já encaminhar notificações de eventos para um traphost SNMP, talvez queira monitorar esse traphost para eventos importantes.



### Opções

- Defina EMS para enviar notificações de eventos.

Se você quiser...	Consulte isto...
O EMS para enviar notificações de eventos importantes para um endereço de e-mail	<a href="#">Configurar eventos importantes do EMS para enviar notificações por e-mail</a>

O EMS para encaminhar notificações de eventos importantes para um servidor syslog	<a href="#">Configure eventos importantes do EMS para encaminhar notificações para um servidor syslog</a>
Se você quiser que o EMS encaminhe notificações de eventos para um traphost SNMP	<a href="#">Configure os hosts SNMP para receber notificações de eventos</a>
Se você quiser que o EMS encaminhe notificações de eventos para um aplicativo webhook	<a href="#">Configure eventos EMS importantes para encaminhar notificações para um aplicativo webhook</a>

## Configurar eventos importantes do EMS para enviar notificações por e-mail

Para receber notificações por e-mail dos eventos mais importantes, você deve configurar o EMS para enviar mensagens de e-mail para eventos que sinalizem atividade importante.

### O que você vai precisar

O DNS deve ser configurado no cluster para resolver os endereços de e-mail.

### Sobre esta tarefa

Você pode executar essa tarefa sempre que o cluster estiver sendo executado inserindo os comandos na linha de comando ONTAP.

### Passos

1. Configure as definições do servidor de correio SMTP de eventos:

```
event config modify -mail-server mailhost.your_domain -mail-from
cluster_admin@your_domain
```

2. Criar um destino de e-mail para notificações de eventos:

```
event notification destination create -name storage-admins -email
your_email@your_domain
```

3. Configure os eventos importantes para enviar notificações por e-mail:

```
event notification create -filter-name important-events -destinations storage-
admins
```

## Configurando eventos importantes do EMS para encaminhar notificações para um servidor syslog

Para Registrar notificações dos eventos mais graves em um servidor syslog, você deve configurar o EMS para encaminhar notificações de eventos que sinalizam atividade importante.

### O que você vai precisar

O DNS deve ser configurado no cluster para resolver o nome do servidor syslog.

### Sobre esta tarefa

Se o seu ambiente ainda não contiver um servidor syslog para notificações de eventos, você deve primeiro criar um. Se o seu ambiente já contiver um servidor syslog para registrar eventos de outros sistemas, talvez você queira usá-lo para notificações de eventos importantes.

Você pode executar essa tarefa sempre que o cluster estiver sendo executado inserindo os comandos na CLI do ONTAP.

A partir do ONTAP 9.12.1, os eventos EMS podem ser enviados para uma porta designada em um servidor syslog remoto através do protocolo TLS (Transport Layer Security). Dois novos parâmetros estão disponíveis:

### **tcp-encrypted**

Quando `tcp-encrypted` for especificado para o `syslog-transport`, o ONTAP verifica a identidade do host de destino validando seu certificado. O valor padrão é `udp-unencrypted`.

### **syslog-port**

O parâmetro valor padrão `syslog-port` depende da configuração do `syslog-transport` parâmetro. Se `syslog-transport` estiver definido como `tcp-encrypted`, `syslog-port` tem o valor padrão 6514.

Para obter detalhes, consulte a `event notification destination create` página de manual.

## **Passos**

1. Crie um destino de servidor syslog para eventos importantes:

```
event notification destination create -name syslog-ems -syslog syslog-server-address -syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}
```

A partir de ONTAP 9.12.1, os seguintes valores podem ser especificados para `syslog-transport`:

- `udp-unencrypted` - Protocolo de datagrama de usuário sem segurança
- `tcp-unencrypted` - Protocolo de Controle de transmissão sem segurança
- `tcp-encrypted` - Protocolo de Controle de transmissão com Transport Layer Security (TLS)

O protocolo predefinido é `udp-unencrypted`.

2. Configure os eventos importantes para encaminhar notificações para o servidor syslog:

```
event notification create -filter-name important-events -destinations syslog-ems
```

## **Configure os hosts SNMP para receber notificações de eventos**

Para receber notificações de eventos em um trap host SNMP, você deve configurar um trap host.

### **O que você vai precisar**

- Os traps SNMP e SNMP devem estar ativados no cluster.



As traps SNMP e SNMP estão ativadas por predefinição.

- O DNS deve ser configurado no cluster para resolver os nomes do trap host.



## Sobre esta tarefa

Se você ainda não tiver um traphost SNMP configurado para receber notificações de eventos (traps SNMP), você deve adicionar um.

Você pode executar essa tarefa sempre que o cluster estiver sendo executado inserindo os comandos na linha de comando ONTAP.

## Passo

1. Se o seu ambiente ainda não tiver um traphost SNMP configurado para receber notificações de eventos, adicione uma:

```
system snmp traphost add -peer-address snmp_traphost_name
```

Todas as notificações de eventos que são suportadas por SNMP por padrão são encaminhadas para o traphost SNMP.

## Configure eventos EMS importantes para encaminhar notificações para um aplicativo webhook

Você pode configurar o ONTAP para encaminhar notificações de eventos importantes para um aplicativo webhook. As etapas de configuração necessárias dependem do nível de segurança escolhido.

### Prepare-se para configurar o encaminhamento de eventos EMS

Há vários conceitos e requisitos que você deve considerar antes de configurar o ONTAP para encaminhar notificações de eventos para um aplicativo webhook.

### Aplicação webhook

Você precisa de um aplicativo webhook capaz de receber as notificações de eventos do ONTAP. Um webhook é uma rotina de retorno de chamada definida pelo usuário que estende a capacidade do aplicativo ou servidor remoto onde ele é executado. Webhooks são chamados ou ativados pelo cliente (neste caso ONTAP) enviando uma solicitação HTTP para o URL de destino. Especificamente, o ONTAP envia uma solicitação HTTP POST para o servidor que hospeda o aplicativo webhook junto com os detalhes de notificação de evento formatados em XML.

### Opções de segurança

Existem várias opções de segurança disponíveis, dependendo de como o protocolo TLS (Transport Layer Security) é usado. A opção escolhida determina a configuração necessária do ONTAP.



TLS é um protocolo criptográfico amplamente utilizado na internet. Ele fornece privacidade, bem como integridade de dados e autenticação usando um ou mais certificados de chave pública. Os certificados são emitidos por autoridades de certificação confiáveis.

### HTTP

Você pode usar HTTP para transportar as notificações de eventos. Com esta configuração, a conexão não é segura. As identidades do cliente ONTAP e da aplicação webhook não são verificadas. Além disso, o tráfego de rede não é criptografado ou protegido. ["Configure um destino de webhook para usar HTTP"](#) Consulte para obter os detalhes de configuração.

## HTTPS

Para segurança adicional, você pode instalar um certificado no servidor que hospeda a rotina do webhook. O protocolo HTTPS é usado pelo ONTAP para verificar a identidade do servidor de aplicativos webhook, bem como por ambas as partes para garantir a privacidade e integridade do tráfego de rede. "[Configure um destino de webhook para usar HTTPS](#)" Consulte para obter os detalhes de configuração.

### HTTPS com autenticação mútua

Você pode aprimorar ainda mais a segurança HTTPS instalando um certificado de cliente no sistema ONTAP que emite as solicitações de webhook. Além de o ONTAP verificar a identidade do servidor de aplicativos webhook e proteger o tráfego de rede, o aplicativo webhook verifica a identidade do cliente ONTAP. Essa autenticação de dois sentidos é conhecida como *Mutual TLS*. "[Configure um destino de webhook para usar HTTPS com autenticação mútua](#)" Consulte para obter os detalhes de configuração.

### Informações relacionadas

- "[O protocolo TLS \(Transport Layer Security\) versão 1,3](#)"

### Configure um destino de webhook para usar HTTP

Você pode configurar o ONTAP para encaminhar notificações de eventos para um aplicativo webhook usando HTTP. Esta é a opção menos segura, mas a mais simples de configurar.

#### Passos

1. Crie um novo destino `restapi-ems` para receber os eventos:

```
event notification destination create -name restapi-ems -rest-api-url  
http://<webhook-application>
```

No comando acima, você deve usar o esquema **HTTP** para o destino.

2. Crie uma notificação vinculando o `important-events` filtro ao `restapi-ems` destino:

```
event notification create -filter-name important-events -destinations restapi-  
ems
```

### Configure um destino de webhook para usar HTTPS

Você pode configurar o ONTAP para encaminhar notificações de eventos para um aplicativo de webhook usando HTTPS. O ONTAP usa o certificado do servidor para confirmar a identidade do aplicativo webhook, bem como proteger o tráfego de rede.

#### Antes de começar

- Gerar uma chave privada e um certificado para o servidor de aplicativos webhook
- Tenha o certificado raiz disponível para instalação no ONTAP

#### Passos

1. Instale a chave privada do servidor e os certificados apropriados no servidor que hospeda seu aplicativo webhook. As etapas de configuração específicas dependem do servidor.
2. Instale o certificado raiz do servidor no ONTAP:

```
security certificate install -type server-ca
```

O comando pedirá o certificado.

3. Crie o `restapi-ems` destino para receber os eventos:

```
event notification destination create -name restapi-ems -rest-api-url
https://<webhook-application>
```

No comando acima, você deve usar o esquema **HTTPS** para o destino.

4. Crie a notificação que vincula o `important-events` filtro ao novo `restapi-ems` destino:

```
event notification create -filter-name important-events -destinations restapi-
ems
```

### Configure um destino de webhook para usar HTTPS com autenticação mútua

Você pode configurar o ONTAP para encaminhar notificações de eventos para um aplicativo de webhook usando HTTPS com autenticação mútua. Com esta configuração existem dois certificados. O ONTAP usa o certificado do servidor para confirmar a identidade do aplicativo webhook e proteger o tráfego de rede. Além disso, o aplicativo que hospeda o webhook usa o certificado de cliente para confirmar a identidade do cliente ONTAP.

#### Antes de começar

Você deve fazer o seguinte antes de configurar o ONTAP:

- Gerar uma chave privada e um certificado para o servidor de aplicativos webhook
- Tenha o certificado raiz disponível para instalação no ONTAP
- Gerar uma chave privada e um certificado para o cliente ONTAP

#### Passos

1. Execute as duas primeiras etapas da tarefa "[Configure um destino de webhook para usar HTTPS](#)" para instalar o certificado do servidor para que o ONTAP possa verificar a identidade do servidor.
2. Instale os certificados raiz e intermediários apropriados no aplicativo webhook para validar o certificado do cliente.
3. Instale o certificado de cliente no ONTAP:

```
security certificate install -type client
```

O comando pedirá a chave privada e o certificado.

4. Crie o `restapi-ems` destino para receber os eventos:

```
event notification destination create -name restapi-ems -rest-api-url
https://<webhook-application> -certificate-authority <issuer of the client
certificate> -certificate-serial <serial of the client certificate>
```

No comando acima, você deve usar o esquema **HTTPS** para destino.

5. Crie a notificação que vincula o `important-events` filtro ao novo `restapi-ems` destino:

```
event notification create -filter-name important-events -destinations restapi-
ems
```

## Atualizar mapeamento de eventos EMS obsoleto

### Modelos de mapeamento de eventos EMS

Antes do ONTAP 9.0, os eventos EMS só podiam ser mapeados para destinos de eventos com base na correspondência do padrão de nomes de eventos. Os conjuntos de comandos ONTAP (`event destination`, `event route`) que utilizam este modelo continuam a estar disponíveis nas versões mais recentes do ONTAP, mas foram obsoletos a partir do ONTAP 9.0.

A partir do ONTAP 9.0, a melhor prática para o mapeamento de destino de eventos do ONTAP EMS é usar o modelo de filtro de eventos mais dimensionável no qual a correspondência de padrões é feita em vários campos, usando os `event filter` conjuntos de comandos, `event notification` e `event notification destination`.

Se o mapeamento EMS estiver configurado usando os comandos obsoletos, você deverá atualizar o mapeamento para usar os `event filter` conjuntos de comandos, `event notification` e `event notification destination`.

Existem dois tipos de destinos de eventos:

1. **Destinos gerados pelo sistema:** Existem cinco destinos de eventos gerados pelo sistema (criados por padrão)

- `allevents`
- `asup`
- `criticals`
- `pager`
- `traphost`

Alguns dos destinos gerados pelo sistema são para fins especiais. Por exemplo, o destino `asup` encaminha os eventos `callhome.*` para o módulo AutoSupport no ONTAP para gerar mensagens AutoSupport.

2. **Destinos criados pelo usuário:** Estes são criados manualmente usando o `event destination create` comando.

```
cluster-1::event*> destination show
```

```
Hide
Name          Mail Dest.      SNMP Dest.      Syslog Dest.
Params
-----
-----
allevents     -              -              -
false
asup          -              -              -
false
criticals    -              -              -
false
pager        -              -              -
false
traphost     -              -              -
false
```

```
5 entries were displayed.
```

```
+
```

```
cluster-1::event*> destination create -name test -mail test@xyz.com
```

```
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
```

```
+
```

```
cluster-1::event*> destination show
```

```
+
```

```
Hide
Name          Mail Dest.      SNMP Dest.      Syslog Dest.
Params
-----
-----
allevents     -              -              -
false
asup          -              -              -
false
criticals    -              -              -
false
pager        -              -              -
false
test          test@xyz.com    -              -
false
traphost     -              -              -
false
```

```
6 entries were displayed.
```

No modelo obsoleto, os eventos EMS são mapeados individualmente para um destino usando o `event route add-destinations` comando.

```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.
```

```
cluster-1::event*> route show -message-name raid.aggr.*
```

Time	Message	Severity	Destinations	Freq	Threshd
	raid.aggr.autoGrow.abort	NOTICE	test	0	0
	raid.aggr.autoGrow.success	NOTICE	test	0	0
	raid.aggr.lock.conflict	INFORMATIONAL	test	0	0
	raid.aggr.log.CP.count	DEBUG	test	0	0

4 entries were displayed.

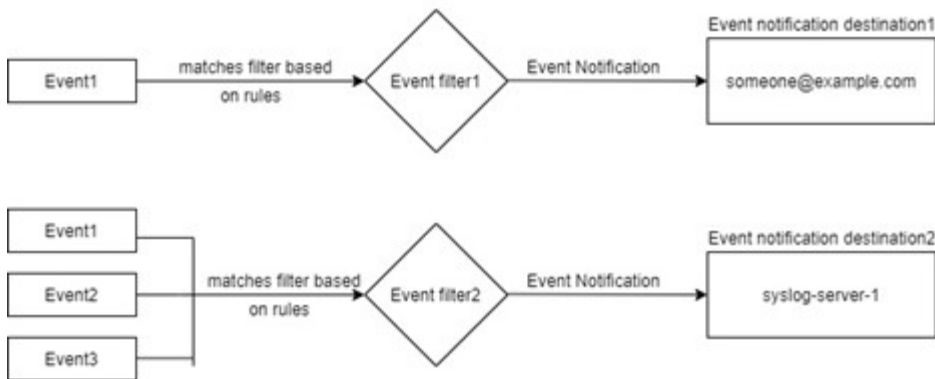
O novo e mais escalável mecanismo de notificações de eventos EMS baseia-se em filtros de eventos e destinos de notificação de eventos. Consulte o seguinte artigo da KB para obter informações detalhadas sobre o novo mecanismo de notificação de eventos:

- ["Visão geral do sistema de gerenciamento de eventos para ONTAP 9"](#)

### Legacy routing based model



### Event notification based model



### Atualize o mapeamento de eventos do EMS a partir de comandos ONTAP obsoletos

Se o mapeamento de eventos do EMS estiver configurado atualmente usando os conjuntos de comandos ONTAP obsoletos (`event destination`, `event route`), siga este procedimento para atualizar o mapeamento para usar os `event filter` conjuntos de comandos, `event notification` e `event notification destination`.

#### Passos

1. Liste todos os destinos de eventos no sistema usando o `event destination show` comando.

```
cluster-1::event*> destination show
```

```
Hide
Name          Mail Dest.      SNMP Dest.      Syslog Dest.
Params
-----
-----
allevents     -              -              -
false
asup          -              -              -
false
criticals     -              -              -
false
pager         -              -              -
false
test          test@xyz.com    -              -
false
traphost      -              -              -
false
6 entries were displayed.
```

2. Para cada destino, liste os eventos que estão sendo mapeados usando o `event route show -destinations <destination name>` comando.

```
cluster-1::event*> route show -destinations test
```

```
Time
Message          Severity      Destinations    Freq
Threshd          Threshd
-----
-----
raid.aggr.autoGrow.abort      NOTICE      test           0      0
raid.aggr.autoGrow.success    NOTICE      test           0      0
raid.aggr.lock.conflict      INFORMATIONAL  test           0      0
raid.aggr.log.CP.count        DEBUG        test           0      0
4 entries were displayed.
```

3. Crie um correspondente `event filter` que inclua todos esses subconjuntos de eventos. Por exemplo, se você quiser incluir apenas os `raid.aggr.*` eventos, use um caractere curinga para o `message-name` parâmetro ao criar o filtro. Você também pode criar filtros para eventos individuais.



Você pode criar até 50 filtros de eventos.



```

cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule      Rule      Message Name      SNMP Trap Type
Severity
      Position Type
-----
test_events
      1      include  raid.aggr.*      *      *
      2      exclude *      *      *
2 entries were displayed.

```

4. Criar um event notification destination para cada um event destination dos endpoints (ou seja, SMTP/SNMP/syslog)

```

cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name      Type      Destination
-----
dest1      email      test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost  snmp      - (from "system snmp traphost")
2 entries were displayed.

```

5. Crie uma notificação de evento mapeando o filtro de evento para o destino de notificação de evento.

```

cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID  Filter Name      Destinations
----
1   default-trap-events  snmp-traphost
2   asup_events        dest1
2 entries were displayed.

```

6. Repita as etapas 1-5 para cada event destination um que tenha um event route mapeamento.



Os eventos roteados para destinos SNMP devem ser mapeados para o `snmp-traphost` destino de notificação de eventos. O destino SNMP traphost usa o sistema SNMP traphost configurado.

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
      scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135>   Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

      Destination Name: snmp-traphost
      Type of Destination: snmp
      Destination: 10.234.166.135 (from "system snmp
traphost")
      Server CA Certificates Present?: -
      Client Certificate Issuing CA: -
Client Certificate Serial Number: -
      Client Certificate Valid?: -
```

## Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPTÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.