Monitores e Alertas

Data Infrastructure Insights

NetApp
February 03, 2026

This PDF was generated from https://docs.netapp.com/pt-br/data-infrastructure-insights/task_create_monitor.html on February 03, 2026. Always check docs.netapp.com for the latest.

Índice

Monitores e Alertas

Alerta com monitores

Configure monitores para rastrear limites de desempenho, registrar eventos e anomalias em seus recursos de infraestrutura. Crie alertas personalizados para métricas como latência de gravação de nó, capacidade de armazenamento ou desempenho do aplicativo e receba notificações quando essas condições forem atendidas.

Os monitores permitem que você defina limites para métricas geradas por objetos de "infraestrutura", como armazenamento, VM, EC2 e portas, bem como para dados de "integração", como aqueles coletados para Kubernetes, métricas avançadas do ONTAP e plug-ins do Telegraf. Esses monitores *métricos* alertam você quando limites de nível de alerta ou nível crítico são ultrapassados.

Você também pode criar monitores para disparar alertas de nível de aviso, crítico ou informativo quando *eventos de log* especificados forem detectados.

O Data Infrastructure Insights fornece uma série de"Monitores definidos pelo sistema" também, com base no seu ambiente.

Melhores práticas de segurança

Os alertas do Data Infrastructure Insights são projetados para destacar pontos de dados e tendências sobre seu locatário, e o Data Infrastructure Insights permite que você insira qualquer endereço de e-mail válido como destinatário do alerta. Se você estiver trabalhando em um ambiente seguro, fique especialmente atento a quem está recebendo a notificação ou tem acesso ao alerta.

Monitor métrico ou de log?

1. No menu Data Infrastructure Insights , clique em **Alertas > Gerenciar Monitores**

   A página Lista de monitores é exibida, mostrando os monitores configurados no momento.

2. Para modificar um monitor existente, clique no nome do monitor na lista.
3. Para adicionar um monitor, clique em **+ Monitor**.

Ao adicionar um novo monitor, você será solicitado a criar um Monitor de Métricas ou um Monitor de Logs.

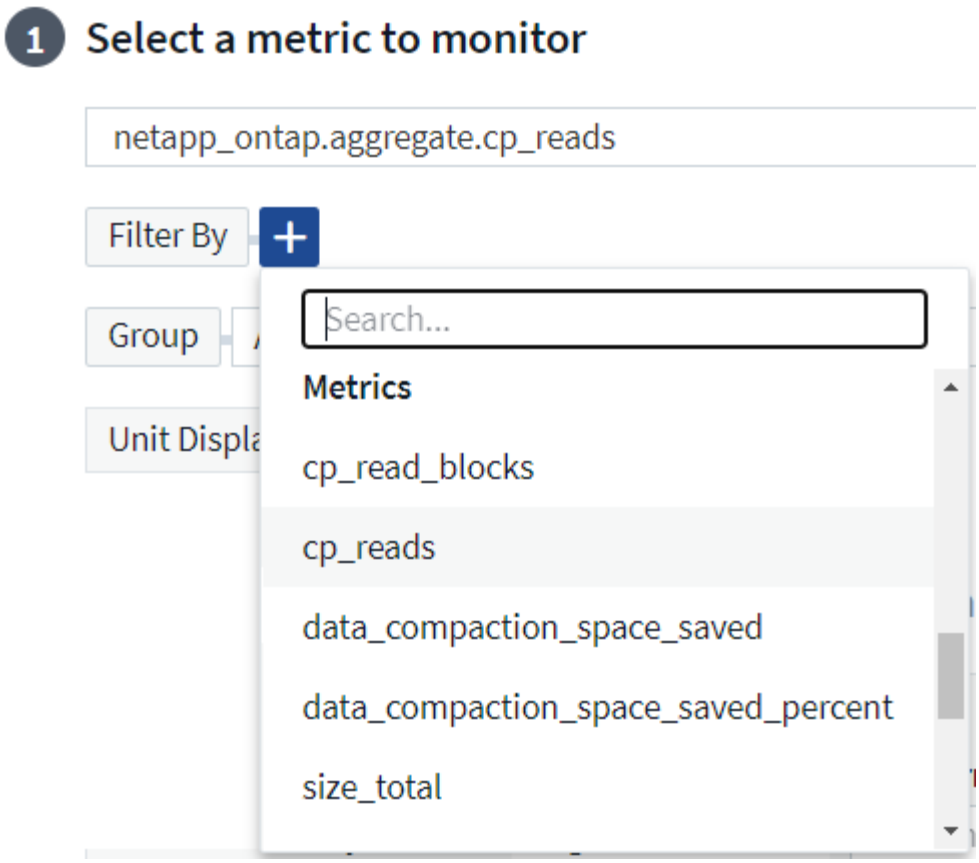
- Monitores *Metric* alertam sobre gatilhos relacionados à infraestrutura ou ao desempenho
- *Log* monitora alertas sobre atividades relacionadas a logs

Depois de escolher o tipo de monitor, a caixa de diálogo Configuração do monitor será exibida. A configuração varia dependendo do tipo de monitor que você está criando.

Monitor Métrico

1. No menu suspenso, pesquise e escolha um tipo de objeto e uma métrica para monitorar.

Você pode definir filtros para restringir quais atributos ou métricas de objeto monitorar.

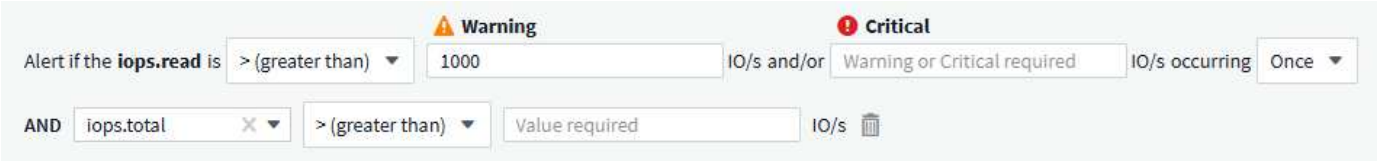


Ao trabalhar com dados de integração (Kubernetes, ONTAP Advanced Data, etc.), a filtragem de métricas remove os pontos de dados individuais/incomparáveis da série de dados plotados, diferentemente dos dados de infraestrutura (armazenamento, VM, portas, etc.), onde os filtros trabalham no valor agregado da série de dados e potencialmente removem o objeto inteiro do gráfico.

Os monitores de métricas se aplicam a objetos de inventário, como armazenamento, switch, host, VM, etc., bem como a métricas de integração, como dados do ONTAP Advanced ou do Kubernetes. Ao monitorar objetos de inventário, observe que você não pode selecionar um método "Agrupar por". Entretanto, o agrupamento *é* permitido ao monitorar dados de integração.

Monitores multicondições

Você pode optar por refinar ainda mais seu monitor métrico adicionando uma segunda condição. Basta expandir o prompt "+Adicionar condição métrica secundária" e configurar a condição adicional.



O monitor emitirá um alerta se ambas as condições forem atendidas.

Observe que você só pode usar "E" uma segunda condição; você não pode escolher alertar sobre uma condição OU sobre a outra.

Defina as condições do monitor.

1. Depois de escolher o objeto e a métrica a serem monitorados, defina os limites de nível de aviso e/ou nível

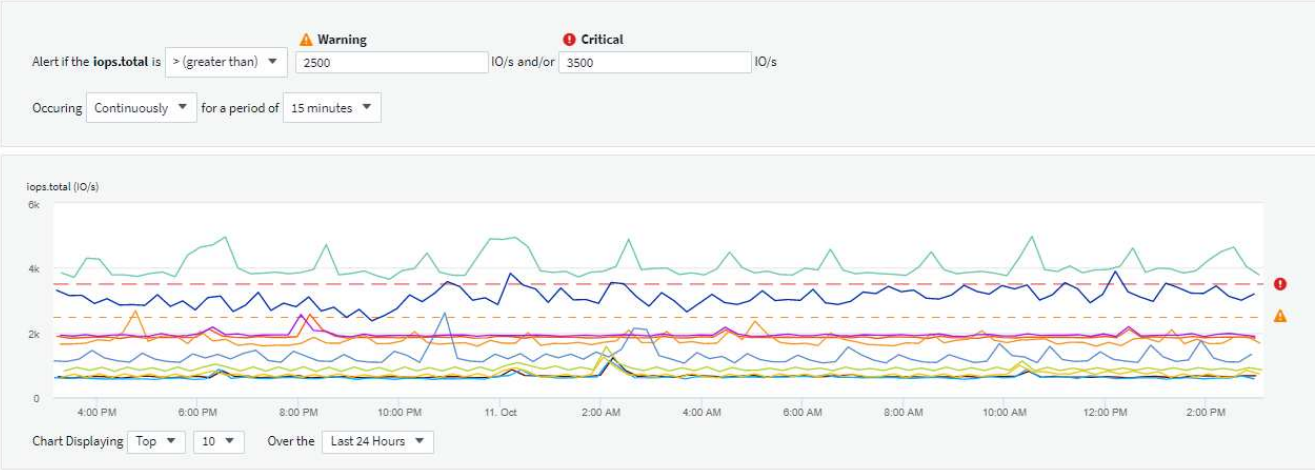
crítico.

2. Para o nível *Warning*, insira 200 para nosso exemplo. A linha tracejada que indica este nível de alerta é exibida no gráfico de exemplo.
3. Para o nível *Crítico*, insira 400. A linha tracejada que indica esse nível crítico é exibida no gráfico de exemplo.

   O gráfico exibe dados históricos. As linhas de nível de Aviso e Crítico no gráfico são uma representação visual do Monitor, para que você possa ver facilmente quando o Monitor pode disparar um alerta em cada caso.

4. Para o intervalo de ocorrência, escolha *Continuamente* por um período de *15 minutos*.

   Você pode optar por disparar um alerta no momento em que um limite for violado ou esperar até que o limite esteja em violação contínua por um período de tempo. Em nosso exemplo, não queremos ser alertados sempre que o IOPS total atingir o pico acima do nível de Aviso ou Crítico, mas apenas quando um objeto monitorado exceder continuamente um desses níveis por pelo menos 15 minutos.



Definir o comportamento de resolução de alerta

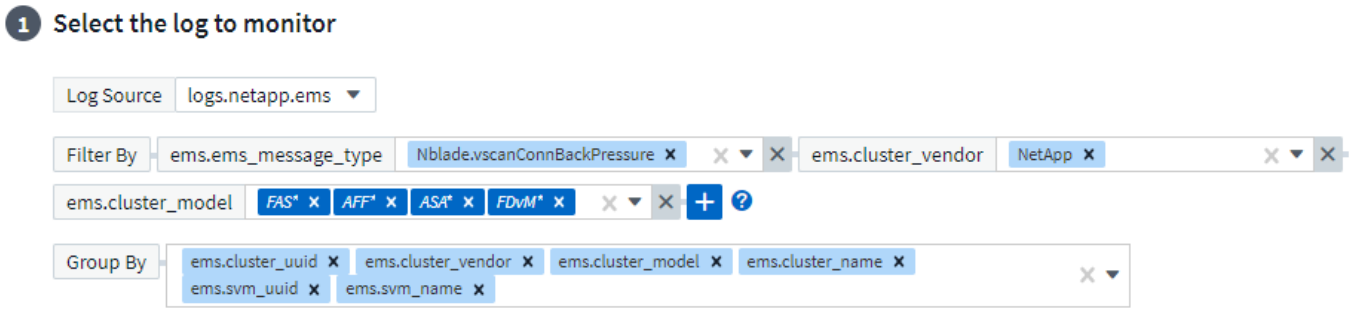
Você pode escolher como um alerta do monitor métrico é resolvido. Duas opções são apresentadas a você:

- Resolva quando a métrica retornar ao intervalo aceitável.
- Resolva quando a métrica estiver dentro do intervalo aceitável por um período de tempo especificado, de 1 minuto a 7 dias.

Monitor de Log

Ao criar um **Monitor de log**, primeiro escolha qual log monitorar na lista de logs disponível. Você pode então filtrar com base nos atributos disponíveis, conforme acima. Você também pode escolher um ou mais atributos "Agrupar por".

O filtro do Log Monitor não pode estar vazio.



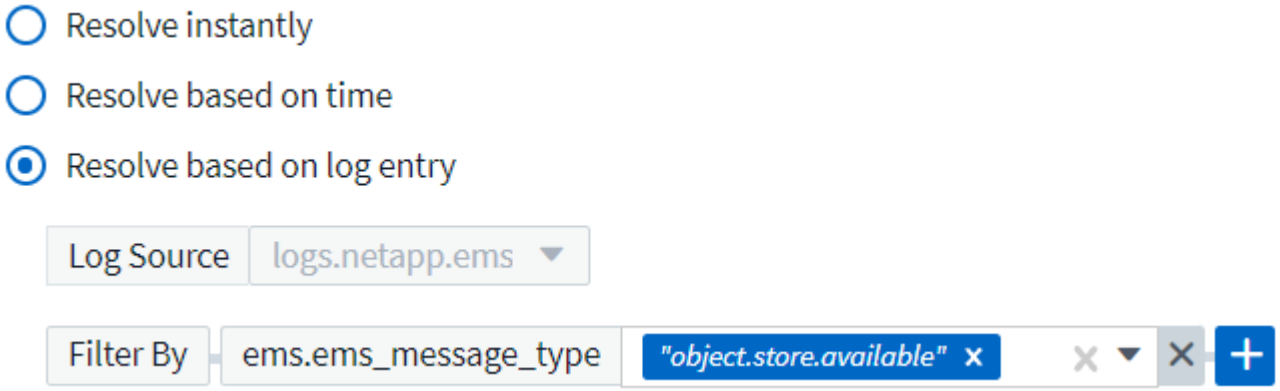
Defina o comportamento do alerta

Você pode criar o monitor para alertar com um nível de gravidade *Crítico*, *Aviso* ou *Informativo* quando as condições definidas acima ocorrerem uma vez (ou seja, imediatamente) ou esperar para alertar até que as condições ocorram 2 vezes ou mais.

Definir o comportamento de resolução de alerta

Você pode escolher como um alerta do monitor de log é resolvido. São apresentadas três opções:

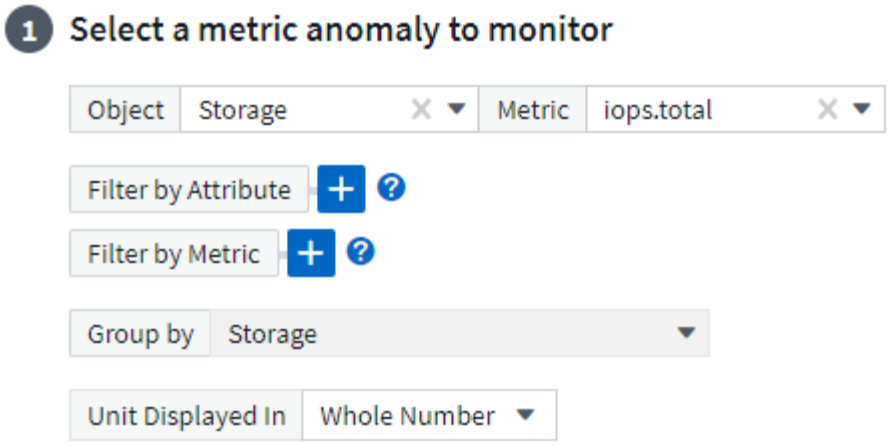
- **Resolver instantaneamente**: O alerta é resolvido imediatamente, sem necessidade de nenhuma outra ação
- **Resolver com base no tempo**: O alerta é resolvido após o tempo especificado ter passado
- **Resolver com base na entrada de log**: O alerta é resolvido quando uma atividade de log subsequente ocorre. Por exemplo, quando um objeto é registrado como "disponível".



Monitor de Detecção de Anomalias

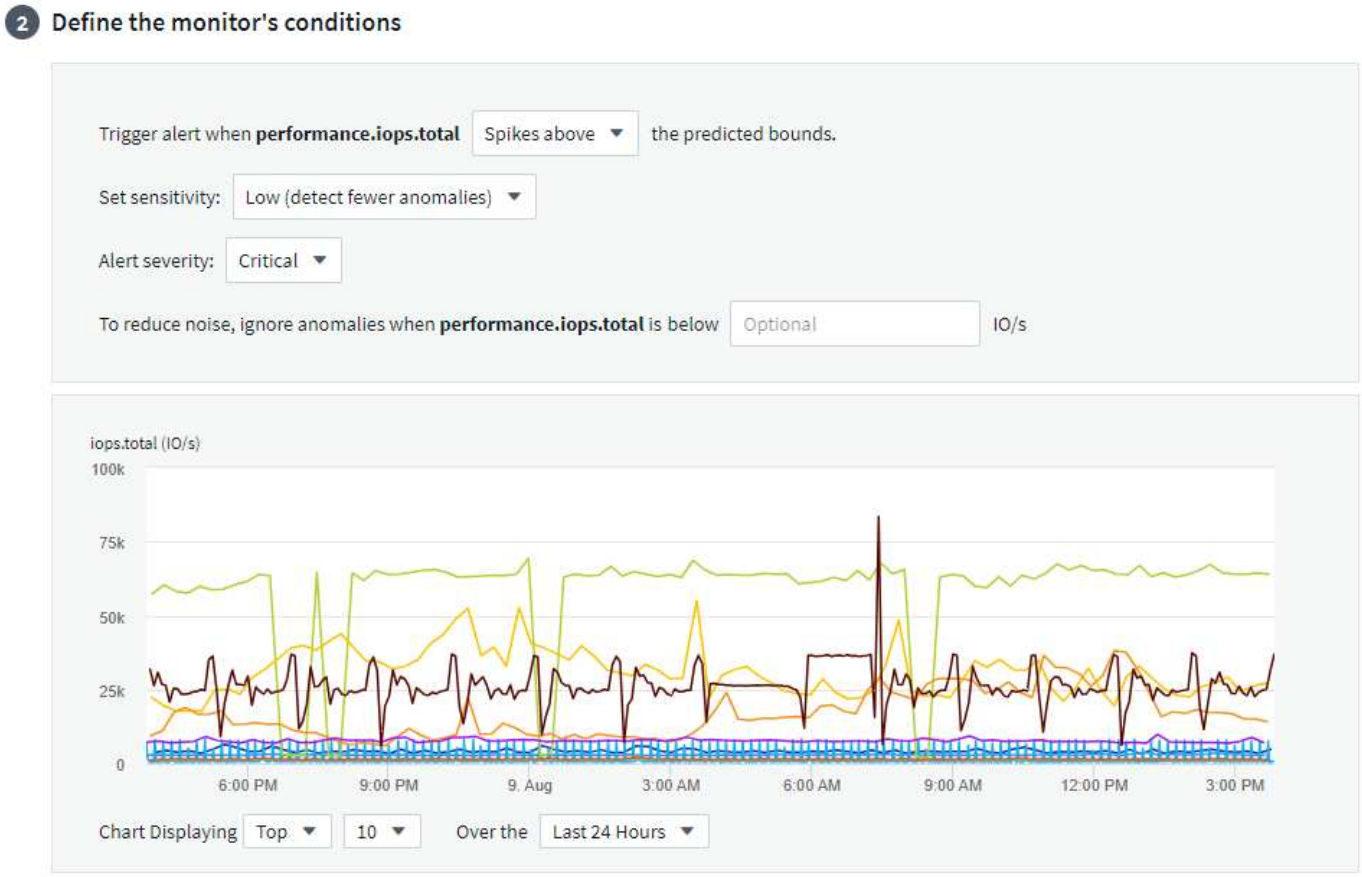
1. No menu suspenso, pesquise e escolha um tipo de objeto e uma métrica para monitorar.

Você pode definir filtros para restringir quais atributos ou métricas de objeto monitorar.



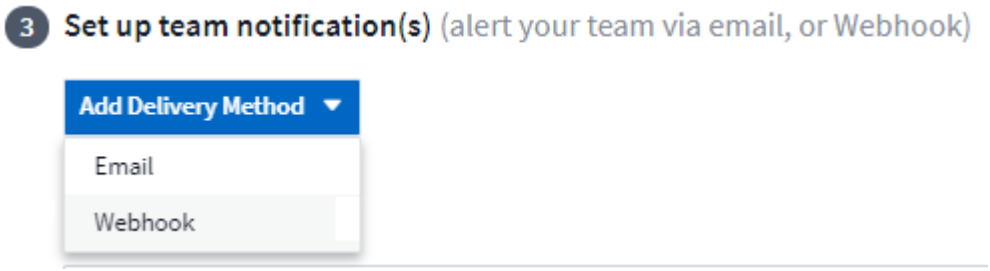
Defina as condições do monitor.

1. Depois de escolher o objeto e a métrica a serem monitorados, você define as condições sob as quais uma anomalia é detectada.
   - Escolha se deseja detectar uma anomalia quando a métrica escolhida **atingir o pico acima** dos limites previstos, **cair abaixo** desses limites ou **atingir o pico acima ou abaixo** dos limites.
   - Defina a **sensibilidade** da detecção. **Baixo** (menos anomalias são detectadas), **Médio** ou **Alto** (mais anomalias são detectadas).
   - Defina os alertas como **Aviso** ou **Crítico**.
   - Se desejar, você pode optar por reduzir o ruído, ignorando anomalias quando a métrica escolhida estiver abaixo de um limite definido por você.



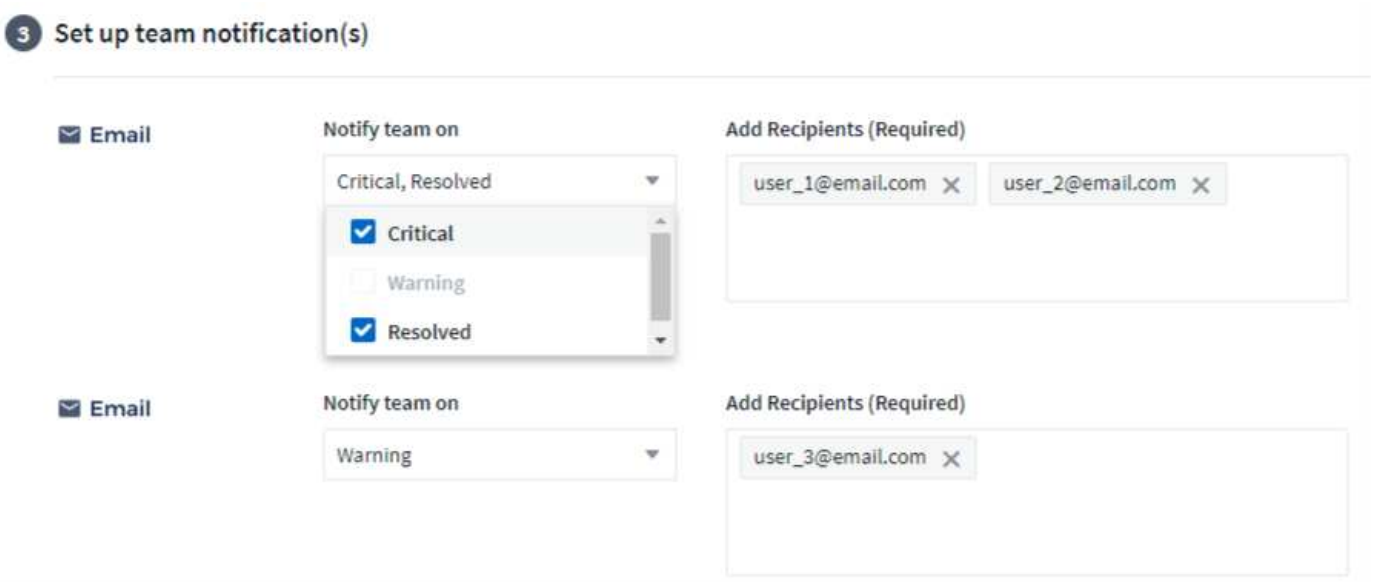
Selecione o tipo de notificação e os destinatários

Na seção *Configurar notificação(ões) da equipe*, você pode escolher se deseja alertar sua equipe por e-mail ou Webhook.



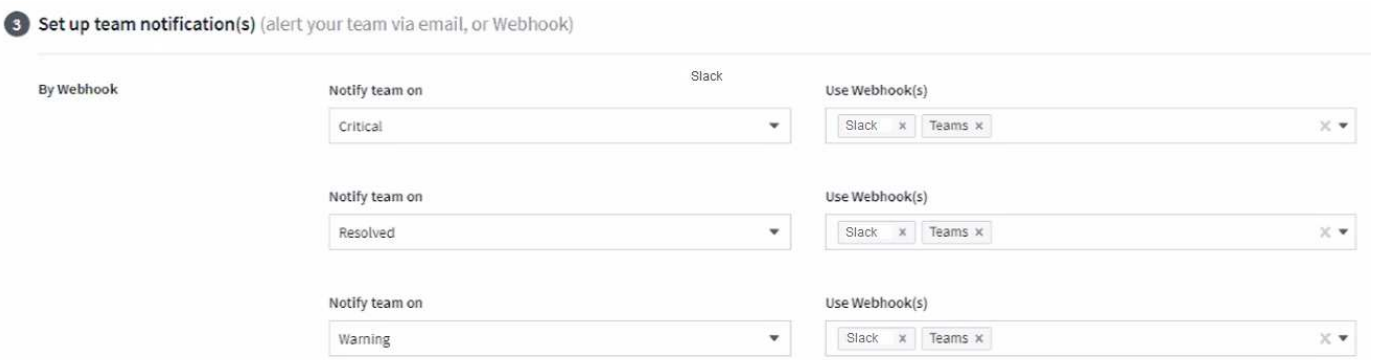
Alerta via e-mail:

Especifique os destinatários de e-mail para notificações de alerta. Se desejar, você pode escolher diferentes destinatários para alertas de aviso ou críticos.



Alerta via Webhook:

Especifique o(s) webhook(s) para notificações de alerta. Se desejar, você pode escolher diferentes webhooks para alertas de aviso ou críticos.



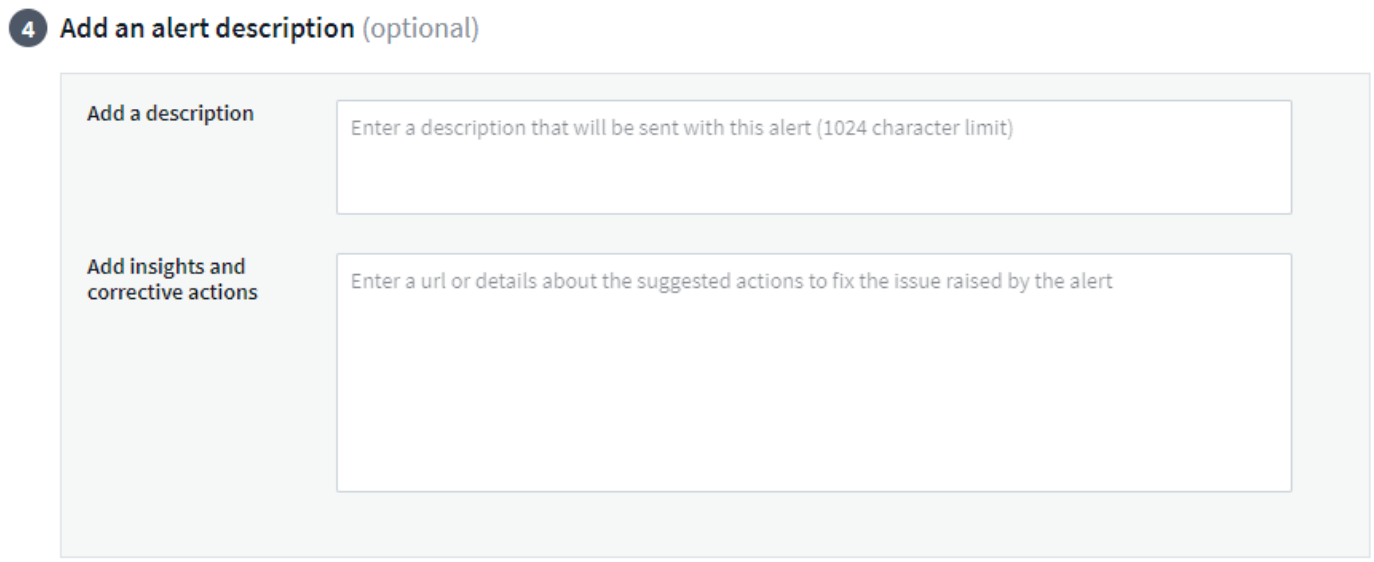
As notificações do ONTAP Data Collector têm precedência sobre quaisquer notificações específicas do Monitor que sejam relevantes para o cluster/coletor de dados. A lista de destinatários que você definiu para o próprio Coletor de Dados receberá os alertas do coletor de dados. Se não houver alertas ativos do coletor de dados, os alertas gerados pelo monitor serão enviados para destinatários específicos do monitor.

Definindo ações corretivas ou informações adicionais

Você pode adicionar uma descrição opcional, bem como insights adicionais e/ou ações corretivas preenchendo a seção **Adicionar uma descrição de alerta**. A descrição pode ter até 1024 caracteres e será enviada com o alerta. O campo de insights/ação corretiva pode ter até 67.000 caracteres e será exibido na seção de resumo da página inicial do alerta.

Nesses campos, você pode fornecer notas, links ou etapas a serem seguidas para corrigir ou abordar o alerta.

Você pode adicionar qualquer atributo de objeto (por exemplo, nome de armazenamento) como um parâmetro para uma descrição de alerta. Por exemplo, você pode definir parâmetros para o nome do volume e o nome do armazenamento em uma descrição como: "Alta latência para volume: *%%relatedObject.volume.name%%*, Armazenamento: *%%relatedObject.storage.name%%*".



Salve seu monitor

1. Se desejar, você pode adicionar uma descrição do monitor.
2. Dê ao Monitor um nome significativo e clique em **Salvar**.

   Seu novo monitor será adicionado à lista de monitores ativos.

Lista de Monitores

A página Monitor lista os monitores configurados atualmente, mostrando o seguinte:

- Nome do monitor
- Status
- Objeto/métrica sendo monitorado

- Condições do Monitor

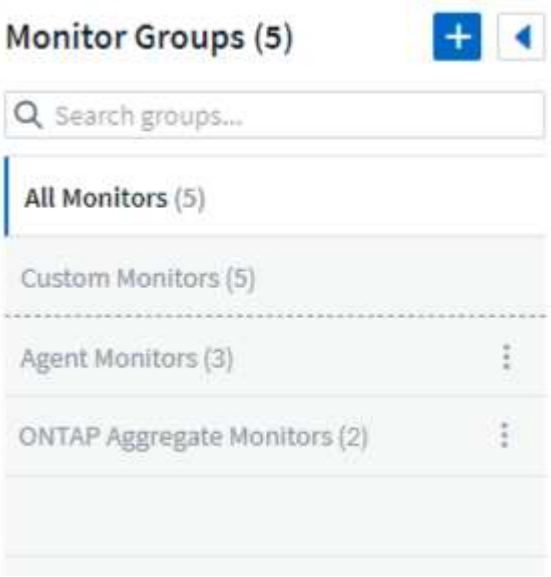
Você pode optar por pausar temporariamente o monitoramento de um tipo de objeto clicando no menu à direita do monitor e selecionando **Pausar**. Quando estiver pronto para retomar o monitoramento, clique em **Retomar**.

Você pode copiar um monitor selecionando **Duplicar** no menu. Você pode então modificar o novo monitor e alterar o objeto/métrica, filtro, condições, destinatários de e-mail, etc.

Se um monitor não for mais necessário, você pode excluí-lo selecionando **Excluir** no menu.

Grupos de Monitoramento

O agrupamento permite que você visualize e gerencie monitores relacionados. Por exemplo, você pode ter um grupo de monitores dedicado ao armazenamento em seu locatário ou monitores relevantes para uma determinada lista de destinatários.



Os seguintes grupos de monitores são mostrados. O número de monitores contidos em um grupo é mostrado ao lado do nome do grupo.

- **Todos os monitores** lista todos os monitores.
- **Monitores personalizados** lista todos os monitores criados pelo usuário.
- **Monitores suspensos** listará todos os monitores do sistema que foram suspensos pelo Data Infrastructure Insights.
- O Data Infrastructure Insights também mostrará uma série de **Grupos de Monitores de Sistema**, que listarão um ou mais grupos de"monitores definidos pelo sistema" , incluindo monitores de infraestrutura e carga de trabalho do ONTAP .

Monitores personalizados podem ser pausados, retomados, excluídos ou movidos para outro grupo. Os monitores definidos pelo sistema podem ser pausados e retomados, mas não podem ser excluídos ou movidos.

Monitores Suspensos

Este grupo só será exibido se o Data Infrastructure Insights tiver suspendido um ou mais monitores. Um monitor pode ser suspenso se estiver gerando alertas excessivos ou contínuos. Se o monitor for personalizado, modifique as condições para evitar o alerta contínuo e, em seguida, retome o monitoramento. O monitor será removido do grupo Monitores Suspensos quando o problema que causou a suspensão for resolvido.

Monitores definidos pelo sistema

Esses grupos mostrarão monitores fornecidos pelo Data Infrastructure Insights, desde que seu ambiente contenha os dispositivos e/ou disponibilidade de log exigidos pelos monitores.

Monitores definidos pelo sistema não podem ser modificados, movidos para outro grupo ou excluídos. No entanto, você pode duplicar um monitor do sistema e modificar ou mover a duplicata.

Os monitores do sistema podem incluir monitores para infraestrutura ONTAP (armazenamento, volume, etc.) ou cargas de trabalho (ou seja, monitores de log) ou outros grupos. A NetApp avalia constantemente as necessidades dos clientes e a funcionalidade do produto e atualizará ou adicionará monitores e grupos do sistema conforme necessário.

Grupos de monitores personalizados

Você pode criar seus próprios grupos para conter monitores com base em suas necessidades. Por exemplo, você pode querer um grupo para todos os seus monitores relacionados ao armazenamento.

Para criar um novo grupo de monitores personalizado, clique no botão **"+" Criar novo grupo de monitores**. Digite um nome para o grupo e clique em **Criar Grupo**. Um grupo vazio é criado com esse nome.

Para adicionar monitores ao grupo, vá para o grupo *Todos os Monitores* (recomendado) e faça um dos seguintes:

- Para adicionar um único monitor, clique no menu à direita do monitor e selecione *Adicionar ao grupo*. Escolha o grupo ao qual deseja adicionar o monitor.
- Clique no nome do monitor para abrir a visualização de edição do monitor e selecione um grupo na seção *Associar a um grupo de monitores*.

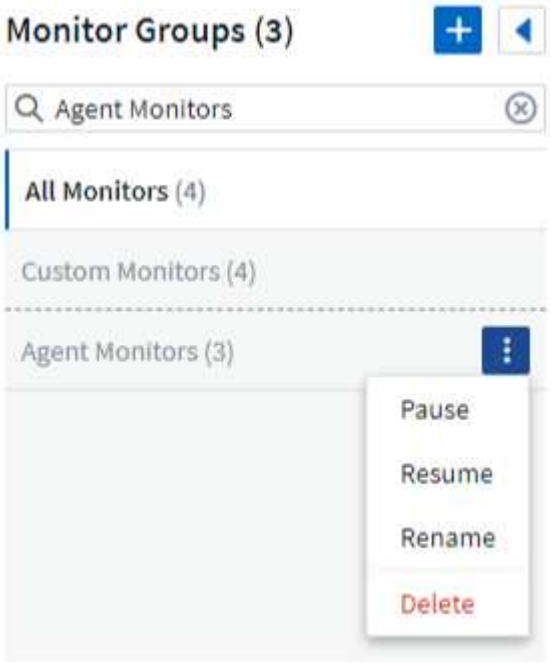
Remova monitores clicando em um grupo e selecionando *Remover do Grupo* no menu. Não é possível remover monitores do grupo *Todos os monitores* ou *Monitores personalizados*. Para excluir um monitor desses grupos, você deve excluir o próprio monitor.

Remover um monitor de um grupo não exclui o monitor do Data Infrastructure Insights. Para remover completamente um monitor, selecione-o e clique em *Excluir*. Isso também o remove do grupo ao qual pertencia e ele não fica mais disponível para nenhum usuário.

Você também pode mover um monitor para um grupo diferente da mesma maneira, selecionando *Mover para Grupo*.

Para pausar ou retomar todos os monitores de um grupo de uma só vez, selecione o menu do grupo e clique em *Pausar* ou *Retomar*.

Use o mesmo menu para renomear ou excluir um grupo. A exclusão de um grupo não exclui os monitores do Data Infrastructure Insights; eles ainda estão disponíveis em *Todos os monitores*.



Monitores definidos pelo sistema

O Data Infrastructure Insights inclui vários monitores definidos pelo sistema para métricas e logs. Os monitores do sistema disponíveis dependem dos coletores de dados presentes no seu locatário. Por isso, os monitores disponíveis no Data Infrastructure Insights podem mudar conforme coletores de dados são adicionados ou suas configurações são alteradas.

Veja o"Monitores definidos pelo sistema" página para descrições dos monitores incluídos no Data Infrastructure Insights.

Mais informações

- "Visualizando e descartando alertas"

Visualizando e gerenciando alertas de monitores

O Data Infrastructure Insights exibe alertas quando"limiares monitorados" são excedidos.

Monitores e alertas estão disponíveis no Data Infrastructure Insights Standard Edition e superiores.

Visualizando e gerenciando alertas

Para visualizar e gerenciar alertas, faça o seguinte.

1. Navegue até a página **Alertas > Todos os alertas**.
2. Uma lista com até 1.000 alertas mais recentes é exibida. Você pode classificar esta lista em qualquer campo clicando no cabeçalho da coluna do campo. A lista exibe as seguintes informações. Observe que nem todas essas colunas são exibidas por padrão. Você pode selecionar colunas para exibir clicando no ícone de "engrenagem":
   - **ID do alerta**: ID de alerta exclusivo gerado pelo sistema
   - **Hora de disparo**: Hora em que o Monitor relevante disparou o alerta
   - **Gravidade atual** (guia Alertas ativos): A gravidade atual do alerta ativo
   - **Gravidade máxima** (guia Alertas resolvidos); A gravidade máxima do alerta antes de ser resolvido
   - **Monitor**: O monitor configurado para disparar o alerta
   - **Acionado em**: O objeto no qual o limite monitorado foi violado
   - **Status**: Status de alerta atual, *Novo* ou *Em andamento*
   - **Status ativo**: *Ativo* ou *Resolvido*
   - **Condição**: A condição limite que acionou o alerta
   - **Métrica**: A métrica do objeto na qual o limite monitorado foi violado
   - **Status do monitor**: Status atual do monitor que disparou o alerta
   - **Possui ação corretiva**: O alerta sugeriu ações corretivas. Abra a página de alertas para visualizá-los.

Você pode gerenciar um alerta clicando no menu à direita do alerta e escolhendo uma das seguintes opções:

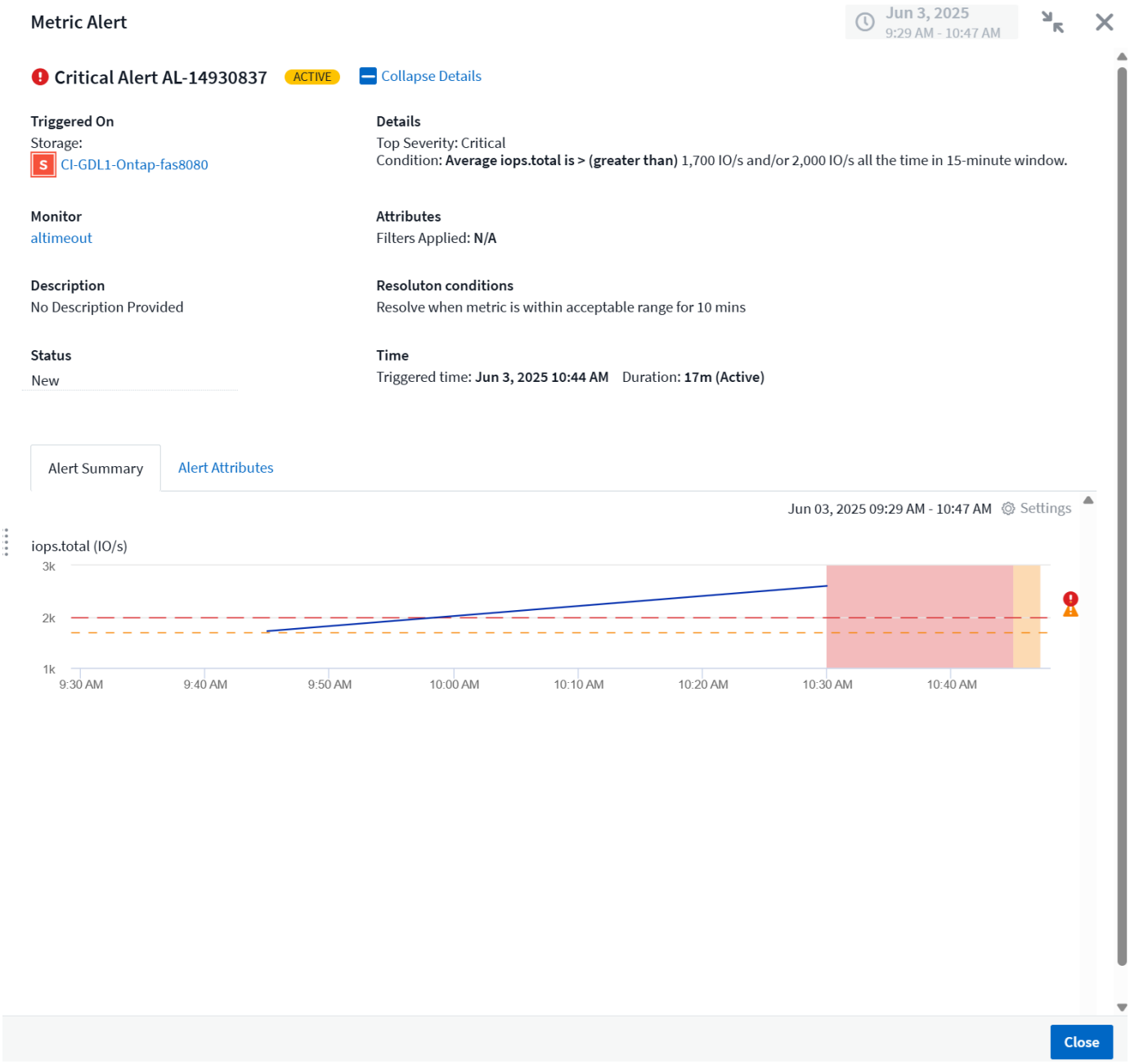
- **Em processo** para indicar que o alerta está sob investigação ou precisa ser mantido aberto
- **Dispensar** para remover o alerta da lista de alertas ativos.

Você pode gerenciar vários alertas marcando a caixa de seleção à esquerda de cada alerta e clicando em *Alterar status dos alertas selecionados*.

Clicar em um ID de alerta abre a página de detalhes do alerta.

Painel de detalhes de alerta

Selecione qualquer linha de alerta para abrir o painel de detalhes do alerta. O painel de detalhes do alerta fornece detalhes adicionais sobre o alerta, incluindo um *Resumo*, uma seção *Desempenho* mostrando gráficos relacionados aos dados do objeto, quaisquer *Ativos Relacionados* e *Comentários* inseridos pelos investigadores do alerta.



Alertas quando dados estão faltando

Em um sistema em tempo real como o Data Infrastructure Insights, para acionar a análise de um Monitor para decidir se um Alerta deve ser gerado, confiamos em uma de duas coisas:

- o próximo ponto de dados a chegar
- um temporizador para disparar quando não houver nenhum ponto de dados e você tiver esperado o tempo suficiente

Como é o caso da chegada lenta de dados (ou da ausência de chegada de dados), o mecanismo de temporizador precisa assumir o controle, pois a taxa de chegada de dados é insuficiente para disparar alertas em "tempo real". Então a pergunta normalmente se torna: "Quanto tempo devo esperar antes de fechar a janela de análise e ver o que tenho?" Se você esperar muito tempo, não estará gerando alertas rápido o suficiente para serem úteis.

Se você tiver um Monitor com uma janela de 30 minutos que percebe que uma condição foi violada pelo último ponto de dados antes de uma perda de dados de longo prazo, um Alerta será gerado porque o Monitor não recebeu nenhuma outra informação para confirmar uma recuperação da métrica ou perceber que a condição persistiu.

Alertas "Permanentemente Ativos"

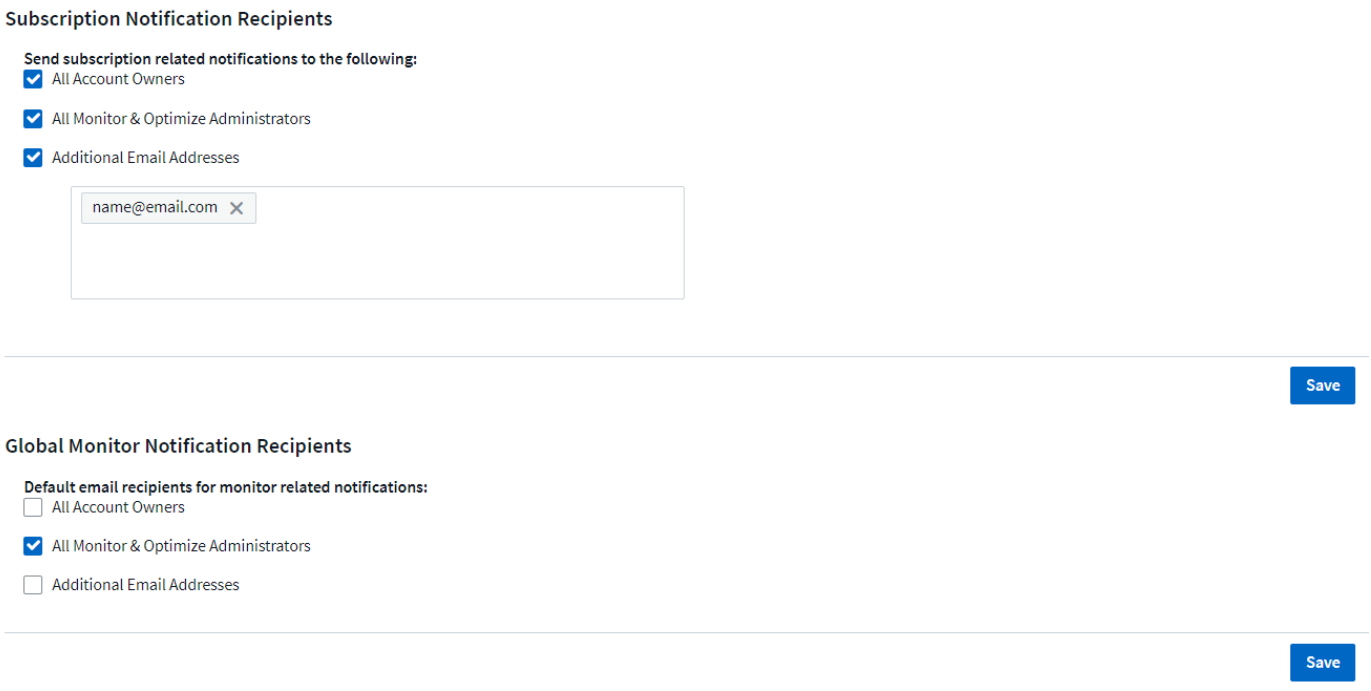
É possível configurar um monitor de forma que a condição **sempre** exista no objeto monitorado — por exemplo, IOPS > 1 ou latência > 0. Eles geralmente são criados como monitores de "teste" e depois esquecidos. Esses monitores criam alertas que ficam permanentemente abertos nos objetos constituintes, o que pode causar estresse no sistema e problemas de estabilidade ao longo do tempo.

Para evitar isso, o Data Infrastructure Insights fechará automaticamente qualquer alerta "permanentemente ativo" após 7 dias. Observe que as condições subjacentes do monitor podem (provavelmente) continuar a existir, fazendo com que um novo alerta seja emitido quase imediatamente, mas esse fechamento de alertas "sempre ativos" alivia parte do estresse do sistema que pode ocorrer de outra forma.

Configurando notificações por e-mail

Você pode configurar uma lista de e-mail para notificações relacionadas à assinatura, bem como uma lista global de e-mail de destinatários para notificação de violações de limites de política de desempenho.

Para configurar as definições do destinatário do e-mail de notificação, acesse a página **Admin > Notificações** e selecione a aba *E-mail*.



Destinatários de Notificação de Assinatura

Para configurar destinatários para notificações de eventos relacionadas à assinatura, vá para a seção "Destinatários de notificação de assinatura". Você pode optar por receber notificações por e-mail sobre eventos relacionados à assinatura para qualquer um ou todos os seguintes destinatários:

- Todos os proprietários de contas
- Todos os administradores de *Monitoramento e Otimização*
- Endereços de e-mail adicionais que você especificar

A seguir estão alguns exemplos dos tipos de notificações que podem ser enviadas e ações do usuário que você pode realizar.

Notificação:	**Ação do usuário:**
O teste ou assinatura foi atualizado	Revise os detalhes da assinatura em"Subscrição" página
A assinatura expirará em 90 dias A assinatura expirará em 30 dias	Nenhuma ação necessária se a “Renovação Automática” estiver habilitada. Entre em contato com as vendas da NetApp para renovar a assinatura.
O julgamento termina em 2 dias	Renovar o julgamento do"Subscrição" página. Você pode renovar um teste uma vez. Entre em contato com a equipe de vendas da NetApp para adquirir uma assinatura
O teste ou a assinatura expirou. A conta deixará de coletar dados em 48 horas. A conta será excluída após 48 horas.	Entre em contato com a equipe de vendas da NetApp para adquirir uma assinatura

Para garantir que seus destinatários recebam notificações do Data Infrastructure Insights, adicione os seguintes endereços de e-mail a quaisquer listas de "permissão":

- accounts@service.cloudinsights.netapp.com
- DoNotReply@cloudinsights.netapp.com

Lista global de destinatários para alertas

Notificações por e-mail de alertas são enviadas para a lista de destinatários do alerta para cada ação no alerta. Você pode optar por enviar notificações de alerta para uma lista global de destinatários.

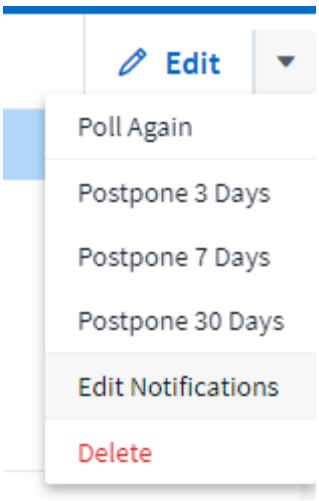
Para configurar destinatários de alertas globais, escolha os destinatários desejados na seção **Destinatários de notificação do Global Monitor**.

Você sempre pode substituir a lista global de destinatários de um monitor individual ao criar ou modificar o monitor.

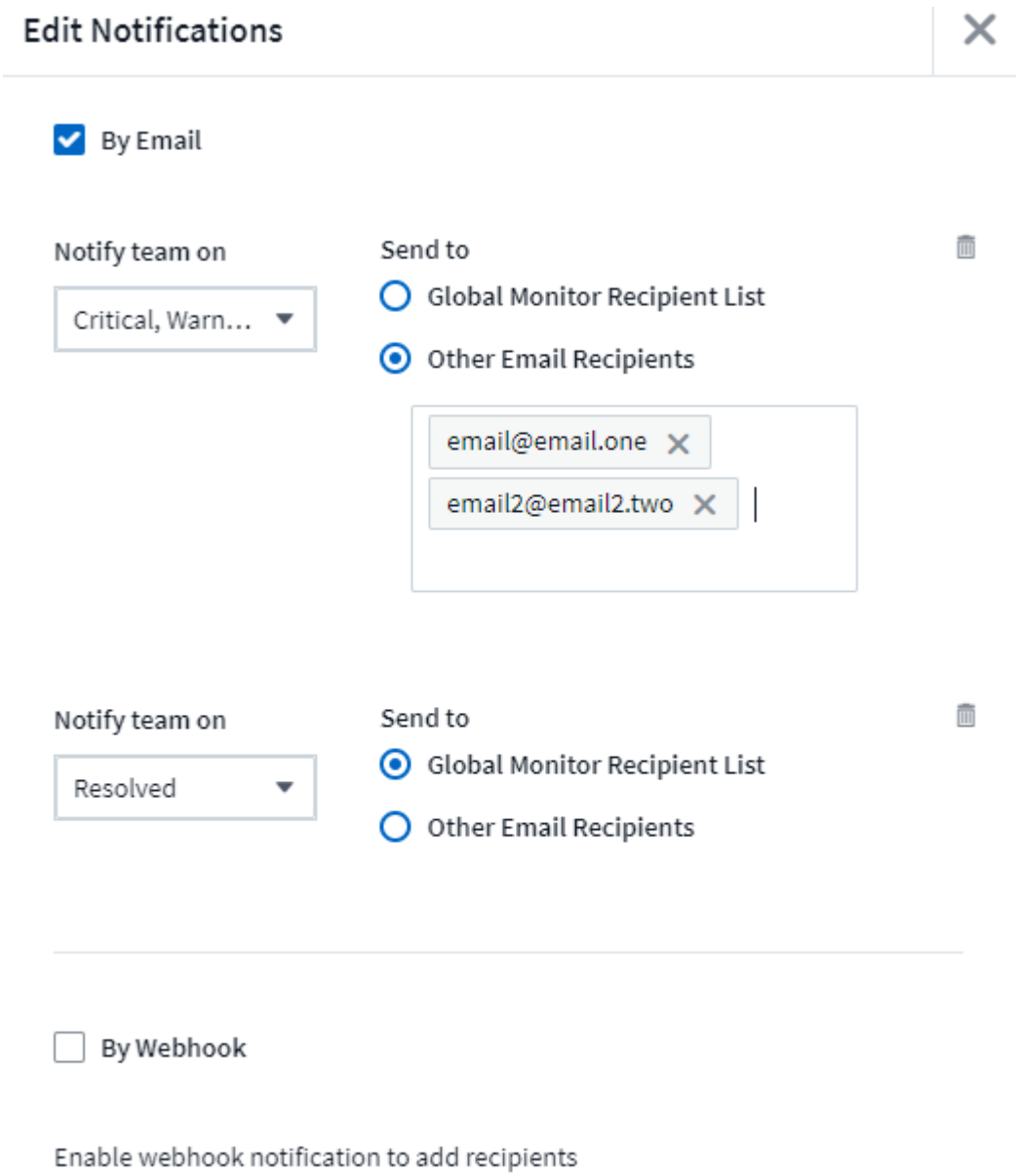
As notificações do ONTAP Data Collector têm precedência sobre quaisquer notificações específicas do Monitor que sejam relevantes para o cluster/coletor de dados. A lista de destinatários que você definiu para o próprio Coletor de Dados receberá os alertas do coletor de dados. Se não houver alertas ativos do coletor de dados, os alertas gerados pelo monitor serão enviados para destinatários específicos do monitor.

Editando notificações para ONTAP

Você pode modificar notificações para clusters ONTAP selecionando *Editar notificações* no menu suspenso superior direito em uma página inicial de armazenamento.



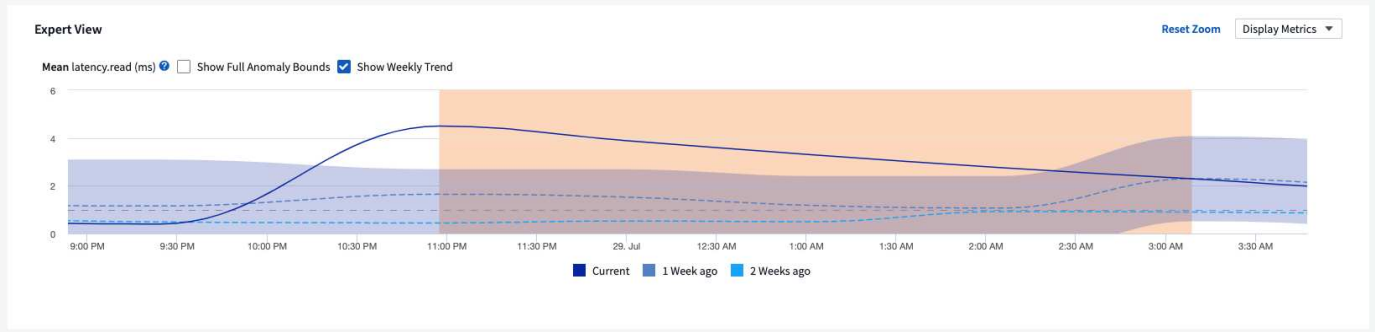
A partir daqui, você pode definir notificações para alertas Críticos, de Aviso, Informativos e/ou Resolvidos. Cada cenário pode notificar a lista de destinatários globais ou outros destinatários que você escolher.



Monitores de Detecção de Anomalias

A detecção de anomalias fornece insights sobre mudanças inesperadas nos padrões de dados do seu locatário. Uma anomalia ocorre quando o padrão de comportamento de um objeto muda. Por exemplo, se um objeto apresentar um certo nível de latência em um determinado horário nas quartas-feiras, mas a latência atingir um pico acima desse nível naquele horário na quarta-feira seguinte, esse pico será considerado uma anomalia. O Data Infrastructure Insights permite a criação de monitores para alertar quando anomalias como essa ocorrem.

A detecção de anomalias é adequada para métricas de objetos que exibem um padrão recorrente e previsível. Quando essas métricas de objetos ultrapassam ou caem abaixo dos níveis esperados, o Data Infrastructure Insights pode gerar um alerta para solicitar uma investigação.



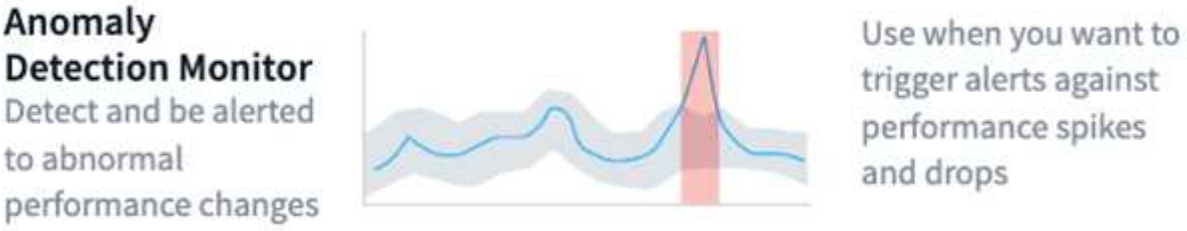
O que é detecção de anomalias?

Uma anomalia ocorre quando o valor médio de uma métrica está a uma série de desvios-padrão da média ponderada dessa métrica nas semanas anteriores, com as semanas recentes tendo mais peso do que as semanas anteriores. O Data Infrastructure Insights oferece a capacidade de monitorar dados e alertar quando anomalias são detectadas. Você tem a opção de definir os níveis de "sensibilidade" de detecção. Por exemplo, uma sensibilidade maior seria quando o valor médio tivesse menos desvios-padrão da média, fazendo com que mais alertas fossem gerados. Por outro lado, menor sensibilidade = mais desvios padrão da média = menos alertas.

O monitoramento de detecção de anomalias é diferente do monitoramento de limites.

- **O monitoramento baseado em limites** funciona quando você tem limites predefinidos para métricas específicas. Em outras palavras, quando você tem uma compreensão clara do que é esperado (ou seja, dentro de uma faixa normal).

- **O monitoramento de detecção de anomalias** usa algoritmos de aprendizado de máquina para identificar valores discrepantes que se desviam da norma, quando a definição de "normal" não é clara.



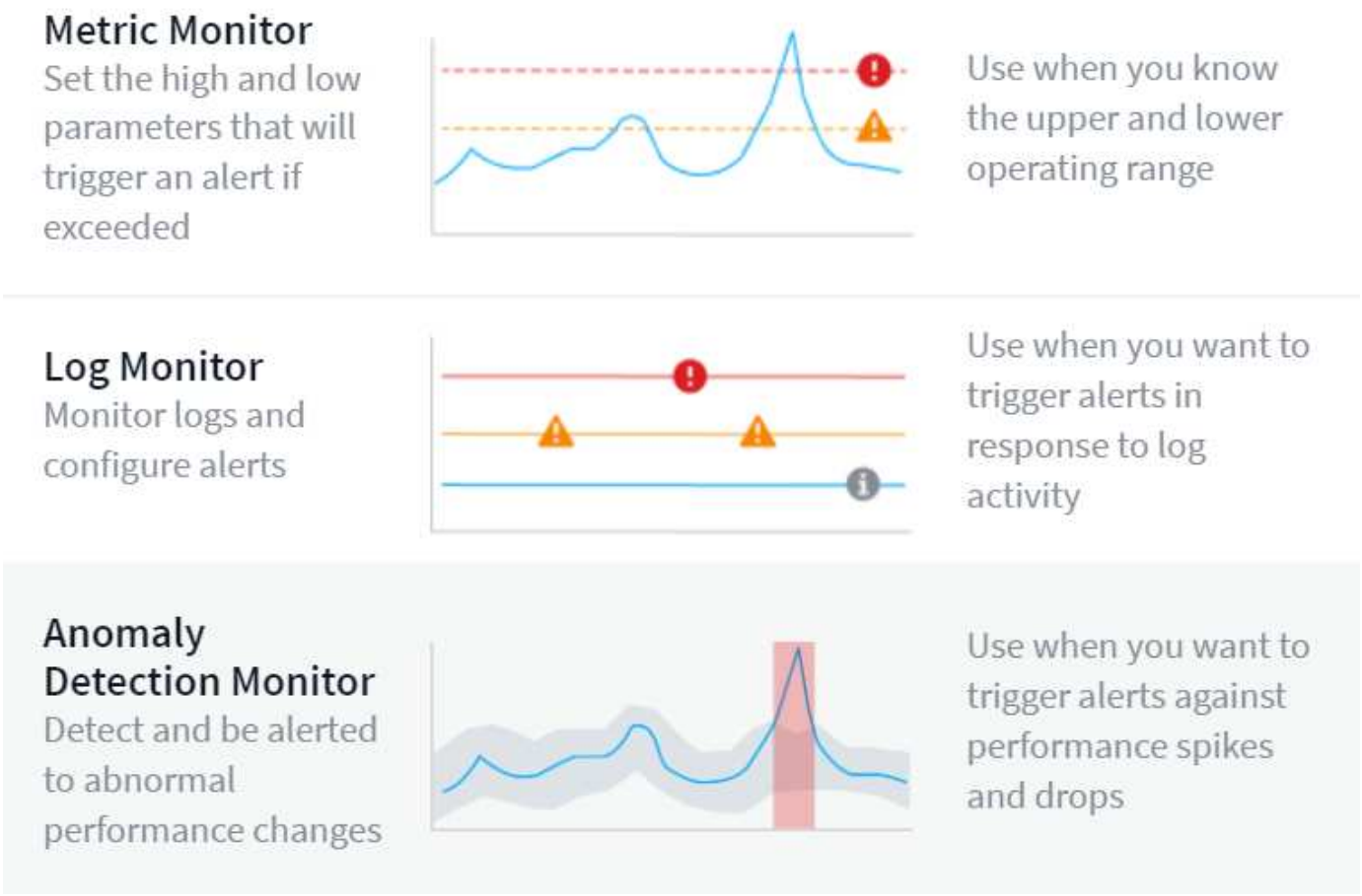
Quando eu precisaria de Detecção de Anomalias?

O monitoramento de detecção de anomalias pode fornecer alertas úteis para muitas situações, incluindo as seguintes:

- Quando a definição de *normal* não é clara. Por exemplo, taxas de erro de SAN podem ser esperadas em quantidades variáveis dependendo da porta. Alertar sobre um erro é barulhento e desnecessário, mas um aumento repentino ou significativo pode indicar um problema generalizado.
- Onde há mudanças ao longo do tempo. Cargas de trabalho que apresentam sazonalidade (ou seja, estão ocupadas ou calmas em determinados horários). Isso pode incluir períodos de silêncio inesperados que podem indicar uma paralisação do lote.
- Trabalhar com grandes quantidades de dados em que definir e ajustar manualmente os limites é impraticável. Por exemplo, um locatário com um grande número de hosts e/ou volumes com cargas de trabalho variadas. Cada um pode ter SLAs diferentes, então é importante entender aqueles que excedem a norma.

Criando um Monitor de Detecção de Anomalias

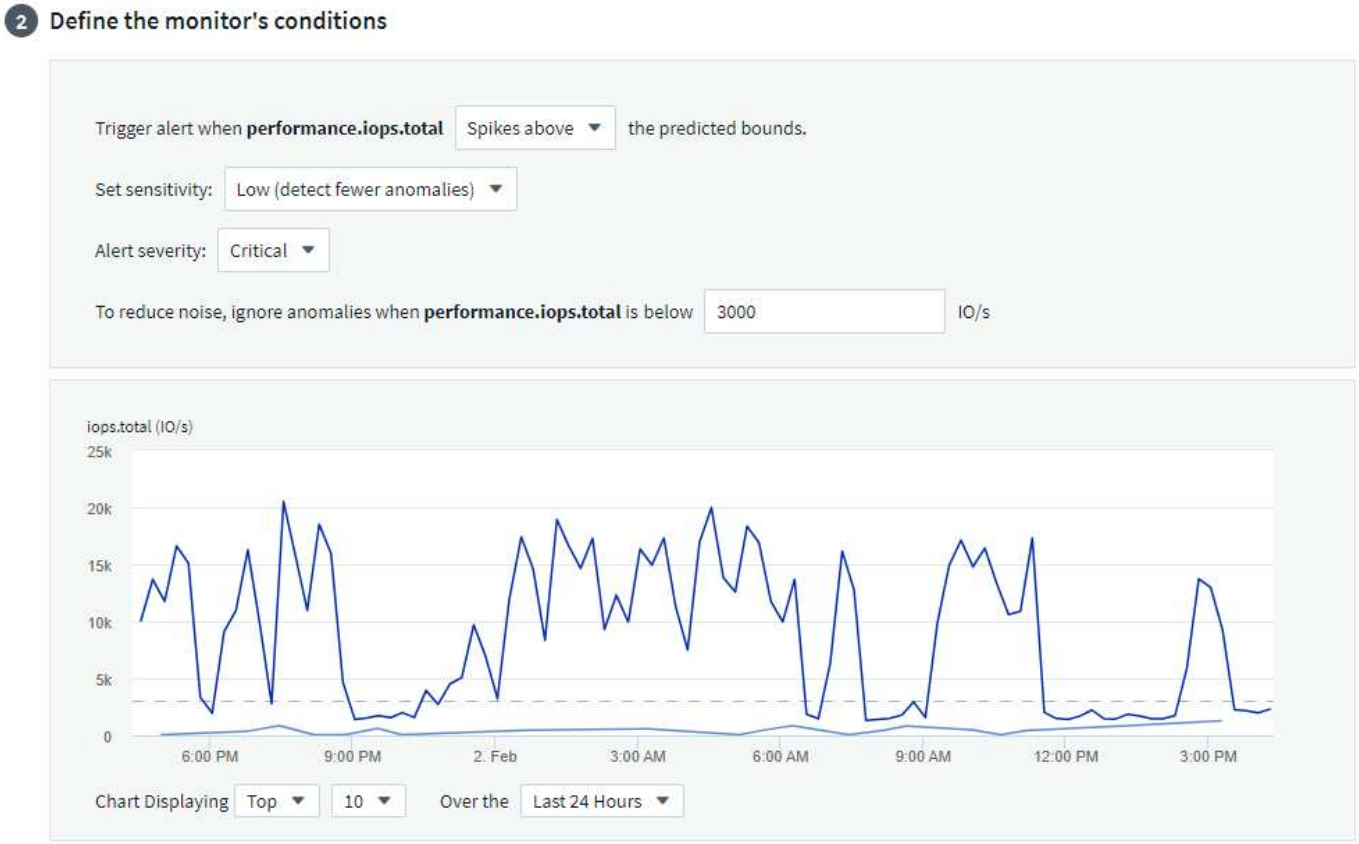
Para alertar sobre anomalias, crie um monitor navegando até **Observabilidade > Alertas > +Monitor**. Selecione *Monitor de detecção de anomalias* como o tipo de monitor.



Escolha o objeto e a métrica que você deseja monitorar. Você pode definir filtros e agrupamentos como em outros tipos de monitores.

Em seguida, defina as condições para o monitor.

- Dispare um alerta quando a métrica selecionada *aumentar acima* dos limites previstos, *cair abaixo* desses limites ou ambos.
- Defina a sensibilidade como *Média*, *Baixa* (menos anomalias são detectadas) ou *Alta* (mais anomalias são detectadas).
- Determine se o nível de alerta é *Crítico* ou *Aviso*.
- Opcionalmente, defina um valor abaixo do qual as anomalias serão *ignoradas*. Isso pode ajudar a reduzir o ruído. Este valor é mostrado como uma linha tracejada no gráfico de amostra.



Por fim, você pode configurar um método de entrega para os alertas (e-mail, webhook ou ambos), dar ao monitor uma descrição opcional ou ações corretivas e adicionar o monitor a um grupo personalizado, se desejar.

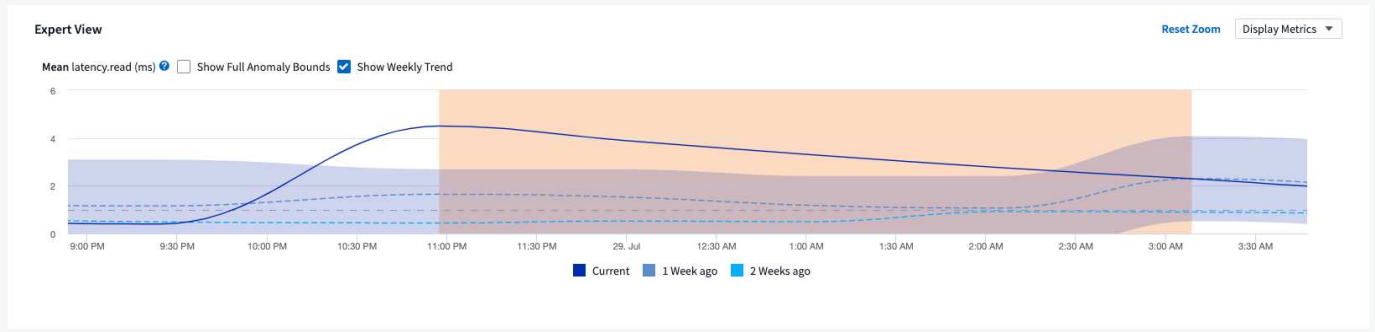
Salve o monitor com um nome significativo e pronto.

Após a criação, o monitor analisa dados da semana anterior para estabelecer uma linha de base inicial. A detecção de anomalias se torna mais precisa à medida que o tempo passa e mais histórico ocorre.

> Quando um monitor é criado, o DII analisa todos os dados existentes da semana anterior em busca de picos ou quedas significativas de dados; essas são consideradas anomalias. Durante a primeira semana após a criação do monitor (a fase de "aprendizagem"), há uma chance de aumento de "ruído" nos alertas. Para atenuar esse ruído, apenas picos ou quedas com duração superior a 30 minutos são considerados anomalias e geram alertas. Na semana seguinte, à medida que mais dados são analisados, o ruído normalmente diminui e um pico ou queda significativa que dure qualquer período de tempo será considerado uma anomalia.

Visualizando as anomalias

Em uma página de destino de alerta, os alertas disparados quando anomalias são detectadas mostrarão uma faixa destacada no gráfico, desde o momento em que a métrica atingiu o pico fora dos limites previstos até quando ela voltou a ficar dentro desses limites.



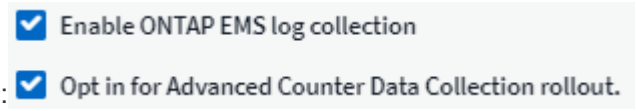
Ao visualizar um gráfico de anomalias em uma página de destino de alerta, você pode escolher as seguintes opções:

- Tendência semanal: compare valores no mesmo horário e dia de semanas anteriores, por até 5 semanas anteriores.
- Limites de anomalia completos: por padrão, o gráfico se concentra no valor da métrica para que você possa analisar melhor o comportamento da métrica. Selecione para mostrar os limites completos da anomalia (valor máximo, etc.)

Você também pode visualizar objetos que contribuíram para a anomalia selecionando-os na seção de desempenho da página de destino. O gráfico mostrará o comportamento dos objetos selecionados.

Monitores de sistema

O Data Infrastructure Insights inclui vários monitores definidos pelo sistema para métricas e logs. Os monitores do sistema disponíveis dependem dos coletores de dados presentes no seu locatário. Por isso, os monitores disponíveis no Data Infrastructure Insights podem mudar conforme coletores de dados são adicionados ou suas configurações são alteradas.

Muitos monitores do sistema estão no estado *Pausado* por padrão. Você pode habilitar um monitor do sistema selecionando a opção *Retomar* para o monitor. Certifique-se de que *Coleta avançada de dados do contador* e *Habilitar coleta de log do ONTAP EMS* estejam habilitados no Coletor de dados. Essas opções podem ser encontradas no ONTAP Data Collector em *Configuração avançada*: 

sumário:[]

Descrições do monitor

Os monitores definidos pelo sistema são compostos de métricas e condições predefinidas, bem como descrições padrão e ações corretivas, que não podem ser modificadas. Você *pode* modificar a lista de destinatários de notificações para monitores definidos pelo sistema. Para visualizar as métricas, condições, descrição e ações corretivas, ou para modificar a lista de destinatários, abra um grupo de monitores definido pelo sistema e clique no nome do monitor na lista.

Grupos de monitores definidos pelo sistema não podem ser modificados ou removidos.

Os seguintes monitores definidos pelo sistema estão disponíveis nos grupos indicados.

- * Infraestrutura ONTAP * inclui monitores para problemas relacionados à infraestrutura em clusters ONTAP .
- * Exemplos de carga de trabalho do ONTAP * incluem monitores para problemas relacionados à carga de trabalho.
- Os monitores em ambos os grupos assumem o estado padrão *Pausado*.

Abaixo estão os monitores de sistema atualmente incluídos no Data Infrastructure Insights:

Monitores Métricos

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva

Alta utilização da porta Fibre Channel	CRÍTICO	As portas do Protocolo Fibre Channel são usadas para receber e transferir o tráfego SAN entre o sistema host do cliente e os LUNs ONTAP . Se a utilização da porta for alta, isso se tornará um gargalo e, em última análise, afetará o desempenho de cargas de trabalho sensíveis do Protocolo Fibre Channel. Um alerta de aviso indica que uma ação planejada deve ser tomada para equilibrar o tráfego de rede. Um alerta crítico indica que a interrupção do serviço é iminente e medidas de emergência devem ser tomadas para equilibrar o tráfego de rede e garantir a continuidade do serviço.	Se o limite crítico for violado, considere ações imediatas para minimizar a interrupção do serviço: 1. Mova as cargas de trabalho para outra porta FCP com menor utilização. 2. Limite o tráfego de determinados LUNs apenas ao trabalho essencial, seja por meio de políticas de QoS no ONTAP ou configuração do lado do host para aliviar a utilização das portas FCP. Se o limite de aviso for ultrapassado, planeje tomar as seguintes ações: 1. Configure mais portas FCP para lidar com o tráfego de dados para que a utilização da porta seja distribuída entre mais portas. 2. Mova as cargas de trabalho para outra porta FCP com menor utilização. 3. Limite o tráfego de determinados LUNs apenas ao trabalho essencial, seja por meio de políticas de QoS no ONTAP ou configuração do lado do host para aliviar a utilização das portas FCP.

Latência Lun Alta	CRÍTICO	LUNs são objetos que atendem ao tráfego de E/S geralmente direcionado por aplicativos sensíveis ao desempenho, como bancos de dados. Altas latências de LUN significam que os próprios aplicativos podem sofrer e não conseguir realizar suas tarefas. Um alerta de aviso indica que uma ação planejada deve ser tomada para mover o LUN para o nó ou agregado apropriado. Um alerta crítico indica que a interrupção do serviço é iminente e medidas de emergência devem ser tomadas para garantir a continuidade do serviço. A seguir estão as latências esperadas com base no tipo de mídia: SSD de até 1 a 2 milissegundos; SAS de até 8 a 10 milissegundos e SATA HDD de 17 a 20 milissegundos	Se o limite crítico for violado, considere as seguintes ações para minimizar a interrupção do serviço: Se o LUN ou seu volume tiver uma política de QoS associada a ele, avalie seus limites e valide se eles estão causando a limitação da carga de trabalho do LUN. Se o limite de aviso for ultrapassado, planeje tomar as seguintes ações: 1. Se o agregado também estiver com alta utilização, mova o LUN para outro agregado. 2. Se o nó também estiver com alta utilização, mova o volume para outro nó ou reduza a carga de trabalho total do nó. 3. Se o LUN ou seu volume tiver uma política de QoS associada a ele, avalie seus limites e valide se eles estão causando a limitação da carga de trabalho do LUN.

Alta utilização da porta de rede	CRÍTICO	As portas de rede são usadas para receber e transferir o tráfego dos protocolos NFS, CIFS e iSCSI entre os sistemas host do cliente e os volumes ONTAP . Se a utilização da porta for alta, isso se tornará um gargalo e afetará o desempenho das cargas de trabalho NFS, CIFS e iSCSI. Um alerta de aviso indica que uma ação planejada deve ser tomada para equilibrar o tráfego de rede. Um alerta crítico indica que a interrupção do serviço é iminente e medidas de emergência devem ser tomadas para equilibrar o tráfego de rede e garantir a continuidade do serviço.	Se o limite crítico for violado, considere as seguintes ações imediatas para minimizar a interrupção do serviço: 1. Limite o tráfego de determinados volumes apenas ao trabalho essencial, seja por meio de políticas de QoS no ONTAP ou análise do lado do host para diminuir a utilização das portas de rede. 2. Configure um ou mais volumes para usar outra porta de rede com menor utilização. Se o limite de advertência for violado, considere as seguintes ações imediatas: 1. Configure mais portas de rede para lidar com o tráfego de dados para que a utilização da porta seja distribuída entre mais portas. 2. Configure um ou mais volumes para usar outra porta de rede menos utilizada.

Latência de namespace NVMe alta	CRÍTICO	Os namespaces NVMe são objetos que atendem ao tráfego de E/S gerado por aplicativos sensíveis ao desempenho, como bancos de dados. A alta latência dos namespaces NVMe significa que os próprios aplicativos podem sofrer e não conseguir realizar suas tarefas. Um alerta de aviso indica que uma ação planejada deve ser tomada para mover o LUN para o nó ou agregado apropriado. Um alerta crítico indica que a interrupção do serviço é iminente e medidas de emergência devem ser tomadas para garantir a continuidade do serviço.	Se o limite crítico for violado, considere ações imediatas para minimizar a interrupção do serviço: se o namespace NVMe ou seu volume tiver uma política de QoS atribuída a eles, avalie seus limites caso estejam causando a limitação da carga de trabalho do namespace NVMe. Se o limite de advertência for violado, considere tomar as seguintes ações: 1. Se o agregado também estiver com alta utilização, mova o LUN para outro agregado. 2. Se o nó também estiver com alta utilização, mova o volume para outro nó ou reduza a carga de trabalho total do nó. 3. Se o namespace NVMe ou seu volume tiver uma política de QoS atribuída a eles, avalie seus limites caso eles estejam causando limitação na carga de trabalho do namespace NVMe.

Capacidade QTree Total	CRÍTICO	Uma qtree é um sistema de arquivos definido logicamente que pode existir como um subdiretório especial do diretório raiz dentro de um volume. Cada qtree tem uma cota de espaço padrão ou uma cota definida por uma política de cota para limitar a quantidade de dados armazenados na árvore dentro da capacidade do volume. Um alerta de aviso indica que uma ação planejada deve ser tomada para aumentar o espaço. Um alerta crítico indica que a interrupção do serviço é iminente e medidas de emergência devem ser tomadas para liberar espaço e garantir a continuidade do serviço.	Se o limite crítico for violado, considere ações imediatas para minimizar a interrupção do serviço: 1. Aumente o espaço da qtree para acomodar o crescimento. 2. Exclua dados indesejados para liberar espaço. Se o limite de alerta for ultrapassado, planeje tomar as seguintes ações imediatas: 1. Aumente o espaço da qtree para acomodar o crescimento. 2. Exclua dados indesejados para liberar espaço.

Limite rígido de capacidade do QTree	CRÍTICO	Uma qtree é um sistema de arquivos definido logicamente que pode existir como um subdiretório especial do diretório raiz dentro de um volume. Cada qtree tem uma cota de espaço medida em KBytes que é usada para armazenar dados a fim de controlar o crescimento do volume de dados do usuário e não exceder sua capacidade total. Uma qtree mantém uma cota de capacidade de armazenamento flexível que fornece alertas ao usuário proativamente antes de atingir o limite de cota de capacidade total na qtree e não conseguir mais armazenar dados. Monitorar a quantidade de dados armazenados em uma qtree garante que o usuário receba serviço de dados ininterrupto.	Se o limite crítico for violado, considere as seguintes ações imediatas para minimizar a interrupção do serviço: 1. Aumentar a cota de espaço das árvores para acomodar o crescimento 2. Instrua o usuário a excluir dados indesejados na árvore para liberar espaço

Limite suave de capacidade do QTree	AVISO	Uma qtree é um sistema de arquivos definido logicamente que pode existir como um subdiretório especial do diretório raiz dentro de um volume. Cada qtree tem uma cota de espaço medida em KBytes que pode ser usada para armazenar dados a fim de controlar o crescimento do volume de dados do usuário e não exceder sua capacidade total. Uma qtree mantém uma cota de capacidade de armazenamento flexível que fornece alertas ao usuário proativamente antes de atingir o limite de cota de capacidade total na qtree e não conseguir mais armazenar dados. Monitorar a quantidade de dados armazenados em uma qtree garante que o usuário receba serviço de dados ininterrupto.	Se o limite de advertência for violado, considere as seguintes ações imediatas: 1. Aumente a cota de espaço das árvores para acomodar o crescimento. 2. Instrua o usuário a excluir dados indesejados na árvore para liberar espaço.
Limite rígido de arquivos QTree	CRÍTICO	Uma qtree é um sistema de arquivos definido logicamente que pode existir como um subdiretório especial do diretório raiz dentro de um volume. Cada qtree tem uma cota do número de arquivos que ela pode conter para manter um tamanho de sistema de arquivos gerenciável dentro do volume. Uma qtree mantém uma cota de número de arquivos rígidos além da qual novos arquivos na árvore são negados. Monitorar o número de arquivos em uma qtree garante que o usuário receba serviço de dados ininterrupto.	Se o limite crítico for violado, considere ações imediatas para minimizar a interrupção do serviço: 1. Aumentar a cota de contagem de arquivos para o qtree. 2. Exclua arquivos indesejados do sistema de arquivos qtree.

Limite suave de arquivos QTree	AVISO	Uma qtree é um sistema de arquivos definido logicamente que pode existir como um subdiretório especial do diretório raiz dentro de um volume. Cada qtree tem uma cota do número de arquivos que pode conter para manter um tamanho de sistema de arquivos gerenciável dentro do volume. Uma qtree mantém uma cota de número de arquivos flexível para fornecer alertas ao usuário proativamente antes de atingir o limite de arquivos na qtree e não conseguir armazenar nenhum arquivo adicional. Monitorar o número de arquivos em uma qtree garante que o usuário receba serviço de dados ininterrupto.	Se o limite de advertência for ultrapassado, planeje tomar as seguintes ações imediatas: 1. Aumentar a cota de contagem de arquivos para o qtree. 2. Exclua arquivos indesejados do sistema de arquivos qtree.

Reserva de espaço instantâneo cheia	CRÍTICO	A capacidade de armazenamento de um volume é necessária para armazenar dados de aplicativos e clientes. Uma parte desse espaço, chamada de espaço reservado para snapshots, é usada para armazenar snapshots que permitem que os dados sejam protegidos localmente. Quanto mais dados novos e atualizados forem armazenados no volume ONTAP , maior será a capacidade de snapshot usada e menor será a capacidade de armazenamento de snapshot disponível para dados novos ou atualizados no futuro. Se a capacidade de dados de instantâneos em um volume atingir o espaço total de reserva de instantâneos, isso poderá fazer com que o cliente não consiga armazenar novos dados de instantâneos e reduzir o nível de proteção dos dados no volume. Monitorar o volume utilizado da capacidade de snapshot garante a continuidade dos serviços de dados.	Se o limite crítico for violado, considere ações imediatas para minimizar a interrupção do serviço: 1. Configure snapshots para usar espaço de dados no volume quando a reserva de snapshots estiver cheia. 2. Exclua alguns instantâneos antigos indesejados para liberar espaço. Se o limite de advertência for ultrapassado, planeje tomar as seguintes ações imediatas: 1. Aumente o espaço de reserva do snapshot dentro do volume para acomodar o crescimento. 2. Configure snapshots para usar espaço de dados no volume quando a reserva de snapshots estiver cheia.

Limite de capacidade de armazenamento	CRÍTICO	Quando um pool de armazenamento (agregado) está ficando cheio, as operações de E/S ficam mais lentas e finalmente param, resultando em um incidente de interrupção de armazenamento. Um alerta de aviso indica que uma ação planejada deve ser tomada em breve para restaurar o espaço livre mínimo. Um alerta crítico indica que a interrupção do serviço é iminente e medidas de emergência devem ser tomadas para liberar espaço e garantir a continuidade do serviço.	Se o limite crítico for violado, considere imediatamente as seguintes ações para minimizar a interrupção do serviço: 1. Exclua instantâneos em volumes não críticos. 2. Exclua volumes ou LUNs que sejam cargas de trabalho não essenciais e que possam ser restaurados de cópias fora do armazenamento. Se o limite de aviso for violado, planeje as seguintes ações imediatas: 1. Mova um ou mais volumes para um local de armazenamento diferente. 2. Adicione mais capacidade de armazenamento. 3. Altere as configurações de eficiência de armazenamento ou coloque dados inativos em camadas no armazenamento em nuvem.

Limite de desempenho de armazenamento	CRÍTICO	Quando um sistema de armazenamento atinge seu limite de desempenho, as operações ficam mais lentas, a latência aumenta e as cargas de trabalho e os aplicativos podem começar a falhar. O ONTAP avalia a utilização do pool de armazenamento para cargas de trabalho e estima qual porcentagem de desempenho foi consumida.…Um alerta de aviso indica que uma ação planejada deve ser tomada para reduzir a carga do pool de armazenamento para garantir que haverá desempenho suficiente do pool de armazenamento para atender aos picos de carga de trabalho.…Um alerta crítico indica que uma queda de desempenho é iminente e medidas de emergência devem ser tomadas para reduzir a carga do pool de armazenamento para garantir a continuidade do serviço.	Se o limite crítico for violado, considere as seguintes ações imediatas para minimizar a interrupção do serviço: 1. Suspenda tarefas agendadas, como Snapshots ou replicação do SnapMirror . 2. Cargas de trabalho ociosas não essenciais.… Se o limite de advertência for ultrapassado, tome as seguintes medidas imediatamente: 1. Mova uma ou mais cargas de trabalho para um local de armazenamento diferente. 2. Adicione mais nós de armazenamento (AFF) ou prateleiras de disco (FAS) e redistribua as cargas de trabalho 3. Alterar características da carga de trabalho (tamanho do bloco, cache do aplicativo).

Limite rígido de capacidade de cota do usuário	CRÍTICO	O ONTAP reconhece os usuários de sistemas Unix ou Windows que têm direitos de acesso a volumes, arquivos ou diretórios dentro de um volume. Como resultado, o ONTAP permite que os clientes configurem a capacidade de armazenamento para seus usuários ou grupos de usuários de seus sistemas Linux ou Windows. A cota da política de usuário ou grupo limita a quantidade de espaço que o usuário pode utilizar para seus próprios dados. Um limite rígido dessa cota permite a notificação do usuário quando a quantidade de capacidade usada dentro do volume estiver próxima de atingir a cota de capacidade total. Monitorar a quantidade de dados armazenados dentro de uma cota de usuário ou grupo garante que o usuário receba serviço de dados ininterrupto.	Se o limite crítico for violado, considere as seguintes ações imediatas para minimizar a interrupção do serviço: 1. Aumente o espaço da cota do usuário ou grupo para acomodar o crescimento. 2. Instrua o usuário ou grupo a excluir dados indesejados para liberar espaço.

Limite suave de capacidade de cota do usuário	AVISO	O ONTAP reconhece os usuários de sistemas Unix ou Windows que têm direitos de acesso a volumes, arquivos ou diretórios dentro de um volume. Como resultado, o ONTAP permite que os clientes configurem a capacidade de armazenamento para seus usuários ou grupos de usuários de seus sistemas Linux ou Windows. A cota da política de usuário ou grupo limita a quantidade de espaço que o usuário pode utilizar para seus próprios dados. Um limite flexível dessa cota permite notificação proativa ao usuário quando a quantidade de capacidade usada dentro do volume está atingindo a cota de capacidade total. Monitorar a quantidade de dados armazenados dentro de uma cota de usuário ou grupo garante que o usuário receba serviço de dados ininterrupto.	Se o limite de advertência for ultrapassado, planeje tomar as seguintes ações imediatas: 1. Aumente o espaço da cota do usuário ou grupo para acomodar o crescimento. 2. Exclua dados indesejados para liberar espaço.

Capacidade de volume total	CRÍTICO	A capacidade de armazenamento de um volume é necessária para armazenar dados de aplicativos e clientes. Quanto mais dados armazenados no volume ONTAP , menor será a disponibilidade de armazenamento para dados futuros. Se a capacidade de armazenamento de dados em um volume atingir a capacidade total de armazenamento, o cliente poderá não conseguir armazenar dados devido à falta de capacidade de armazenamento. O monitoramento do volume utilizado da capacidade de armazenamento garante a continuidade dos serviços de dados.	Se o limite crítico for violado, considere as seguintes ações imediatas para minimizar a interrupção do serviço: 1. Aumente o espaço do volume para acomodar o crescimento. 2. Exclua dados indesejados para liberar espaço. 3. Se as cópias de snapshots ocuparem mais espaço do que a reserva de snapshots, exclua snapshots antigos ou ative a exclusão automática de snapshots de volume. Se o limite de aviso for violado, planeje tomar as seguintes ações imediatas: 1. Aumentar o espaço do volume para acomodar o crescimento 2. Se as cópias de snapshots ocuparem mais espaço do que a reserva de snapshots, exclua os snapshots antigos ou habilite a exclusão automática de snapshots de volume.……

Limite de Inodes de Volume	CRÍTICO	Volumes que armazenam arquivos usam nós de índice (inode) para armazenar metadados de arquivos. Quando um volume esgota sua alocação de inodes, nenhum outro arquivo pode ser adicionado a ele. Um alerta de aviso indica que uma ação planejada deve ser tomada para aumentar o número de inodes disponíveis. Um alerta crítico indica que o esgotamento do limite de arquivos é iminente e medidas de emergência devem ser tomadas para liberar inodes para garantir a continuidade do serviço.	Se o limite crítico for violado, considere as seguintes ações imediatas para minimizar a interrupção do serviço: 1. Aumente o valor dos inodes para o volume. Se o valor dos inodes já estiver no valor máximo, divida o volume em dois ou mais volumes porque o sistema de arquivos cresceu além do tamanho máximo. 2. Use o FlexGroup , pois ele ajuda a acomodar grandes sistemas de arquivos. Se o limite de alerta for ultrapassado, planeje tomar as seguintes ações imediatas: 1. Aumente o valor dos inodes para o volume. Se o valor dos inodes já estiver no máximo, divida o volume em dois ou mais volumes porque o sistema de arquivos cresceu além do tamanho máximo. 2. Use o FlexGroup , pois ele ajuda a acomodar grandes sistemas de arquivos

Latência de volume alta	CRÍTICO	Volumes são objetos que atendem ao tráfego de E/S, geralmente direcionado por aplicativos sensíveis ao desempenho, incluindo aplicativos devOps, diretórios pessoais e bancos de dados. Latências de alto volume significam que os próprios aplicativos podem sofrer e não conseguir realizar suas tarefas. Monitorar latências de volume é essencial para manter o desempenho consistente do aplicativo. As latências esperadas com base no tipo de mídia são: SSD de até 1 a 2 milissegundos; SAS de até 8 a 10 milissegundos e SATA HDD de 17 a 20 milissegundos.	Se o limite crítico for violado, considere as seguintes ações imediatas para minimizar a interrupção do serviço: Se o volume tiver uma política de QoS atribuída a ele, avalie seus limites, caso eles estejam causando a limitação da carga de trabalho do volume. Se o limite de advertência for violado, considere as seguintes ações imediatas: 1. Se o agregado também estiver com alta utilização, mova o volume para outro agregado. 2. Se o volume tiver uma política de QoS atribuída a ele, avalie seus limites, caso eles estejam causando limitação na carga de trabalho do volume. 3. Se o nó também estiver com alta utilização, mova o volume para outro nó ou reduza a carga de trabalho total do nó.
Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva

Nó de alta latência	AVISO / CRÍTICO	A latência do nó atingiu níveis em que pode afetar o desempenho dos aplicativos no nó. A menor latência do nó garante um desempenho consistente dos aplicativos. As latências esperadas com base no tipo de mídia são: SSD de até 1-2 milissegundos; SAS de até 8-10 milissegundos e SATA HDD de 17-20 milissegundos.	Se o limite crítico for violado, ações imediatas devem ser tomadas para minimizar a interrupção do serviço: 1. Suspender tarefas agendadas, Snapshots ou replicação do SnapMirror 2. Reduza a demanda de cargas de trabalho de menor prioridade por meio de limites de QoS 3. Desative cargas de trabalho não essenciais. Considere ações imediatas quando o limite de aviso for violado: 1. Mova uma ou mais cargas de trabalho para um local de armazenamento diferente 2. Reduza a demanda de cargas de trabalho de menor prioridade por meio de limites de QoS 3. Adicione mais nós de armazenamento (AFF) ou prateleiras de disco (FAS) e redistribua as cargas de trabalho 4. Alterar características da carga de trabalho (tamanho do bloco, cache do aplicativo etc.)

Limite de desempenho do nó	AVISO / CRÍTICO	A utilização do desempenho do nó atingiu níveis em que pode afetar o desempenho dos IOs e dos aplicativos suportados pelo nó. A baixa utilização do desempenho do nó garante um desempenho consistente dos aplicativos.	Ações imediatas devem ser tomadas para minimizar a interrupção do serviço se o limite crítico for violado: 1. Suspender tarefas agendadas, Snapshots ou replicação do SnapMirror 2. Reduza a demanda de cargas de trabalho de menor prioridade por meio de limites de QoS 3. Desative cargas de trabalho não essenciais. Considere as seguintes ações se o limite de aviso for violado: 1. Mova uma ou mais cargas de trabalho para um local de armazenamento diferente 2. Reduza a demanda de cargas de trabalho de menor prioridade por meio de limites de QoS 3. Adicione mais nós de armazenamento (AFF) ou prateleiras de disco (FAS) e redistribua as cargas de trabalho 4. Alterar características da carga de trabalho (tamanho do bloco, cache do aplicativo etc.)

VM de armazenamento de alta latência	AVISO / CRÍTICO	A latência da VM de armazenamento (SVM) atingiu níveis que podem afetar o desempenho dos aplicativos na VM de armazenamento. A menor latência da VM de armazenamento garante um desempenho consistente dos aplicativos. As latências esperadas com base no tipo de mídia são: SSD de até 1-2 milissegundos; SAS de até 8-10 milissegundos e SATA HDD de 17-20 milissegundos.	Se o limite crítico for violado, avalie imediatamente os limites para volumes da VM de armazenamento com uma política de QoS atribuída, para verificar se eles estão causando a limitação das cargas de trabalho do volume. Considere as seguintes ações imediatas quando o limite de aviso for violado: 1. Se o agregado também estiver com alta utilização, mova alguns volumes da VM de armazenamento para outro agregado. 2. Para volumes da VM de armazenamento com uma política de QoS atribuída, avalie os limites se eles estão causando a limitação das cargas de trabalho do volume 3. Se o nó estiver com alta utilização, mova alguns volumes da VM de armazenamento para outro nó ou reduza a carga de trabalho total do nó
Limite rígido de arquivos de cota de usuário	CRÍTICO	O número de arquivos criados no volume atingiu o limite crítico e arquivos adicionais não podem ser criados. Monitorar o número de arquivos armazenados garante que o usuário receba serviço de dados ininterrupto.	Ações imediatas são necessárias para minimizar a interrupção do serviço se o limite crítico for violado. Considere tomar as seguintes ações: 1. Aumentar a cota de contagem de arquivos para o usuário específico 2. Exclua arquivos indesejados para reduzir a pressão na cota de arquivos do usuário específico

Limite suave de arquivos de cota de usuário	AVISO	O número de arquivos criados no volume atingiu o limite da cota e está próximo do limite crítico. Você não pode criar arquivos adicionais se a cota atingir o limite crítico. Monitorar o número de arquivos armazenados por um usuário garante que ele receba serviço de dados ininterrupto.	Considere ações imediatas se o limite de advertência for violado: 1. Aumentar a cota de contagem de arquivos para a cota de usuário específica 2. Exclua arquivos indesejados para reduzir a pressão na cota de arquivos do usuário específico
Taxa de perda de cache de volume	AVISO / CRÍTICO	A taxa de falhas do cache de volume é a porcentagem de solicitações de leitura dos aplicativos clientes que são retornadas do disco em vez de serem retornadas do cache. Isso significa que o volume atingiu o limite definido.	Se o limite crítico for violado, ações imediatas devem ser tomadas para minimizar a interrupção do serviço: 1. Mova algumas cargas de trabalho para fora do nó do volume para reduzir a carga de E/S 2. Se ainda não estiver no nó do volume, aumente o cache WAFL comprando e adicionando um Flash Cache 3. Reduza a demanda de cargas de trabalho de menor prioridade no mesmo nó por meio de limites de QoS. Considere ações imediatas quando o limite de aviso for violado: 1. Mova algumas cargas de trabalho para fora do nó do volume para reduzir a carga de E/S 2. Se ainda não estiver no nó do volume, aumente o cache WAFL comprando e adicionando um Flash Cache 3. Reduza a demanda de cargas de trabalho de menor prioridade no mesmo nó por meio de limites de QoS 4. Alterar características da carga de trabalho (tamanho do bloco, cache do aplicativo etc.)

Sobrecomprometimento de cota do Volume Qtree	AVISO / CRÍTICO	O Volume Qtree Quota Overcommit especifica a porcentagem na qual um volume é considerado supercomprometido pelas cotas qtree. O limite definido para a cota qtree foi atingido para o volume. Monitorar o excesso de comprometimento da cota do qtree do volume garante que o usuário receba serviço de dados ininterrupto.	Se o limite crítico for violado, ações imediatas devem ser tomadas para minimizar a interrupção do serviço: 1. Aumentar o espaço do volume 2. Excluir dados indesejados Quando o limite de aviso for ultrapassado, considere aumentar o espaço do volume.

Voltar ao topo

Monitores de Log

Nome do monitor	Gravidade	Descrição	Ação corretiva
Credenciais da AWS não inicializadas	INFORMAÇÕES	Este evento ocorre quando um módulo tenta acessar credenciais baseadas em função do Amazon Web Services (AWS) Identity and Access Management (IAM) do thread de credenciais da nuvem antes que elas sejam inicializadas.	Aguarde até que o thread de credenciais da nuvem, bem como o sistema, concluam a inicialização.

Camada de nuvem inacessível	CRÍTICO	Um nó de armazenamento não pode se conectar à API de armazenamento de objetos do Cloud Tier. Alguns dados ficarão inacessíveis.	Se você usar produtos locais, execute as seguintes ações corretivas: …Verifique se o LIF intercluster está on-line e funcional usando o comando "network interface show"….Verifique a conectividade de rede com o servidor de armazenamento de objetos usando o comando "ping" no LIF intercluster do nó de destino.…Certifique-se do seguinte:…A configuração do seu armazenamento de objetos não foi alterada….As informações de login e conectividade ainda são válidas.…Entre em contato com o suporte técnico da NetApp se o problema persistir. Se você usar o Cloud Volumes ONTAP, execute as seguintes ações corretivas: …Certifique-se de que a configuração do seu armazenamento de objetos não tenha sido alterada.… Certifique-se de que as informações de login e conectividade ainda sejam válidas. Entre em contato com o suporte técnico da NetApp se o problema persistir.
Disco fora de serviço	INFORMAÇÕES	Este evento ocorre quando um disco é removido do serviço porque foi marcado como falha, está sendo higienizado ou entrou no Centro de Manutenção.	Nenhum.

FlexGroup Constituinte Completo	CRÍTICO	Um constituinte dentro de um volume FlexGroup está cheio, o que pode causar uma possível interrupção do serviço. Você ainda pode criar ou expandir arquivos no volume FlexGroup . Entretanto, nenhum dos arquivos armazenados no constituinte pode ser modificado. Como resultado, você poderá ver erros aleatórios de falta de espaço ao tentar executar operações de gravação no volume FlexGroup .	É recomendável adicionar capacidade ao volume FlexGroup usando o comando "volume modify -files +X". Como alternativa, exclua arquivos do volume FlexGroup . No entanto, é difícil determinar quais arquivos chegaram ao constituinte.
Constituinte do Flexgroup quase cheio	AVISO	Um constituinte dentro de um volume FlexGroup está quase sem espaço, o que pode causar uma possível interrupção do serviço. Os arquivos podem ser criados e expandidos. Entretanto, se o constituinte ficar sem espaço, talvez você não consiga anexar ou modificar os arquivos no constituinte.	É recomendável adicionar capacidade ao volume FlexGroup usando o comando "volume modify -files +X". Como alternativa, exclua arquivos do volume FlexGroup . No entanto, é difícil determinar quais arquivos chegaram ao constituinte.
Constituinte FlexGroup quase sem inodes	AVISO	Um constituinte dentro de um volume FlexGroup está quase sem inodes, o que pode causar uma possível interrupção do serviço. O constituinte recebe menos solicitações de criação do que a média. Isso pode afetar o desempenho geral do volume FlexGroup , porque as solicitações são roteadas para constituintes com mais inodes.	É recomendável adicionar capacidade ao volume FlexGroup usando o comando "volume modify -files +X". Como alternativa, exclua arquivos do volume FlexGroup . No entanto, é difícil determinar quais arquivos chegaram ao constituinte.

Constituinte FlexGroup fora dos inodes	CRÍTICO	Um constituinte de um volume FlexGroup ficou sem inodes, o que pode causar uma possível interrupção do serviço. Você não pode criar novos arquivos neste constituinte. Isso pode levar a uma distribuição geral desequilibrada de conteúdo no volume FlexGroup .	É recomendável adicionar capacidade ao volume FlexGroup usando o comando "volume modify -files +X". Como alternativa, exclua arquivos do volume FlexGroup . No entanto, é difícil determinar quais arquivos chegaram ao constituinte.
LUN offline	INFORMAÇÕES	Este evento ocorre quando um LUN é colocado offline manualmente.	Coloque o LUN novamente online.
Falha no ventilador da unidade principal	AVISO	Um ou mais ventiladores da unidade principal falharam. O sistema permanece operacional… No entanto, se a condição persistir por muito tempo, o excesso de temperatura pode desencadear um desligamento automático.	Recoloque os ventiladores com defeito. Se o erro persistir, substitua-os.
Ventilador da unidade principal em estado de alerta	INFORMAÇÕES	Este evento ocorre quando um ou mais ventiladores da unidade principal estão em estado de alerta.	Substitua os ventiladores indicados para evitar superaquecimento.

Bateria NVRAM fraca	AVISO	A capacidade da bateria NVRAM está criticamente baixa. Pode haver uma possível perda de dados se a bateria ficar sem carga. Seu sistema gera e transmite uma mensagem de AutoSupport ou "call home" para o suporte técnico da NetApp e os destinos configurados, se estiver configurado para isso. A entrega bem-sucedida de uma mensagem do AutoSupport melhora significativamente a determinação e a resolução de problemas.	Execute as seguintes ações corretivas:…Exiba o status atual, a capacidade e o estado de carregamento da bateria usando o comando "system node environment sensors show".…Se a bateria foi substituída recentemente ou o sistema ficou inoperante por um longo período de tempo, monitore a bateria para verificar se ela está carregando corretamente.…Entre em contato com o suporte técnico da NetApp se o tempo de execução da bateria continuar a diminuir abaixo dos níveis críticos e o sistema de armazenamento desligar automaticamente.
Processador de serviço não configurado	AVISO	Este evento ocorre semanalmente para lembrá-lo de configurar o Processador de Serviço (SP). O SP é um dispositivo físico incorporado ao seu sistema para fornecer recursos de acesso e gerenciamento remotos. Você deve configurar o SP para usar toda a sua funcionalidade.	Execute as seguintes ações corretivas:…Configure o SP usando o comando "system service-processor network modify".…Opcionalmente, obtenha o endereço MAC do SP usando o comando "system service-processor network show".…Verifique a configuração de rede do SP usando o comando "system service-processor network show".…Verifique se o SP pode enviar um e-mail de AutoSupport usando o comando "system service-processor autosupport invoke". OBSERVAÇÃO: Os hosts e destinatários de e-mail do AutoSupport devem ser configurados no ONTAP antes de você emitir este comando.

Processador de serviço offline	CRÍTICO	O ONTAP não está mais recebendo pulsações do Processador de Serviço (SP), mesmo que todas as ações de recuperação do SP tenham sido tomadas. O ONTAP não pode monitorar a saúde do hardware sem o SP.…O sistema será desligado para evitar danos ao hardware e perda de dados. Configure um alerta de pânico para ser notificado imediatamente se o SP ficar offline.	Desligue e ligue o sistema executando as seguintes ações:… Puxe o controlador para fora do chassi.… Empurre o controlador de volta.… Ligue o controlador novamente.… Se o problema persistir, substitua o módulo do controlador.
Ventiladores de prateleira falharam	CRÍTICO	O ventilador de resfriamento indicado ou o módulo do ventilador da prateleira falhou. Os discos na prateleira podem não receber fluxo de ar de resfriamento suficiente, o que pode resultar em falha do disco.	Execute as seguintes ações corretivas:…Verifique se o módulo do ventilador está totalmente encaixado e seguro. OBSERVAÇÃO: O ventilador é integrado ao módulo de fonte de alimentação em algumas prateleiras de disco. Se o problema persistir, substitua o módulo do ventilador. Se o problema persistir, entre em contato com o suporte técnico da NetApp para obter assistência.
O sistema não pode operar devido a falha do ventilador da unidade principal	CRÍTICO	Um ou mais ventiladores da unidade principal falharam, interrompendo a operação do sistema. Isso pode levar a uma possível perda de dados.	Substitua os ventiladores com defeito.
Discos não atribuídos	INFORMAÇÕES	O sistema tem discos não atribuídos - a capacidade está sendo desperdiçada e seu sistema pode ter alguma configuração incorreta ou alteração parcial de configuração aplicada.	Execute as seguintes ações corretivas:…Determine quais discos não estão atribuídos usando o comando "disk show -n".…Atribua os discos a um sistema usando o comando "disk assign".

Servidor antivírus ocupado	AVISO	O servidor antivírus está muito ocupado para aceitar novas solicitações de verificação.	Se esta mensagem ocorrer com frequência, certifique-se de que haja servidores antivírus suficientes para lidar com a carga de verificação de vírus gerada pelo SVM.
Credenciais da AWS para função do IAM expiradas	CRÍTICO	O Cloud Volume ONTAP ficou inacessível. As credenciais baseadas em função do Identity and Access Management (IAM) expiraram. As credenciais são adquiridas do servidor de metadados da Amazon Web Services (AWS) usando a função do IAM e são usadas para assinar solicitações de API para o Amazon Simple Storage Service (Amazon S3).	Execute o seguinte:…Faça login no AWS EC2 Management Console.…Navegue até a página Instâncias.…Encontre a instância para a implantação do Cloud Volumes ONTAP e verifique sua integridade.…Verifique se a função do AWS IAM associada à instância é válida e recebeu os privilégios adequados para a instância.
Credenciais da AWS para função do IAM não encontradas	CRÍTICO	O thread de credenciais de nuvem não pode adquirir as credenciais baseadas em função do Amazon Web Services (AWS) Identity and Access Management (IAM) do servidor de metadados da AWS. As credenciais são usadas para assinar solicitações de API para o Amazon Simple Storage Service (Amazon S3). O Cloud Volume ONTAP ficou inacessível.…	Execute o seguinte:…Faça login no AWS EC2 Management Console.…Navegue até a página Instâncias.…Encontre a instância para a implantação do Cloud Volumes ONTAP e verifique sua integridade.…Verifique se a função do AWS IAM associada à instância é válida e recebeu os privilégios adequados para a instância.

Credenciais da AWS para função do IAM inválidas	CRÍTICO	As credenciais baseadas em função do Identity and Access Management (IAM) não são válidas. As credenciais são adquiridas do servidor de metadados da Amazon Web Services (AWS) usando a função do IAM e são usadas para assinar solicitações de API para o Amazon Simple Storage Service (Amazon S3). O Cloud Volume ONTAP ficou inacessível.	Execute o seguinte:…Faça login no AWS EC2 Management Console.…Navegue até a página Instâncias.…Encontre a instância para a implantação do Cloud Volumes ONTAP e verifique sua integridade.…Verifique se a função do AWS IAM associada à instância é válida e recebeu os privilégios adequados para a instância.
Função do AWS IAM não encontrada	CRÍTICO	O thread de funções do Identity and Access Management (IAM) não consegue encontrar uma função do IAM da Amazon Web Services (AWS) no servidor de metadados da AWS. A função do IAM é necessária para adquirir credenciais baseadas em função usadas para assinar solicitações de API para o Amazon Simple Storage Service (Amazon S3). O Cloud Volume ONTAP ficou inacessível.…	Execute o seguinte:…Faça login no AWS EC2 Management Console.…Navegue até a página Instâncias.…Encontre a instância para a implantação do Cloud Volumes ONTAP e verifique sua integridade.…Verifique se a função do AWS IAM associada à instância é válida.
Função do AWS IAM inválida	CRÍTICO	A função de Gerenciamento de Identidade e Acesso (IAM) da Amazon Web Services (AWS) no servidor de metadados da AWS não é válida. O Cloud Volume ONTAP ficou inacessível.…	Execute o seguinte:…Faça login no AWS EC2 Management Console.…Navegue até a página Instâncias.…Encontre a instância para a implantação do Cloud Volumes ONTAP e verifique sua integridade.…Verifique se a função do AWS IAM associada à instância é válida e recebeu os privilégios adequados para a instância.

Falha na conexão do servidor de metadados da AWS	CRÍTICO	O thread de funções do Identity and Access Management (IAM) não consegue estabelecer um link de comunicação com o servidor de metadados da Amazon Web Services (AWS). A comunicação deve ser estabelecida para adquirir as credenciais baseadas em função do AWS IAM necessárias para assinar solicitações de API para o Amazon Simple Storage Service (Amazon S3). O Cloud Volume ONTAP ficou inacessível.…	Execute o seguinte:…Faça login no AWS EC2 Management Console.…Navegue até a página Instâncias.…Encontre a instância para a implantação do Cloud Volumes ONTAP e verifique sua integridade.…
Limite de uso de espaço do FabricPool quase atingido	AVISO	O uso total do espaço do FabricPool em todo o cluster de armazenamentos de objetos de provedores licenciados por capacidade quase atingiu o limite licenciado.	Execute as seguintes ações corretivas:… Verifique a porcentagem da capacidade licenciada usada por cada camada de armazenamento do FabricPool usando o comando "storage aggregate object-store show-space".… Exclua cópias de instantâneo de volumes com a política de camadas "snapshot" ou "backup" usando o comando "volume snapshot delete" para liberar espaço.… Instale uma nova licença no cluster para aumentar a capacidade licenciada.

Limite de uso de espaço do FabricPool atingido	CRÍTICO	O uso total do espaço do FabricPool em todo o cluster de armazenamentos de objetos de provedores licenciados por capacidade atingiu o limite de licença.	Execute as seguintes ações corretivas:… Verifique a porcentagem da capacidade licenciada usada por cada camada de armazenamento do FabricPool usando o comando "storage aggregate object-store show-space"…. Exclua cópias de instantâneo de volumes com a política de camadas "snapshot" ou "backup" usando o comando "volume snapshot delete" para liberar espaço.… Instale uma nova licença no cluster para aumentar a capacidade licenciada.

Falha na devolução do agregado	CRÍTICO	Este evento ocorre durante a migração de um agregado como parte de um failover de armazenamento (SFO), quando o nó de destino não consegue alcançar os armazenamentos de objetos.	Execute as seguintes ações corretivas:…Verifique se o LIF intercluster está on-line e funcional usando o comando "network interface show"….Verifique a conectividade de rede com o servidor de armazenamento de objetos usando o comando "ping" no LIF intercluster do nó de destino. …Verifique se a configuração do seu armazenamento de objetos não foi alterada e se as informações de login e conectividade ainda estão precisas usando o comando "aggregate object-store config show"….Como alternativa, você pode substituir o erro especificando false para o parâmetro "require-partner-waiting" do comando giveback.…Entre em contato com o suporte técnico da NetApp para obter mais informações ou assistência.

Interconexão HA inativa	AVISO	A interconexão de alta disponibilidade (HA) está inativa. Risco de interrupção do serviço quando o failover não estiver disponível.	As ações corretivas dependem do número e do tipo de links de interconexão HA suportados pela plataforma, bem como do motivo pelo qual a interconexão está inativa. …Se os links estiverem inativos:…Verifique se ambos os controladores no par HA estão operacionais.…Para links conectados externamente, certifique-se de que os cabos de interconexão estejam conectados corretamente e que os conectores de fator de forma pequeno (SFPs), se aplicável, estejam encaixados corretamente em ambos os controladores.…Para links conectados internamente, desabilite e reabilite os links, um após o outro, usando os comandos "ic link off" e "ic link on". …Se os links estiverem desabilitados, habilite-os usando o comando "ic link on". …Se um peer não estiver conectado, desative e reative os links, um após o outro, usando os comandos "ic link off" e "ic link on".…Entre em contato com o suporte técnico da NetApp se o problema persistir.

Máximo de sessões por usuário excedido	AVISO	Você excedeu o número máximo de sessões permitidas por usuário em uma conexão TCP. Qualquer solicitação para estabelecer uma sessão será negada até que algumas sessões sejam liberadas. …	Execute as seguintes ações corretivas: …Inspecione todos os aplicativos em execução no cliente e encerre aqueles que não estiverem funcionando corretamente.…Reinicialize o cliente.…Verifique se o problema é causado por um aplicativo novo ou existente:…Se o aplicativo for novo, defina um limite mais alto para o cliente usando o comando "cifs option modify -max-opens -same-file-per-tree". Em alguns casos, os clientes operam conforme o esperado, mas exigem um limite mais alto. Você deve ter privilégios avançados para definir um limite mais alto para o cliente. …Se o problema for causado por um aplicativo existente, pode haver um problema com o cliente. Entre em contato com o suporte técnico da NetApp para obter mais informações ou assistência.

Tempo máximo de abertura por arquivo excedido	AVISO	Você excedeu o número máximo de vezes que pode abrir o arquivo em uma conexão TCP. Qualquer solicitação para abrir este arquivo será negada até que você feche algumas instâncias abertas do arquivo. Isso normalmente indica um comportamento anormal do aplicativo.	Execute as seguintes ações corretivas:…Inspecione os aplicativos executados no cliente usando esta conexão TCP. O cliente pode estar operando incorretamente por causa do aplicativo em execução nele. Reinicie o cliente. Verifique se o problema é causado por um aplicativo novo ou existente: Se o aplicativo for novo, defina um limite mais alto para o cliente usando o comando "cifs option modify -max -opens-same-file-per -tree". Em alguns casos, os clientes operam conforme o esperado, mas exigem um limite mais alto. Você deve ter privilégios avançados para definir um limite mais alto para o cliente. …Se o problema for causado por um aplicativo existente, pode haver um problema com o cliente. Entre em contato com o suporte técnico da NetApp para obter mais informações ou assistência.

Conflito de nome NetBIOS	CRÍTICO	O Serviço de Nomes NetBIOS recebeu uma resposta negativa a uma solicitação de registro de nome de uma máquina remota. Isso geralmente é causado por um conflito no nome NetBIOS ou em um alias. Como resultado, os clientes podem não conseguir acessar dados ou se conectar ao nó de serviço de dados correto no cluster.	Execute qualquer uma das seguintes ações corretivas:…Se houver um conflito no nome NetBIOS ou em um alias, execute uma das seguintes ações:…Exclua o alias NetBIOS duplicado usando o comando "vserver cifs delete -aliases alias -vserver vserver".…Renomeie um alias NetBIOS excluindo o nome duplicado e adicionando um alias com um novo nome usando o comando "vserver cifs create -aliases alias -vserver vserver". …Se não houver aliases configurados e houver um conflito no nome NetBIOS, renomeie o servidor CIFS usando os comandos "vserver cifs delete -vserver vserver" e "vserver cifs create -cifs -server netbiosname". OBSERVAÇÃO: Excluir um servidor CIFS pode tornar os dados inacessíveis. …Remova o nome NetBIOS ou renomeie o NetBIOS na máquina remota.
Pool de armazenamento NFSv4 esgotado	CRÍTICO	Um pool de armazenamento NFSv4 foi esgotado.	Se o servidor NFS não responder por mais de 10 minutos após esse evento, entre em contato com o suporte técnico da NetApp .

Nenhum mecanismo de varredura registrado	CRÍTICO	O conector antivírus notificou o ONTAP de que não possui um mecanismo de verificação registrado. Isso pode causar indisponibilidade de dados se a opção "scan-mandatory" estiver habilitada.	Execute as seguintes ações corretivas:…Certifique-se de que o software do mecanismo de verificação instalado no servidor antivírus seja compatível com o ONTAP.…Certifique-se de que o software do mecanismo de verificação esteja em execução e configurado para se conectar ao conector antivírus por meio de loopback local.
Sem conexão Vscan	CRÍTICO	O ONTAP não tem conexão com o Vscan para atender solicitações de verificação de vírus. Isso pode causar indisponibilidade de dados se a opção "scan-mandatory" estiver habilitada.	Certifique-se de que o pool de scanners esteja configurado corretamente e que os servidores antivírus estejam ativos e conectados ao ONTAP.
Espaço de volume da raiz do nó baixo	CRÍTICO	O sistema detectou que o volume raiz está perigosamente com pouco espaço. O nó não está totalmente operacional. Os LIFs de dados podem ter falhado dentro do cluster, o que limita o acesso NFS e CIFS no nó. A capacidade administrativa é limitada aos procedimentos de recuperação local para o nó liberar espaço no volume raiz.	Execute as seguintes ações corretivas:… Libere espaço no volume raiz excluindo cópias antigas do Snapshot, excluindo arquivos que não são mais necessários do diretório /mroot ou expandindo a capacidade do volume raiz.… Reinicialize o controlador.… Entre em contato com o suporte técnico da NetApp para obter mais informações ou assistência.
Compartilhamento de administrador inexistente	CRÍTICO	Problema no Vscan: um cliente tentou se conectar a um compartilhamento ONTAP_ADMIN$ inexistente.	Certifique-se de que o Vscan esteja habilitado para o ID SVM mencionado. Habilitar o Vscan em um SVM faz com que o compartilhamento ONTAP_ADMIN$ seja criado para o SVM automaticamente.

Namespace NVMe sem espaço	CRÍTICO	Um namespace NVMe foi colocado offline devido a uma falha de gravação causada por falta de espaço.	Adicione espaço ao volume e coloque o namespace NVMe on-line usando o comando "vserver nvme namespace modify".
Período de carência NVMe-oF ativo	AVISO	Este evento ocorre diariamente quando o protocolo NVMe over Fabrics (NVMe-oF) está em uso e o período de carência da licença está ativo. A funcionalidade NVMe-oF requer uma licença após o término do período de carência da licença. A funcionalidade NVMe-oF é desativada quando o período de carência da licença termina.	Entre em contato com seu representante de vendas para obter uma licença NVMe-oF e adicioná-la ao cluster ou remover todas as instâncias da configuração NVMe-oF do cluster.
Período de carência do NVMe-oF expirado	AVISO	O período de carência da licença NVMe over Fabrics (NVMe-oF) terminou e a funcionalidade NVMe-oF está desabilitada.	Entre em contato com seu representante de vendas para obter uma licença NVMe-oF e adicioná-la ao cluster.
Início do período de carência do NVMe-oF	AVISO	A configuração NVMe sobre Fabrics (NVMe-oF) foi detectada durante a atualização para o software ONTAP 9.5. A funcionalidade NVMe-oF requer uma licença após o término do período de carência da licença.	Entre em contato com seu representante de vendas para obter uma licença NVMe-oF e adicioná-la ao cluster.
Host de armazenamento de objetos não resolvível	CRÍTICO	O nome do host do servidor de armazenamento de objetos não pode ser resolvido para um endereço IP. O cliente de armazenamento de objetos não pode se comunicar com o servidor de armazenamento de objetos sem resolver para um endereço IP. Como resultado, os dados podem ficar inacessíveis.	Verifique a configuração de DNS para verificar se o nome do host está configurado corretamente com um endereço IP.

Armazenamento de Objetos Intercluster LIF Inativo	CRÍTICO	O cliente de armazenamento de objetos não consegue encontrar um LIF operacional para se comunicar com o servidor de armazenamento de objetos. O nó não permitirá tráfego de cliente de armazenamento de objetos até que o LIF intercluster esteja operacional. Como resultado, os dados podem ficar inacessíveis.	Execute as seguintes ações corretivas:…Verifique o status do LIF intercluster usando o comando "network interface show -role intercluster"….Verifique se o LIF intercluster está configurado corretamente e operacional.…Se um LIF intercluster não estiver configurado, adicione-o usando o comando "network interface create -role intercluster".
Incompatibilidade de assinatura do armazenamento de objetos	CRÍTICO	A assinatura da solicitação enviada ao servidor de armazenamento de objetos não corresponde à assinatura calculada pelo cliente. Como resultado, os dados podem ficar inacessíveis.	Verifique se a chave de acesso secreta está configurada corretamente. Se estiver configurado corretamente, entre em contato com o suporte técnico da NetApp para obter assistência.

Tempo limite de READDIR	CRÍTICO	Uma operação de arquivo READDIR excedeu o tempo limite permitido para execução no WAFL. Isso pode ocorrer devido a diretórios muito grandes ou esparsos. Recomenda-se uma ação corretiva.	Execute as seguintes ações corretivas:…Encontre informações específicas sobre diretórios recentes que tiveram operações de arquivo READDIR expiradas usando o seguinte comando CLI 'diag' privilege nodeshell: wafl readdir notice show.…Verifique se os diretórios são indicados como esparsos ou não:…Se um diretório for indicado como esparso, é recomendável copiar o conteúdo do diretório para um novo diretório para remover a dispersão do arquivo de diretório. …Se um diretório não for indicado como esparso e for grande, é recomendável reduzir o tamanho do arquivo de diretório reduzindo o número de entradas de arquivo no diretório.

Falha na realocação do agregado	CRÍTICO	Este evento ocorre durante a realocação de um agregado, quando o nó de destino não consegue alcançar os armazenamentos de objetos.	Execute as seguintes ações corretivas:…Verifique se o LIF intercluster está on-line e funcional usando o comando "network interface show"….Verifique a conectividade de rede com o servidor de armazenamento de objetos usando o comando "ping" no LIF intercluster do nó de destino. …Verifique se a configuração do seu armazenamento de objetos não foi alterada e se as informações de login e conectividade ainda estão precisas usando o comando "aggregate object-store config show"….Como alternativa, você pode substituir o erro usando o parâmetro "override-destination-checks" do comando de realocação.…Entre em contato com o suporte técnico da NetApp para obter mais informações ou assistência.

Falha na cópia de sombra	CRÍTICO	Falha no Serviço de Cópias de Sombra de Volume (VSS), uma operação de serviço de backup e restauração do Microsoft Server.	Verifique o seguinte usando as informações fornecidas na mensagem do evento:…A configuração de cópia de sombra está habilitada?…As licenças apropriadas estão instaladas? …Em quais compartilhamentos a operação de cópia de sombra é executada?…O nome do compartilhamento está correto?…O caminho do compartilhamento existe?…Quais são os estados do conjunto de cópias de sombra e suas cópias de sombra?
Falha nas fontes de alimentação do switch de armazenamento	AVISO	Há uma fonte de alimentação faltando no interruptor do cluster. A redundância é reduzida e há risco de interrupção no fornecimento de energia caso haja novas falhas.	Execute as seguintes ações corretivas:…Certifique-se de que a rede elétrica, que fornece energia ao switch do cluster, esteja ligada.…Certifique-se de que o cabo de alimentação esteja conectado à fonte de alimentação.…Entre em contato com o suporte técnico da NetApp se o problema persistir.
Muita autenticação CIFS	AVISO	Muitas negociações de autenticação ocorreram simultaneamente. Há 256 novas solicitações de sessão incompletas deste cliente.	Investigue por que o cliente criou 256 ou mais novas solicitações de conexão. Talvez seja necessário entrar em contato com o fornecedor do cliente ou do aplicativo para determinar o motivo do erro.

Acesso de usuário não autorizado ao compartilhamento de administrador	AVISO	Um cliente tentou se conectar ao compartilhamento privilegiado ONTAP_ADMIN$, embora seu usuário conectado não seja um usuário permitido.	Execute as seguintes ações corretivas:…Certifique-se de que o nome de usuário e o endereço IP mencionados estejam configurados em um dos pools de scanners Vscan ativos.…Verifique a configuração do pool de scanners que está atualmente ativa usando o comando "vserver vscan scanner pool show-active".
Vírus detectado	AVISO	Um servidor Vscan relatou um erro ao sistema de armazenamento. Isso normalmente indica que um vírus foi encontrado. Entretanto, outros erros no servidor Vscan podem causar esse evento.…O acesso do cliente ao arquivo foi negado. O servidor Vscan pode, dependendo de suas configurações e definições, limpar o arquivo, colocá-lo em quarentena ou excluí-lo.	Verifique o log do servidor Vscan relatado no evento "syslog" para ver se ele conseguiu limpar, colocar em quarentena ou excluir o arquivo infectado com sucesso. Caso não seja possível fazer isso, o administrador do sistema poderá ter que excluir o arquivo manualmente.
Volume Offline	INFORMAÇÕES	Esta mensagem indica que um volume foi criado offline.	Coloque o volume novamente online.
Volume restrito	INFORMAÇÕES	Este evento indica que um volume flexível foi restringido.	Coloque o volume novamente online.
Parada da VM de armazenamento bem-sucedida	INFORMAÇÕES	Esta mensagem ocorre quando uma operação 'vserver stop' é bem-sucedida.	Use o comando 'vserver start' para iniciar o acesso aos dados em uma VM de armazenamento.
Pânico do Nó	AVISO	Este evento é emitido quando ocorre pânico	Entre em contato com o suporte ao cliente da NetApp .

Voltar ao topo

Monitores de log anti-ransomware

Nome do monitor	Gravidade	Descrição	Ação corretiva

Monitoramento anti-ransomware de VM de armazenamento desabilitado	AVISO	O monitoramento anti-ransomware para a VM de armazenamento está desabilitado. Habilite o anti-ransomware para proteger a VM de armazenamento.	Nenhum
Monitoramento anti-ransomware de VM de armazenamento habilitado (modo de aprendizagem)	INFORMAÇÕES	O monitoramento anti-ransomware para a VM de armazenamento é habilitado no modo de aprendizado.	Nenhum
Monitoramento anti-ransomware de volume habilitado	INFORMAÇÕES	O monitoramento anti-ransomware do volume está habilitado.	Nenhum
Monitoramento anti-ransomware de volume desabilitado	AVISO	O monitoramento anti-ransomware do volume está desabilitado. Habilite o anti-ransomware para proteger o volume.	Nenhum
Monitoramento anti-ransomware de volume habilitado (modo de aprendizagem)	INFORMAÇÕES	O monitoramento anti-ransomware do volume é habilitado no modo de aprendizagem.	Nenhum
Monitoramento anti-ransomware de volume pausado (modo de aprendizagem)	AVISO	O monitoramento anti-ransomware do volume é pausado no modo de aprendizado.	Nenhum
Monitoramento anti-ransomware de volume pausado	AVISO	O monitoramento anti-ransomware do volume está pausado.	Nenhum
Desativação do monitoramento anti-ransomware de volume	AVISO	O monitoramento anti-ransomware do volume está desabilitado.	Nenhum

Atividade de ransomware detectada	CRÍTICO	Para proteger os dados do ransomware detectado, foi feita uma cópia instantânea que pode ser usada para restaurar os dados originais. Seu sistema gera e transmite uma mensagem de AutoSupport ou "call home" para o suporte técnico da NetApp e quaisquer destinos configurados. A mensagem do AutoSupport melhora a determinação e a resolução de problemas.	Consulte o "FINAL-DOCUMENT-NAME" para tomar medidas corretivas para atividades de ransomware.

Voltar ao topo

FSx para monitores NetApp ONTAP

Nome do monitor	Limiares	Descrição do monitor	Ação corretiva
A capacidade do volume FSx está cheia	Aviso @ > 85 %…Crítico @ > 95 %	A capacidade de armazenamento de um volume é necessária para armazenar dados de aplicativos e clientes. Quanto mais dados armazenados no volume ONTAP , menor será a disponibilidade de armazenamento para dados futuros. Se a capacidade de armazenamento de dados em um volume atingir a capacidade total de armazenamento, o cliente poderá não conseguir armazenar dados devido à falta de capacidade de armazenamento. O monitoramento do volume utilizado da capacidade de armazenamento garante a continuidade dos serviços de dados.	Ações imediatas são necessárias para minimizar a interrupção do serviço se o limite crítico for violado:…1. Considere excluir dados que não são mais necessários para liberar espaço

FSx Volume Alta Latência	Aviso @ > 1000 µs…Crítico @ > 2000 µs	Volumes são objetos que atendem ao tráfego de E/S, geralmente direcionado por aplicativos sensíveis ao desempenho, incluindo aplicativos devOps, diretórios pessoais e bancos de dados. Latências de alto volume significam que os próprios aplicativos podem sofrer e não conseguir realizar suas tarefas. Monitorar latências de volume é essencial para manter o desempenho consistente do aplicativo.	Ações imediatas são necessárias para minimizar a interrupção do serviço se o limite crítico for violado:…1. Se o volume tiver uma política de QoS atribuída a ele, avalie seus limites caso eles estejam causando a limitação da carga de trabalho do volume… Planeje tomar as seguintes ações em breve se o limite de aviso for violado:…1. Se o volume tiver uma política de QoS atribuída a ele, avalie seus limites, caso eles estejam causando limitação na carga de trabalho do volume.…2. Se o nó também estiver com alta utilização, mova o volume para outro nó ou reduza a carga de trabalho total do nó.
Limite de Inodes de Volume FSx	Aviso @ > 85 %…Crítico @ > 95 %	Volumes que armazenam arquivos usam nós de índice (inode) para armazenar metadados de arquivos. Quando um volume esgota sua alocação de inode, nenhum outro arquivo pode ser adicionado a ele. Um alerta de aviso indica que uma ação planejada deve ser tomada para aumentar o número de inodes disponíveis. Um alerta crítico indica que o esgotamento do limite de arquivos é iminente e medidas de emergência devem ser tomadas para liberar inodes para garantir a continuidade do serviço	Ações imediatas são necessárias para minimizar a interrupção do serviço se o limite crítico for violado:…1. Considere aumentar o valor dos inodes para o volume. Se o valor dos inodes já estiver no máximo, considere dividir o volume em dois ou mais volumes porque o sistema de arquivos cresceu além do tamanho máximo… Planeje tomar as seguintes ações em breve se o limite de aviso for violado:… 1. Considere aumentar o valor dos inodes para o volume. Se o valor dos inodes já estiver no máximo, considere dividir o volume em dois ou mais volumes porque o sistema de arquivos cresceu além do tamanho máximo

Comprometimento excessivo de cota do FSx Volume Qtree	Aviso @ > 95 %…Crítico @ > 100 %	O Volume Qtree Quota Overcommit especifica a porcentagem na qual um volume é considerado supercomprometido pelas cotas qtree. O limite definido para a cota qtree foi atingido para o volume. Monitorar o excesso de comprometimento da cota do qtree do volume garante que o usuário receba serviço de dados ininterrupto.	Se o limite crítico for violado, ações imediatas devem ser tomadas para minimizar a interrupção do serviço: 1. Exclua dados indesejados… Quando o limite de aviso for ultrapassado, considere aumentar o espaço do volume.

O espaço de reserva do FSx Snapshot está cheio	Aviso @ > 90 %…Crítico @ > 95 %	A capacidade de armazenamento de um volume é necessária para armazenar dados de aplicativos e clientes. Uma parte desse espaço, chamada de espaço reservado para snapshots, é usada para armazenar snapshots que permitem que os dados sejam protegidos localmente. Quanto mais dados novos e atualizados forem armazenados no volume ONTAP , maior será a capacidade de snapshot usada e menos capacidade de armazenamento de snapshot estará disponível para dados novos ou atualizados no futuro. Se a capacidade de dados de instantâneos em um volume atingir o espaço total de reserva de instantâneos, isso poderá fazer com que o cliente não consiga armazenar novos dados de instantâneos e reduzir o nível de proteção dos dados no volume. Monitorar o volume utilizado da capacidade de snapshot garante a continuidade dos serviços de dados.	Ações imediatas são necessárias para minimizar a interrupção do serviço se o limite crítico for violado:…1. Considere configurar snapshots para usar espaço de dados no volume quando a reserva de snapshots estiver cheia…2. Considere excluir alguns instantâneos mais antigos que podem não ser mais necessários para liberar espaço… Planeje tomar as seguintes ações em breve se o limite de aviso for violado:…1. Considere aumentar o espaço de reserva de instantâneo dentro do volume para acomodar o crescimento…2. Considere configurar snapshots para usar espaço de dados no volume quando a reserva de snapshots estiver cheia

Taxa de falha de cache de volume FSx	Aviso @ > 95 %…Crítico @ > 100 %	A taxa de falhas do cache de volume é a porcentagem de solicitações de leitura dos aplicativos clientes que são retornadas do disco em vez de serem retornadas do cache. Isso significa que o volume atingiu o limite definido.	Se o limite crítico for violado, ações imediatas devem ser tomadas para minimizar a interrupção do serviço: 1. Mova algumas cargas de trabalho para fora do nó do volume para reduzir a carga de E/S 2. Reduza a demanda de cargas de trabalho de menor prioridade no mesmo nó por meio de limites de QoS… Considere ações imediatas quando o limite de aviso for violado: 1. Mova algumas cargas de trabalho para fora do nó do volume para reduzir a carga de E/S 2. Reduza a demanda de cargas de trabalho de menor prioridade no mesmo nó por meio de limites de QoS 3. Alterar características da carga de trabalho (tamanho do bloco, cache do aplicativo etc.)

Voltar ao topo

Monitores K8s

Nome do monitor	Descrição	Ações corretivas	Gravidade/Limite

Latência de volume persistente alta	Latências de alto volume persistente significam que os próprios aplicativos podem sofrer e não conseguir realizar suas tarefas. Monitorar latências de volume persistentes é essencial para manter o desempenho consistente do aplicativo. As latências esperadas com base no tipo de mídia são: SSD de até 1 a 2 milissegundos; SAS de até 8 a 10 milissegundos e SATA HDD de 17 a 20 milissegundos.	**Ações imediatas** Se o limite crítico for violado, considere ações imediatas para minimizar a interrupção do serviço: se o volume tiver uma política de QoS atribuída a ele, avalie seus limites, caso eles estejam causando a limitação da carga de trabalho do volume. **Ações a serem tomadas em breve** Se o limite de alerta for ultrapassado, planeje as seguintes ações imediatas: 1. Se o pool de armazenamento também estiver com alta utilização, mova o volume para outro pool de armazenamento. 2. Se o volume tiver uma política de QoS atribuída a ele, avalie seus limites, caso eles estejam causando limitação na carga de trabalho do volume. 3. Se o controlador também estiver com alta utilização, mova o volume para outro controlador ou reduza a carga de trabalho total do controlador.	Aviso @ > 6.000 µs Crítico @ > 12.000 µs
Alta saturação de memória do cluster	A saturação da memória alocável do cluster é alta. A saturação da CPU do cluster é calculada como a soma do uso de memória dividida pela soma da memória alocável em todos os nós K8s.	Adicionar nós. Corrija quaisquer nós não agendados. Dimensione pods corretamente para liberar memória nos nós.	Aviso @ > 80% Crítico @ > 90%
Falha na conexão do POD	Este alerta ocorre quando há falha na anexação de um volume com POD.		Aviso

Alta taxa de retransmissão	Alta taxa de retransmissão TCP	Verifique se há congestionamento na rede - identifique cargas de trabalho que consomem muita largura de banda da rede. Verifique se há alta utilização da CPU do Pod. Verifique o desempenho da rede de hardware.	Aviso @ > 10% Crítico @ > 25%
Capacidade do sistema de arquivos do nó alta	Capacidade do sistema de arquivos do nó alta	- Aumente o tamanho dos discos dos nós para garantir que haja espaço suficiente para os arquivos do aplicativo. - Diminua o uso de arquivos do aplicativo.	Aviso @ > 80% Crítico @ > 90%
Alta instabilidade da rede de carga de trabalho	Alto TCP Jitter (altas variações de latência/tempo de resposta)	Verifique se há congestionamento na rede. Identifique cargas de trabalho que consomem muita largura de banda da rede. Verifique se há alta utilização da CPU do Pod. Verifique o desempenho da rede de hardware	Aviso @ > 30 ms Crítico @ > 50 ms

Taxa de transferência de volume persistente	Os limites de MBPS em volumes persistentes podem ser usados para alertar um administrador quando volumes persistentes excedem as expectativas de desempenho predefinidas, potencialmente impactando outros volumes persistentes. A ativação deste monitor gerará alertas apropriados para o perfil de taxa de transferência típico de volumes persistentes em SSDs. Este monitor cobrirá todos os volumes persistentes no seu locatário. Os valores de limite de aviso e crítico podem ser ajustados com base em suas metas de monitoramento, duplicando este monitor e definindo limites apropriados para sua classe de armazenamento. Um monitor duplicado pode ser direcionado ainda mais para um subconjunto dos volumes persistentes no seu locatário.	**Ações imediatas** Se o limite crítico for violado, planeje ações imediatas para minimizar a interrupção do serviço: 1. Introduzir limites de QoS MBPS para o volume. 2. Revise o aplicativo que está direcionando a carga de trabalho no volume em busca de anomalias. **Ações a serem tomadas em breve** Se o limite de alerta for ultrapassado, planeje tomar as seguintes ações imediatas: 1. Introduzir limites de QoS MBPS para o volume. 2. Revise o aplicativo que está direcionando a carga de trabalho no volume em busca de anomalias.	Aviso @ > 10.000 MB/s Crítico @ > 15.000 MB/s
Contêiner corre o risco de ficar fora de estoque	Os limites de memória do contêiner estão definidos muito baixos. O contêiner corre risco de despejo (Out of Memory Kill).	Aumente os limites de memória do contêiner.	Aviso @ > 95%
Carga de trabalho reduzida	A carga de trabalho não possui pods saudáveis.		Crítico @ < 1
Falha na vinculação da reivindicação de volume persistente	Este alerta ocorre quando uma ligação falha em um PVC.		Aviso
Limites de memória do ResourceQuota prestes a exceder	Os limites de memória para Namespace estão prestes a exceder ResourceQuota		Aviso @ > 80% Crítico @ > 90%

Solicitações de membros do ResourceQuota prestes a exceder	As solicitações de memória para o Namespace estão prestes a exceder ResourceQuota		Aviso @ > 80% Crítico @ > 90%
Falha na criação do nó	O nó não pôde ser agendado devido a um erro de configuração.	Verifique o log de eventos do Kubernetes para saber a causa da falha de configuração.	Crítico
Falha na recuperação de volume persistente	O volume falhou na recuperação automática.		Aviso @ > 0 B
Limitação de CPU do contêiner	Os limites de CPU do contêiner estão definidos muito baixos. Os processos de contêineres ficam mais lentos.	Aumente os limites de CPU do contêiner.	Aviso @ > 95% Crítico @ > 98%
Falha ao excluir o balanceador de carga de serviço			Aviso
IOPS de volume persistente	Os limites de IOPS em volumes persistentes podem ser usados para alertar um administrador quando volumes persistentes excedem as expectativas de desempenho predefinidas. A ativação deste monitor gerará alertas apropriados para o perfil IOPS típico de volumes de persistência. Este monitor cobrirá todos os volumes persistentes no seu locatário. Os valores de limite de aviso e crítico podem ser ajustados com base em suas metas de monitoramento, duplicando este monitor e definindo limites apropriados para sua carga de trabalho.	**Ações imediatas** Se o limite crítico for violado, planeje ações imediatas para minimizar a interrupção do serviço: 1. Introduzir limites de QoS IOPS para o volume. 2. Revise o aplicativo que está direcionando a carga de trabalho no volume em busca de anomalias. **Ações a serem tomadas em breve** Se o limite de alerta for ultrapassado, planeje as seguintes ações imediatas: 1. Introduzir limites de QoS IOPS para o volume. 2. Revise o aplicativo que está direcionando a carga de trabalho no volume em busca de anomalias.	Aviso @ > 20.000 IO/s Crítico @ > 25.000 IO/s
Falha na atualização do balanceador de carga de serviço			Aviso
Falha na montagem do POD	Este alerta ocorre quando uma montagem falha em um POD.		Aviso

Pressão PID do nó	Os identificadores de processo disponíveis no nó (Linux) caíram abaixo do limite de despejo.	Localize e corrija pods que geram muitos processos e privam o nó de IDs de processo disponíveis. Configure o PodPidsLimit para proteger seu nó contra pods ou contêineres que geram muitos processos.	Crítico @ > 0
Falha na extração da imagem do pod	O Kubernetes falhou ao extrair a imagem do contêiner do pod.	- Certifique-se de que a imagem do pod esteja escrita corretamente na configuração do pod. - Verifique se a tag de imagem existe no seu registro. - Verifique as credenciais do registro de imagens. - Verifique se há problemas de conectividade no registro. - Verifique se você não está atingindo os limites de taxas impostos pelos provedores de registro público.	Aviso
O trabalho está demorando muito	O trabalho está em execução há muito tempo		Aviso @ > 1 h Crítico @ > 5 h
Memória do nó alta	O uso de memória do nó é alto	Adicionar nós. Corrija quaisquer nós não agendados. Dimensione pods corretamente para liberar memória nos nós.	Aviso @ > 85% Crítico @ > 90%
Limites de CPU do ResourceQuota prestes a exceder	Os limites da CPU para Namespace estão prestes a exceder ResourceQuota		Aviso @ > 80% Crítico @ > 90%
Recuo do loop de colisão do pod	O pod travou e tentou reiniciar diversas vezes.		Crítico @ > 3
CPU do nó alta	O uso da CPU do nó é alto.	Adicionar nós. Corrija quaisquer nós não agendados. Pods de tamanho correto para liberar CPU nos nós.	Aviso @ > 80% Crítico @ > 90%

Latência de rede de carga de trabalho RTT alta	Alta latência TCP RTT (Round Trip Time)	Verifique se há congestionamento na rede ▒ Identifique cargas de trabalho que consomem muita largura de banda da rede. Verifique se há alta utilização da CPU do Pod. Verifique o desempenho da rede de hardware.	Aviso @ > 150 ms Crítico @ > 300 ms
Falha na tarefa	O trabalho não foi concluído com sucesso devido a uma falha ou reinicialização do nó, exaustão de recursos, tempo limite do trabalho ou falha no agendamento do pod.	Verifique os logs de eventos do Kubernetes para detectar causas de falhas.	Aviso @ > 1
Volume persistente completo em poucos dias	O Volume Persistente ficará sem espaço em alguns dias	-Aumente o tamanho do volume para garantir que haja espaço suficiente para os arquivos do aplicativo. -Reduza a quantidade de dados armazenados em aplicativos.	Aviso @ < 8 dias Crítico @ < 3 dias
Pressão de memória do nó	O nó está ficando sem memória. A memória disponível atingiu o limite de despejo.	Adicionar nós. Corrija quaisquer nós não agendados. Dimensione pods corretamente para liberar memória nos nós.	Crítico @ > 0
Nó não pronto	O nó não está pronto há 5 minutos	Verifique se o nó tem recursos de CPU, memória e disco suficientes. Verifique a conectividade da rede do nó. Verifique os logs de eventos do Kubernetes para detectar causas de falhas.	Crítico @ < 1
Capacidade de Volume Persistente Alta	A capacidade utilizada do backend de volume persistente é alta.	- Aumente o tamanho do volume para garantir que haja espaço suficiente para os arquivos do aplicativo. - Reduza a quantidade de dados armazenados em aplicativos.	Aviso @ > 80% Crítico @ > 90%

Falha ao criar o balanceador de carga de serviço	Falha na criação do balanceador de carga de serviço		Crítico
Incompatibilidade de réplica de carga de trabalho	Alguns pods não estão disponíveis no momento para uma implantação ou DaemonSet.		Aviso @ > 1
Solicitações de CPU ResourceQuota prestes a exceder	As solicitações de CPU para o Namespace estão prestes a exceder ResourceQuota		Aviso @ > 80% Crítico @ > 90%
Alta taxa de retransmissão	Alta taxa de retransmissão TCP	Verifique se há congestionamento na rede - identifique cargas de trabalho que consomem muita largura de banda da rede. Verifique se há alta utilização da CPU do Pod. Verifique o desempenho da rede de hardware.	Aviso @ > 10% Crítico @ > 25%
Pressão do disco do nó	O espaço em disco disponível e os inodes no sistema de arquivos raiz ou no sistema de arquivos de imagem do nó atenderam a um limite de despejo.	- Aumente o tamanho dos discos dos nós para garantir que haja espaço suficiente para os arquivos do aplicativo. - Diminua o uso de arquivos do aplicativo.	Crítico @ > 0
Saturação alta da CPU do cluster	A saturação da CPU alocável do cluster é alta. A saturação da CPU do cluster é calculada como a soma do uso da CPU dividida pela soma da CPU alocável em todos os nós do K8s.	Adicionar nós. Corrija quaisquer nós não agendados. Pods de tamanho correto para liberar CPU nos nós.	Aviso @ > 80% Crítico @ > 90%

Voltar ao topo

Monitores de Log de Alterações

Nome do monitor	Gravidade	Descrição do monitor
Volume interno descoberto	Informativo	Esta mensagem ocorre quando um Volume Interno é descoberto.
Volume interno modificado	Informativo	Esta mensagem ocorre quando um Volume Interno é modificado.

Nó de armazenamento descoberto	Informativo	Esta mensagem ocorre quando um nó de armazenamento é descoberto.
Nó de armazenamento removido	Informativo	Esta mensagem ocorre quando um nó de armazenamento é removido.
Pool de armazenamento descoberto	Informativo	Esta mensagem ocorre quando um pool de armazenamento é descoberto.
Máquina virtual de armazenamento descoberta	Informativo	Esta mensagem ocorre quando uma Máquina Virtual de Armazenamento é descoberta.
Máquina Virtual de Armazenamento Modificada	Informativo	Esta mensagem ocorre quando uma Máquina Virtual de Armazenamento é modificada.

Voltar ao topo

Monitores de coleta de dados

Nome do monitor	Descrição	Ação corretiva
Desligamento da Unidade de Aquisição	As Unidades de Aquisição de Data Infrastructure Insights são reiniciadas periodicamente como parte de atualizações para introduzir novos recursos. Isso acontece uma vez por mês ou menos em um ambiente típico. Um Alerta de Aviso de que uma Unidade de Aquisição foi desligada deve ser seguido logo depois por uma Resolução observando que a Unidade de Aquisição recém-reiniciada concluiu um registro no Data Infrastructure Insights. Normalmente, esse ciclo de desligamento para registro leva de 5 a 15 minutos.	Se o alerta ocorrer com frequência ou durar mais de 15 minutos, verifique a operação do sistema que hospeda a Unidade de Aquisição, a rede e qualquer proxy que conecte a UA à Internet.
Coletor falhou	A pesquisa de um coletor de dados encontrou uma situação de falha inesperada.	Visite a página do coletor de dados no Data Infrastructure Insights para saber mais sobre a situação.

Aviso ao Colecionador	Este alerta geralmente pode surgir devido a uma configuração errônea do coletor de dados ou do sistema de destino. Revise as configurações para evitar alertas futuros. Também pode ser devido à recuperação de dados incompletos, em que o coletor de dados reuniu todos os dados que pôde. Isso pode acontecer quando as situações mudam durante a coleta de dados (por exemplo, uma máquina virtual presente no início da coleta de dados é excluída durante a coleta de dados e antes que seus dados sejam capturados).	Verifique a configuração do coletor de dados ou do sistema de destino. Observe que o monitor de Aviso do Coletor pode enviar mais alertas do que outros tipos de monitor, portanto, é recomendável não definir destinatários de alerta, a menos que você esteja solucionando problemas.

Voltar ao topo

Monitores de segurança

Nome do monitor	Limite	Descrição do monitor	Ação corretiva
Transporte HTTPS de AutoSupport desabilitado	Aviso @ < 1	O AutoSupport suporta HTTPS, HTTP e SMTP para protocolos de transporte. Devido à natureza sensível das mensagens do AutoSupport , a NetApp recomenda fortemente o uso de HTTPS como o protocolo de transporte padrão para enviar mensagens do AutoSupport ao suporte da NetApp .	Para definir HTTPS como o protocolo de transporte para mensagens AutoSupport , execute o seguinte comando ONTAP :…system node autosupport modify -transport https
Cifras inseguras de cluster para SSH	Aviso @ < 1	Indica que o SSH está usando cifras inseguras, por exemplo, cifras que começam com *cbc.	Para remover as cifras CBC, execute o seguinte comando ONTAP :…security ssh remove -vserver <admin vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc

Banner de login do cluster desabilitado	Aviso @ < 1	Indica que o banner de login está desabilitado para usuários que acessam o sistema ONTAP . Exibir um banner de login é útil para estabelecer expectativas de acesso e uso do sistema.	Para configurar o banner de login para um cluster, execute o seguinte comando ONTAP :…security login banner modify -vserver <admin svm> -message "Acesso restrito a usuários autorizados"
Comunicação entre pares do cluster não criptografada	Aviso @ < 1	Ao replicar dados para recuperação de desastres, armazenamento em cache ou backup, você deve proteger esses dados durante o transporte pela rede de um cluster ONTAP para outro. A criptografia deve ser configurada nos clusters de origem e de destino.	Para habilitar a criptografia em relacionamentos de pares de cluster criados antes do ONTAP 9.6, o cluster de origem e de destino deve ser atualizado para a versão 9.6. Em seguida, use o comando "cluster peer modify" para alterar os peers de cluster de origem e de destino para usar a Criptografia de Peering de Cluster. Consulte o Guia de Fortalecimento de Segurança da NetApp para ONTAP 9 para obter detalhes.
Usuário administrador local padrão habilitado	Aviso @ > 0	A NetApp recomenda bloquear (desabilitar) quaisquer contas desnecessárias de Usuário Administrador Padrão (integradas) com o comando lock. Elas são basicamente contas padrão cujas senhas nunca foram atualizadas ou alteradas.	Para bloquear a conta "admin" interna, execute o seguinte comando ONTAP :…security login lock -username admin
Modo FIPS desabilitado	Aviso @ < 1	Quando a conformidade com o FIPS 140-2 está ativada, TLSv1 e SSLv3 são desativados, e somente TLSv1.1 e TLSv1.2 permanecem ativados. O ONTAP impede que você habilite TLSv1 e SSLv3 quando a conformidade com FIPS 140-2 estiver habilitada.	Para habilitar a conformidade com o FIPS 140-2 em um cluster, execute o seguinte comando ONTAP no modo de privilégio avançado:…security config modify -interface SSL -is-fips-enabled true

Encaminhamento de log não criptografado	Aviso @ < 1	O descarregamento de informações do syslog é necessário para limitar o escopo ou a pegada de uma violação a um único sistema ou solução. Portanto, a NetApp recomenda descarregar com segurança as informações do syslog para um local de armazenamento ou retenção seguro.	Depois que um destino de encaminhamento de log é criado, seu protocolo não pode ser alterado. Para mudar para um protocolo criptografado, exclua e recrie o destino de encaminhamento de log usando o seguinte comando ONTAP :…cluster log-forwarding create -destination <destination ip> -protocol tcp-encrypted
Senha com hash MD5	Aviso @ > 0	A NetApp recomenda fortemente o uso da função de hash SHA-512 mais segura para senhas de contas de usuários do ONTAP . Contas que usam a função de hash MD5 menos segura devem migrar para a função de hash SHA-512.	A NetApp recomenda fortemente que as contas de usuário migrem para a solução SHA-512 mais segura, fazendo com que os usuários alterem suas senhas.…para bloquear contas com senhas que usam a função hash MD5, execute o seguinte comando ONTAP :…security login lock -vserver * -username * -hash-function md5
Nenhum servidor NTP está configurado	Aviso @ < 1	Indica que o cluster não tem servidores NTP configurados. Para redundância e serviço ideal, a NetApp recomenda que você associe pelo menos três servidores NTP ao cluster.	Para associar um servidor NTP ao cluster, execute o seguinte comando ONTAP : cluster time-service ntp server create -server <nome do host ou endereço IP do servidor NTP>
A contagem do servidor NTP é baixa	Aviso @ < 3	Indica que o cluster tem menos de 3 servidores NTP configurados. Para redundância e serviço ideal, a NetApp recomenda que você associe pelo menos três servidores NTP ao cluster.	Para associar um servidor NTP ao cluster, execute o seguinte comando ONTAP :…cluster time-service ntp server create -server <nome do host ou endereço IP do servidor NTP>

Shell remoto habilitado	Aviso @ > 0	O Remote Shell não é um método seguro para estabelecer acesso de linha de comando à solução ONTAP . O Remote Shell deve ser desabilitado para acesso remoto seguro.	A NetApp recomenda o Secure Shell (SSH) para acesso remoto seguro.…Para desabilitar o Remote Shell em um cluster, execute o seguinte comando ONTAP no modo de privilégio avançado:…security protocol modify -application rsh- enabled false
Log de auditoria de VM de armazenamento desabilitado	Aviso @ < 1	Indica que o registro de auditoria está desabilitado para o SVM.	Para configurar o log de auditoria para um vserver, execute o seguinte comando ONTAP :…vserver audit enable -vserver <svm>
Cifras inseguras de VM de armazenamento para SSH	Aviso @ < 1	Indica que o SSH está usando cifras inseguras, por exemplo, cifras que começam com *cbc.	Para remover as cifras CBC, execute o seguinte comando ONTAP :…security ssh remove -vserver <vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
Banner de login da VM de armazenamento desabilitado	Aviso @ < 1	Indica que o banner de login está desabilitado para usuários que acessam SVMs no sistema. Exibir um banner de login é útil para estabelecer expectativas de acesso e uso do sistema.	Para configurar o banner de login para um cluster, execute o seguinte comando ONTAP :…security login banner modify -vserver <svm> -message "Acesso restrito a usuários autorizados"
Protocolo Telnet habilitado	Aviso @ > 0	O Telnet não é um método seguro para estabelecer acesso de linha de comando à solução ONTAP . O Telnet deve ser desabilitado para acesso remoto seguro.	A NetApp recomenda o Secure Shell (SSH) para acesso remoto seguro. Para desabilitar o Telnet em um cluster, execute o seguinte comando ONTAP no modo de privilégio avançado:…security protocol modify -application telnet -enabled false

Voltar ao topo

Monitores de Proteção de Dados

Nome do monitor	Limiares	Descrição do monitor	Ação corretiva
Espaço insuficiente para cópia do instantâneo Lun	(Filtro contains_luns = Sim) Aviso @ > 95 %…Crítico @ > 100 %	A capacidade de armazenamento de um volume é necessária para armazenar dados de aplicativos e clientes. Uma parte desse espaço, chamada de espaço reservado para snapshots, é usada para armazenar snapshots que permitem que os dados sejam protegidos localmente. Quanto mais dados novos e atualizados forem armazenados no volume ONTAP , maior será a capacidade de snapshot usada e menos capacidade de armazenamento de snapshot estará disponível para dados novos ou atualizados no futuro. Se a capacidade de dados de instantâneos em um volume atingir o espaço total de reserva de instantâneos, isso poderá fazer com que o cliente não consiga armazenar novos dados de instantâneos e reduzir o nível de proteção dos dados nas LUNs do volume. Monitorar o volume utilizado da capacidade de snapshot garante a continuidade dos serviços de dados.	**Ações imediatas** Se o limite crítico for violado, considere ações imediatas para minimizar a interrupção do serviço: 1. Configure snapshots para usar espaço de dados no volume quando a reserva de snapshots estiver cheia. 2. Exclua alguns instantâneos antigos indesejados para liberar espaço. **Ações a serem tomadas em breve** Se o limite de alerta for ultrapassado, planeje tomar as seguintes ações imediatas: 1. Aumente o espaço de reserva do snapshot dentro do volume para acomodar o crescimento. 2. Configure snapshots para usar espaço de dados no volume quando a reserva de snapshots estiver cheia.

Atraso no relacionamento do SnapMirror	Aviso @ > 150%…Crítico @ > 300%	O atraso no relacionamento do SnapMirror é a diferença entre o registro de data e hora do instantâneo e o horário no sistema de destino. O lag_time_percent é a proporção do tempo de atraso em relação ao intervalo de agendamento da Política SnapMirror . Se o tempo de atraso for igual ao intervalo de agendamento, o lag_time_percent será 100%. Se a política SnapMirror não tiver um agendamento, lag_time_percent não será calculado.	Monitore o status do SnapMirror usando o comando "snapmirror show". Verifique o histórico de transferência do SnapMirror usando o comando "snapmirror show-history"

Voltar ao topo

Monitores de volume de nuvem (CVO)

Nome do monitor	Gravidade do CI	Descrição do monitor	Ação corretiva
Disco CVO fora de serviço	INFORMAÇÕES	Este evento ocorre quando um disco é removido do serviço porque foi marcado como falha, está sendo higienizado ou entrou no Centro de Manutenção.	Nenhum

Falha na devolução do pool de armazenamento do CVO	CRÍTICO	Este evento ocorre durante a migração de um agregado como parte de um failover de armazenamento (SFO), quando o nó de destino não consegue alcançar os armazenamentos de objetos.	Execute as seguintes ações corretivas: Verifique se o seu LIF intercluster está on-line e funcional usando o comando "network interface show". Verifique a conectividade de rede com o servidor de armazenamento de objetos usando o comando "ping" no LIF do intercluster do nó de destino. Verifique se a configuração do seu armazenamento de objetos não foi alterada e se as informações de login e conectividade ainda estão precisas usando o comando "aggregate object-store config show". Como alternativa, você pode substituir o erro especificando false para o parâmetro "require-partner-waiting" do comando giveback. Entre em contato com o suporte técnico da NetApp para obter mais informações ou assistência.

Interconexão CVO HA inativa	AVISO	A interconexão de alta disponibilidade (HA) está inativa. Risco de interrupção do serviço quando o failover não estiver disponível.	As ações corretivas dependem do número e do tipo de links de interconexão HA suportados pela plataforma, bem como do motivo pelo qual a interconexão está inativa. Se os links estiverem inativos: verifique se ambos os controladores no par HA estão operacionais. Para links conectados externamente, certifique-se de que os cabos de interconexão estejam conectados corretamente e que os conectores de fator de forma pequeno (SFPs), se aplicável, estejam encaixados corretamente em ambos os controladores. Para links conectados internamente, desative e reative os links, um após o outro, usando os comandos "ic link off" e "ic link on". Se os links estiverem desabilitados, habilite-os usando o comando "ic link on". Se um peer não estiver conectado, desative e reative os links, um após o outro, usando os comandos "ic link off" e "ic link on". Entre em contato com o suporte técnico da NetApp se o problema persistir.

Máximo de sessões de CVO por usuário excedido	AVISO	Você excedeu o número máximo de sessões permitidas por usuário em uma conexão TCP. Qualquer solicitação para estabelecer uma sessão será negada até que algumas sessões sejam liberadas.	Execute as seguintes ações corretivas: inspecione todos os aplicativos em execução no cliente e encerre aqueles que não estiverem funcionando corretamente. Reinicie o cliente. Verifique se o problema é causado por um aplicativo novo ou existente: se o aplicativo for novo, defina um limite mais alto para o cliente usando o comando "cifs option modify -max-opens -same-file-per-tree". Em alguns casos, os clientes operam conforme o esperado, mas exigem um limite mais alto. Você deve ter privilégios avançados para definir um limite mais alto para o cliente. Se o problema for causado por um aplicativo existente, pode haver um problema com o cliente. Entre em contato com o suporte técnico da NetApp para obter mais informações ou assistência.

Conflito de nome NetBIOS CVO	CRÍTICO	O Serviço de Nomes NetBIOS recebeu uma resposta negativa a uma solicitação de registro de nome de uma máquina remota. Isso geralmente é causado por um conflito no nome NetBIOS ou em um alias. Como resultado, os clientes podem não conseguir acessar dados ou se conectar ao nó de serviço de dados correto no cluster.	Execute qualquer uma das seguintes ações corretivas: Se houver um conflito no nome NetBIOS ou em um alias, execute uma das seguintes ações: Exclua o alias NetBIOS duplicado usando o comando "vserver cifs delete -aliases alias -vserver vserver". Renomeie um alias NetBIOS excluindo o nome duplicado e adicionando um alias com um novo nome usando o comando "vserver cifs create -aliases alias -vserver vserver". Se não houver aliases configurados e houver um conflito no nome NetBIOS, renomeie o servidor CIFS usando os comandos "vserver cifs delete -vserver vserver" e "vserver cifs create -cifs -server netbiosname". OBSERVAÇÃO: Excluir um servidor CIFS pode tornar os dados inacessíveis. Remova o nome NetBIOS ou renomeie o NetBIOS na máquina remota.
Pool de armazenamento CVO NFSv4 esgotado	CRÍTICO	Um pool de armazenamento NFSv4 foi esgotado.	Se o servidor NFS não responder por mais de 10 minutos após esse evento, entre em contato com o suporte técnico da NetApp .
Pânico do Nó CVO	AVISO	Este evento é emitido quando ocorre pânico	Entre em contato com o suporte ao cliente da NetApp .

Espaço de volume raiz do nó CVO baixo	CRÍTICO	O sistema detectou que o volume raiz está perigosamente com pouco espaço. O nó não está totalmente operacional. Os LIFs de dados podem ter falhado dentro do cluster, o que limita o acesso NFS e CIFS no nó. A capacidade administrativa é limitada aos procedimentos de recuperação local para o nó liberar espaço no volume raiz.	Execute as seguintes ações corretivas: libere espaço no volume raiz excluindo cópias antigas do Snapshot, excluindo arquivos que não são mais necessários do diretório /mroot ou expandindo a capacidade do volume raiz. Reinicie o controlador. Entre em contato com o suporte técnico da NetApp para obter mais informações ou assistência.
Compartilhamento de administrador CVO inexistente	CRÍTICO	Problema no Vscan: um cliente tentou se conectar a um compartilhamento ONTAP_ADMIN$ inexistente.	Certifique-se de que o Vscan esteja habilitado para o ID SVM mencionado. Habilitar o Vscan em um SVM faz com que o compartilhamento ONTAP_ADMIN$ seja criado para o SVM automaticamente.
Host de armazenamento de objetos CVO não resolvível	CRÍTICO	O nome do host do servidor de armazenamento de objetos não pode ser resolvido para um endereço IP. O cliente de armazenamento de objetos não pode se comunicar com o servidor de armazenamento de objetos sem resolver para um endereço IP. Como resultado, os dados podem ficar inacessíveis.	Verifique a configuração de DNS para verificar se o nome do host está configurado corretamente com um endereço IP.

Armazenamento de Objetos CVO Intercluster LIF Inativo	CRÍTICO	O cliente de armazenamento de objetos não consegue encontrar um LIF operacional para se comunicar com o servidor de armazenamento de objetos. O nó não permitirá tráfego de cliente de armazenamento de objetos até que o LIF intercluster esteja operacional. Como resultado, os dados podem ficar inacessíveis.	Execute as seguintes ações corretivas: Verifique o status do LIF entre clusters usando o comando "network interface show -role intercluster". Verifique se o LIF intercluster está configurado corretamente e operacional. Se um LIF intercluster não estiver configurado, adicione-o usando o comando "network interface create -role intercluster".
Incompatibilidade de assinatura do repositório de objetos CVO	CRÍTICO	A assinatura da solicitação enviada ao servidor de armazenamento de objetos não corresponde à assinatura calculada pelo cliente. Como resultado, os dados podem ficar inacessíveis.	Verifique se a chave de acesso secreta está configurada corretamente. Se estiver configurado corretamente, entre em contato com o suporte técnico da NetApp para obter assistência.
Memória do monitor CVO QoS esgotada	CRÍTICO	A memória dinâmica do subsistema QoS atingiu seu limite para o hardware da plataforma atual. Alguns recursos de QoS podem operar com capacidade limitada.	Exclua algumas cargas de trabalho ou fluxos ativos para liberar memória. Use o comando “statistics show -object workload -counter ops” para determinar quais cargas de trabalho estão ativas. Cargas de trabalho ativas mostram operações diferentes de zero. Em seguida, use o comando “workload delete <workload_name>” várias vezes para remover cargas de trabalho específicas. Como alternativa, use o comando “stream delete -workload <nome da carga de trabalho> *” para excluir os fluxos associados da carga de trabalho ativa.

Tempo limite de leitura do CVO	CRÍTICO	Uma operação de arquivo READDIR excedeu o tempo limite permitido para execução no WAFL. Isso pode ocorrer devido a diretórios muito grandes ou esparsos. Recomenda-se uma ação corretiva.	Execute as seguintes ações corretivas: encontre informações específicas sobre diretórios recentes que tiveram operações de arquivo READDIR expiradas usando o seguinte comando CLI 'diag' privilege nodeshell: wafl readdir notice show. Verifique se os diretórios são indicados como esparsos ou não: Se um diretório for indicado como esparso, é recomendável copiar o conteúdo do diretório para um novo diretório para remover a escassez do arquivo de diretório. Se um diretório não for indicado como esparso e for grande, é recomendável reduzir o tamanho do arquivo de diretório reduzindo o número de entradas de arquivo no diretório.

Falha na realocação do pool de armazenamento do CVO	CRÍTICO	Este evento ocorre durante a realocação de um agregado, quando o nó de destino não consegue alcançar os armazenamentos de objetos.	Execute as seguintes ações corretivas: Verifique se o seu LIF intercluster está on-line e funcional usando o comando "network interface show". Verifique a conectividade de rede com o servidor de armazenamento de objetos usando o comando "ping" no LIF do intercluster do nó de destino. Verifique se a configuração do seu armazenamento de objetos não foi alterada e se as informações de login e conectividade ainda estão precisas usando o comando "aggregate object-store config show". Como alternativa, você pode substituir o erro usando o parâmetro "override-destination-checks" do comando de realocação. Entre em contato com o suporte técnico da NetApp para obter mais informações ou assistência.
Falha na cópia de sombra do CVO	CRÍTICO	Falha no Serviço de Cópias de Sombra de Volume (VSS), uma operação de serviço de backup e restauração do Microsoft Server.	Verifique o seguinte usando as informações fornecidas na mensagem do evento: a configuração de cópia de sombra está habilitada? As licenças apropriadas estão instaladas? Em quais compartilhamentos a operação de cópia de sombra é executada? O nome do compartilhamento está correto? O caminho de compartilhamento existe? Quais são os estados do conjunto de cópias de sombra e suas cópias de sombra?

Parada da VM de armazenamento CVO bem-sucedida	INFORMAÇÕES	Esta mensagem ocorre quando uma operação 'vserver stop' é bem-sucedida.	Use o comando 'vserver start' para iniciar o acesso aos dados em uma VM de armazenamento.
CVO Autenticação CIFS em excesso	AVISO	Muitas negociações de autenticação ocorreram simultaneamente. Há 256 novas solicitações de sessão incompletas deste cliente.	Investigue por que o cliente criou 256 ou mais novas solicitações de conexão. Talvez seja necessário entrar em contato com o fornecedor do cliente ou do aplicativo para determinar o motivo do erro.
Discos CVO não atribuídos	INFORMAÇÕES	O sistema tem discos não atribuídos - a capacidade está sendo desperdiçada e seu sistema pode ter alguma configuração incorreta ou alteração parcial de configuração aplicada.	Execute as seguintes ações corretivas: Determine quais discos não estão atribuídos usando o comando "disk show -n". Atribua os discos a um sistema usando o comando "disk assign".
Acesso de usuário não autorizado do CVO ao compartilhamento de administrador	AVISO	Um cliente tentou se conectar ao compartilhamento privilegiado ONTAP_ADMIN$, embora seu usuário conectado não seja um usuário permitido.	Execute as seguintes ações corretivas: Certifique-se de que o nome de usuário e o endereço IP mencionados estejam configurados em um dos pools de scanners Vscan ativos. Verifique a configuração do pool de scanners que está ativa no momento usando o comando "vserver vscan scanner pool show-active".

Vírus CVO detectado	AVISO	Um servidor Vscan relatou um erro ao sistema de armazenamento. Isso normalmente indica que um vírus foi encontrado. Entretanto, outros erros no servidor Vscan podem causar esse evento. O acesso do cliente ao arquivo foi negado. O servidor Vscan pode, dependendo de suas configurações e definições, limpar o arquivo, colocá-lo em quarentena ou excluí-lo.	Verifique o log do servidor Vscan relatado no evento "syslog" para ver se ele conseguiu limpar, colocar em quarentena ou excluir o arquivo infectado com sucesso. Caso não seja possível fazer isso, o administrador do sistema poderá ter que excluir o arquivo manualmente.
Volume CVO offline	INFORMAÇÕES	Esta mensagem indica que um volume foi criado offline.	Coloque o volume novamente online.
Volume CVO restrito	INFORMAÇÕES	Este evento indica que um volume flexível foi restringido.	Coloque o volume novamente online.

Voltar ao topo

Monitores de log do mediador SnapMirror for Business Continuity (SMBC)

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
Mediador ONTAP adicionado	INFORMAÇÕES	Esta mensagem ocorre quando o ONTAP Mediator é adicionado com sucesso em um cluster.	Nenhum
Mediador ONTAP não acessível	CRÍTICO	Esta mensagem ocorre quando o ONTAP Mediator é redirecionado ou o pacote do Mediator não está mais instalado no servidor do Mediator. Como resultado, o failover do SnapMirror não é possível.	Remova a configuração do Mediador ONTAP atual usando o comando "snapmirror mediator remove". Reconfigure o acesso ao Mediador ONTAP usando o comando "snapmirror mediator add".
Mediador ONTAP removido	INFORMAÇÕES	Esta mensagem ocorre quando o ONTAP Mediator é removido com sucesso de um cluster.	Nenhum

Mediador ONTAP inacessível	AVISO	Esta mensagem ocorre quando o Mediador ONTAP está inacessível em um cluster. Como resultado, o failover do SnapMirror não é possível.	Verifique a conectividade de rede com o ONTAP Mediator usando os comandos "network ping" e "network traceroute". Se o problema persistir, remova a configuração do Mediador ONTAP atual usando o comando "snapmirror mediator remove". Reconfigure o acesso ao Mediador ONTAP usando o comando "snapmirror mediator add".
Certificado SMBC CA expirado	CRÍTICO	Esta mensagem ocorre quando o certificado da autoridade de certificação (CA) do ONTAP Mediator expirou. Como resultado, nenhuma comunicação posterior com o Mediador do ONTAP será possível.	Remova a configuração do Mediador ONTAP atual usando o comando "snapmirror mediator remove". Atualize um novo certificado de CA no servidor ONTAP Mediator. Reconfigure o acesso ao Mediador ONTAP usando o comando "snapmirror mediator add".
Certificado SMBC CA expirando	AVISO	Esta mensagem ocorre quando o certificado da autoridade de certificação (CA) do ONTAP Mediator está prestes a expirar nos próximos 30 dias.	Antes que este certificado expire, remova a configuração do Mediador ONTAP atual usando o comando "snapmirror mediator remove". Atualize um novo certificado de CA no servidor ONTAP Mediator. Reconfigure o acesso ao Mediador ONTAP usando o comando "snapmirror mediator add".
Certificado de cliente SMBC expirado	CRÍTICO	Esta mensagem ocorre quando o certificado do cliente do ONTAP Mediator expirou. Como resultado, nenhuma comunicação posterior com o Mediador do ONTAP será possível.	Remova a configuração do Mediador ONTAP atual usando o comando "snapmirror mediator remove". Reconfigure o acesso ao Mediador ONTAP usando o comando "snapmirror mediator add".

Certificado de cliente SMBC expirando	AVISO	Esta mensagem ocorre quando o certificado do cliente do ONTAP Mediator está prestes a expirar nos próximos 30 dias.	Antes que este certificado expire, remova a configuração do Mediador ONTAP atual usando o comando "snapmirror mediator remove". Reconfigure o acesso ao Mediador ONTAP usando o comando "snapmirror mediator add".
Relação SMBC fora de sincronia Nota: A UM não tem esta	CRÍTICO	Esta mensagem ocorre quando um relacionamento do SnapMirror for Business Continuity (SMBC) muda de status de "em sincronia" para "fora de sincronia". Devido a este RPO=0 a proteção de dados será interrompida.	Verifique a conexão de rede entre os volumes de origem e destino. Monitore o status do relacionamento SMBC usando o comando "snapmirror show" no destino e o comando "snapmirror list-destinations" na origem. A ressincronização automática tentará trazer o relacionamento de volta ao status "sincronizado". Se a ressincronização falhar, verifique se todos os nós no cluster estão no quorum e íntegros.
Certificado do servidor SMBC expirado	CRÍTICO	Esta mensagem ocorre quando o certificado do servidor ONTAP Mediator expirou. Como resultado, nenhuma comunicação posterior com o Mediador do ONTAP será possível.	Remova a configuração do Mediador ONTAP atual usando o comando "snapmirror mediator remove". Atualize um novo certificado de servidor no servidor ONTAP Mediator. Reconfigure o acesso ao Mediador ONTAP usando o comando "snapmirror mediator add".

Certificado do servidor SMBC expirando	AVISO	Esta mensagem ocorre quando o certificado do servidor ONTAP Mediator está prestes a expirar nos próximos 30 dias.	Antes que este certificado expire, remova a configuração do Mediador ONTAP atual usando o comando "snapmirror mediator remove". Atualize um novo certificado de servidor no servidor ONTAP Mediator. Reconfigure o acesso ao Mediador ONTAP usando o comando "snapmirror mediator add".

Voltar ao topo

Monitores adicionais de energia, pulsação e sistemas diversos

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
Fonte de alimentação de prateleira de disco descoberta	INFORMATIVO	Esta mensagem ocorre quando uma fonte de alimentação é adicionada à prateleira de disco.	NENHUM
Prateleiras de disco Fonte de alimentação removida	INFORMATIVO	Esta mensagem ocorre quando uma fonte de alimentação é removida da prateleira de disco.	NENHUM
Troca automática não planejada do MetroCluster desabilitada	CRÍTICO	Esta mensagem ocorre quando o recurso de comutação automática não planejada está desabilitado.	Execute o comando "metrocluster modify -node-name <nodename> -automatic-switchover -onfailure true" para cada nó no cluster para habilitar a alternância automática.
Ponte de armazenamento MetroCluster inacessível	CRÍTICO	A ponte de armazenamento não pode ser acessada pela rede de gerenciamento	1) Se a ponte for monitorada por SNMP, verifique se o LIF de gerenciamento do nó está ativo usando o comando "network interface show". Verifique se a ponte está ativa usando o comando "network ping". 2) Se a ponte for monitorada dentro da banda, verifique o cabeamento de malha até a ponte e, em seguida, verifique se a ponte está ligada.

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
Temperatura da ponte MetroCluster anormal - abaixo do crítico	CRÍTICO	O sensor na ponte Fibre Channel está relatando uma temperatura abaixo do limite crítico.	1) Verifique o status operacional dos ventiladores na ponte de armazenamento. 2) Verifique se a ponte está operando sob as condições de temperatura recomendadas.
Temperatura da ponte MetroCluster anormal - acima do crítico	CRÍTICO	O sensor na ponte Fibre Channel está relatando uma temperatura acima do limite crítico.	1) Verifique o status operacional do sensor de temperatura do chassi na ponte de armazenamento usando o comando "storage bridge show -cooling". 2) Verifique se a ponte de armazenamento está operando sob as condições de temperatura recomendadas.
Agregado MetroCluster deixado para trás	AVISO	O agregado foi deixado para trás durante o retorno.	1) Verifique o estado agregado usando o comando "aggr show". 2) Se o agregado estiver online, devolva-o ao seu proprietário original usando o comando "metrocluster switchback".

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
Todos os links entre os parceiros do Metrocluster estão inativos	CRÍTICO	Os adaptadores de interconexão RDMA e os LIFs interclusters interromperam as conexões com o cluster peering ou o cluster peering está inativo.	1) Certifique-se de que os LIFs intercluster estejam ativos e funcionando. Repare os LIFs intercluster se eles estiverem inativos. 2) Verifique se o cluster emparelhado está ativo e em execução usando o comando "cluster peer ping". Consulte o Guia de Recuperação de Desastres do MetroCluster se o cluster peering estiver inativo. 3) Para o fabric MetroCluster, verifique se os ISLs de fabric de back-end estão ativos e em execução. Repare os ISLs de malha de back-end se eles estiverem inativos. 4) Para configurações MetroCluster não fabric, verifique se o cabeamento está correto entre os adaptadores de interconexão RDMA. Reconfigure o cabeamento se os links estiverem inativos.
Parceiros do MetroCluster não podem ser contatados pela rede peering	CRÍTICO	A conectividade com o cluster de pares está quebrada.	1) Certifique-se de que a porta esteja conectada à rede/switch correto. 2) Certifique-se de que o LIF intercluster esteja conectado ao cluster emparelhado. 3) Certifique-se de que o cluster emparelhado esteja ativo e em execução usando o comando "cluster peer ping". Consulte o Guia de Recuperação de Desastres do MetroCluster se o cluster peering estiver inativo.

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
MetroCluster Inter Switch Todos os links inativos	CRÍTICO	Todos os Inter-Switch Links (ISLs) no switch de armazenamento estão inativos.	1) Repare os ISLs de malha de back-end no switch de armazenamento. 2) Certifique-se de que o switch do parceiro esteja ativo e seus ISLs estejam operacionais. 3) Certifique-se de que os equipamentos intermediários, como dispositivos xWDM, estejam operacionais.
Link SAS do nó do MetroCluster para a pilha de armazenamento inativo	AVISO	O adaptador SAS ou o cabo conectado pode estar com defeito.	1. Verifique se o adaptador SAS está on-line e em execução. 2. Verifique se a conexão física do cabo está segura e funcionando e substitua o cabo, se necessário. 3. Se o adaptador SAS estiver conectado às prateleiras de disco, certifique-se de que os IOMs e os discos estejam encaixados corretamente.
Links do iniciador do MetroClusterFC inativos	CRÍTICO	O adaptador iniciador FC está com defeito.	1. Certifique-se de que o link do iniciador FC não foi adulterado. 2. Verifique o status operacional do adaptador iniciador FC usando o comando "system node run -node local -command storage show adapter".
Link de interconexão FC-VI inativo	CRÍTICO	O link físico na porta FC-VI está offline.	1. Certifique-se de que o link FC-VI não foi adulterado. 2. Verifique se o status físico do adaptador FC-VI é "Ativo" usando o comando "metrocluster interconnect adapter show". 3. Se a configuração incluir switches de malha, certifique-se de que eles estejam devidamente cabeados e configurados.

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
Discos sobressalentes do MetroCluster deixados para trás	AVISO	O disco reserva foi deixado para trás durante o retorno.	Se o disco não apresentar falha, devolva-o ao seu proprietário original usando o comando "metrocluster switchback".
Ponte de armazenamento MetroCluster Port Down	CRÍTICO	A porta na ponte de armazenamento está offline.	1) Verifique o status operacional das portas na ponte de armazenamento usando o comando "storage bridge show -ports". 2) Verifique a conectividade lógica e física com a porta.
Falha nos ventiladores do switch de armazenamento MetroCluster	CRÍTICO	O ventilador do switch de armazenamento falhou.	1) Certifique-se de que os ventiladores do switch estejam operando corretamente usando o comando "storage switch show -cooling". 2) Certifique-se de que as FRUs do ventilador estejam inseridas corretamente e operacionais.
Switch de armazenamento MetroCluster inacessível	CRÍTICO	O switch de armazenamento não pode ser acessado pela rede de gerenciamento.	1) Certifique-se de que o LIF de gerenciamento do nó esteja ativo usando o comando "network interface show". 2) Certifique-se de que o switch esteja ativo usando o comando "network ping". 3) Certifique-se de que o switch pode ser acessado via SNMP verificando suas configurações SNMP após efetuar login no switch.

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
Falha nas fontes de alimentação do switch MetroCluster	CRÍTICO	Uma unidade de fonte de alimentação no switch de armazenamento não está operacional.	1) Verifique os detalhes do erro usando o comando "storage switch show -error -switch-name <nome do switch>". 2) Identifique a unidade de fonte de alimentação com defeito usando o comando "storage switch show -power -switch-name <nome do switch>". 3) Certifique-se de que a fonte de alimentação esteja inserida corretamente no chassi do switch de armazenamento e totalmente operacional.
Falha nos sensores de temperatura do switch MetroCluster	CRÍTICO	O sensor no switch Fibre Channel falhou.	1) Verifique o status operacional dos sensores de temperatura no switch de armazenamento usando o comando "storage switch show -cooling". 2) Verifique se o interruptor está operando sob as condições de temperatura recomendadas.
Temperatura anormal do switch MetroCluster	CRÍTICO	O sensor de temperatura no switch Fibre Channel relatou temperatura anormal.	1) Verifique o status operacional dos sensores de temperatura no switch de armazenamento usando o comando "storage switch show -cooling". 2) Verifique se o interruptor está operando sob as condições de temperatura recomendadas.

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
Pulsação do processador de serviço perdida	INFORMATIVO	Esta mensagem ocorre quando o ONTAP não recebe um sinal de "pulsação" esperado do Processador de Serviço (SP). Junto com esta mensagem, os arquivos de log do SP serão enviados para depuração. O ONTAP redefinirá o SP para tentar restaurar a comunicação. O SP ficará indisponível por até dois minutos enquanto reinicia.	Entre em contato com o suporte técnico da NetApp .
Processador de serviço com pulsação interrompida	AVISO	Esta mensagem ocorre quando o ONTAP não está mais recebendo heartbeats do Processador de Serviço (SP). Dependendo do design do hardware, o sistema pode continuar a fornecer dados ou pode decidir desligar para evitar perda de dados ou danos ao hardware. O sistema continua a fornecer dados, mas como o SP pode não estar funcionando, o sistema não pode enviar notificações de dispositivos inativos, erros de inicialização ou erros de autoteste de inicialização (POST) do Open Firmware (OFW). Se o seu sistema estiver configurado para isso, ele gera e transmite uma mensagem de AutoSupport (ou "call home") para o suporte técnico da NetApp e para os destinos configurados. A entrega bem-sucedida de uma mensagem de AutoSupport melhora significativamente a determinação e a resolução de problemas.	Se o sistema tiver desligado, tente um ciclo de energia forçado: retire o controlador do chassi, empurre-o de volta e ligue o sistema. Entre em contato com o suporte técnico da NetApp se o problema persistir após o ciclo de energia ou se houver qualquer outra condição que exija atenção.

Voltar ao topo

Mais informações

- "Visualizando e descartando alertas"

Notificações de webhook

Notificação usando Webhooks

Os webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado.

Muitos aplicativos comerciais oferecem suporte a webhooks como uma interface de entrada padrão, por exemplo: Slack, PagerDuty, Teams e Discord, todos oferecem suporte a webhooks. Ao oferecer suporte a um canal webhook genérico e personalizável, o Data Infrastructure Insights pode oferecer suporte a muitos desses canais de entrega. Informações sobre webhooks podem ser encontradas nestes sites de aplicativos. Por exemplo, o Slack fornece"este guia útil" .

Você pode criar vários canais de webhook, cada canal direcionado a uma finalidade diferente; aplicativos separados, destinatários diferentes, etc.

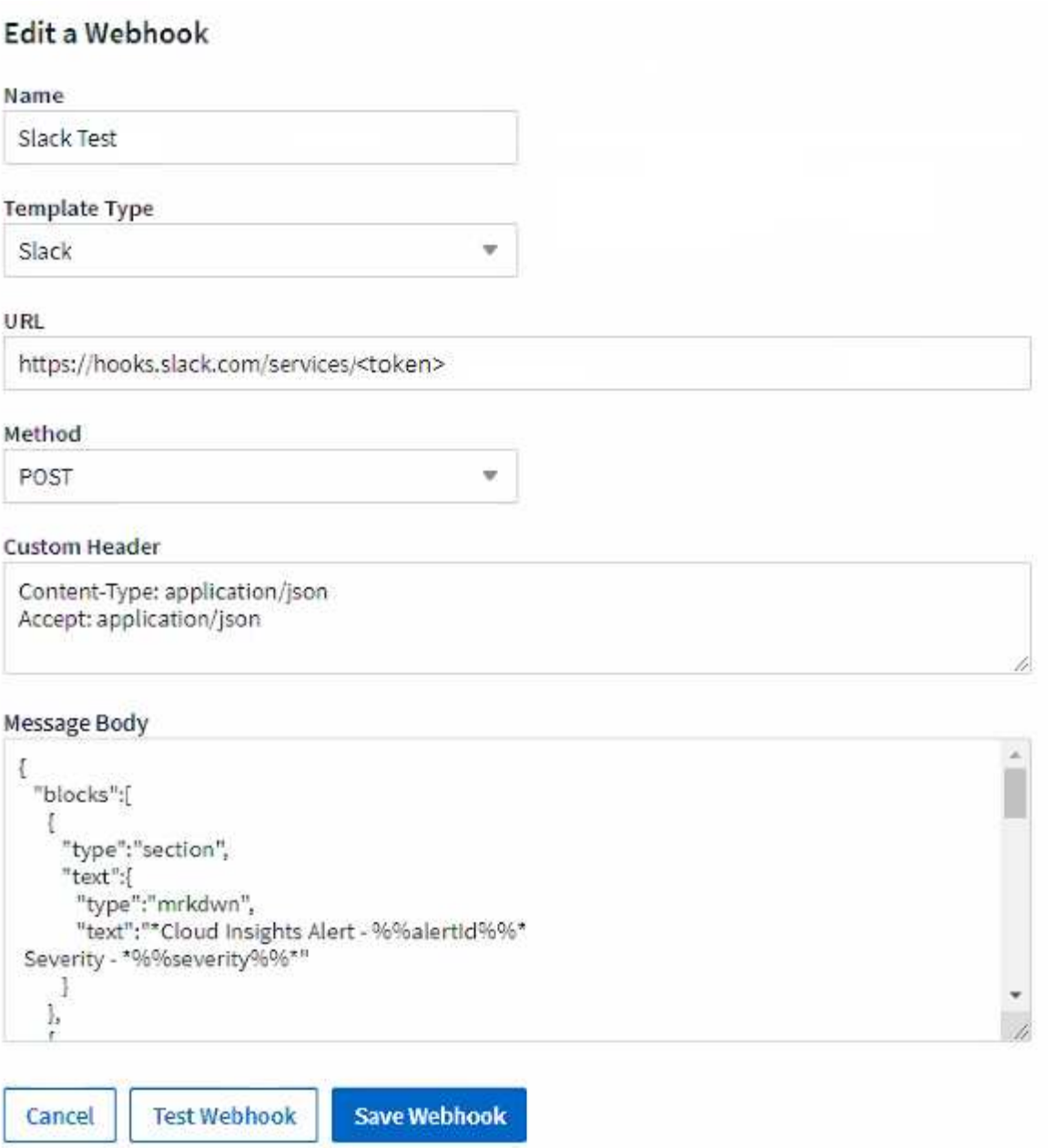
A instância do canal webhook é composta pelos seguintes elementos:

Nome	Nome único
URL	URL de destino do webhook, incluindo o prefixo *http://* ou *https://* junto com os parâmetros de URL
Método	GET, POST - O padrão é POST
Cabeçalho personalizado	Especifique quaisquer linhas de cabeçalho personalizadas aqui
Corpo da mensagem	Coloque o corpo da sua mensagem aqui
Parâmetros de alerta padrão	Lista os parâmetros padrão para o webhook
Parâmetros e segredos personalizados	Parâmetros e segredos personalizados permitem que você adicione parâmetros exclusivos e elementos seguros, como senhas

Criando um Webhook

Para criar um webhook do Data Infrastructure Insights , acesse **Admin > Notificações** e selecione a aba **Webhooks**.

A imagem a seguir mostra um exemplo de webhook configurado para o Slack:



Insira as informações apropriadas para cada um dos campos e clique em "Salvar" quando terminar.

Você também pode clicar no botão "Testar Webhook" para testar a conexão. Observe que isso enviará o "Corpo da Mensagem" (sem substituições) para a URL definida de acordo com o Método selecionado.

Os webhooks do Data Infrastructure Insights compreendem uma série de parâmetros padrão. Além disso, você pode criar seus próprios parâmetros ou segredos personalizados.

Default Alert Parameters

Name	Description
%%alertDescription%%	Alert description
%%alertId%%	Alert ID
%%alertRelativeUrl%%	Relative URL to the Alert page. To build alert link use https://%%cloudInsightsHostName%%%%alertRelativeUrl%%
%%metricName%%	Monitored metric
%%monitorName%%	Monitor name
%%objectType%%	Monitored object type
%%severity%%	Alert severity level
%%alertCondition%%	Alert condition
%%triggerTime%%	Alert trigger time in GMT ('Tue, 27 Oct 2020 01:20:30 GMT')
%%triggerTimeEpoch%%	Alert trigger time in Epoch format (milliseconds)
%%triggeredOn%%	Triggered On (key:value pairs separated by commas)
%%value%%	Metric value that triggered the alert
%%cloudInsightsLogoUrl%%	Cloud Insights logo URL
%%cloudInsightsHostname%%	Cloud Insights Hostname (concatenate with relative URL to build alert link)

Custom Parameters and Secrets

Name	Value	Description
No Data Available		

+ Parameter

Parâmetros: O que são e como usá-los?

Parâmetros de alerta são valores dinâmicos preenchidos por alerta. Por exemplo, o parâmetro *%%TriggeredOn%%* será substituído pelo objeto no qual o alerta foi disparado.

Você pode adicionar qualquer atributo de objeto (por exemplo, nome de armazenamento) como um parâmetro para um webhook. Por exemplo, você pode definir parâmetros para o nome do volume e o nome do armazenamento em uma descrição de webhook como: "Alta latência para volume: *%%relatedObject.volume.name%%*, Armazenamento: *%%relatedObject.storage.name%%*".

Observe que nesta seção, as substituições *não* são realizadas ao clicar no botão "Testar Webhook"; o botão envia uma carga útil que mostra as %% substituições, mas não as substitui por dados.

Parâmetros e segredos personalizados

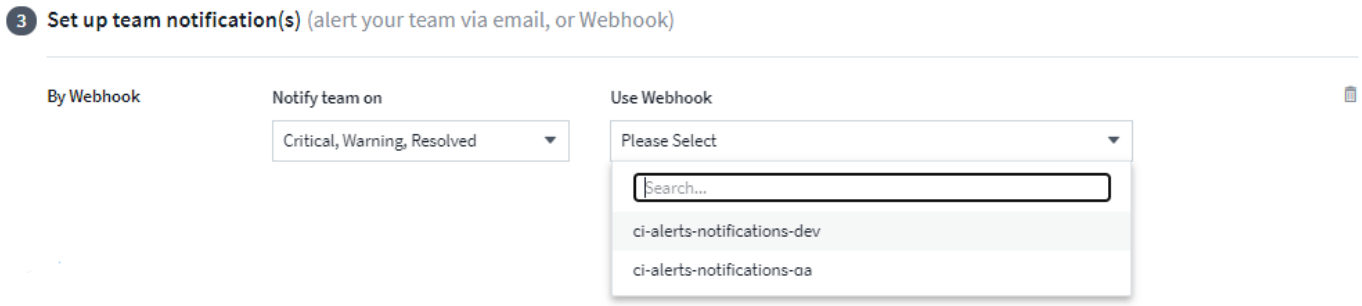
Nesta seção, você pode adicionar quaisquer parâmetros personalizados e/ou segredos que desejar. Por motivos de segurança, se um segredo for definido, somente o criador do webhook poderá modificar este canal do webhook. É somente leitura para outros. Você pode usar segredos em URL/Cabeçalhos como *%%<secret_name>%%*.

Página de lista de webhooks

Na página da lista Webhooks, são exibidos os campos Nome, Criado por, Criado em, Status, Seguro e Último relatório.

Escolhendo Notificação de Webhook em um Monitor

Para escolher a notificação do webhook em um"monitor" , vá para **Alertas > Gerenciar Monitores** e selecione o monitor desejado ou adicione um novo monitor. Na seção *Configurar notificações da equipe*, escolha *Webhook* como método de entrega. Selecione os níveis de alerta (Crítico, Aviso, Resolvido) e escolha o webhook desejado.



Exemplos de webhook:

Webhooks para"Folga" Webhooks para"PagerDuty" Webhooks para"Equipes" Webhooks para"Discórdia"

Exemplo de webhook para Discord

Os webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado. Esta página fornece um exemplo de configuração de webhooks para o Discord.

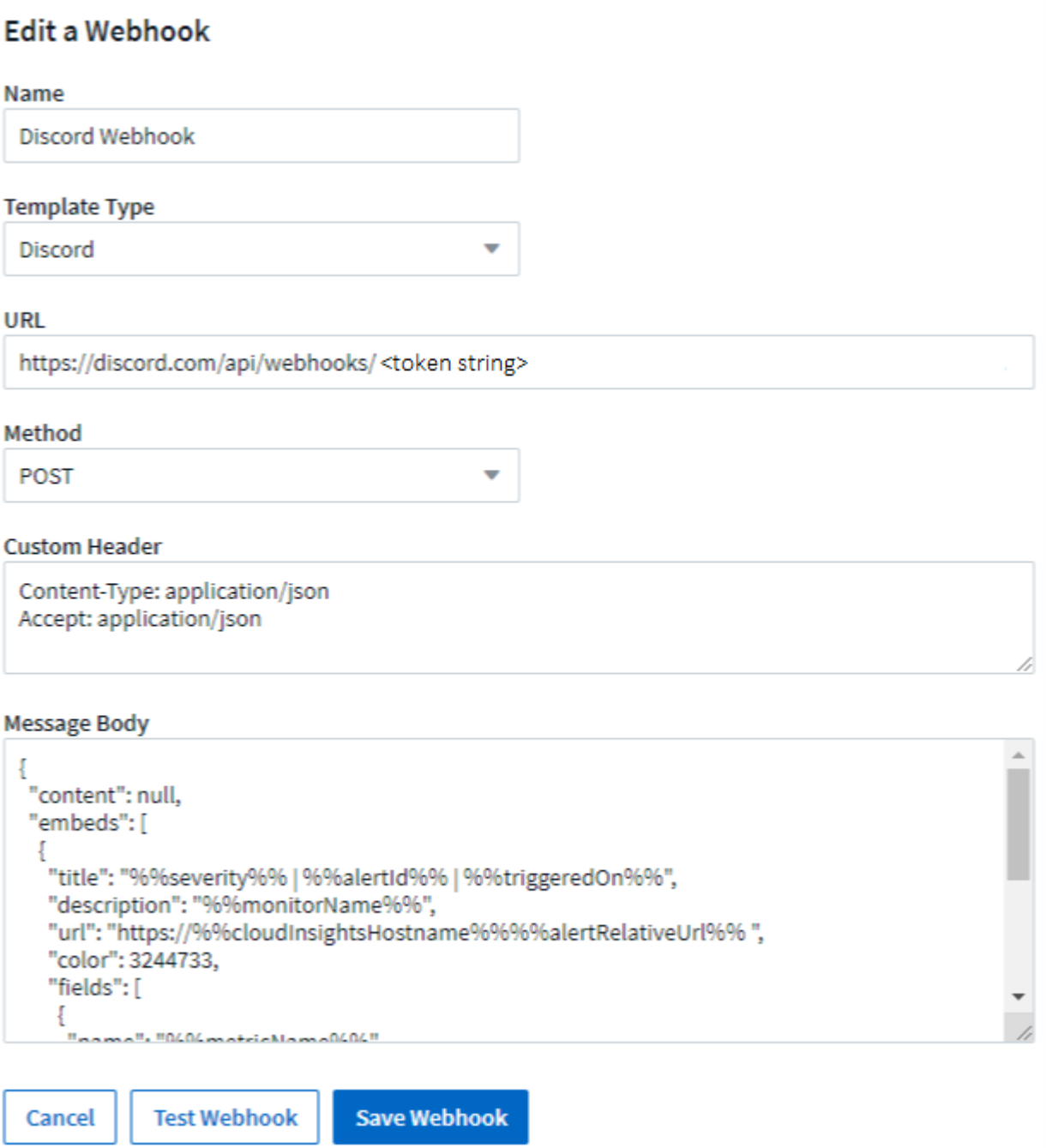
Esta página se refere a instruções de terceiros, que podem estar sujeitas a alterações. Consulte o"Documentação do Discord" para obter as informações mais atualizadas.

Configuração do Discord:

- No Discord, selecione o Servidor, em Canais de Texto, selecione Editar Canal (ícone de engrenagem)
- Selecione **Integrações > Exibir Webhooks** e clique em **Novo Webhook**
- Copie o URL do Webhook. Você precisará colar isso na configuração do webhook do Data Infrastructure Insights .

Criar webhook de Data Infrastructure Insights :

1. No Data Infrastructure Insights, navegue até **Admin > Notificações** e selecione a guia **Webhooks**. Clique em **+Webhook** para criar um novo webhook.
2. Dê ao webhook um nome significativo, como "Discord".
3. No menu suspenso *Tipo de modelo*, selecione **Discord**.
4. Cole a URL acima no campo *URL*.

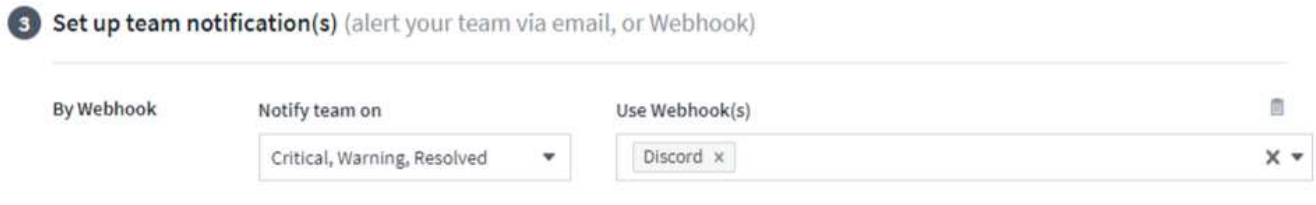


Para testar o webhook, substitua temporariamente o valor da URL no corpo da mensagem por qualquer URL válida (como *https://netapp.com*) e clique no botão *Testar Webhook*. Não se esqueça de redefinir o corpo da mensagem quando o teste for concluído.

Notificações via Webhook

Para notificar eventos via webhook, no Data Infrastructure Insights navegue até **Alertas > Monitores** e clique em **+Monitor** para criar um novo"monitor" .

- Selecione uma métrica e defina as condições do monitor.
- Em _Configurar notificação(ões) da equipe, escolha o Método de entrega **Webhook**.
- Selecione o webhook "Discord" para os eventos desejados (Crítico, Aviso, Resolvido)



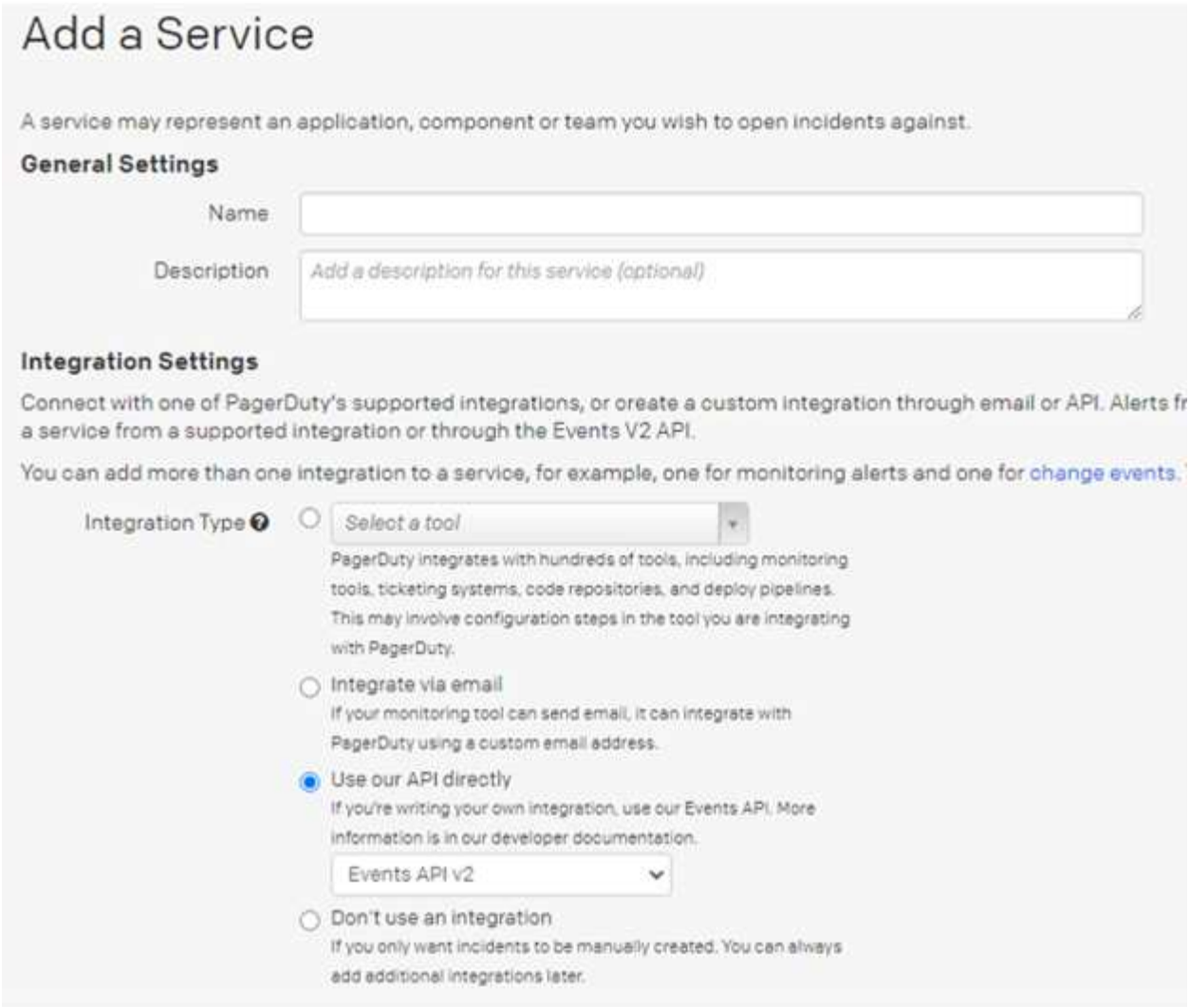
Exemplo de webhook para PagerDuty

Os webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado. Esta página fornece um exemplo de configuração de webhooks para o PagerDuty.

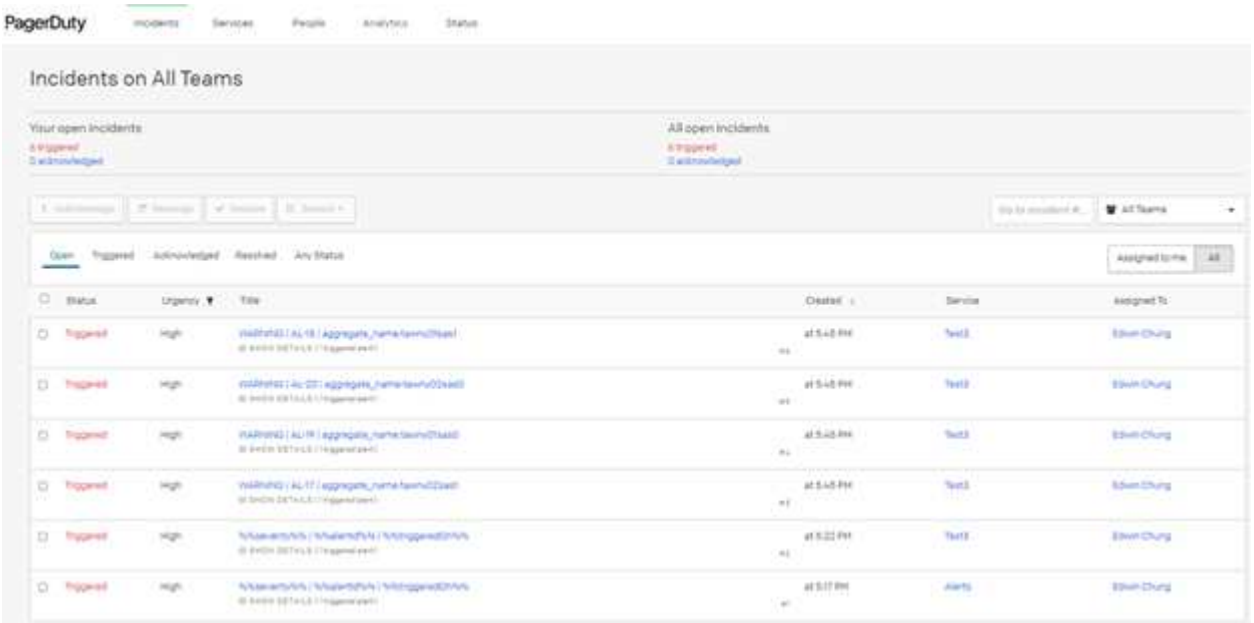
Esta página se refere a instruções de terceiros, que podem estar sujeitas a alterações. Consulte o"Documentação do PagerDuty" para obter as informações mais atualizadas.

Configuração do PagerDuty:

1. No PagerDuty, navegue até **Serviços > Diretório de serviços** e clique no botão **+Novo serviço**
2. Digite um *Nome* e selecione *Usar nossa API diretamente*. Clique em *Adicionar serviço*.

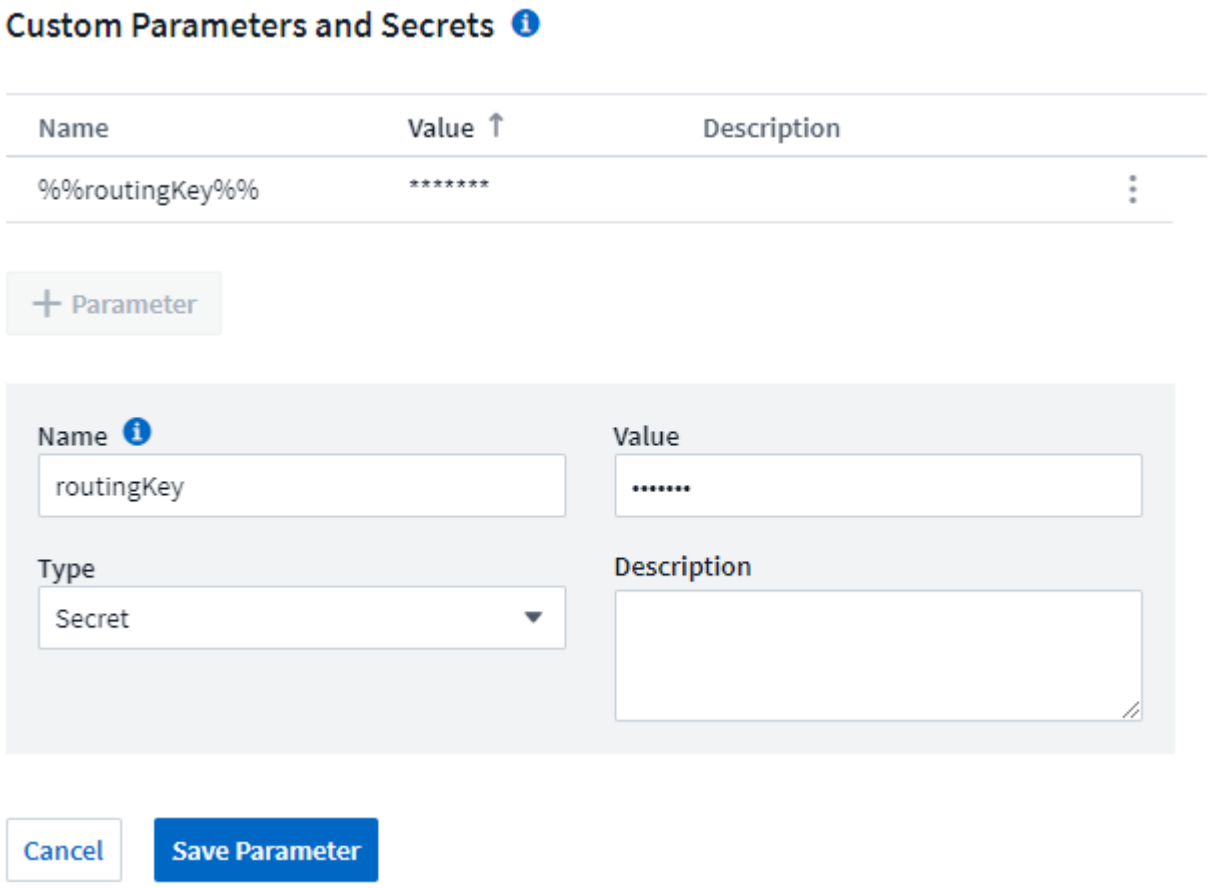


3. Clique na aba *Integrações* para ver a **Chave de Integração**. Você precisará dessa chave ao criar o webhook do Data Infrastructure Insights abaixo.
4. Acesse **Incidentes** ou **Serviços** para visualizar Alertas.



Criar webhook de Data Infrastructure Insights :

1. No Data Infrastructure Insights, navegue até **Admin > Notificações** e selecione a guia **Webhooks**. Clique em **+Webhook** para criar um novo webhook.
2. Dê ao webhook um nome significativo, como "PagerDuty Trigger". Você usará este webhook para eventos de nível crítico e de aviso.
3. No menu suspenso *Tipo de modelo*, selecione **PagerDuty**.
4. Crie um segredo de parâmetro personalizado chamado *routingKey* e defina o valor como o valor da *Chave de Integração* do PagerDuty acima.



Repita essas etapas para criar um webhook "PagerDuty Resolve" para eventos resolvidos.

Mapeamento de campos de Data Infrastructure Insights do PagerDuty

A tabela e a imagem a seguir mostram o mapeamento de campos entre o PagerDuty e o Data Infrastructure Insights:

PagerDuty	Data Infrastructure Insights
Chave de alerta	ID de alerta
Fonte	Acionado em
Componente	Nome da métrica
Grupo	Tipo de objeto

PagerDuty	Data Infrastructure Insights
Aula	Nome do monitor

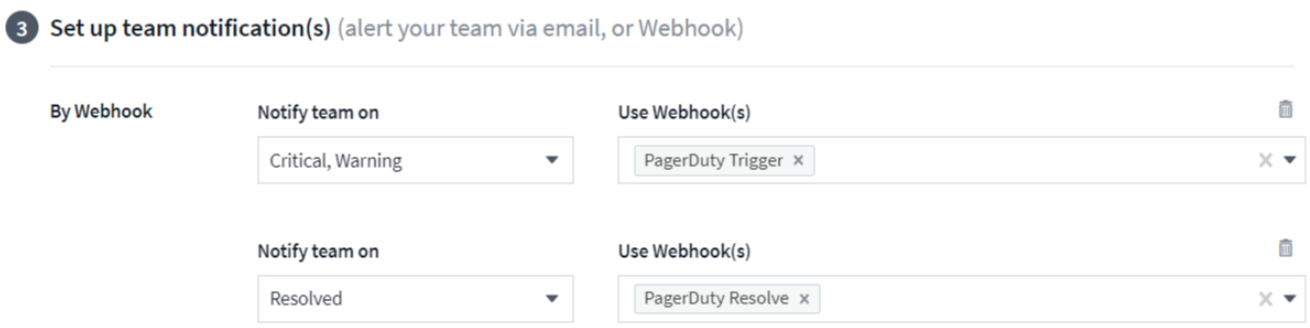
Message Body

```
{
 "dedup_key": "%%alertId%%",
 "event_action": "trigger",
 "links": [
  {
   "href": "https://%%cloudInsightsHostname%%%%alertRelativeUrl%%",
   "text": "'%%metricName%%' value of %%value%% (%%alertCondition%%) for
%%triggeredOn%%"
  }
 ],
 "payload": {
  "class": "%%monitorName%%",
  "component": "%%metricName%%",
  "group": "%%objectType%%",
  "severity": "critical",
  "source": "%%triggeredOn%%",
  "summary": "%%severity%% | %%alertId%% | %%triggeredOn%%"
 },
 "routing_key": "%%routingKey%%"
}
```

Notificações via Webhook

Para notificar eventos via webhook, no Data Infrastructure Insights navegue até **Alertas > Monitores** e clique em **+Monitor** para criar um novo"monitor" .

- Selecione uma métrica e defina as condições do monitor.
- Em _Configurar notificação(ões) da equipe, escolha o Método de entrega **Webhook**.
- Escolha o webhook "PagerDuty Trigger" para eventos de nível Crítico e de Aviso.
- Selecione "PagerDuty Resolve" para eventos resolvidos.



Definir notificações separadas para eventos de gatilho e eventos resolvidos é uma prática recomendada, pois o PagerDuty lida com eventos de gatilho de forma diferente dos eventos resolvidos.

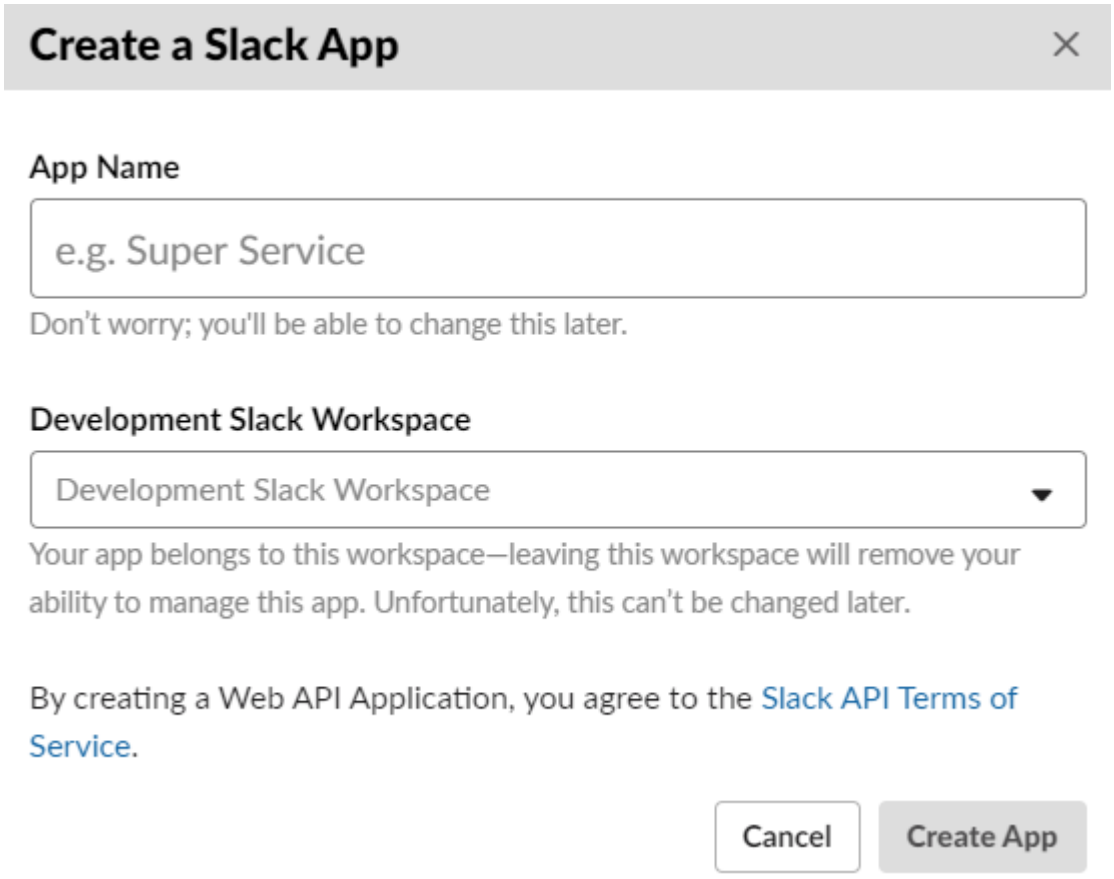
Exemplo de webhook para Slack

Os webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado. Esta página fornece um exemplo de configuração de webhooks para o Slack.

Esta página se refere a instruções de terceiros, que podem estar sujeitas a alterações. Consulte o"Documentação do Slack" para obter as informações mais atualizadas.

Exemplo de folga:

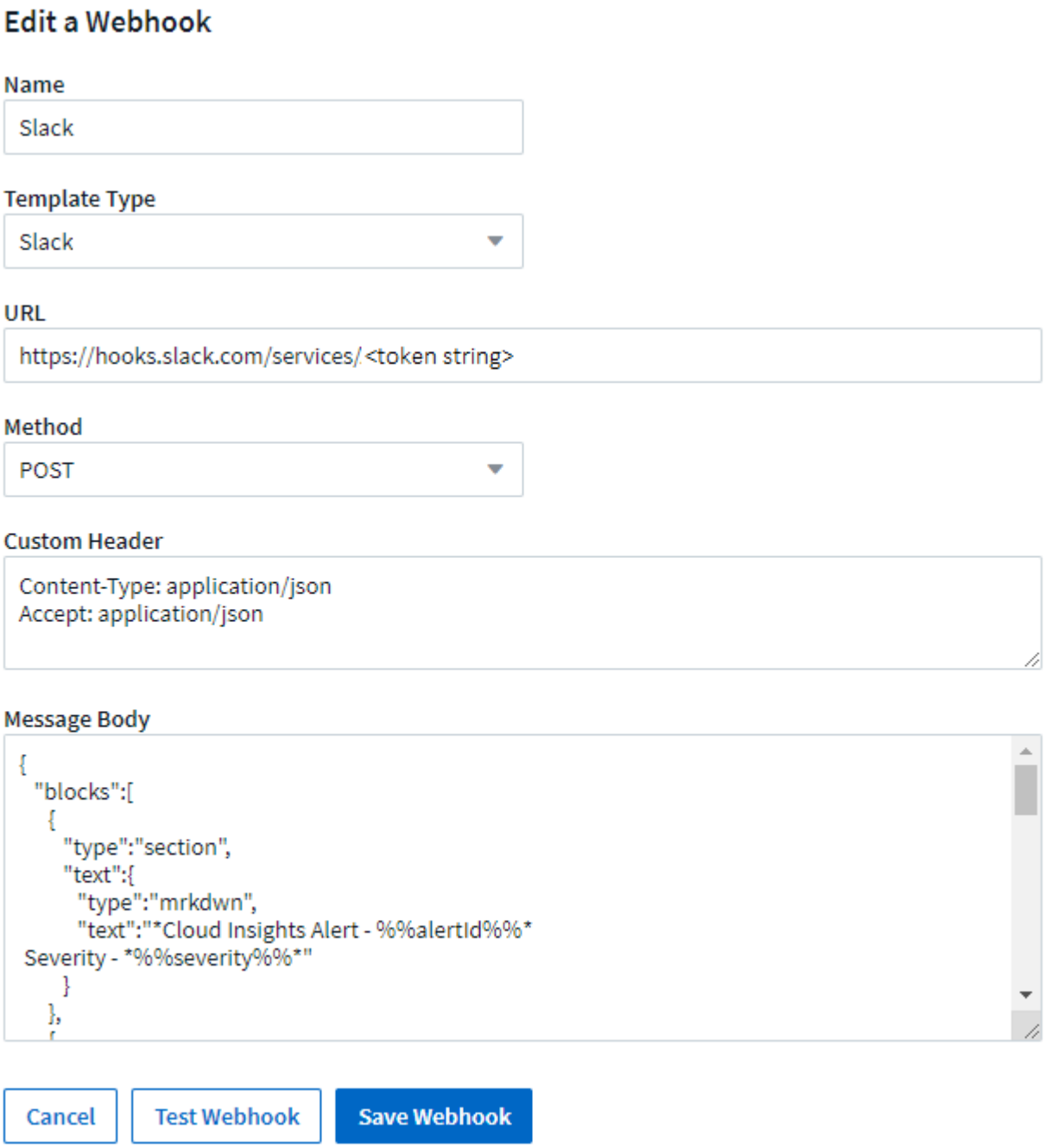
- Vá para https://api.slack.com/apps e crie um novo aplicativo. Dê um nome significativo e selecione o Slack Workspace.



- Vá para Webhooks de entrada, clique em *Ativar Webhooks de entrada*, Solicitar para *Adicionar novo Webhook* e selecione o canal no qual deseja postar.
- Copie o URL do Webhook. Você precisará colar isso na configuração do webhook do Data Infrastructure Insights .

Criar webhook de Data Infrastructure Insights :

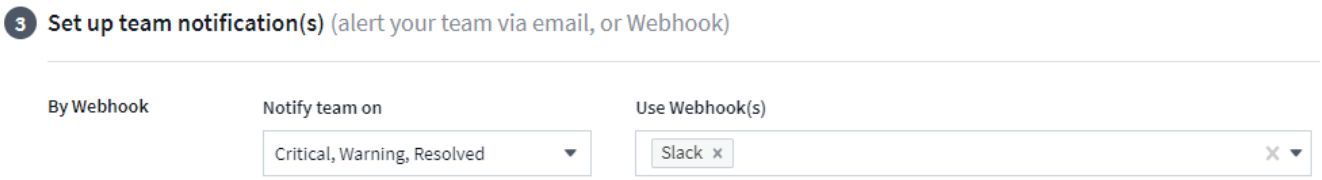
1. No Data Infrastructure Insights, navegue até **Admin > Notificações** e selecione a guia **Webhooks**. Clique em **+Webhook** para criar um novo webhook.
2. Dê ao webhook um nome significativo, como "Slack Webhook".
3. No menu suspenso *Tipo de modelo*, selecione **Slack**.
4. Cole a URL acima no campo *URL*.



Notificações via Webhook

Para notificar eventos via webhook, no Data Infrastructure Insights navegue até **Alertas > Monitores** e clique em **+Monitor** para criar um novo"monitor" .

- Selecione uma métrica e defina as condições do monitor.
- Em _Configurar notificação(ões) da equipe, escolha o Método de entrega **Webhook**.
- Selecione o webhook "Slack" para os eventos desejados (Crítico, Aviso, Resolvido)



Mais informações:

- Para modificar o formato e o layout da mensagem, consulte https://api.slack.com/messaging/composing
- Tratamento de erros: https://api.slack.com/messaging/webhooks#handling_errors

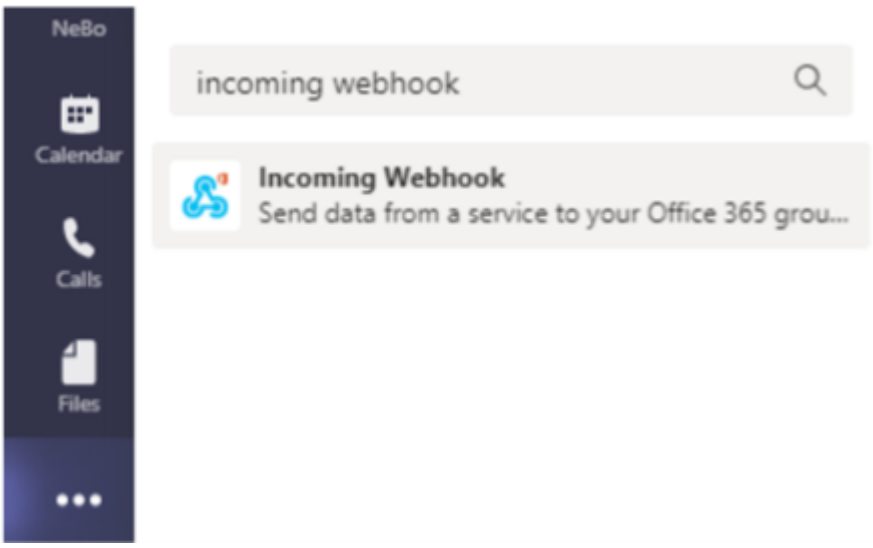
Exemplo de webhook para Microsoft Teams

Os webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado. Esta página fornece um exemplo de configuração de webhooks para o Teams.

Esta página se refere a instruções de terceiros, que podem estar sujeitas a alterações. Consulte o"Documentação das equipes" para obter as informações mais atualizadas.

Configuração das equipes:

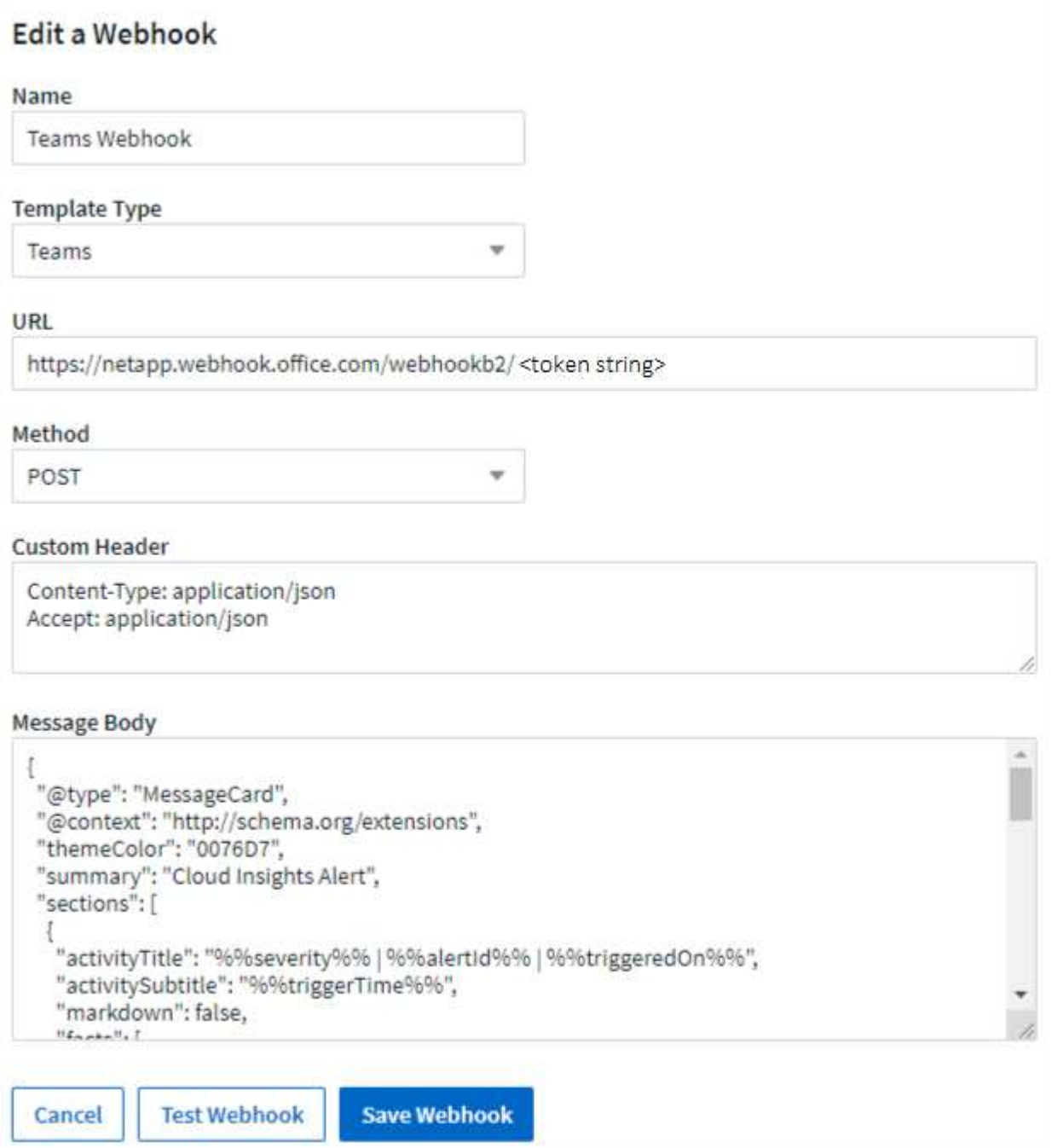
1. No Teams, selecione o kebab e pesquise por Webhook de entrada.



2. Selecione **Adicionar a uma equipe > Selecionar uma equipe > Configurar um conector**.
3. Copie o URL do Webhook. Você precisará colar isso na configuração do webhook do Data Infrastructure Insights .

Criar webhook de Data Infrastructure Insights :

1. No Data Infrastructure Insights, navegue até **Admin > Notificações** e selecione a guia **Webhooks**. Clique em **+Webhook** para criar um novo webhook.
2. Dê ao webhook um nome significativo, como "Teams Webhook".
3. No menu suspenso *Tipo de modelo*, selecione **Equipes**.

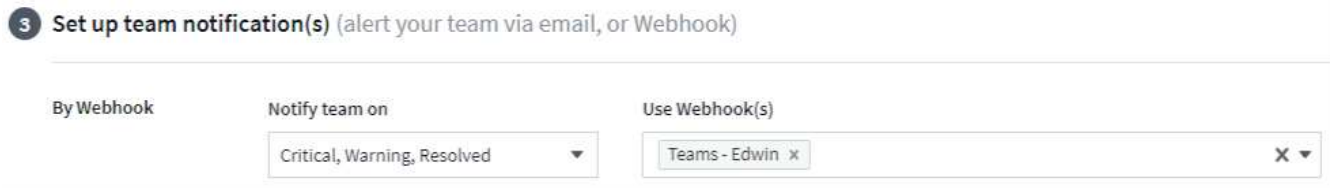


1. Cole a URL acima no campo *URL*.

Notificações via Webhook

Para notificar eventos via webhook, no Data Infrastructure Insights navegue até **Alertas > Monitores** e clique em **+Monitor** para criar um novo"monitor" .

- Selecione uma métrica e defina as condições do monitor.
- Em _Configurar notificação(ões) da equipe, escolha o Método de entrega **Webhook**.
- Selecione o webhook "Equipes" para os eventos desejados (Crítico, Aviso, Resolvido)



Informações sobre direitos autorais

Copyright © 2026 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 DESTE DOCUMENTO. 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 SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO 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 DESTE SOFTWARE, 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.