Monitores e alertas

Data Infrastructure Insights

NetApp
September 09, 2025

Índice

Monitores e alertas

Alertas 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 tais condições forem atendidas.

Os monitores permitem definir limites para métricas geradas por objetos de "infraestrutura", como armazenamento, VM, EC2 e portas, bem como para dados de "integração", como os coletados para Kubernetes, métricas avançadas do ONTAP e plugins do Telegraf. Esses monitores *métricos* alertam você quando os limites de nível de aviso ou nível crítico são cruzados.

Você também pode criar monitores para acionar alertas de nível de aviso, crítico ou informativo quando os eventos *log* especificados são detetados.

O Data Infrastructure Insights também fornece várias opções"Monitores definidos pelo sistema", com base no seu ambiente.

Melhores práticas de segurança

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

Monitor métrico ou de registo?

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

   É apresentada a página da lista de monitores, mostrando os monitores atualmente configurados.

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 Registros.

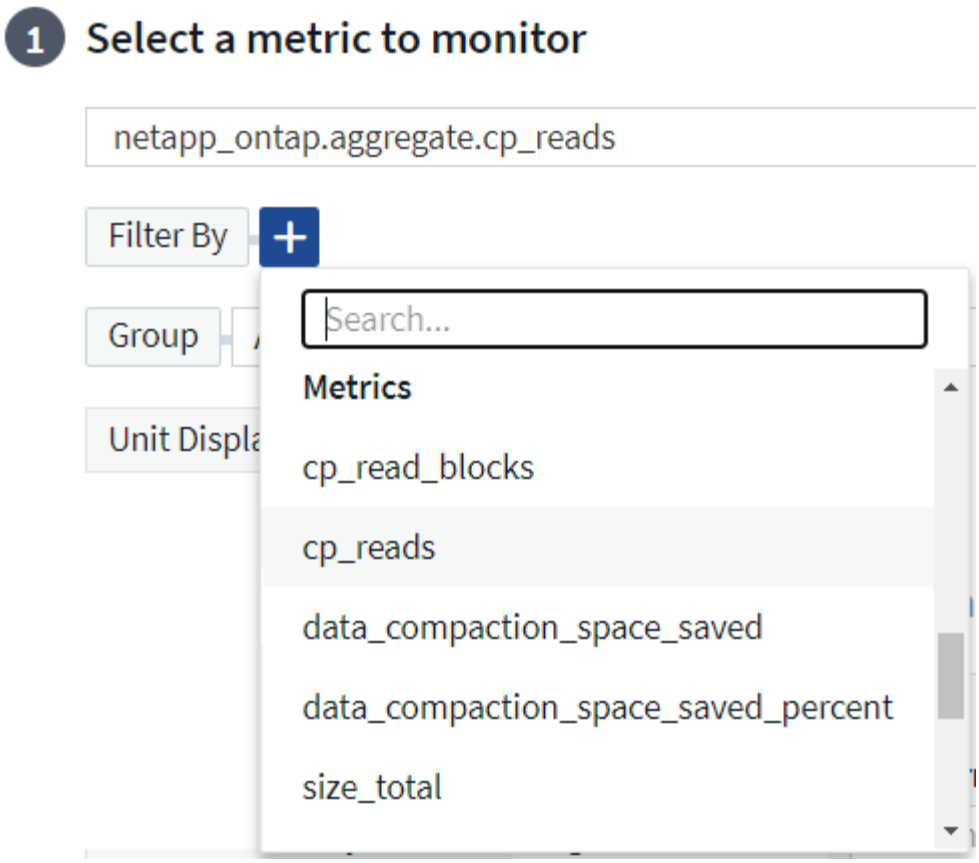
- *Metric* monitora alertas sobre gatilhos relacionados à infraestrutura ou ao desempenho
- *Log* monitora o alerta na atividade relacionada ao log

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

Monitor métrico

1. Na lista suspensa, procure e escolha um tipo de objeto e uma métrica para monitorar.

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



Ao trabalhar com dados de integração (Kubernetes, dados avançados do ONTAP, etc.), a filtragem de métricas remove os pontos de dados individuais/não correspondidos da série de dados plotados, ao contrário dos dados de infraestrutura (armazenamento, VM, portas, etc.), onde os filtros funcionam no valor agregado da série de dados e potencialmente removem todo o objeto do gráfico.

Para criar um monitor de várias condições (por exemplo, IOPS > X e latência > Y), defina a primeira condição como um limite e a segunda condição como um filtro.

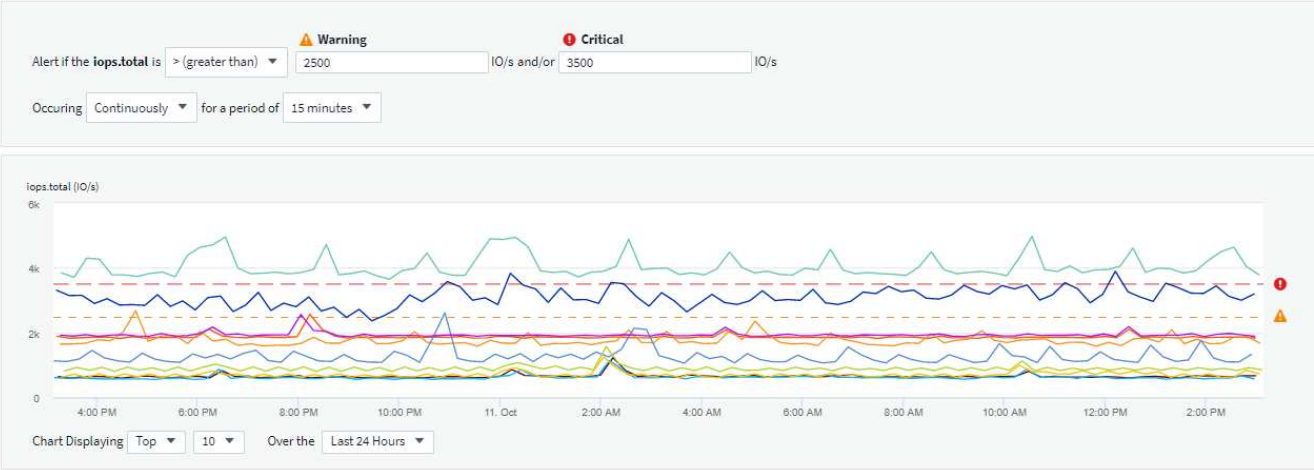
Defina as condições do Monitor.

1. Depois de escolher o objeto e a métrica a monitorar, defina os limites nível de Advertência e/ou nível crítico.
2. Para o nível *Warning*, digite 200 para nosso exemplo. A linha tracejada que indica este nível de aviso é apresentada no gráfico de exemplo.
3. Para o nível *Critical*, digite 400. A linha tracejada indicando este nível crítico é exibida no gráfico de exemplo.

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

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

   Você pode optar por acionar um alerta no momento em que um limite é 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 total de IOPS atingir picos acima do nível de Aviso ou crítico, mas apenas quando um objeto monitorado excede continuamente um desses níveis por pelo menos 15 minutos.



Defina o comportamento da resolução de alerta

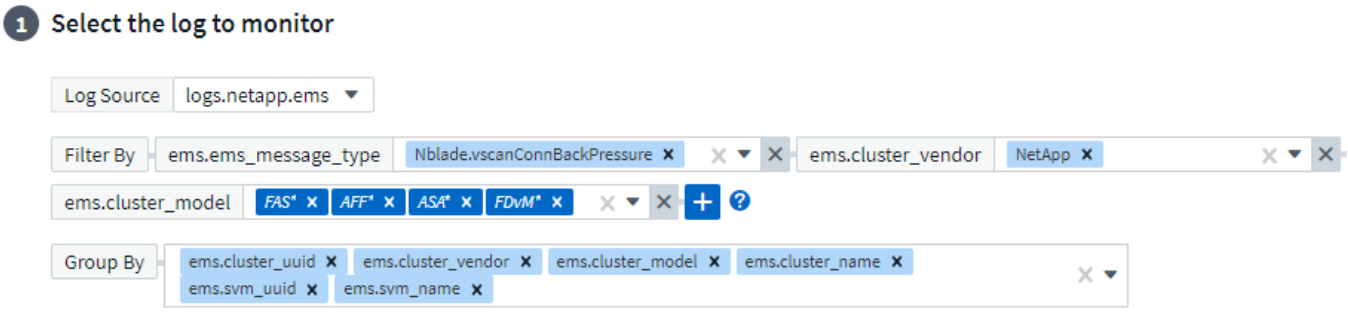
Você pode escolher como um alerta de monitor métrico é resolvido. São apresentadas duas opções:

- 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 registo

Ao criar um **monitor de log**, primeiro escolha qual log monitorar na lista de Registros disponíveis. Em seguida, você pode filtrar com base nos atributos disponíveis como acima. Você também pode escolher um ou mais atributos "Agrupar por".

ⓘ O filtro do Monitor de Registos não pode estar vazio.



Defina o comportamento do alerta

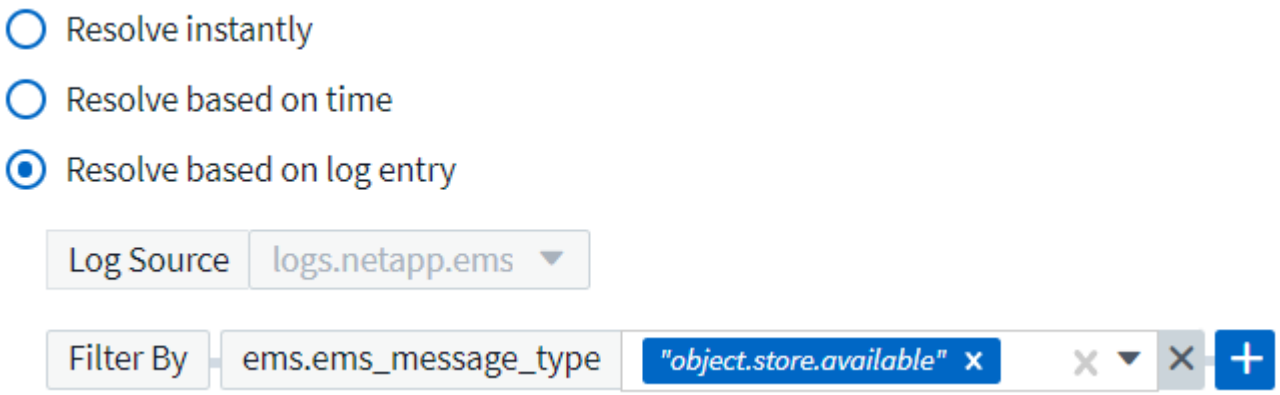
Você pode criar o monitor para alertar com um nível de gravidade de *crítico*, *Aviso* ou *informacional*, quando as condições definidas acima ocorrem uma vez (ou seja, imediatamente), ou esperar para alertar até que as condições ocorram 2 vezes ou mais.

Defina o comportamento da resolução de alerta

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

- **Resolve instantaneamente**: O alerta é imediatamente resolvido sem necessidade de qualquer outra ação

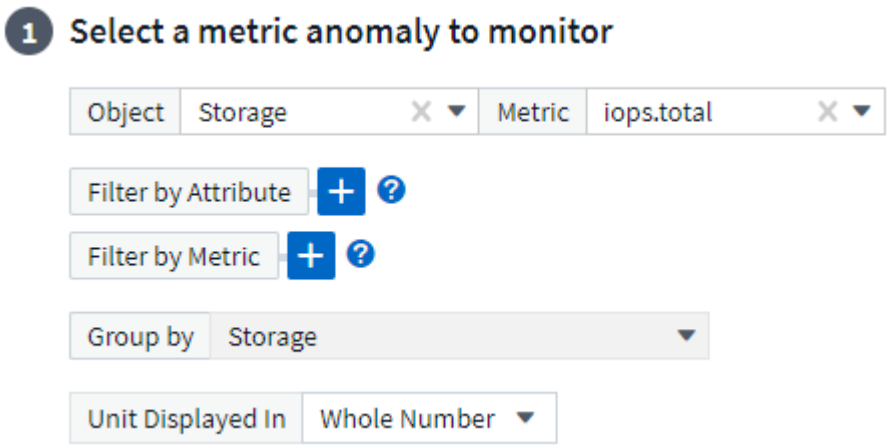
- **Resolver com base no tempo**: O alerta é resolvido após o tempo especificado ter passado
- **Resolver com base na entrada de log**: O alerta é resolvido quando uma atividade de log subsequente ocorreu. Por exemplo, quando um objeto é registrado como "disponível".



Monitor de deteção de anomalias

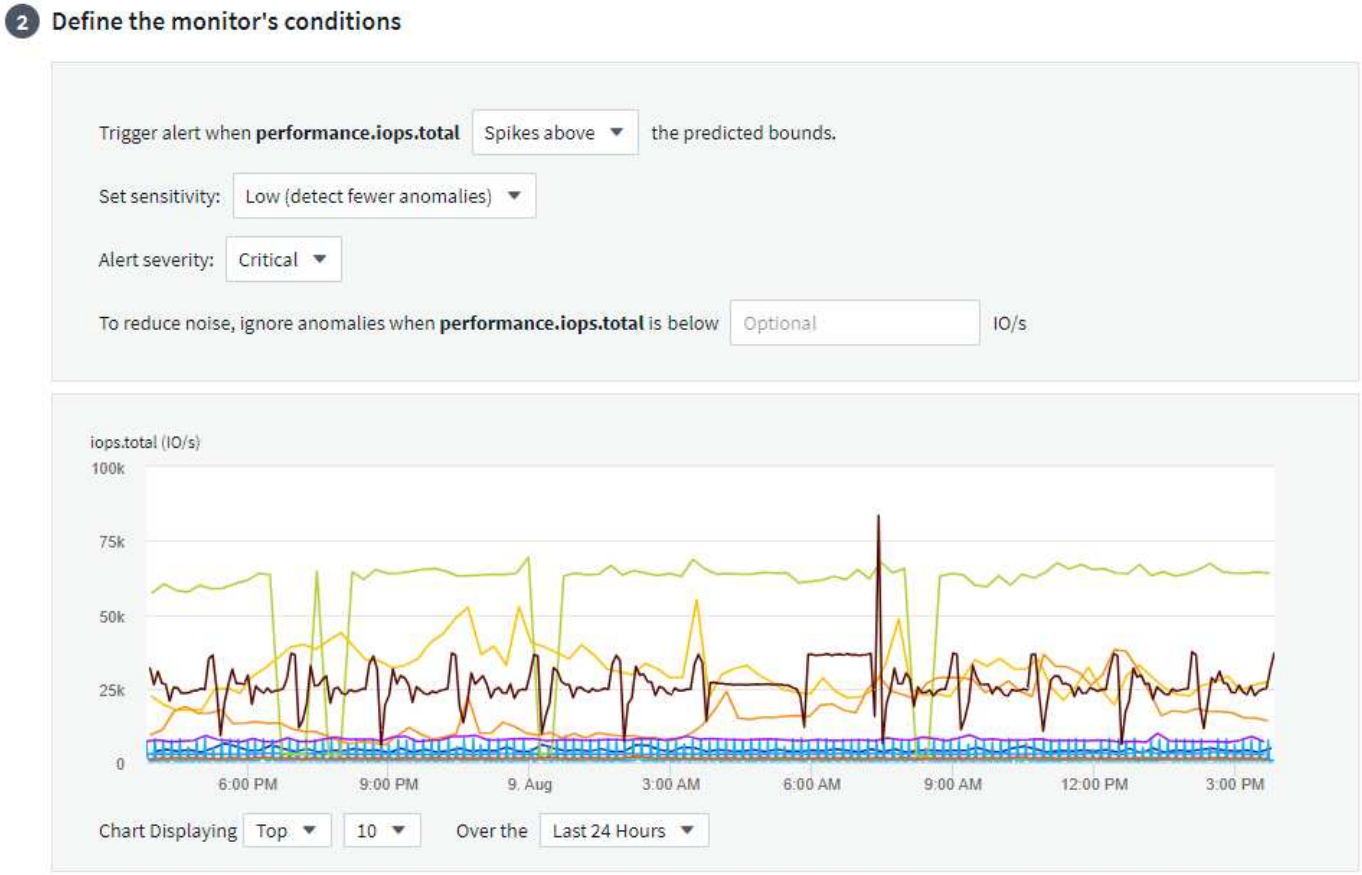
1. Na lista suspensa, procure e escolha um tipo de objeto e uma métrica para monitorar.

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



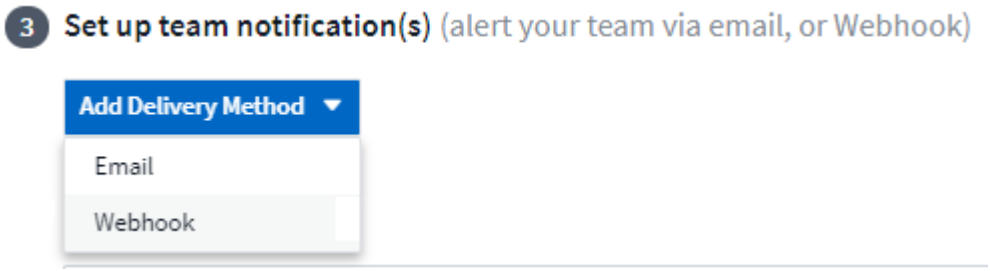
Defina as condições do Monitor.

1. Depois de escolher o objeto e a métrica para monitorar, yous et as condições em que uma anomalia é detetada.
   - Escolha se deseja detetar uma anomalia quando a métrica escolhida **picos acima** dos limites previstos, **cai abaixo** desses limites, ou **picos acima ou abaixo** dos limites.
   - Defina a **sensibilidade** da deteção. **Low** (menos anomalias são detcted), **Medium** ou **High** (mais anomalias são detetadas).
   - 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.



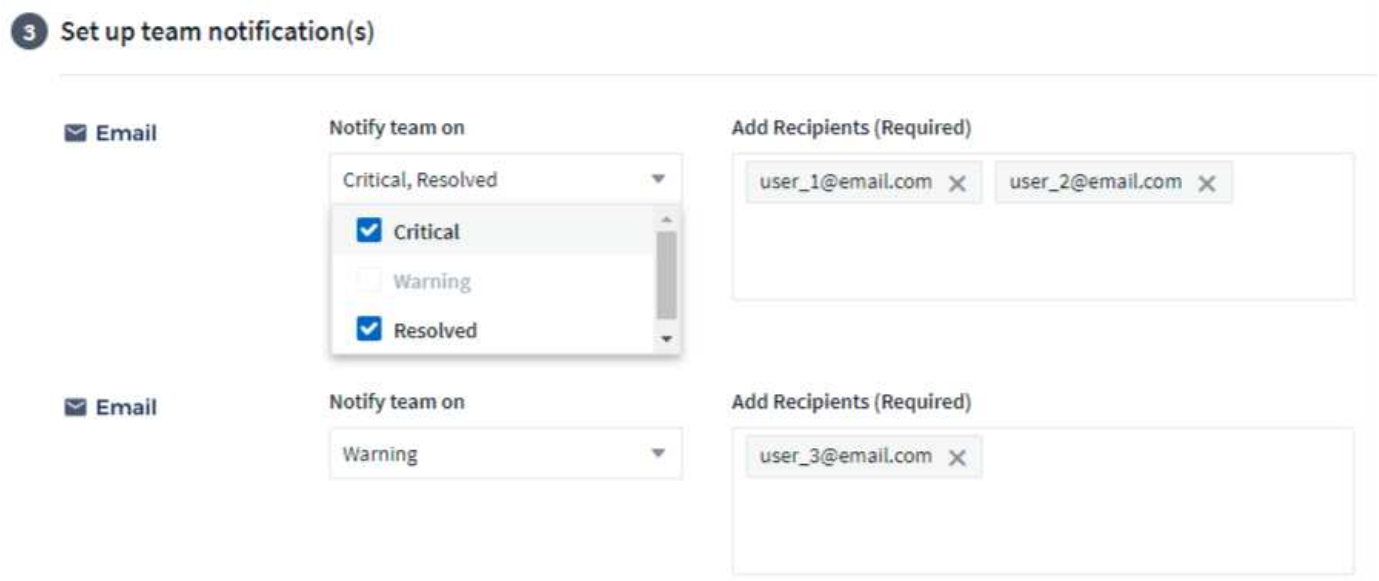
Selecione o tipo de notificação e destinatários

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



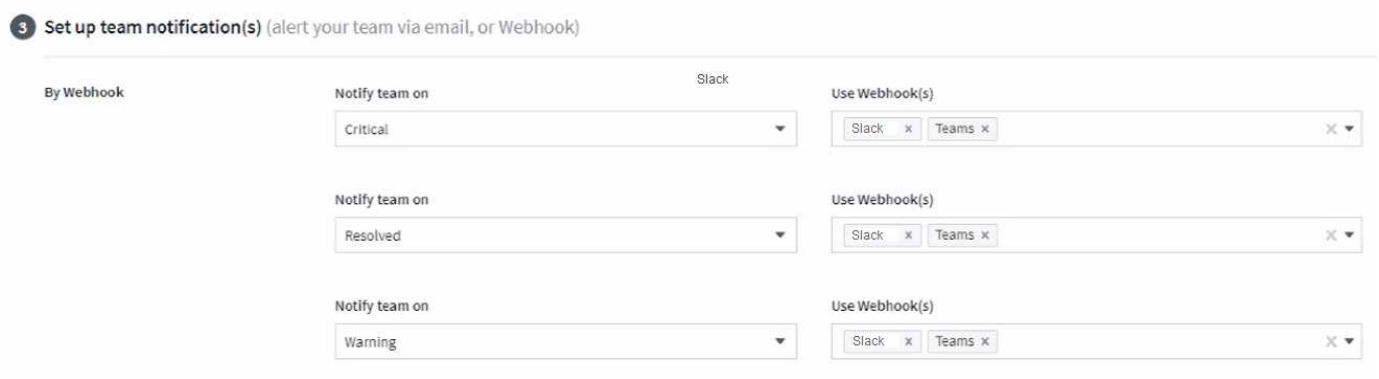
Alerta via e-mail:

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



Alerting via Webhook:

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



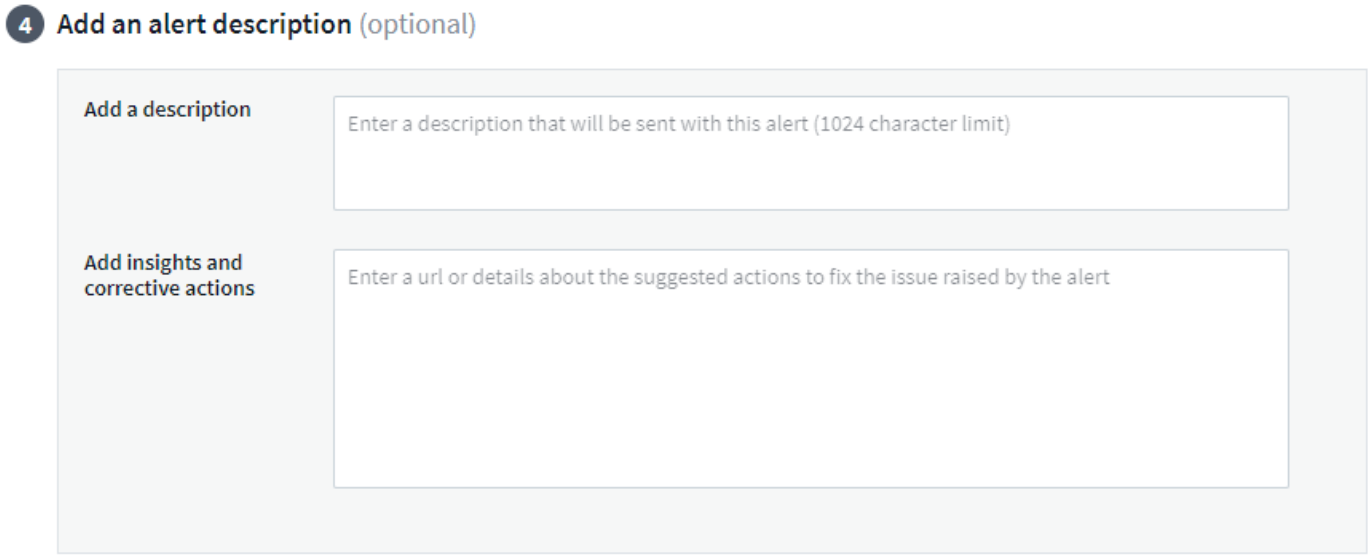
As notificações do ONTAP Data Collector têm precedência sobre quaisquer notificações específicas do Monitor que sejam relevantes para o cluster/coletor de dados. A lista de destinatários definida para o coletor de dados receberá os alertas do coletor de dados. Se não houver alertas ativos do coletor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

Definir ações corretivas ou informações adicionais

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

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

Você pode adicionar qualquer atributo de objeto (por exemplo, nome de armazenamento) como um parâmetro a 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%%*".



Guarde o monitor

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

   O novo monitor é adicionado à lista de monitores ativos.

Lista de monitores

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

- Nome do monitor
- Estado
- Objeto/métrica sendo monitorado
- Condições do monitor

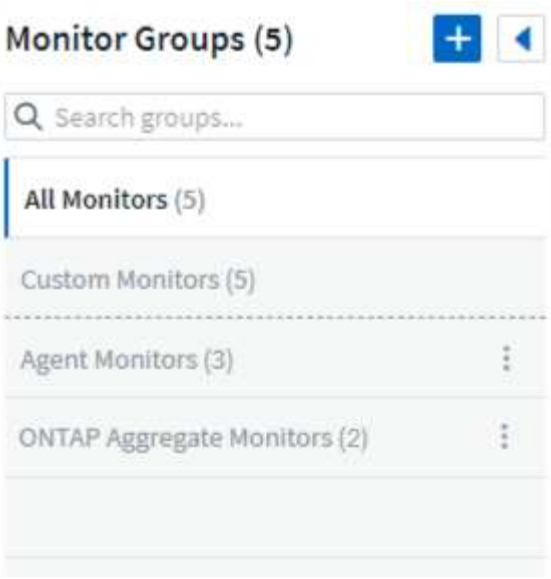
Você pode optar por pausar temporariamente o monitoramento de um tipo de objeto clicando no menu à direita do monitor e selecionando **Pausa**. Quando estiver pronto para retomar a monitorização, clique em **Resume**.

Você pode copiar um monitor selecionando **duplicar** no menu. Em seguida, você pode 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.

Monitorar grupos

O agrupamento permite visualizar e gerir monitores relacionados. Por exemplo, você pode ter um grupo de monitores dedicado ao armazenamento no locatário ou monitores relevantes para uma determinada lista de destinatários.



São apresentados os seguintes grupos de monitorização. 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** listarão todos os monitores do sistema que foram suspensos pelo Data Infrastructure Insights.
- Os Insights de infraestrutura de dados também mostrarão vários **grupos de Monitor do sistema**, que listarão um ou mais grupos de "monitores definidos pelo sistema", incluindo monitores de infraestrutura e carga de trabalho do ONTAP.

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

Monitores suspensos

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

Monitores definidos pelo sistema

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

Os monitores definidos pelo sistema não podem ser modificados, movidos para outro grupo ou eliminados. 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 (storage, volume, etc.) ou cargas de trabalho (ou seja, monitores de log) ou outros grupos. A NetApp está constantemente avaliando as necessidades do cliente e a funcionalidade do produto e atualizará ou adicionará aos 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 monitores relacionados ao armazenamento.

Para criar um novo grupo de monitores personalizados, 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 siga um destes procedimentos:

- 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*.

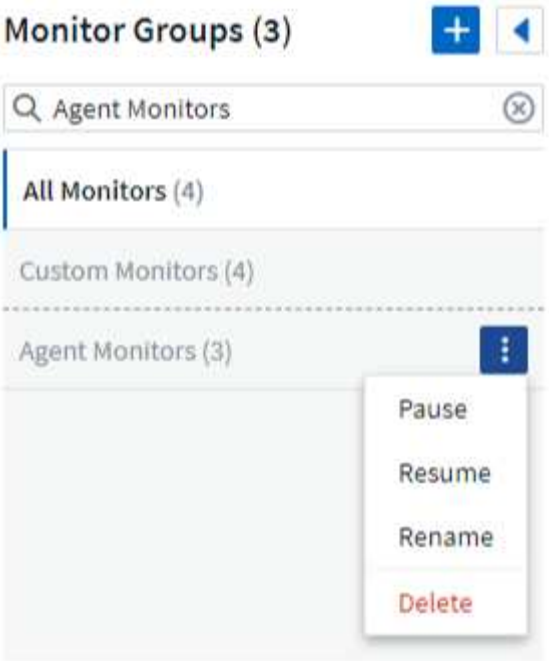
Remova os monitores clicando em um grupo e selecionando *Remover do Grupo* no menu. Não é possível remover monitores do grupo *todos os monitores* ou *monitores personalizados*. Para excluir um monitor desses grupos, você deve excluir o próprio monitor.

> A remoção de um monitor de um grupo não exclui o monitor do Data Infrastructure Insights. Para remover completamente um monitor, selecione o monitor e clique em *Delete*. Isso também o remove do grupo ao qual pertencia e não está 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 em um grupo de uma vez, selecione o menu do grupo e clique em *Pausa* 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 locatário. Devido a isso, os monitores disponíveis no Data Infrastructure Insights podem mudar à medida que os coletores de dados são adicionados ou suas configurações alteradas.

Consulte "Monitores definidos pelo sistema"a página para obter descrições de monitores incluídos no Data Infrastructure Insights.

Mais informações

- "Visualização e ausência de alertas"

Visualizar e gerir alertas a partir de monitores

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

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

Visualizar e gerir alertas

Para visualizar e gerenciar alertas, faça o seguinte.

1. Navegue até a página **Alertas > todos os Alertas**.
2. É apresentada uma lista de até 1.000 alertas mais recentes. Você pode classificar essa lista em qualquer campo clicando no cabeçalho da coluna do campo. A lista apresenta as seguintes informações. Observe que nem todas essas colunas são exibidas por padrão. Você pode selecionar colunas para exibir clicando no ícone "engrenagem":
   - **ID de alerta**: ID de alerta exclusivo gerado pelo sistema

- **Hora desencadeada**: A hora em que o Monitor relevante acionou o alerta
- **Gravidade atual** (guia alertas ativos): A gravidade atual do alerta ativo
- **Gravidade superior** (guia alertas resolvidos); a gravidade máxima do alerta antes de ser resolvido
- **Monitor**: O monitor configurado para acionar o alerta
- **Triggered on**: O objeto no qual o limite monitorado foi violado
- **Status**: Status de alerta atual, *novo* ou *em processo*
- **Status Ativo**: *Ativo* ou *resolvido*
- **Condição**: A condição limite que acionou o alerta
- **Metric**: A métrica do objeto na qual o limite monitorado foi violado
- **Status do monitor**: Status atual do monitor que acionou o alerta
- **Tem ação corretiva**: O alerta sugeriu ações corretivas. Abra a página de alerta para visualizá-los.

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

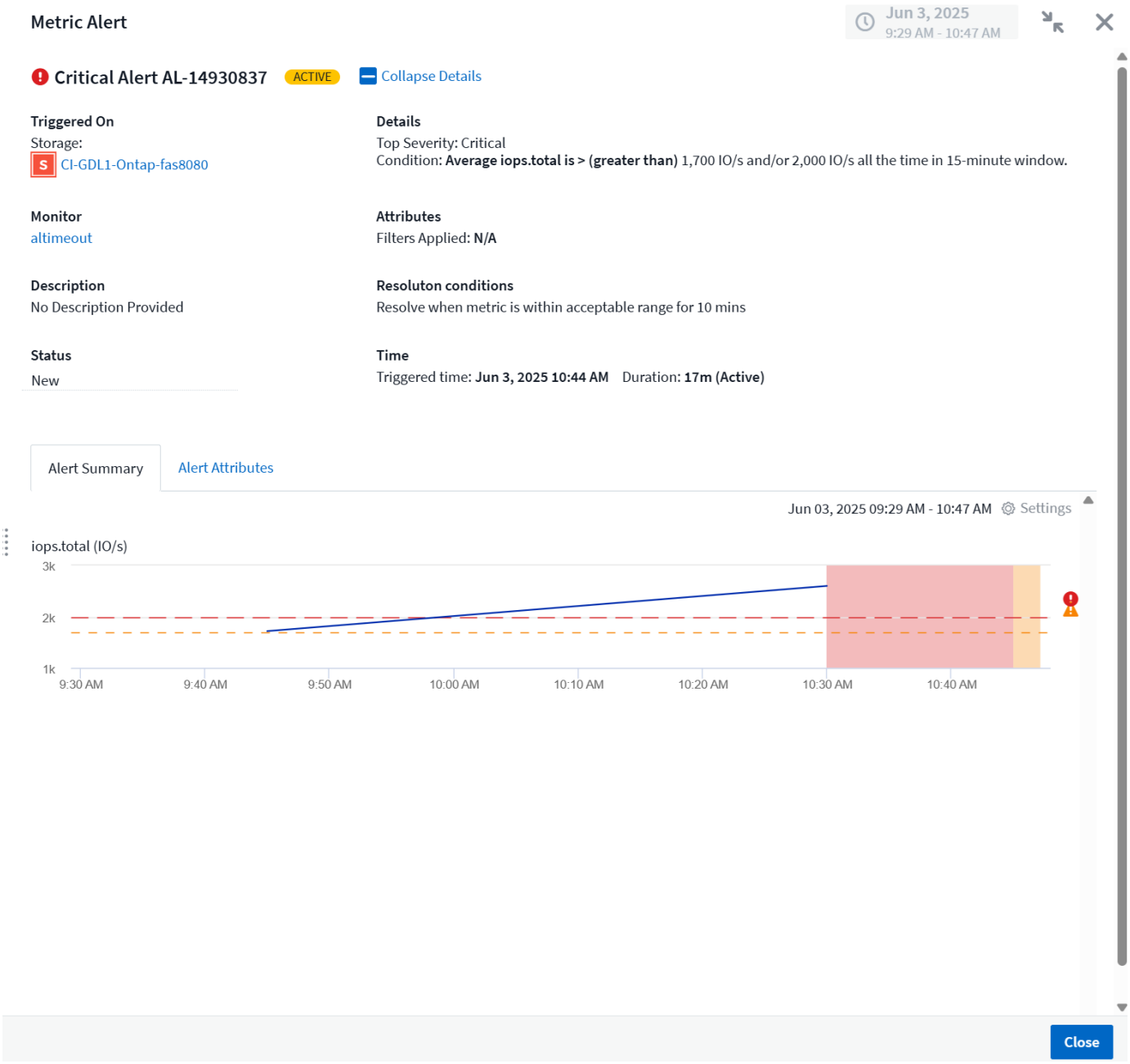
- **Em processo** para indicar que o alerta está sob investigação ou precisa ser mantido aberto
- **Dismiss** para remover o alerta da lista de alertas ativos.

Você pode gerenciar vários alertas selecionando 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 de 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 *Visualização de Especialista* mostrando gráficos relacionados aos dados do objeto, quaisquer *Ativos Relacionados* e *Comentários* inseridos pelos investigadores do alerta.



Alerta quando os dados estão em falta

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, contamos com uma de duas coisas:

- a próxima datapoint para chegar
- um temporizador para disparar quando não há datapoint e você esperou o suficiente

Como é o caso com chegada lenta de dados - ou sem chegada de dados - o mecanismo do temporizador precisa assumir o controle, pois a taxa de chegada de dados é insuficiente para acionar alertas em "tempo real". Então, a pergunta geralmente se torna "quanto tempo eu espero antes de fechar a janela de análise e olhar para o que eu tenho?" Se você esperar muito tempo, então você não está gerando os alertas rápido o suficiente para ser útil.

Se você tiver um Monitor com uma janela de 30 minutos que perceba que uma condição é violada pelo último

ponto de dados antes de uma perda de dados a longo prazo, um Alerta será gerado porque o Monitor não recebeu outras informações para usar para confirmar uma recuperação da métrica ou notar que a condição persistiu.

Alertas "permanentemente ativos"

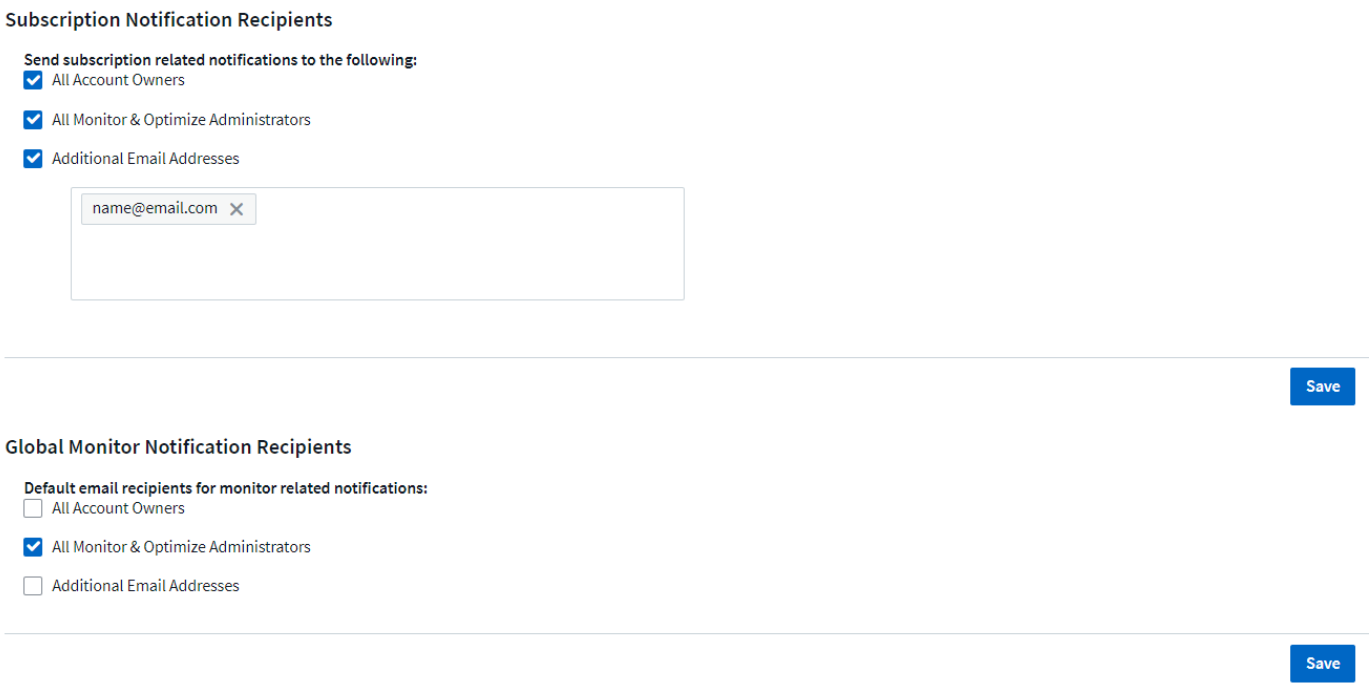
É possível configurar um monitor de tal forma que a condição **Always** exista no objeto monitorado - por exemplo, IOPS > 1 ou latência > 0. Estes são frequentemente criados como monitores de "teste" e depois esquecidos. Esses monitores criam alertas que permanecem permanentemente abertos nos objetos constituintes, o que pode causar problemas de estresse e estabilidade do sistema 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 algumas das tensões do sistema que podem ocorrer de outra forma.

Configurar notificações por e-mail

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

Para configurar as configurações do destinatário de e-mail de notificação, vá para a página **Admin > notificações** e selecione a guia *e-mail*.



Destinatários da notificação de assinatura

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

- Todos os proprietários de contas
- Todos os administradores *Monitor & Otimize*
- Endereços de e-mail adicionais que você especificar

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

Notificação:	**Ação do Usuário:**
A versão de avaliação ou subscrição foi atualizada	Reveja os detalhes da subscrição "Subscrição"na página
A assinatura expirará em 90 dias. A assinatura expirará em 30 dias	Nenhuma ação necessária se a "renovação automática" estiver ativada entre em Contato com as vendas da NetApp para renovar a assinatura
O teste termina em 2 dias	Renove o teste a partir "Subscrição"da página. Você pode renovar um teste uma vez. Entre em Contato com a NetApp Sales para comprar uma assinatura
A conta de teste ou assinatura expirou deixará de coletar dados em 48 horas a conta será excluída após 48 horas	Entre em Contato com a NetApp Sales para comprar uma assinatura

Para garantir que seus destinatários recebam notificações do Data Infrastructure Insights, adicione os seguintes endereços de e-mail a qualquer lista de "permitir":

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

Lista de destinatários globais para alertas

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

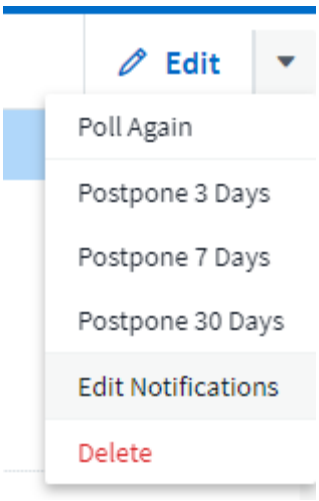
Para configurar destinatários de alerta global, escolha os destinatários desejados na seção **destinatários de notificação do Monitor Global**.

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

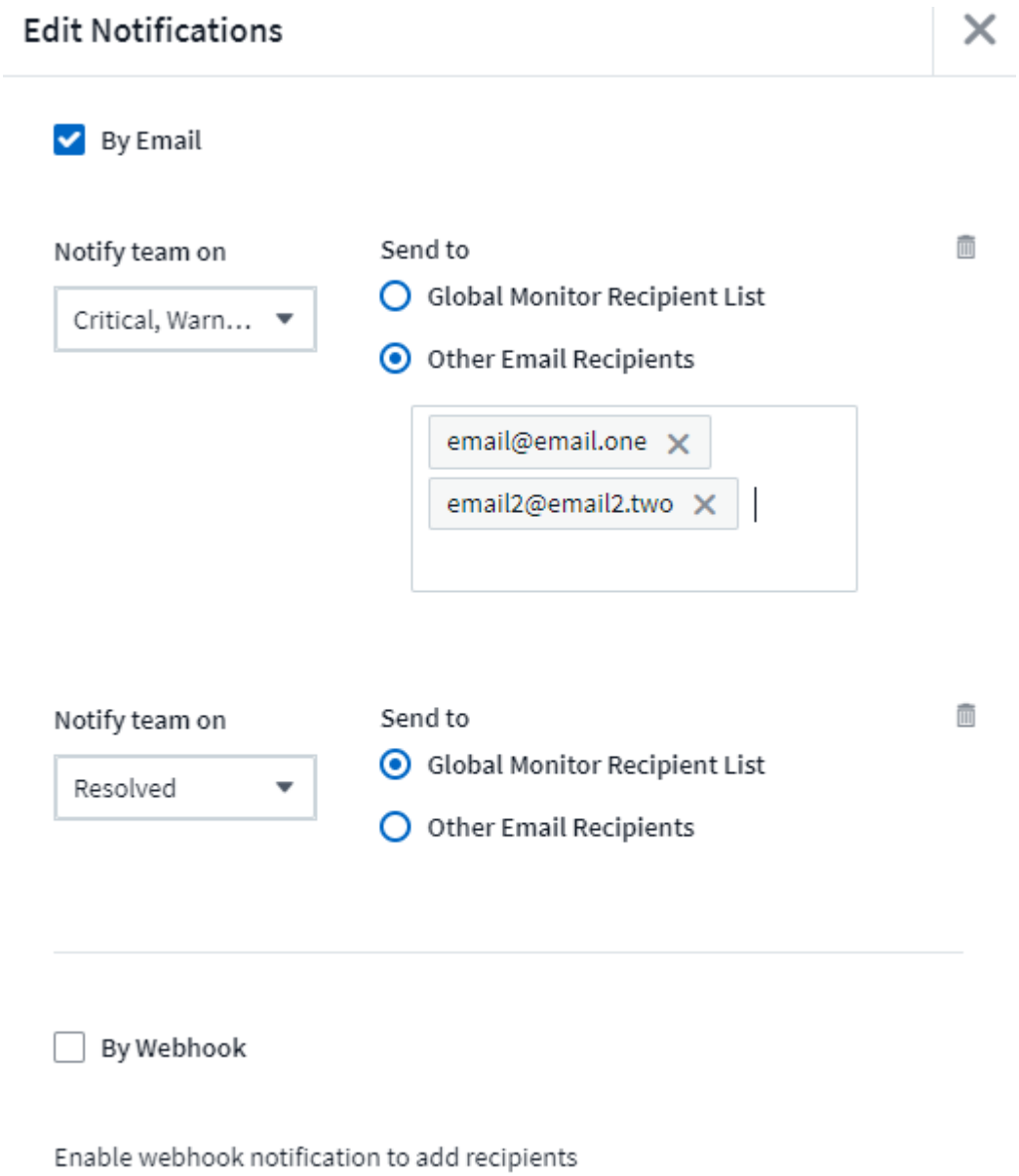
As notificações do ONTAP Data Collector têm precedência sobre quaisquer notificações específicas do Monitor que sejam relevantes para o cluster/coletor de dados. A lista de destinatários definida para o coletor de dados receberá os alertas do coletor de dados. Se não houver alertas ativos do coletor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

Editando notificações para ONTAP

Você pode modificar notificações para clusters do ONTAP selecionando *Editar notificações* na lista suspensa superior direita em uma página inicial do armazenamento.



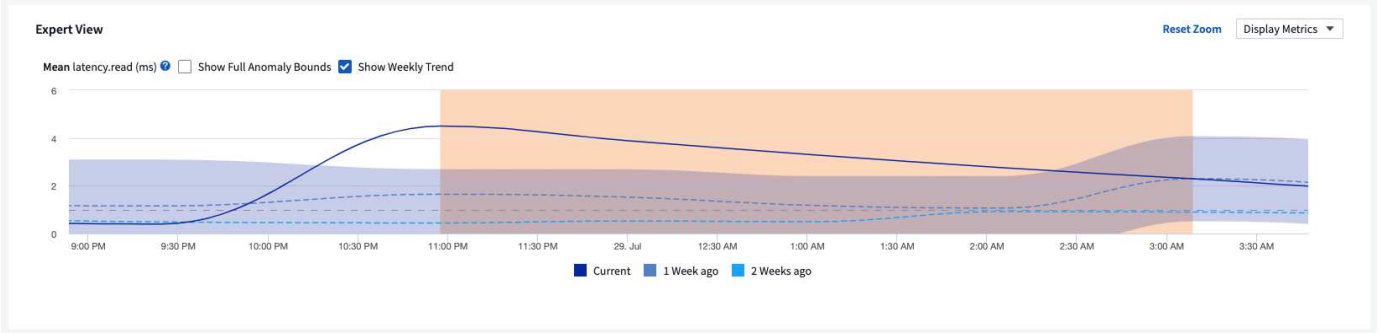
A partir daqui, você pode definir notificações para alertas críticos, de aviso, informativos e/ou resolvidos. Cada cenário pode notificar a lista de destinatários globais ou outros destinatários que você escolher.



Monitores de deteção de anomalias

Detecção de anomalias fornece informações sobre alterações inesperadas nos padrões de dados no locatário. Uma anomalia ocorre quando o padrão de comportamento de um objeto muda, por exemplo, se um objeto experimenta um certo nível de latência em um determinado momento às quartas-feiras, mas picos de latência acima desse nível naquele momento na quarta-feira seguinte, esse pico seria considerado uma anomalia. O Data Infrastructure Insights permite a criação de monitores para alertar quando ocorrem anomalias como essa.

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



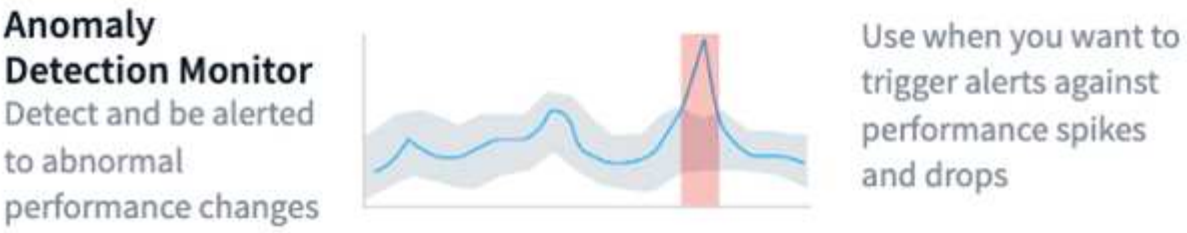
O que é detecção de anomalias?

Uma anomalia ocorre quando o valor médio de uma métrica é um número de desvios padrão longe da média ponderada dessa métrica para as semanas anteriores, com semanas recentes tendo mais peso do que as semanas anteriores. O Data Infrastructure Insights permite monitorar dados e alertas quando anomalias são detetadas. Você tem a opção de definir os níveis de "sensibilidade" de deteção. Por exemplo, uma sensibilidade maior seria quando o valor médio é menos desvios padrão da média, causando mais alertas a serem gerados. Por outro lado, menor sensibilidade: Mais desvios padrão da média: Menos alertas.

A monitorização da deteção de anomalias difere da monitorização 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 um intervalo normal).

- **O monitoramento de deteção de anomalias** usa algoritmos de aprendizado de máquina para identificar outliers que se desviam da norma, para quando a definição de "normal" não está clara.



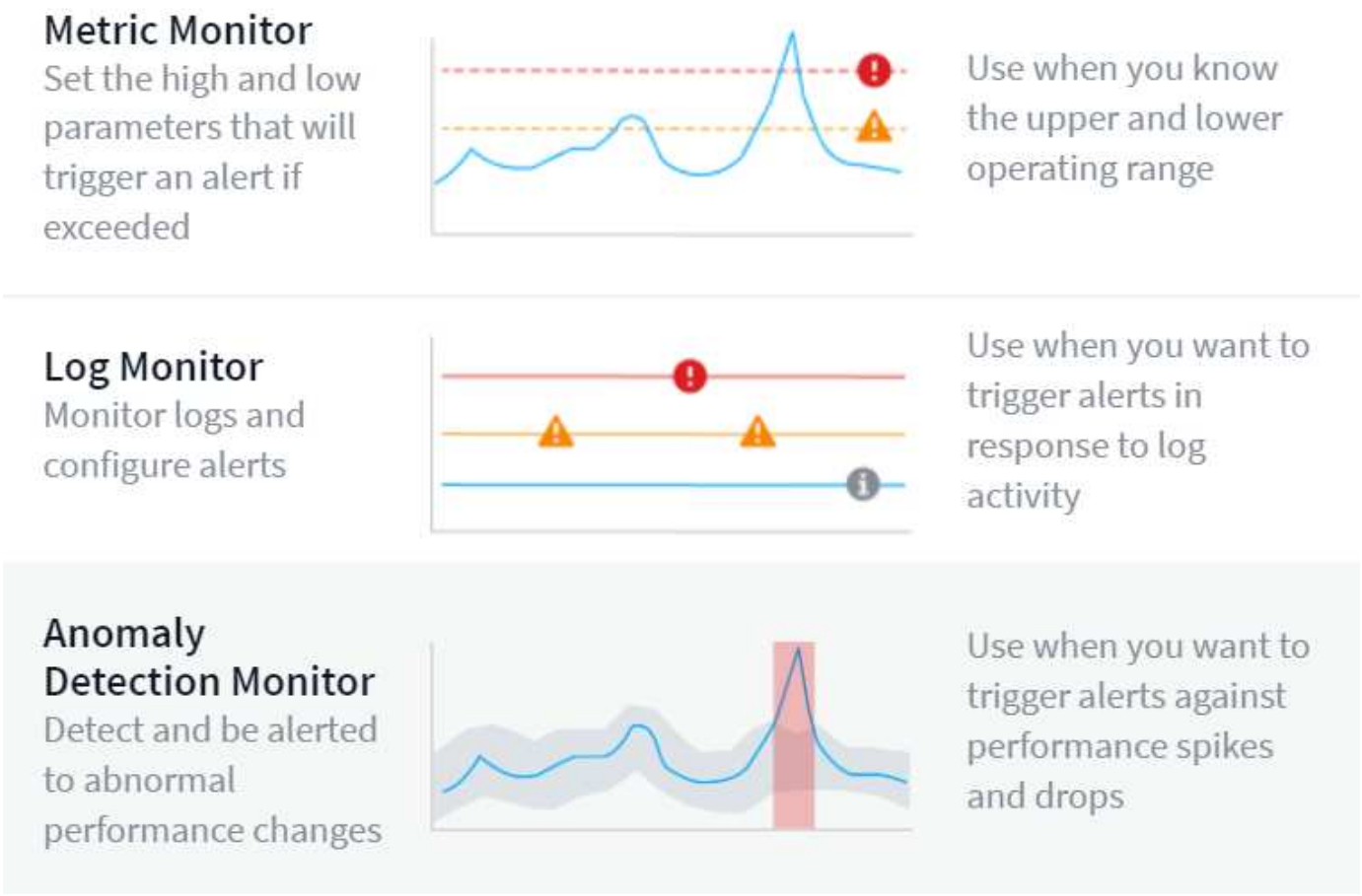
Quando eu precisaria de deteção de anomalias?

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

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

Criando um monitor de deteção de anomalias

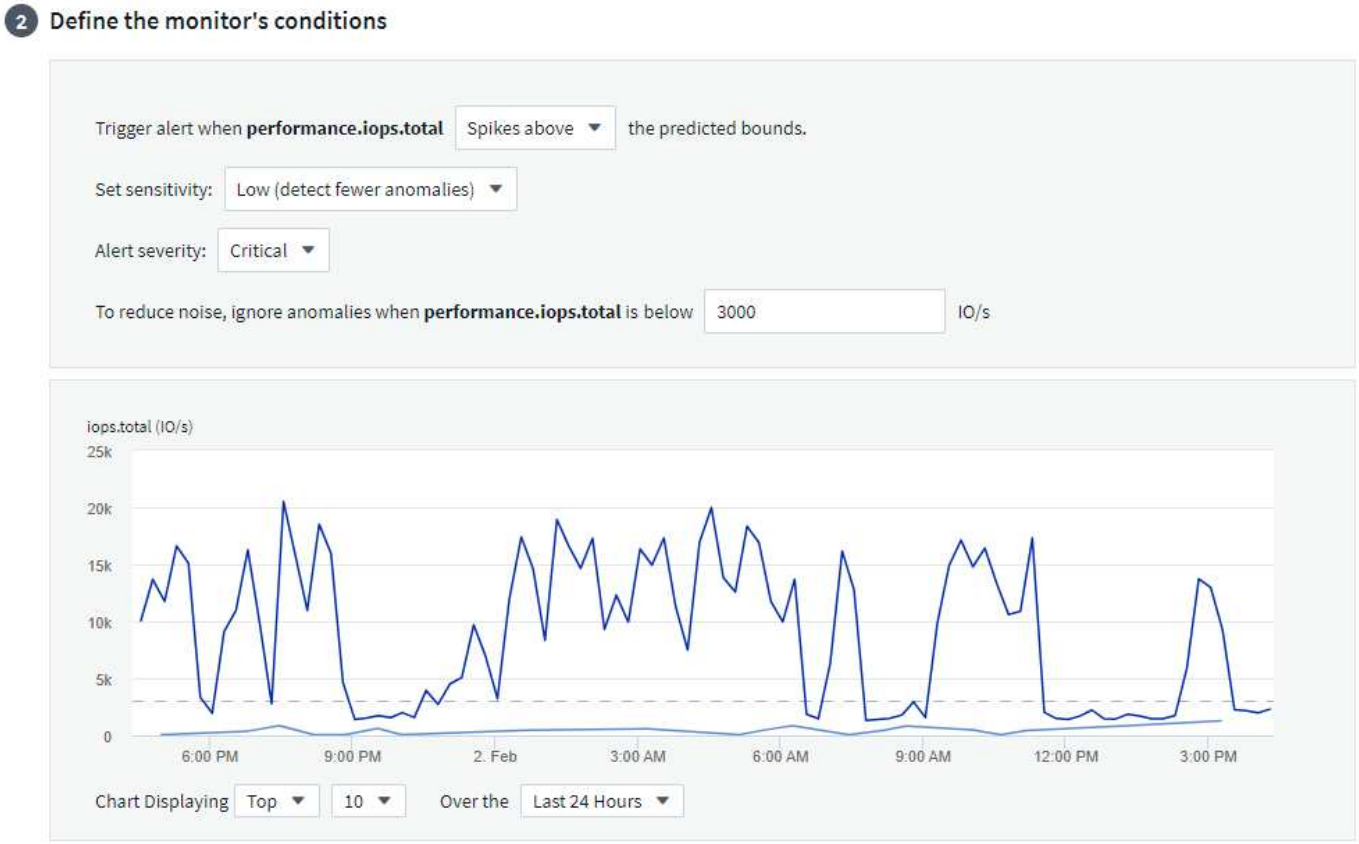
Para alertar sobre anomalias, crie um monitor navegando até **observabilidade > Alertas > Monitor**. Selecione *Anomaly Detection Monitor* como o tipo de monitor.



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

Em seguida, defina as condições para o monitor.

- Acione um alerta quando a métrica selecionada for _Spikes acima dos limites previstos, _drops abaixo desses limites, ou ambos.
- Defina a sensibilidade para *Medium*, *Low* (menos anomalias são detetadas) ou *High* (mais anomalias são detetadas).
- Determine se o nível de alerta é *Critical* ou *Warning*.
- Opcionalmente, defina um valor abaixo do qual anomalias são *ignoradas*. Isto pode ajudar a reduzir o ruído. Este valor é mostrado como uma linha tracejada no gráfico de amostra.



Finalmente, 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 desejado.

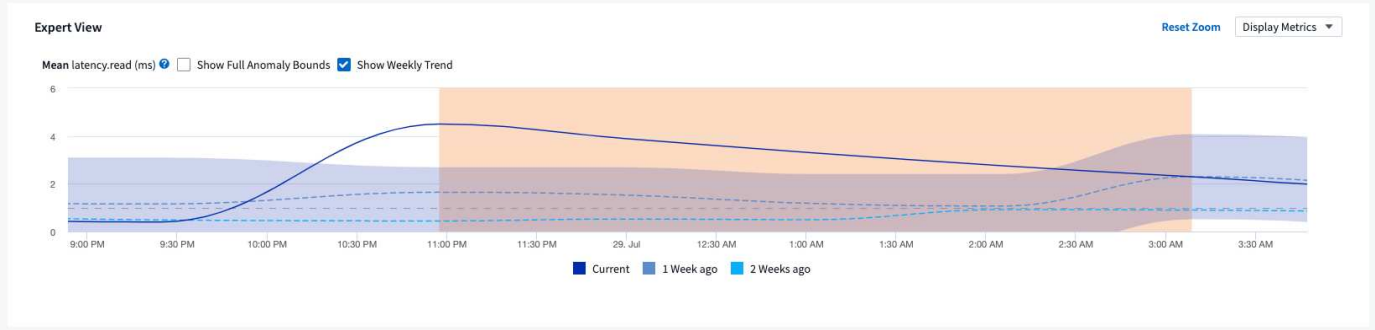
Salve o monitor com um nome significativo e pronto.

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

> Quando um monitor é criado, o DII analisa os dados existentes da semana anterior em busca de picos ou quedas significativas; essas são consideradas anomalias. Durante a primeira semana após a criação do monitor (a fase de "aprendizado"), há uma chance de aumento de "ruído" nos alertas. Para mitigar 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.

Visualização das anomalias

Em uma Landing page de alerta, os alertas acionados quando as anomalias são detetadas mostrarão uma banda destacada no gráfico, desde o momento em que a métrica subiu fora dos limites previstos até quando ela foi movida de volta para dentro desses limites.



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

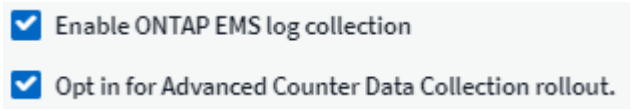
- Tendência semanal: Compare valores com a mesma hora, mesmo dia nas semanas anteriores, por até 5 semanas anteriores.
- Limites completos de anomalias: Por padrão, o gráfico se concentra no valor da métrica para que você possa analisar melhor o comportamento da métrica. Selecione para mostrar limites de anomalia completos (valor máximo, etc.)

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

Monitores do 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 locatário. Devido a isso, os monitores disponíveis no Data Infrastructure Insights podem mudar à medida que os coletores de dados são adicionados ou suas configurações alteradas.

Muitos monitores do sistema estão no estado *Pausado* por padrão. Você pode ativar um monitor de sistema selecionando a opção *Resume* para o monitor. Certifique-se de que *coleta avançada de dados de contador* e *enable ONTAP EMS log Collection* estão habilitados no coletor de dados. Essas opções podem ser encontradas no Coletor de dados do ONTAP em *Configuração Avançada*:



índice:[]

Descrições do monitor

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

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

Os seguintes monitores definidos pelo sistema estão disponíveis, nos grupos anotados.

- **A infraestrutura da ONTAP** inclui monitores para problemas relacionados à infraestrutura nos clusters do ONTAP.
- **Exemplos de carga de trabalho do ONTAP** inclui monitores para problemas relacionados à carga de trabalho.
- Os monitores em ambos os grupos são padrão para o estado *Pausado*.

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

Monitores métricos

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva

Utilização alta da porta do canal de fibra	CRÍTICO	As portas de 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, ela se tornará um gargalo e, em última análise, afetará o desempenho de cargas de trabalho sensíveis do Protocolo de Canal de fibra. Um alerta indica que ações planejadas devem ser tomadas 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 da rede para garantir a continuidade do serviço.	Se o limite crítico for violado, considere ações imediatas para minimizar a interrupção do serviço: 1. Mova workloads para outra porta FCP de baixa utilização. 2. Limite o tráfego de certos 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 violado, 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 workloads para outra porta FCP de baixa utilização. 3. Limite o tráfego de certos LUNs apenas ao trabalho essencial, seja por meio de políticas de QoS no ONTAP ou configuração no lado do host para aliviar a utilização das portas FCP.

Latência de LUN alta	CRÍTICO	LUNs são objetos que atendem ao tráfego de e/S geralmente orientados por aplicações sensíveis à performance, como bancos de dados. Altas latências de LUN significam que os próprios aplicativos podem sofrer e não podem realizar suas tarefas…. Um alerta de alerta indica que ações planejadas devem ser tomadas 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 1-2 milissegundos; SAS de até 8-10 milissegundos e HDD SATA de 17-20 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 de limite e valide se eles estão fazendo com que a carga de trabalho LUN seja estrangulada. Se o limite de aviso for violado, Planeje tomar as seguintes ações: 1. Se o agregado também estiver tendo 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 o workload total do nó. 3. Se o LUN ou seu volume tiver uma política de QoS associada a ele, avalie seus limites de limite e valide se eles estão fazendo com que a carga de trabalho de LUN seja limitada.

Alta utilização da porta de rede	CRÍTICO	As portas de rede são usadas para receber e transferir o tráfego de protocolos NFS, CIFS e iSCSI entre os sistemas host do cliente e os volumes ONTAP. Se a utilização da porta for alta, ela se tornará um gargalo e, em última análise, afetará o desempenho das cargas de trabalho NFS, CIFS e iSCSI…. Um alerta de aviso indica que ações planejadas devem ser tomadas 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 para 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 certos 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 menos utilizada. Se o limite de aviso 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 utilizada inferior.

Latência de namespace NVMe alta	CRÍTICO	Namespaces NVMe são objetos que atendem ao tráfego de e/S impulsionado por aplicações sensíveis à performance, como bancos de dados. Uma alta latência de namespaces NVMe significa que as próprias aplicações podem sofrer e não podem realizar suas tarefas…. Um alerta de aviso indica que ações planejadas devem ser tomadas 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 do NVMe ou seu volume tiver uma política de QoS atribuída a eles, avalie seus limites de limite caso eles estejam fazendo com que o workload do namespace do NVMe seja estrangulado. Se o limite de aviso for violado, considere tomar as seguintes ações: 1. Se o agregado também estiver tendo 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 o workload total do nó. 3. Se o namespace do NVMe ou seu volume tiver uma política de QoS atribuída a eles, avalie seus limites de limite caso eles estejam fazendo com que o workload do namespace do NVMe seja estrangulado.

QTree capacidade cheia	CRÍTICO	Uma qtree é um sistema de arquivos logicamente definido 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 de volume…. Um alerta de alerta indica que a 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 para garantir a continuidade do serviço.	Se o limite crítico for violado, considere ações imediatas para minimizar a interrupção do serviço: 1. Aumentar o espaço da qtree para acomodar o crescimento. 2. Exclua dados indesejados para liberar espaço. Se o limite de aviso for violado, Planeje tomar as seguintes ações imediatas: 1. Aumentar o espaço da qtree para acomodar o crescimento. 2. Elimine dados indesejados para libertar espaço.
Limite rígido da capacidade do QTree	CRÍTICO	Uma qtree é um sistema de arquivos logicamente definido 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 de dados do usuário em volume e não exceder sua capacidade total…. Uma cota de capacidade de armazenamento suave que fornece alerta ao usuário proativamente antes de atingir o limite de cota de capacidade total na qtree e não ser mais capaz de armazenar dados. Monitorar a quantidade de dados armazenados em uma qtree garante que o usuário receba um serviço de dados ininterrupto.	Se o limite crítico for violado, considere as seguintes ações imediatas para minimizar a interrupção do serviço: 1. Aumente a cota de espaço em árvore para acomodar o crescimento 2. Instrua o usuário a excluir dados indesejados na árvore para liberar espaço

Limite macio da capacidade de QTree	AVISO	Uma qtree é um sistema de arquivos logicamente definido 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 de dados do usuário em volume e não exceder sua capacidade total…. Uma qtree mantém uma cota de capacidade de armazenamento suave que fornece alerta ao usuário de forma proativa 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 um serviço de dados ininterrupto.	Se o limite de aviso for violado, considere as seguintes ações imediatas: 1. Aumente a cota de espaço em árvore para acomodar o crescimento. 2. Instrua o usuário a excluir dados indesejados na árvore para liberar espaço.
Limite rígido dos ficheiros QTree	CRÍTICO	Uma qtree é um sistema de arquivos logicamente definido que pode existir como um subdiretório especial do diretório raiz dentro de um volume. Cada qtree tem uma cota do número de arquivos que ele pode conter para manter um tamanho de sistema de arquivos gerenciável dentro do volume… Uma qtree mantém uma cota de número de arquivo rígido além da qual novos arquivos na árvore são negados. Monitorar o número de arquivos dentro de 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. Aumente a cota de contagem de arquivos para a qtree. 2. Exclua arquivos indesejados do sistema de arquivos de qtree.

Limite suave dos ficheiros QTree	AVISO	Uma qtree é um sistema de arquivos logicamente definido que pode existir como um subdiretório especial do diretório raiz dentro de um volume. Cada qtree tem uma cota do número de arquivos que ele pode conter para manter um tamanho de sistema de arquivos gerenciável dentro do volume…. Uma qtree mantém uma cota de número de arquivo suave para fornecer alerta ao usuário de forma proativa antes de atingir o limite de arquivos na qtree e não conseguir armazenar arquivos adicionais. Monitorar o número de arquivos dentro de uma qtree garante que o usuário receba serviço de dados ininterrupto.	Se o limite de aviso for violado, Planeje tomar as seguintes ações imediatas: 1. Aumente a cota de contagem de arquivos para a qtree. 2. Exclua arquivos indesejados do sistema de arquivos de qtree.

Espaço de reserva instantâneo cheio	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 instantâneo, é usada para armazenar snapshots que permitem que os dados sejam protegidos localmente. Quanto mais dados novos e atualizados forem armazenados no volume ONTAP, mais capacidade de snapshot será usada e menos capacidade de storage snapshot estará disponível para dados novos ou atualizados futuros. Se a capacidade de dados do snapshot dentro de um volume atingir o espaço total de reserva do snapshot, isso pode levar o cliente a não conseguir armazenar novos dados do snapshot e a reduzir o nível de proteção dos dados no volume. O monitoramento do volume usado da capacidade do 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 instantâneos para usar o espaço de dados no volume quando a reserva de snapshot estiver cheia. 2. Elimine alguns instantâneos indesejados mais antigos para libertar espaço. Se o limite de aviso for violado, Planeje tomar as seguintes ações imediatas: 1. Aumente o espaço de reserva do snapshot dentro do volume para acomodar o crescimento. 2. Configure instantâneos para usar o espaço de dados no volume quando a reserva de snapshot estiver cheia.

Limite de capacidade de armazenamento	CRÍTICO	Quando um pool de storage (agregado) está sendo enchido, as operações de e/S diminuem e, por fim, param de resultar em um incidente de interrupção do storage. Um alerta de aviso indica que a 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 para garantir a continuidade do serviço.	Se o limite crítico for violado, considere imediatamente as seguintes ações para minimizar a interrupção do serviço: 1. Eliminar instantâneos em volumes não críticos. 2. Exclua volumes ou LUNs que são workloads não essenciais e que podem ser restaurados de cópias de 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. Alterar as configurações de eficiência de storage ou categorizar dados inativos no storage de nuvem.

Limite de desempenho de storage	CRÍTICO	Quando um sistema de storage atinge seu limite de desempenho, as operações diminuem, a latência aumenta e os workloads e as aplicações 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 indica que deve ser tomada uma ação planejada para reduzir a carga do pool de armazenamento para garantir que haverá desempenho suficiente do pool de armazenamento deixado para os picos de carga de trabalho de serviço… Um alerta crítico indica que um brownout de desempenho é iminente e medidas de emergência devem ser tomadas para reduzir a carga do pool de armazenamento para garantir a fim de serviço.	Se o limite crítico for violado, considere as seguintes ações imediatas para minimizar a interrupção do serviço: 1. Suspender tarefas agendadas, como snapshots ou replicação do SnapMirror. 2. Cargas de trabalho não essenciais ociosas. Se o limite de aviso for violado, tome as seguintes ações imediatamente: 1. Mova um ou mais workloads para um local de storage diferente. 2. Adicionar mais nós de storage (AFF) ou compartimentos de disco (FAS) e redistribuir workloads 3. Alterar as características do workload (tamanho do bloco, armazenamento em cache do aplicativo).

Limite rígido da capacidade da quota do utilizador	CRÍTICO	O ONTAP reconhece os usuários de sistemas Unix ou Windows que têm os direitos de acessar 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 de 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 é certa antes 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 um 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 de usuário ou grupo para acomodar o crescimento. 2. Instrua o usuário ou grupo a excluir dados indesejados para liberar espaço.

Limite de capacidade da quota do utilizador	AVISO	O ONTAP reconhece os usuários de sistemas Unix ou Windows que têm os direitos de acessar 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 de política de usuário ou grupo limita a quantidade de espaço que o usuário pode utilizar para seus próprios dados…. Um limite suave dessa cota permite a 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 um serviço de dados ininterrupto.	Se o limite de aviso for violado, Planeje tomar as seguintes ações imediatas: 1. Aumente o espaço da cota de usuário ou grupo para acomodar o crescimento. 2. Elimine dados indesejados para libertar espaço.

Capacidade de volume cheia	CRÍTICO	A capacidade de armazenamento de um volume é necessária para armazenar dados de aplicativos e clientes. Quanto mais dados armazenados no volume ONTAP, menos disponibilidade de storage para dados futuros. Se a capacidade de armazenamento de dados dentro de um volume atingir a capacidade total de armazenamento pode levar o cliente a não conseguir armazenar dados devido à falta de capacidade de armazenamento. O monitoramento do volume usado de 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. Elimine dados indesejados para libertar espaço. 3. Se as cópias snapshot ocuparem mais espaço do que a reserva de snapshot, exclua snapshots antigos ou habilite o volume Snapshot Autodelete.. Se o limite de aviso for violado, Planeje executar as seguintes ações imediatas: 1. Aumentar o espaço do volume para acomodar o crescimento 2. Se as cópias snapshot ocuparem mais espaço do que a reserva de snapshot, exclua snapshots antigos ou ative o volume Snapshot Autodelete.

Limite de inodes de volume	CRÍTICO	Os volumes que armazenam arquivos usam nós de índice (inode) para armazenar metadados de arquivos. Quando um volume esgota sua alocação de inodes, não mais arquivos podem ser adicionados a ele…. Um alerta de alerta indica que a ação planejada deve ser tomada para aumentar o número de inodes disponíveis…. Um alerta crítico indica que a exaustão do limite do arquivo 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 inodes para o volume. Se o valor 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 ajuda a acomodar grandes sistemas de arquivos. Se o limite de aviso for violado, Planeje tomar as seguintes ações imediatas: 1. Aumente o valor inodes para o volume. Se o valor 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 ajuda a acomodar grandes sistemas de arquivos

Latência de volume alta	CRÍTICO	Os volumes são objetos que atendem ao tráfego de e/S geralmente orientados por aplicações sensíveis à performance, incluindo aplicações DevOps, diretórios base e bancos de dados. Com latências de alto volume, as próprias aplicações podem sofrer e não conseguir realizar suas tarefas. Monitorar latências de volume é essencial para manter a performance consistente com as aplicações. A seguir estão as latências esperadas com base no tipo de Mídia - SSD de até 1-2 milissegundos; SAS de até 8-10 milissegundos e HDD SATA de 17-20 milissegundos.	Se o limite crítico for violado, considere seguir ações imediatas para minimizar a interrupção do serviço: Se o volume tiver uma política de QoS atribuída a ele, avalie seus limites de limite caso eles estejam fazendo com que a carga de trabalho de volume seja limitada. Se o limite de aviso for violado, considere as seguintes ações imediatas: 1. Se o agregado também estiver tendo alta utilização, mova o volume para outro agregado. 2. Se o volume tiver uma política de QoS atribuída a ele, avalie seus limites de limite caso eles estejam fazendo com que o workload de volume seja estrangulado. 3. Se o nó também estiver com alta utilização, mova o volume para outro nó ou reduza o workload total do nó.
Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva

Alta latência do nó	AVISO / CRÍTICO	A latência do nó atingiu os níveis onde pode afetar o desempenho dos aplicativos no nó. A menor latência dos nós garante o desempenho consistente das aplicações. As latências esperadas com base no tipo de Mídia são: SSD de até 1-2 milissegundos; SAS de até 8-10 milissegundos e HDD SATA 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. Reduzir a demanda de workloads de prioridade mais baixa por meio dos limites de QoS 3. Inativar cargas de trabalho não essenciais considere ações imediatas quando o limite de aviso for violado: 1. Mova um ou mais workloads para um local de storage diferente 2. Reduzir a demanda de workloads de prioridade mais baixa por meio dos limites de QoS 3. Adicionar mais nós de storage (AFF) ou compartimentos de disco (FAS) e redistribuir workloads 4. Alterar as características da carga de trabalho (tamanho do bloco, armazenamento em cache do aplicativo, etc.)

Limite de desempenho do nó	AVISO / CRÍTICO	A utilização do desempenho do nó atingiu os níveis onde pode afetar o desempenho do iOS e dos aplicativos suportados pelo nó. A baixa utilização de performance de nós garante a performance consistente das aplicações.	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. Reduzir a demanda de workloads de prioridade mais baixa por meio dos limites de QoS 3. Inativar cargas de trabalho não essenciais considere as seguintes ações se o limite de aviso for violado: 1. Mova um ou mais workloads para um local de storage diferente 2. Reduzir a demanda de workloads de prioridade mais baixa por meio dos limites de QoS 3. Adicionar mais nós de storage (AFF) ou shelves de disco (FAS) e redistribuir workloads 4. Alterar as características da carga de trabalho (tamanho do bloco, armazenamento em cache do aplicativo, etc.)

Storage VM alta latência	AVISO / CRÍTICO	A latência da VM de storage (SVM) atingiu os níveis onde pode afetar a performance das aplicações na VM de storage. A menor latência da VM de storage garante a performance consistente das aplicações. As latências esperadas com base no tipo de Mídia são: SSD de até 1-2 milissegundos; SAS de até 8-10 milissegundos e HDD SATA de 17-20 milissegundos.	Se o limite crítico for violado, avalie imediatamente os limites de limite para volumes da VM de storage com uma política de QoS atribuída para verificar se eles estão fazendo com que os workloads de volume sejam estrangulados considere as seguintes ações imediatas quando o limite de aviso for violado: 1. Se o agregado também estiver tendo alta utilização, mova alguns volumes da VM de storage para outro agregado. 2. No caso de volumes da VM de storage com uma política de QoS atribuída, avalie os limites de limite se eles estiverem fazendo com que os workloads de volume sejam 3 estrangulados. Se o nó estiver com alta utilização, mova alguns volumes da VM de storage para outro nó ou reduza o workload total do nó
Limite rígido dos ficheiros de quota de utilizador	CRÍTICO	O número de arquivos criados dentro do 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. Aumente a cota de contagem de arquivos para o usuário específico 2. Exclua arquivos indesejados para reduzir a pressão na cota de arquivos para o usuário específico

Limite de software dos ficheiros de quota do utilizador	AVISO	O número de arquivos criados dentro do volume atingiu o limite da cota e está próximo ao 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 o usuário receba serviço de dados ininterrupto.	Considere ações imediatas se o limite de aviso for violado: 1. Aumente a cota de contagem de arquivos para a cota de usuário específica 2. Exclua arquivos indesejados para reduzir a pressão na cota de arquivos para o usuário específico
Taxa de perda de cache de volume	AVISO / CRÍTICO	A taxa de perda de cache de volume é a porcentagem de solicitações de leitura dos aplicativos clientes que são retornados do disco em vez de serem retornados do cache. Isto 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 alguns workloads 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 cache Flash 3. Reduzir a demanda de workloads de prioridade mais baixa no mesmo nó por limites de QoS considere ações imediatas quando o limite de aviso for violado: 1. Mova alguns workloads 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 cache Flash 3. Reduzir a demanda de workloads de prioridade mais baixa no mesmo nó por meio dos limites de QoS 4. Alterar as características da carga de trabalho (tamanho do bloco, armazenamento em cache do aplicativo, etc.)

Volume Qtree quota comprometer em excesso	AVISO / CRÍTICO	Volume Qtree quota comprometer especifica a porcentagem em que um volume é considerado sobrecarregado pelas cotas de qtree. O limite definido para a cota de qtree é atingido para o volume. O monitoramento do volume de cota de qtree em excesso garante que o usuário receba um serviço de dados ininterrupto.	Se o limite crítico for violado, ações imediatas devem ser tomadas para minimizar a interrupção do serviço: 1. Aumente o espaço do volume 2. Exclua dados indesejados quando o limite de aviso é violado e considere aumentar o espaço do volume.

Voltar ao topo

Monitores de registo

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

Nível de nuvem inacessível	CRÍTICO	Um nó de storage não pode se conetar 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 seu LIF está on-line e funcional usando o comando "network interface show".. Verifique a conetividade de rede com o servidor de armazenamento de objetos usando o comando "ping" sobre o nó de destino LIF entre clusters NetApp. Se você usar o Cloud Volumes ONTAP, execute as seguintes ações corretivas:… Certifique-se de que a configuração do seu armazenamento de objetos não foi alterada. Verifique se as informações de login e conetividade ainda são válidas. Contate o suporte técnico da NetApp se o problema persistir.
Disco fora de serviço	INFORMAÇÕES	Esse evento ocorre quando um disco é removido do serviço porque foi marcado como com falha, está sendo higienizado ou entrou no Centro de Manutenção.	Nenhum.
FlexGroup Constituinte completo	CRÍTICO	Um componente 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. No entanto, nenhum dos arquivos armazenados no componente pode ser modificado. Como resultado, você pode ver erros aleatórios fora do espaço quando você tenta executar operações de gravação no volume FlexGroup.	Recomenda-se que você adicione capacidade ao volume FlexGroup usando o comando "volume modificar -arquivos -X". Alternativamente, exclua arquivos do volume FlexGroup. No entanto, é difícil determinar quais arquivos aterraram no constituinte.

FlexGroup Constituinte quase cheio	AVISO	Um componente dentro de um volume FlexGroup está quase fora do espaço, o que pode causar uma possível interrupção do serviço. Os arquivos podem ser criados e expandidos. No entanto, se o constituinte ficar sem espaço, você pode não ser capaz de anexar ou modificar os arquivos no constituinte.	Recomenda-se que você adicione capacidade ao volume FlexGroup usando o comando "volume modificar -arquivos -X". Alternativamente, exclua arquivos do volume FlexGroup. No entanto, é difícil determinar quais arquivos aterraram no constituinte.
FlexGroup Constituente quase fora de inodes	AVISO	Um constituinte dentro de um volume FlexGroup está quase fora de inodes, o que pode causar uma possível interrupção do serviço. O constituinte recebe solicitações de criação menores do que a média. Isso pode afetar o desempenho geral do volume FlexGroup, porque as solicitações são roteadas para componentes com mais inodes.	Recomenda-se que você adicione capacidade ao volume FlexGroup usando o comando "volume modificar -arquivos -X". Alternativamente, exclua arquivos do volume FlexGroup. No entanto, é difícil determinar quais arquivos aterraram no constituinte.
FlexGroup Constituinte fora de inodes	CRÍTICO	Um componente 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 global desequilibrada de conteúdo pelo volume FlexGroup.	Recomenda-se que você adicione capacidade ao volume FlexGroup usando o comando "volume modificar -arquivos -X". Alternativamente, exclua arquivos do volume FlexGroup. No entanto, é difícil determinar quais arquivos aterraram no constituinte.
LUN Offline	INFORMAÇÕES	Este evento ocorre quando um LUN é colocado offline manualmente.	Coloque o LUN novamente online.

Falha na ventoinha da unidade principal	AVISO	Uma ou mais ventoinhas da unidade principal falharam. No entanto, se a condição persistir por muito tempo, a temperatura excessiva pode desencadear um desligamento automático.	Recoloque os ventiladores com falha. Se o erro persistir, substitua-os.
Ventoinha da unidade principal no estado de aviso	INFORMAÇÕES	Este evento ocorre quando uma ou mais ventoinhas da unidade principal estão num estado de aviso.	Substitua as ventoinhas indicadas para evitar o sobreaquecimento.
Bateria do NVRAM fraca	AVISO	A capacidade da bateria do NVRAM é extremamente baixa. Pode haver uma perda de dados potencial se a bateria ficar sem energia…. seu sistema gera e transmite uma mensagem AutoSupport ou "chamar para casa" para o suporte técnico da NetApp e os destinos configurados se estiver configurado para fazê-lo. A entrega bem-sucedida de uma mensagem AutoSupport melhora significativamente a determinação e resolução de problemas.	Execute as seguintes ações corretivas:… Veja o estado atual da bateria, a capacidade e o estado de carregamento usando o comando "show dos sensores de ambiente do nó do sistema"…. se a bateria foi substituída recentemente ou o sistema não estava operacional por um longo período de tempo, monitore a bateria para verificar se está carregando corretamente NetApp.

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 acesso remoto e recursos de gerenciamento remoto. Você deve configurar o SP para usar toda a sua funcionalidade.	Execute as seguintes ações corretivas:… Configurar 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 da rede do SP usando o comando "system Service-processor network show". .. Verifique se o SP pode enviar um e-mail do 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 emitir este comando.
Processador de serviço offline	CRÍTICO	O ONTAP não está mais recebendo batimentos cardíacos do processador de Serviço (SP), mesmo que todas as ações de recuperação do SP tenham sido tomadas. O ONTAP não pode monitorar a integridade 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 o sistema executando as seguintes ações:… puxe o controlador para fora do chassi…. empurre o controlador novamente para dentro…. ligue o controlador novamente…. se o problema persistir, substitua o módulo do controlador.

Falha nas ventoinhas da prateleira	CRÍTICO	A ventoinha de arrefecimento indicada ou o módulo do ventilador da prateleira falhou. Os discos na gaveta podem não receber fluxo de ar de resfriamento suficiente, o que pode resultar em falha de disco.	Execute as seguintes ações corretivas:… Verifique se o módulo da ventoinha está totalmente encaixado e fixo. NOTA: O ventilador está 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	Uma ou mais ventoinhas da unidade principal falharam, interrompendo o funcionamento do sistema. Isso pode levar a uma possível perda de dados.	Substitua as ventoinhas com falha.
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 são 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 ocupado demais para aceitar novas solicitações de verificação.	Se essa mensagem ocorrer com frequência, verifique se há servidores antivírus suficientes para lidar com a carga de verificação de vírus gerada pelo SVM.

Credenciais da AWS para a função do IAM expiradas	CRÍTICO	O Cloud volume ONTAP tornou-se 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 IAM e são usadas para assinar solicitações de API para o Amazon Simple Storage Service (Amazon S3).	Execute o seguinte:… Faça login no Console de Gerenciamento do AWS EC2. Navegue até a página instâncias.. Localize 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 Privileges adequado para a instância.
Credenciais da AWS para função do IAM não encontrada	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 tornou-se inacessível.	Execute o seguinte:… Faça login no Console de Gerenciamento do AWS EC2. Navegue até a página instâncias.. Localize 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 Privileges adequado para a instância.
Credenciais da AWS para função do IAM não válidas	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 IAM e são usadas para assinar solicitações de API para o Amazon Simple Storage Service (Amazon S3). O Cloud volume ONTAP tornou-se inacessível.	Execute o seguinte:… Faça login no Console de Gerenciamento do AWS EC2. Navegue até a página instâncias.. Localize 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 Privileges adequado para a instância.

Função do AWS IAM não encontrada	CRÍTICO	O thread de funções de gerenciamento de identidade e acesso (IAM) não consegue localizar uma função IAM do Amazon Web Services (AWS) no servidor de metadados da AWS. A função IAM é necessária para adquirir credenciais baseadas em funções usadas para assinar solicitações de API ao Amazon Simple Storage Service (Amazon S3). O Cloud volume ONTAP tornou-se inacessível.	Execute o seguinte:… entre no Console de Gerenciamento do AWS EC2. Navegue até a página instâncias.. Localize 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 não válida	CRÍTICO	A função do Amazon Web Services (AWS) Identity and Access Management (IAM) no servidor de metadados da AWS não é válida. O Cloud volume ONTAP tornou-se inacessível.	Execute o seguinte:… Faça login no Console de Gerenciamento do AWS EC2. Navegue até a página instâncias.. Localize 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 Privileges adequado para a instância.
Falha na conexão do servidor de metadados da AWS	CRÍTICO	O thread de funções de gerenciamento de identidade e acesso (IAM) não pode 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 usadas para assinar solicitações de API ao Amazon Simple Storage Service (Amazon S3). O Cloud volume ONTAP tornou-se inacessível.	Execute o seguinte:… entre no Console de Gerenciamento do AWS EC2. Navegue até a página instâncias.. Localize a instância para a implantação do Cloud Volumes ONTAP e verifique sua integridade.

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

Falha de reembolso de agregado	CRÍTICO	Esse evento ocorre durante a migração de um agregado como parte de um failover de armazenamento (SFO), quando o nó de destino não pode alcançar os armazenamentos de objetos.	Execute as seguintes ações corretivas:… Verifique se o LIF entre clusters está on-line e funcional usando o comando "network interface show". .. Verifique a conetividade de rede com o servidor de armazenamento de objetos usando o comando"'ping" sobre o LIF do nó de destino. … Verifique se a configuração do seu armazenamento de objetos não foi alterada e que as informações de login e conetividade ainda são precisas usando o comando "agreed object-store config show".. Alternativamente, você pode substituir o erro especificando false para o parâmetro "require-Partner-waiting" do comando giveback NetApp.

Interconexão HA desativada	AVISO	A interconexão de alta disponibilidade (HA) está inativa. Risco de interrupção de serviço quando o failover não está disponível.	As ações corretivas dependem do número e do tipo de links de interconexão de 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 conetados externamente, certifique-se de que os cabos de interconexão estão conetados corretamente e que os SFPs (Small Form-factor Pluggables), se aplicável, estão encaixados corretamente em ambos os controladores.. …Se os links estiverem desativados, ative os links usando o comando "ic link on". …Se um par não estiver conetado, 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 utilizador 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 que são executados no cliente e termine qualquer um que não esteja funcionando corretamente…. reinicie o cliente…. Verifique se o problema é causado por um aplicativo novo ou existente:… se o aplicativo é novo, defina um limite mais alto para o cliente usando o comando "cifs Option Modify -Max -abre-same-file-per-tree". Em alguns casos, os clientes operam como 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.

Máximo de vezes aberto por ficheiro excedido	AVISO	Excedeu o número máximo de vezes que pode abrir o ficheiro através de uma ligação TCP. Qualquer solicitação para abrir esse arquivo será negada até que você feche algumas instâncias abertas do arquivo. Isso normalmente indica comportamento anormal da aplicação.	Execute as seguintes ações corretivas:… Inspecione os aplicativos que são executados no cliente usando essa 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 é novo, defina um limite mais alto para o cliente usando o comando "cifs option modify -Max -abre-same-file-per-tree". Em alguns casos, os clientes operam como 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 nomes NetBIOS	CRÍTICO	O serviço de nomes NetBIOS recebeu uma resposta negativa a uma solicitação de Registro de nomes de uma máquina remota. Isso geralmente é causado por um conflito no nome NetBIOS ou um alias. Como resultado, os clientes podem não conseguir acessar dados ou se conetar ao nó certo de fornecimento de dados no cluster.	Execute qualquer uma das seguintes ações corretivas:… se houver um conflito no nome NetBIOS ou um alias, execute uma das seguintes ações:… Excluir o alias NetBIOS duplicado usando o comando "vserver delete -aliases alias -vserver 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.
NFSv4 Store Pool esgotado	CRÍTICO	Uma piscina de loja NFSv4 foi esgotada.	Se o servidor NFS não responder por mais de 10 minutos após este evento, entre em Contato com o suporte técnico da NetApp.
Nenhum motor de digitalização registado	CRÍTICO	O conetor antivírus notificou o ONTAP de que ele não possui um mecanismo de verificação registrado. Isso pode causar indisponibilidade de dados se a opção "Scan-mandatory" (digitalização obrigatória) estiver ativada.	Execute as seguintes ações corretivas:… Certifique-se de que o software do mecanismo de verificação instalado no servidor antivírus é compatível com o ONTAP…. Certifique-se de que o software do mecanismo de verificação está em execução e configurado para se conetar ao conetor antivírus por meio de loopback local.

Sem ligação Vscan	CRÍTICO	O ONTAP não tem uma ligação Vscan a pedidos de verificação de vírus de serviço. Isso pode causar indisponibilidade de dados se a opção "Scan-mandatory" (digitalização obrigatória) estiver ativada.	Certifique-se de que o conjunto do scanner está configurado corretamente e que os servidores antivírus estão ativos e conetados ao ONTAP.
Espaço de volume de raiz do nó baixo	CRÍTICO	O sistema detetou que o volume raiz está perigosamente baixo no espaço. O nó não está totalmente operacional. As LIFs de dados podem ter falhado no cluster, por causa do qual o acesso NFS e CIFS é limitado no nó. A capacidade administrativa está limitada aos procedimentos de recuperação locais para que o nó limpe o espaço no volume raiz.	Execute as seguintes ações corretivas:… limpe o espaço no volume raiz excluindo cópias Snapshot antigas, excluindo arquivos que você não precisa mais 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 Admin inexistente	CRÍTICO	Problema Vscan: Um cliente tentou se conetar a um compartilhamento inexistente do ONTAP_ADMIN.	Certifique-se de que o Vscan esteja habilitado para o ID SVM mencionado. Ativar o Vscan em um SVM faz com que o compartilhamento ONTAP_ADMIN seja criado automaticamente para o SVM.
Namespace NVMe fora do espaço	CRÍTICO	Um namespace NVMe foi colocado off-line devido a uma falha de gravação causada pela falta de espaço.	Adicione espaço ao volume e, em seguida, coloque o namespace NVMe on-line usando o comando "vserver nvme namespace modify".

Período de carência NVMe-of Ativo	AVISO	Esse evento ocorre diariamente quando o protocolo NVMe sobre Fabrics (NVMe-of) está em uso e o período de carência da licença está ativo. O recurso NVMe-of requer uma licença após o período de carência da licença expirar. O recurso NVMe-of é desativado quando o período de carência da licença terminar.	Entre em Contato com seu representante de vendas para obter uma licença NVMe-of e adicioná-la ao cluster ou remover todas as instâncias de configuração NVMe-of do cluster.
O período de carência do NVMe-of expirou	AVISO	O período de carência da licença NVMe over Fabrics (NVMe-of) acabou e o recurso NVMe-of é desativado.	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 over Fabrics (NVMe-of) foi detetada durante a atualização para o software ONTAP 9.5. O recurso NVMe-of requer uma licença após o período de carência da licença expirar.	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 um endereço IP. Como resultado, os dados podem estar inacessíveis.	Verifique a configuração DNS para verificar se o nome do host está configurado corretamente com um endereço IP.

Object Store Intercluster LIF para baixo	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 o tráfego do cliente de armazenamento de objetos até que o LIF entre clusters esteja operacional. Como resultado, os dados podem estar inacessíveis.	Execute as seguintes ações corretivas:… Verifique o status de clusters de LIF usando o comando "network interface show -role"…. Verifique se o LIF entre clusters está configurado corretamente e operacional…. se um LIF entre clusters não estiver configurado, adicione-o usando o comando "network interface create -role".
Incompatibilidade de assinatura do armazenamento de objetos	CRÍTICO	A assinatura de solicitação enviada ao servidor de armazenamento de objetos não corresponde à assinatura calculada pelo cliente. Como resultado, os dados podem estar inacessíveis.	Verifique se a chave de acesso secreto está configurada corretamente. Se estiver configurado corretamente, contacte o suporte técnico da NetApp para obter assistência.
Tempo limite READDIR	CRÍTICO	Uma operação de ARQUIVO READDIR excedeu o tempo limite que é permitido executar no WAFL. Isso pode ser por causa de diretórios muito grandes ou esparsos. Recomenda-se a ação corretiva.	Execute as seguintes ações corretivas:… Encontre informações específicas para diretórios recentes que tiveram operações de arquivo READDIR expiram usando o seguinte comando 'dag' privilegiar nodeshell CLI: WAFL readdir notice show…. Verifique se os diretórios são indicados como esparsos ou não:… se um diretório é indicado como esparso, é recomendado que você copie o conteúdo do diretório para um novo para remover a frouxidão do diretório. … Se um diretório não for indicado como esparso e o diretório for grande, é recomendável que você reduza o tamanho do arquivo de diretório reduzindo o número de entradas de arquivo no diretório.

Falha na realocação do agregado	CRÍTICO	Esse evento ocorre durante a realocação de um agregado, quando o nó de destino não pode alcançar os armazenamentos de objetos.	Execute as seguintes ações corretivas:… Verifique se o LIF entre clusters está on-line e funcional usando o comando "network interface show". .. Verifique a conetividade de rede com o servidor de armazenamento de objetos usando o comando"'ping" sobre o LIF do nó de destino. … Verifique se a configuração do seu armazenamento de objetos não foi alterada e se as informações de login e conetividade ainda são precisas usando o comando "Aggregate object-store config show". .. Alternativamente, você pode substituir o erro usando o parâmetro "override-destination-checks" do comando relocation. .. Entre em Contato com o suporte técnico da NetApp para obter mais informações ou assistência.
Cópia sombra falhou	CRÍTICO	Um serviço de cópia de sombra de volume (VSS), uma operação de serviço de backup e restauração do Microsoft Server, falhou.	Verifique o seguinte usando as informações fornecidas na mensagem de evento:… a configuração de cópia de sombra está ativada?… as licenças apropriadas estão instaladas? Em que compartilhamentos é realizada a operação de cópia sombra?… o nome da ação está correto?… o caminho da ação existe?… quais são os estados do conjunto de cópias sombra e suas cópias de sombra?

Falha nas fontes de alimentação do interrutor de armazenamento	AVISO	Existe uma fonte de alimentação em falta no interrutor do painel de instrumentos. A redundância é reduzida, o risco de interrupção com quaisquer outras falhas de energia.	Execute as seguintes ações corretivas:… Certifique-se de que a rede elétrica da fonte de alimentação, que fornece energia ao switch do cluster, esteja ligada…. Certifique-se de que o cabo de alimentação está conetado à fonte de alimentação. Contate o suporte técnico da NetApp se o problema persistir.
Demasiadas Autenticação CIFS	AVISO	Muitas negociações de autenticação ocorreram simultaneamente. Existem 256 solicitações de nova sessão incompletas deste cliente.	Investigue por que o cliente criou 256 ou mais solicitações de conexão novas. Você pode ter que entrar em Contato com o fornecedor do cliente ou do aplicativo para determinar por que o erro ocorreu.
Acesso não autorizado ao Admin Share	AVISO	Um cliente tentou se conetar ao compartilhamento privilegiado do ONTAP_ADMIN, mesmo que seu usuário conetado não seja um usuário permitido.	Execute as seguintes ações corretivas:… Certifique-se de que o nome de usuário e o endereço IP mencionados estão configurados em um dos pools de scanner Vscan ativos. .. Verifique a configuração do pool de scanner que está atualmente ativa usando o comando "vserver vscan pool show-active".
Vírus detetado	AVISO	Um servidor Vscan comunicou um erro ao sistema de armazenamento. Isso normalmente indica que um vírus foi encontrado. No entanto, outros erros no servidor Vscan podem causar esse evento…. o acesso do cliente ao arquivo é negado. O servidor Vscan pode, dependendo de suas configurações e configurações, limpar o arquivo, colocá-lo em quarentena ou excluí-lo.	Verifique o log do servidor Vscan relatado no evento "syslog" para ver se ele foi capaz de limpar, colocar em quarentena ou excluir o arquivo infetado com sucesso. Se não conseguir fazê-lo, um administrador de sistema poderá ter de eliminar manualmente o ficheiro.

Volume off-line	INFORMAÇÕES	Esta mensagem indica que um volume está offline.	Traga o volume de volta online.
Volume restrito	INFORMAÇÕES	Este evento indica que um volume flexível é restringido.	Traga o volume de volta 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 a dados em uma VM de armazenamento.
Pânico de nó	AVISO	Este evento é emitido quando ocorre um 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 storage VM desativado	AVISO	O monitoramento anti-ransomware da VM de storage é desativado. Habilite o anti-ransomware para proteger a VM de storage.	Nenhum
Monitoramento anti-ransomware da VM de storage ativado (modo de aprendizado)	INFORMAÇÕES	O monitoramento anti-ransomware da VM de storage é ativado no modo de aprendizado.	Nenhum
Monitoramento de volume Anti-ransomware habilitado	INFORMAÇÕES	O monitoramento anti-ransomware do volume está ativado.	Nenhum
Monitoramento de volume Anti-ransomware desativado	AVISO	O monitoramento anti-ransomware do volume está desativado. Habilite o anti-ransomware para proteger o volume.	Nenhum
Monitoramento anti-ransomware de volume ativado (modo de aprendizado)	INFORMAÇÕES	O monitoramento anti-ransomware do volume é ativado no modo de aprendizado.	Nenhum
Monitoramento de volume Anti-ransomware em pausa (modo de aprendizado)	AVISO	O monitoramento anti-ransomware para o volume é pausado no modo de aprendizado.	Nenhum

Monitoramento de volume Anti-ransomware pausado	AVISO	O monitoramento anti-ransomware do volume é pausado.	Nenhum
Desativação da monitorização de volume Anti-ransomware	AVISO	O monitoramento anti-ransomware do volume está desabilitado.	Nenhum
Atividade de ransomware detetada	CRÍTICO	Para proteger os dados contra o ransomware detetado, foi feita uma cópia Snapshot que pode ser usada para restaurar os dados originais. O seu sistema gera e transmite uma mensagem AutoSupport ou "Call Home" para o suporte técnico da NetApp e para quaisquer destinos configurados. A mensagem AutoSupport melhora a determinação e resolução de problemas.	Consulte o "NOME DO DOCUMENTO FINAL" para tomar medidas corretivas para a atividade de ransomware.

Voltar ao topo

FSX para monitores NetApp ONTAP

Nome do monitor	Limites	Descrição do monitor	Ação corretiva

A capacidade de volume do FSX é cheia	Aviso a > 85 %… crítico a > 95 %	A capacidade de armazenamento de um volume é necessária para armazenar dados de aplicativos e clientes. Quanto mais dados armazenados no volume ONTAP, menos disponibilidade de storage para dados futuros. Se a capacidade de armazenamento de dados dentro de um volume atingir a capacidade total de armazenamento pode levar o cliente a não conseguir armazenar dados devido à falta de capacidade de armazenamento. O monitoramento do volume usado de 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 a > 1000 µs…crítico a > 2000 µs	Os volumes são objetos que atendem ao tráfego de e/S geralmente orientados por aplicações sensíveis à performance, incluindo aplicações DevOps, diretórios base e bancos de dados. Com latências de alto volume, as próprias aplicações podem sofrer e não conseguir realizar suas tarefas. Monitorar latências de volume é essencial para manter a performance consistente com as aplicações.	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 de limite caso eles estejam fazendo com que a carga de trabalho de volume seja estrangulada… 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 de limite caso eles estejam fazendo com que a carga de trabalho de volume seja limitada… 2. Se o nó também estiver com alta utilização, mova o volume para outro nó ou reduza o workload total do nó.

Limite de inodes de volume FSX	Aviso a > 85 %… crítico a > 95 %	Os volumes que armazenam arquivos usam nós de índice (inode) para armazenar metadados de arquivos. Quando um volume esgota sua alocação de inode não mais arquivos podem ser adicionados a ele. Um alerta de alerta indica que deve ser tomada uma ação planejada 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 inodes para o volume. Se o valor 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 inodes para o volume. Se o valor inodes já estiver no máximo, considere dividir o volume em dois ou mais volumes porque o sistema de arquivos cresceu além do tamanho máximo
Comprometer a cota do FSX volume Qtree	Aviso a > 95 %… crítico a > 100 %	Volume Qtree quota comprometer especifica a porcentagem em que um volume é considerado sobrecarregado pelas cotas de qtree. O limite definido para a cota de qtree é atingido para o volume. O monitoramento do volume de cota de qtree em excesso garante que o usuário receba um serviço de dados ininterrupto.	Se o limite crítico for violado, ações imediatas devem ser tomadas para minimizar a interrupção do serviço: 1. Quando o limite de aviso é violado, considere aumentar o espaço do volume.

O FSX Snapshot Reserve Space está cheio	Aviso a > 90 %… crítico a > 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 instantâneo, é usada para armazenar snapshots que permitem que os dados sejam protegidos localmente. Quanto mais dados novos e atualizados forem armazenados no volume ONTAP, mais capacidade de snapshot será usada e menos capacidade de storage snapshot estarão disponíveis para dados novos ou atualizados futuros. Se a capacidade de dados do snapshot dentro de um volume atingir o espaço total de reserva do snapshot, isso pode levar o cliente a não conseguir armazenar novos dados do snapshot e a reduzir o nível de proteção para os dados no volume. O monitoramento do volume usado da capacidade do 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 snapshot estiver cheia… 2. Considere excluir alguns snapshots 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 snapshot dentro do volume para acomodar o crescimento… 2. Considere configurar snapshots para usar espaço de dados no volume quando a reserva de snapshot estiver cheia

Taxa de perda de cache de volume FSX	Aviso a > 95 %… crítico a > 100 %	A taxa de perda de cache de volume é a porcentagem de solicitações de leitura dos aplicativos clientes que são retornados do disco em vez de serem retornados do cache. Isto 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 alguns workloads para fora do nó do volume para reduzir a carga de e/S 2. Reduza a demanda de workloads de prioridade mais baixa no mesmo nó por meio de limites de QoS… considere ações imediatas quando o limite de aviso for violado: 1. Mova alguns workloads para fora do nó do volume para reduzir a carga de e/S 2. Reduzir a demanda de workloads de prioridade mais baixa no mesmo nó por meio dos limites de QoS 3. Alterar as características da carga de trabalho (tamanho do bloco, armazenamento em cache do aplicativo, etc.)

Voltar ao topo

K8s monitores

Nome do monitor	Descrição	Ações corretivas	Gravidade/limiar

Latência de volume persistente alta	Com latências de volume persistentes altas significa que as próprias aplicações podem sofrer e não podem realizar suas tarefas. O monitoramento de latências de volume persistentes é essencial para manter a performance consistente com as aplicações. A seguir estão as latências esperadas com base no tipo de Mídia - SSD de até 1-2 milissegundos; SAS de até 8-10 milissegundos e HDD SATA de 17-20 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 de limite caso eles estejam fazendo com que a carga de trabalho de volume seja limitada. **Ações a serem feitas em breve** se o limite de aviso for violado, Planeje as seguintes ações imediatas: 1. Se o pool de storage também estiver com alta utilização, mova o volume para outro pool de storage. 2. Se o volume tiver uma política de QoS atribuída a ele, avalie seus limites de limite caso eles estejam fazendo com que o workload de volume seja estrangulado. 3. Se o controlador também estiver tendo alta utilização, mova o volume para outro controlador ou reduza a carga de trabalho total do controlador.	Aviso a > 6.000 µs crítico a > 12.000 µs
Saturação de memória de cluster alta	A saturação de memória alocável do cluster é alta. A saturação da CPU do cluster é calculada como a soma do uso da memória dividida pela soma da memória alocável em todos os K8s nós.	Adicionar nós. Corrija todos os nós não programados. Pods do tamanho direito para liberar memória em nós.	Aviso a > 80 % crítico a > 90 %
Falha na ligação DO POD	Este alerta ocorre quando um anexo de volume com POD falha.		Aviso

Alta taxa de retransmissão	Alta taxa de retransmissão TCP	Verifique se há congestionamento de 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 a > 10 % crítico a > 25 %
Alta capacidade do sistema de arquivos de nó	Alta capacidade do sistema de arquivos de nó	- Aumente o tamanho dos discos do nó para garantir que haja espaço suficiente para os arquivos do aplicativo. - Diminuir o uso do arquivo do aplicativo.	Aviso a > 80 % crítico a > 90 %
Fluxo de trabalho de rede alta	Alta TCP Jitter (alta latência/variações de tempo de resposta)	Verifique o congestionamento da 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 a > 30 ms crítico a > 50 ms

Taxa de transferência de volume persistente	Os limites DE MBPS em volumes persistentes podem ser usados para alertar um administrador quando os volumes persistentes excederem as expetativa de desempenho predefinidas, o que pode afetar outros volumes persistentes. A ativação desse monitor gerará alertas apropriados para o perfil de taxa de transferência típica de volumes persistentes em SSDs. Esse monitor cobrirá todos os volumes persistentes em seu locatário. Os valores de limite críticos e de aviso podem ser ajustados com base em suas metas de monitoramento duplicando esse monitor e definindo limites apropriados para sua classe de armazenamento. Um monitor duplicado pode ser direcionado ainda mais para um subconjunto dos volumes persistentes em 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 a aplicação que conduz o workload no volume para verificar se há anomalias. **Ações a serem feitas em breve** se o limite de aviso for violado, Planeje tomar as seguintes ações imediatas: 1. Introduzir limites de QoS MBPS para o volume. 2. Revise a aplicação que conduz o workload no volume para verificar se há anomalias.	Aviso a > 10.000 MB/s crítico a > 15.000 MB/s
Recipiente em risco de ir OOM morto	Os limites de memória do recipiente estão definidos demasiado baixos. O contentor está em risco de despejo (out of Memory Kill).	Aumente os limites de memória do recipiente.	Aviso a > 95 %
Carga de trabalho reduzida	O workload não tem pods íntegros.		Crítico a menos de 1
Falha na vinculação da reclamação de volume persistente	Este alerta ocorre quando uma ligação é falhou em um PVC.		Aviso
ResourceQuota Mem limites prestes a exceder	Os limites de memória para namespace estão prestes a exceder o ResourceQuota		Aviso a > 80 % crítico a > 90 %
ResourceQuota Mem pedidos prestes a exceder	As solicitações de memória para namespace estão prestes a exceder o ResourceQuota		Aviso a > 80 % crítico a > 90 %

Falha na criação do nó	Não foi possível agendar o nó devido a um erro de configuração.	Verifique o log de eventos do Kubernetes para ver a causa da falha de configuração.	Crítico
Falha na gravação de volume persistente	O volume falhou a sua recuperação automática.		Aviso a > 0 B
Limitação da CPU do contêiner	Os limites de CPU do contentor estão definidos demasiado baixos. Os processos de contentor são lentos.	Aumente os limites da CPU do contentor.	Aviso a > 95 % crítico a > 98 %
Falha ao eliminar o Service Load Balancer			Aviso
IOPS do volume persistente	Os limites de IOPS em volumes persistentes podem ser usados para alertar um administrador quando os volumes persistentes excederem as expectativas de desempenho predefinidas. A ativação deste monitor gerará alertas apropriados para o perfil IOPS típico dos volumes de persistência. Esse monitor cobrirá todos os volumes persistentes em seu locatário. Os valores de limite críticos e de aviso podem ser ajustados com base em suas metas de monitoramento duplicando esse 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. Introduza limites de IOPS de QoS para o volume. 2. Revise a aplicação que conduz o workload no volume para verificar se há anomalias. **Ações a serem feitas em breve** se o limite de aviso for violado, Planeje as seguintes ações imediatas: 1. Introduza limites de IOPS de QoS para o volume. 2. Revise a aplicação que conduz o workload no volume para verificar se há anomalias.	Aviso a > 20.000 IO/s críticos a > 25.000 IO/s
Falha ao atualizar o Service Load Balancer			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 de um limite de despejo.	Encontre e corrija pods que geram muitos processos e passam fome no nó das IDs de processo disponíveis. Configure o PodPidsLimit para proteger seu nó contra pods ou contentores que geram muitos processos.	Crítico a > 0
Falha na tração da imagem do pod	O Kubernetes não conseguiu extrair a imagem de contêiner de pod.	- Certifique-se de que a imagem do pod está escrita corretamente na configuração do pod. - Verifique a etiqueta de imagem existe no seu Registro. - Verifique as credenciais para o Registro de imagem. - Verifique se há problemas de conetividade do Registro. - Verifique se você não está atingindo os limites de taxa impostos pelos provedores de Registro público.	Aviso
Trabalho em execução demasiado longo	O trabalho está em execução por muito tempo		Aviso a > 1 h crítico a > 5 h
Memória do nó alta	O uso da memória do nó é alto	Adicionar nós. Corrija todos os nós não programados. Pods do tamanho direito para liberar memória em nós.	Aviso a > 85 % crítico a > 90 %
ResourceQuota limites de CPU prestes a exceder	Os limites de CPU para namespace estão prestes a exceder o ResourceQuota		Aviso a > 80 % crítico a > 90 %
Pod Crash Loop backoff	O pod travou e tentou reiniciar várias vezes.		Crítico a > 3
CPU do nó alta	O uso da CPU do nó é alto.	Adicionar nós. Corrija todos os nós não programados. Pods do tamanho direito para liberar a CPU nos nós.	Aviso a > 80 % crítico a > 90 %

Latência de rede de carga de trabalho RTT alta	Alta latência TCP RTT (Round Trip Time)	Verificar congestionamento de rede ▒ identificar cargas de trabalho que consomem muita largura de banda de rede. Verifique se há alta utilização da CPU do Pod. Verifique o desempenho da rede de hardware.	Aviso a > 150 ms crítico a > 300 ms
Falha no trabalho	A tarefa não foi concluída com êxito devido a uma falha ou reinicialização do nó, esgotamento de recursos, tempo limite da tarefa ou falha no agendamento do pod.	Verifique os logs de eventos do Kubernetes quanto a causas de falha.	Aviso a > 1
Volume persistente cheio em alguns 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. -Reduzir a quantidade de dados armazenados em aplicações.	Aviso a menos de 8 dia crítico a menos de 3 dia
Pressão da memória do nó	O nó está ficando sem memória. A memória disponível atingiu o limite de despejo.	Adicionar nós. Corrija todos os nós não programados. Pods do tamanho direito para liberar memória em nós.	Crítico a > 0
Nó despronto	O nó está despronto por 5 minutos	Verifique se o nó tem recursos suficientes de CPU, memória e disco. Verifique a conetividade de rede do nó. Verifique os logs de eventos do Kubernetes quanto a causas de falha.	Crítico a menos de 1
Capacidade de volume persistente alta	A capacidade usada no back-end de volume persistente é alta.	- Aumentar o tamanho do volume para garantir que haja espaço suficiente para os arquivos do aplicativo. - Reduzir a quantidade de dados armazenados nas aplicações.	Aviso a > 80 % crítico a > 90 %
Falha ao criar o Service Load Balancer	Falha na criação do Service Load Balancer		Crítico

Incompatibilidade da réplica do workload	Alguns pods atualmente não estão disponíveis para uma implantação ou DaemonSet.		Aviso a > 1
ResourceQuota CPU requests prestes a exceder	As solicitações de CPU para namespace estão prestes a exceder o ResourceQuota		Aviso a > 80 % crítico a > 90 %
Alta taxa de retransmissão	Alta taxa de retransmissão TCP	Verifique se há congestionamento de 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 a > 10 % crítico a > 25 %
Pressão do disco do nó	Espaço em disco disponível e inodes no sistema de arquivos raiz do nó ou no sistema de arquivos de imagem satisfizeram um limite de despejo.	- Aumente o tamanho dos discos do nó para garantir que haja espaço suficiente para os arquivos do aplicativo. - Diminuir o uso do arquivo do aplicativo.	Crítico a > 0
Saturação alta da CPU do cluster	A saturação alocável da CPU do cluster é alta. A saturação da CPU do cluster é calculada como a soma do uso da CPU dividida pela soma alocável da CPU em todos os K8s nós.	Adicionar nós. Corrija todos os nós não programados. Pods do tamanho direito para liberar a CPU nos nós.	Aviso a > 80 % crítico a > 90 %

Voltar ao topo

Alterar monitores de registo

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 storage descoberto	Informativo	Esta mensagem ocorre quando um nó de storage é descoberto.
Nó de storage 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 storage é descoberta.
Máquina virtual de armazenamento Modificada	Informativo	Esta mensagem ocorre quando uma máquina virtual de storage é modificada.

Voltar ao topo

Monitores de coleta de dados

Nome do monitor	Descrição	Ação corretiva
Desativação da unidade de aquisição	As unidades de aquisição do Data Infrastructure Insights são reiniciadas periodicamente como parte das 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 após por uma resolução, observando que a unidade de aquisição recém-reiniciada concluiu um registo com o Data Infrastructure Insights. Normalmente, este ciclo de desligamento para Registro leva de 5 a 15 minutos.	Se o alerta ocorrer com frequência ou durar mais de 15 minutos, verifique o funcionamento do sistema que hospeda a Unidade de aquisição, a rede e qualquer proxy que conete a AU à Internet.
O coletor falhou	A pesquisa de um coletor de dados encontrou uma situação de falha inesperada.	Visite a página do coletor de dados em Data Infrastructure Insights para saber mais sobre a situação.

Aviso do coletor	Este alerta normalmente pode surgir devido a uma configuração incorreta do coletor de dados ou do sistema de destino. Revisite as configurações para evitar alertas futuros. Também pode ser devido a uma recuperação de dados menos que completos, onde o coletor de dados reuniu todos os dados que ele poderia. 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 de Coletor pode enviar mais alertas do que outros tipos de monitor, por isso 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 AutoSupport desativado	Aviso a menos de 1	O AutoSupport suporta HTTPS, HTTP e SMTP para protocolos de transporte. Devido à natureza sensível das mensagens AutoSupport, a NetApp recomenda fortemente o uso de HTTPS como o protocolo de transporte padrão para enviar mensagens AutoSupport para o suporte ao NetApp.	Para definir o 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 a menos de 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 de cluster desativado	Aviso a menos de 1	Indica que o banner Login está desativado para usuários que acessam o sistema ONTAP. A exibição de um banner de login é útil para estabelecer expetativa de acesso e uso do sistema.	Para configurar o banner de login para um cluster, execute o seguinte comando ONTAP:… security login banner modificar -vserver <admin svm> -mensagem "Acesso restrito a usuários autorizados"
Comunicação por pares de cluster não encriptada	Aviso a menos de 1	Ao replicar dados para recuperação de desastre, armazenamento em cache ou backup, você precisa proteger esses dados durante o transporte por cabo de um cluster ONTAP para outro. A criptografia deve ser configurada nos clusters de origem e destino.	Para habilitar a criptografia em relacionamentos de pares de cluster criados antes do ONTAP 9.6, o cluster de origem e destino deve ser atualizado para 9,6. Em seguida, use o comando "cluster peer Modify" para alterar os pares de cluster de origem e destino para usar a criptografia de peering de cluster. Consulte o Guia de endurecimento de segurança do NetApp para ONTAP 9 para obter detalhes.
Utilizador Admin local predefinido ativado	Aviso a > 0	O NetApp recomenda bloquear (desativar) quaisquer contas de usuário administrador padrão (internas) desnecessárias com o comando LOCK. São principalmente contas padrão para as quais as senhas nunca foram atualizadas ou alteradas.	Para bloquear a conta "admin" interna, execute o seguinte comando ONTAP:… security login lock -username admin
Modo FIPS desativado	Aviso a menos de 1	Quando a conformidade com o FIPS 140-2 está ativada, o TLSv1 e o SSLv3 são desativados e apenas o TLSv1,1 e o TLSv1,2 permanecem ativados. O ONTAP impede que você ative o TLSv1 e o SSLv3 quando a conformidade com o 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 modifique -interface SSL -is-fips-enabled true

Encaminhamento de registo não encriptado	Aviso a menos de 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 seguro de armazenamento ou retenção.	Uma vez criado um destino de encaminhamento de registo, o respetivo 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
MD5 Palavra-passe com hash	Aviso a > 0	A NetApp recomenda fortemente usar a função hash SHA-512 mais segura para senhas de contas de usuário do ONTAP. As contas que usam a função hash MD5 menos segura devem migrar para a função hash SHA-512.	O 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 a menos de 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 servidor ntp create -Server [Nome do host do servidor ntp ou endereço ip>
A contagem do servidor NTP é baixa	Aviso a menos de 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

Shell remoto ativado	Aviso a > 0	O Shell remoto não é um método seguro para estabelecer acesso de linha de comando à solução ONTAP. O Shell remoto deve ser desativado para acesso remoto seguro.	Para desativar o shell remoto em um cluster, execute o seguinte comando ONTAP no modo de privilégio avançado:…Protocolo de segurança modificar -application rsh- enabled false NetApp
Registo de auditoria da VM de armazenamento desativado	Aviso a menos de 1	Indica que o log de auditoria está desativado para SVM.	Para configurar o log de auditoria para um vserver, execute o seguinte comando ONTAP:… vserver audit enable -vserver <svm>
Armazenamento VM cifras inseguras para SSH	Aviso a menos de 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 desativado	Aviso a menos de 1	Indica que o banner Login está desativado para usuários que acessam SVMs no sistema. A exibição de um banner de login é útil para estabelecer expetativa de acesso e uso do sistema.	Para configurar o banner de login para um cluster, execute o seguinte comando ONTAP:… security login banner modificar -vserver <svm> -mensagem "Acesso restrito a usuários autorizados"
Protocolo Telnet ativado	Aviso a > 0	O Telnet não é um método seguro para estabelecer acesso à linha de comando à solução ONTAP. O Telnet deve ser desativado para acesso remoto seguro.	A NetApp recomenda o Shell seguro (SSH) para acesso remoto seguro. Para desativar o Telnet em um cluster, execute o seguinte comando ONTAP no modo de privilégio avançado: .. Protocolo de segurança modificar -Application telnet -enabled false

Voltar ao topo

Monitores de proteção de dados

Nome do monitor	Limites	Descrição do monitor	Ação corretiva

Espaço insuficiente para cópia Snapshot LUN	(O filtro contém_luns: Sim) Aviso a > 95 %… crítico a > 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 instantâneo, é usada para armazenar snapshots que permitem que os dados sejam protegidos localmente. Quanto mais dados novos e atualizados forem armazenados no volume ONTAP, mais capacidade de snapshot será usada e menos capacidade de storage snapshot estarão disponíveis para dados novos ou atualizados futuros. Se a capacidade de dados do snapshot dentro de um volume atingir o espaço total de reserva do snapshot, isso pode levar o cliente a não conseguir armazenar novos dados do snapshot e a reduzir o nível de proteção dos dados nos LUNs no volume. O monitoramento do volume usado da capacidade do 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 instantâneos para usar o espaço de dados no volume quando a reserva de snapshot estiver cheia. 2. Elimine alguns instantâneos indesejados mais antigos para libertar espaço. **Ações a serem feitas em breve** se o limite de aviso for violado, Planeje tomar as seguintes ações imediatas: 1. Aumente o espaço de reserva do snapshot dentro do volume para acomodar o crescimento. 2. Configure instantâneos para usar o espaço de dados no volume quando a reserva de snapshot estiver cheia.

Atraso no relacionamento com o SnapMirror	Aviso a > 150%… crítico a > 300%	O atraso no relacionamento do SnapMirror é a diferença entre o carimbo de data/hora do snapshot e a hora no sistema de destino. O lag_time_percent é a relação entre o tempo de atraso e o intervalo de programação da Política SnapMirror. Se o tempo de atraso for igual ao intervalo de programação, o lag_time_percent será de 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 do volume de nuvem (CVO)

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

CVO Giveback do pool de armazenamento falhou	CRÍTICO	Esse evento ocorre durante a migração de um agregado como parte de um failover de armazenamento (SFO), quando o nó de destino não pode alcançar os armazenamentos de objetos.	Execute as seguintes ações corretivas: Verifique se o LIF entre clusters está on-line e funcional usando o comando "network interface show". Verifique a conetividade de rede ao servidor de armazenamento de objetos usando o comando"'ping" sobre o LIF entre clusters de nó de destino. Verifique se a configuração do seu armazenamento de objetos não foi alterada e se as informações de login e conetividade ainda são precisas usando o comando "Aggregate object-store config show". Alternativamente, 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 do CVO HA desativada	AVISO	A interconexão de alta disponibilidade (HA) está inativa. Risco de interrupção de serviço quando o failover não está disponível.	As ações corretivas dependem do número e do tipo de links de interconexão de HA suportados pela plataforma, bem como do motivo pelo qual a interconexão está inativa. Se os links estiverem inativos: Verifique se ambas as controladoras no par de HA estão operacionais. Para links conetados externamente, verifique se os cabos de interconexão estão conetados corretamente e se os SFPs (Small Form-factor Pluggables), se aplicável, estão encaixados corretamente em ambos os controladores. Para ligações ligadas internamente, desative e volte a ativar as ligações, uma após a outra, utilizando os comandos "ic link Off" (ligação ic desligada) e "ic link ON" (ligação ic ligada). Se as ligações estiverem desativadas, ative as ligações utilizando o comando "ic link ON". Se um par não estiver conetado, desative e reative os links, um após o outro, usando os comandos "ic link off" e "ic link on". Contacte o suporte técnico da NetApp se o problema persistir.

Sessões máx. CVO por utilizador excedidas	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 que são executados no cliente e encerre qualquer um que não esteja 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 modificar -Max -abre-same-file-per-tree". Em alguns casos, os clientes operam como 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 nomes NetBIOS CVO	CRÍTICO	O serviço de nomes NetBIOS recebeu uma resposta negativa a uma solicitação de Registro de nomes de uma máquina remota. Isso geralmente é causado por um conflito no nome NetBIOS ou um alias. Como resultado, os clientes podem não conseguir acessar dados ou se conetar ao nó certo de fornecimento de dados no cluster.	Execute qualquer uma das seguintes ações corretivas: Se houver um conflito no nome NetBIOS ou um alias, execute uma das seguintes ações: Exclua o alias NetBIOS duplicado usando o comando "vserver cifs delete -aliases alias -vserver 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.
CVO NFSv4 Store Pool esgotado	CRÍTICO	Uma piscina de loja NFSv4 foi esgotada.	Se o servidor NFS não responder por mais de 10 minutos após este evento, entre em Contato com o suporte técnico da NetApp.
Pânico do nó CVO	AVISO	Este evento é emitido quando ocorre um pânico	Entre em Contato com o suporte ao cliente da NetApp.

Espaço de volume raiz do nó CVO baixo	CRÍTICO	O sistema detetou que o volume raiz está perigosamente baixo no espaço. O nó não está totalmente operacional. As LIFs de dados podem ter falhado no cluster, por causa do qual o acesso NFS e CIFS é limitado no nó. A capacidade administrativa está limitada aos procedimentos de recuperação locais para que o nó limpe o espaço no volume raiz.	Execute as seguintes ações corretivas: Limpe o espaço no volume raiz excluindo cópias Snapshot antigas, excluindo arquivos que você não precisa mais 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 Admin inexistente do CVO	CRÍTICO	Problema Vscan: Um cliente tentou se conetar a um compartilhamento inexistente do ONTAP_ADMIN.	Certifique-se de que o Vscan esteja habilitado para o ID SVM mencionado. Ativar o Vscan em um SVM faz com que o compartilhamento ONTAP_ADMIN seja criado automaticamente para o SVM.
Host do 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 um endereço IP. Como resultado, os dados podem estar inacessíveis.	Verifique a configuração DNS para verificar se o nome do host está configurado corretamente com um endereço IP.

LIF entre clusters do armazenamento de objetos CVO 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 o tráfego do cliente de armazenamento de objetos até que o LIF entre clusters esteja operacional. Como resultado, os dados podem estar inacessíveis.	Execute as seguintes ações corretivas: Verifique o status de clusters de LIF usando o comando "network interface show -role". Verifique se o LIF entre clusters está configurado corretamente e operacional. Se um LIF entre clusters não estiver configurado, adicione-o usando o comando "network interface create -role".
Incompatibilidade da assinatura do armazenamento de objetos CVO	CRÍTICO	A assinatura de solicitação enviada ao servidor de armazenamento de objetos não corresponde à assinatura calculada pelo cliente. Como resultado, os dados podem estar inacessíveis.	Verifique se a chave de acesso secreto está configurada corretamente. Se estiver configurado corretamente, contacte o suporte técnico da NetApp para obter assistência.
Memória do monitor QoS CVO maximizada	CRÍTICO	A memória dinâmica do subsistema QoS atingiu seu limite para o hardware atual da plataforma. Alguns recursos de QoS podem operar em uma 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. Workloads ativos mostram operações que não são 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 <workload name> *" 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 que é permitido executar no WAFL. Isso pode ser por causa de diretórios muito grandes ou esparsos. Recomenda-se a ação corretiva.	Execute as seguintes ações corretivas: Encontre informações específicas para diretórios recentes que tiveram operações de ARQUIVO READDIR expiram usando o seguinte comando 'deag' Privilege nodeshell CLI: WAFL readdir notice show. Verifique se os diretórios são indicados como esparsos ou não: Se um diretório é indicado como esparso, é recomendável que você copie o conteúdo do diretório para um novo diretório para remover a frouxidão do arquivo de diretório. Se um diretório não for indicado como esparso e o diretório for grande, é recomendável reduzir o tamanho do arquivo de diretório reduzindo o número de entradas de arquivo no diretório.

Falha na realocação do CVO do pool de storage	CRÍTICO	Esse evento ocorre durante a realocação de um agregado, quando o nó de destino não pode alcançar os armazenamentos de objetos.	Execute as seguintes ações corretivas: Verifique se o LIF entre clusters está on-line e funcional usando o comando "network interface show". Verifique a conetividade de rede ao servidor de armazenamento de objetos usando o comando"'ping" sobre o LIF entre clusters de nó de destino. Verifique se a configuração do seu armazenamento de objetos não foi alterada e se as informações de login e conetividade ainda são precisas usando o comando "Aggregate object-store config show". Alternativamente, você pode substituir o erro usando o parâmetro "override-destination-checks" do comando relocation. Entre em Contato com o suporte técnico da NetApp para obter mais informações ou assistência.
Cópia sombra CVO falhou	CRÍTICO	Um serviço de cópia de sombra de volume (VSS), uma operação de serviço de backup e restauração do Microsoft Server, falhou.	Verifique o seguinte usando as informações fornecidas na mensagem de evento: A configuração de cópia de sombra está ativada? As licenças apropriadas estão instaladas? Em que compartilhamentos é realizada a operação de cópia sombra? O nome da partilha está correto? O caminho de compartilhamento existe? Quais são os estados do conjunto de cópias de sombra e suas cópias de sombra?
Interrupção da VM de armazenamento do CVO com êxito	INFORMAÇÕES	Esta mensagem ocorre quando uma operação 'vserver stop' é bem-sucedida.	Use o comando 'vserver start' para iniciar o acesso a dados em uma VM de armazenamento.

Autenticação CIFS do CVO demais	AVISO	Muitas negociações de autenticação ocorreram simultaneamente. Existem 256 solicitações de nova sessão incompletas deste cliente.	Investigue por que o cliente criou 256 ou mais solicitações de conexão novas. Você pode ter que entrar em Contato com o fornecedor do cliente ou do aplicativo para determinar por que o erro ocorreu.
Discos não atribuídos CVO	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 são atribuídos usando o comando "Disk show -n". Atribua os discos a um sistema usando o comando "Disk Assign" (atribuir disco).
CVO Acesso não autorizado do Usuário ao Admin Share	AVISO	Um cliente tentou se conetar ao compartilhamento privilegiado do ONTAP_ADMIN, mesmo que seu usuário conetado não seja um usuário permitido.	Execute as seguintes ações corretivas: Certifique-se de que o nome de usuário e o endereço IP mencionados estão configurados em um dos conjuntos de scanners Vscan ativos. Verifique a configuração do conjunto do scanner que está atualmente ativa usando o comando "vserver vscan pool show-active".
Vírus CVO detetado	AVISO	Um servidor Vscan comunicou um erro ao sistema de armazenamento. Isso normalmente indica que um vírus foi encontrado. No entanto, outros erros no servidor Vscan podem causar este evento. O acesso do cliente ao ficheiro é negado. O servidor Vscan pode, dependendo de suas configurações e configurações, limpar o arquivo, colocá-lo em quarentena ou excluí-lo.	Verifique o log do servidor Vscan relatado no evento "syslog" para ver se ele foi capaz de limpar, colocar em quarentena ou excluir o arquivo infetado com sucesso. Se não conseguir fazê-lo, um administrador de sistema poderá ter de eliminar manualmente o ficheiro.

CVO volume Offline	INFORMAÇÕES	Esta mensagem indica que um volume está offline.	Traga o volume de volta online.
Volume CVO restrito	INFORMAÇÕES	Este evento indica que um volume flexível é restringido.	Traga o volume de volta online.

Voltar ao topo

Monitores de log do mediador da continuidade de negócios (SnapMirror for Business Continuity)

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
ONTAP Mediador adicionado	INFORMAÇÕES	Esta mensagem ocorre quando o Mediador ONTAP é adicionado com sucesso em um cluster.	Nenhum
Mediador ONTAP não acessível	CRÍTICO	Esta mensagem ocorre quando o Mediador ONTAP é reutilizado ou o pacote Mediador não é mais instalado no servidor Mediador. 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".
ONTAP Mediador removido	INFORMAÇÕES	Esta mensagem ocorre quando o Mediador ONTAP é removido com sucesso de um cluster.	Nenhum
ONTAP Mediador inalcançável	AVISO	Esta mensagem ocorre quando o Mediador ONTAP não está acessível em um cluster. Como resultado, o failover do SnapMirror não é possível.	Verifique a conetividade de rede ao Mediador ONTAP 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 CA SMBC expirado	CRÍTICO	Esta mensagem ocorre quando o certificado de autoridade de certificação do mediador (CA) do ONTAP expirou. Como resultado, não será possível qualquer comunicação adicional com o Mediador ONTAP.	Remova a configuração do Mediador ONTAP atual usando o comando "SnapMirror Mediator remove". Atualize um novo certificado de CA no servidor do 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 de autoridade de certificação do mediador (CA) da ONTAP expira nos próximos 30 dias.	Antes que esse certificado expire, remova a configuração do Mediador ONTAP atual usando o comando "SnapMirror Mediator remove". Atualize um novo certificado de CA no servidor do ONTAP Mediator. Reconfigure o acesso ao Mediador ONTAP usando o comando "SnapMirror Mediator add".
Certificado Cliente SMBC expirado	CRÍTICO	Esta mensagem ocorre quando o certificado de cliente do Mediador ONTAP expirou. Como resultado, não será possível qualquer comunicação adicional com o Mediador ONTAP.	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 Cliente SMBC a expirar	AVISO	Esta mensagem ocorre quando o certificado de cliente do Mediador ONTAP expira nos próximos 30 dias.	Antes que esse 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 sincronização Nota: O UM não tem este	CRÍTICO	Esta mensagem ocorre quando uma relação SnapMirror for Business Continuity (SMBC) muda o status de "in-Sync" para "out-of-Sync". Devido a essa proteção de dados RPO igual a 0 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 usando o comando "SnapMirror list-destinations" na origem. A ressincronização automática tentará trazer a relação de volta ao status "in-sync". Se a ressincronização falhar, verifique se todos os nós no cluster estão em quórum e estão em bom estado.
Certificado do servidor SMBC expirou	CRÍTICO	Esta mensagem ocorre quando o certificado do servidor do Mediador ONTAP expirou. Como resultado, não será possível qualquer comunicação adicional com o Mediador ONTAP.	Remova a configuração do Mediador ONTAP atual usando o comando "SnapMirror Mediator remove". Atualize um novo certificado de servidor no servidor do ONTAP Mediator. Reconfigure o acesso ao Mediador ONTAP usando o comando "SnapMirror Mediator add".
O certificado do servidor SMBC está a expirar	AVISO	Esta mensagem ocorre quando o certificado do servidor do Mediador ONTAP expira nos próximos 30 dias.	Antes que esse certificado expire, remova a configuração do Mediador ONTAP atual usando o comando "SnapMirror Mediator remove". Atualize um novo certificado de servidor no servidor do ONTAP Mediator. Reconfigure o acesso ao Mediador ONTAP usando o comando "SnapMirror Mediator add".

Voltar ao topo

Monitores adicionais de alimentação, Heartbeat e diversos do sistema

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
Fonte de alimentação do compartimento de disco descoberta	INFORMATIVO	Esta mensagem ocorre quando uma unidade de fonte de alimentação é adicionada ao compartimento de disco.	NENHUM
Fonte de alimentação de prateleiras de disco removida	INFORMATIVO	Esta mensagem ocorre quando uma unidade de fonte de alimentação é removida do compartimento de disco.	NENHUM
Switchover não planejado automático da MetroCluster desativado	CRÍTICO	Esta mensagem ocorre quando a capacidade de comutação não planejada automática é desativada.	Execute o comando "MetroCluster Modify -node-name <nodename> -automatic-switchover -onfailure true" para cada nó no cluster para habilitar o switchover automático.
Ponte de armazenamento MetroCluster inacessível	CRÍTICO	A ponte de armazenamento não é acessível através da rede de gerenciamento	1) se a ponte for monitorada pelo SNMP, verifique se o LIF de gerenciamento do nó está ativo usando o comando "network interface show". Verifique se a ponte está viva usando o comando "ping de rede". 2) se a ponte for monitorada na banda, verifique o cabeamento da malha para a ponte e verifique se a ponte está ligada.
Temperatura da ponte do MetroCluster anormal - abaixo de 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 condições de temperatura recomendadas.

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
Temperatura da ponte do MetroCluster anormal - acima de crítico	CRÍTICO	O sensor na ponte Fibre Channel está relatando uma temperatura acima do limite crítico.	1) verificar o estado operacional do sensor de temperatura do chassis na ponte de armazenamento utilizando o comando "Storage bridge show -cooling". 2) Verifique se a ponte de armazenamento está operando sob condições de temperatura recomendadas.
Agregado de MetroCluster deixado para trás	AVISO	O agregado foi deixado para trás durante o switchback.	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".
Todos os links entre parceiros da MetroCluster para baixo	CRÍTICO	Os adaptadores de interconexão RDMA e os LIFs entre clusters têm conexões quebradas com o cluster de peering ou o cluster de peering está inativo.	1) assegurar que os LIFs entre clusters estão em funcionamento. Repare os LIFs entre clusters se estiverem inativos. 2) Verifique se o cluster com peering está funcionando usando o comando "cluster peer ping". Consulte o Guia de recuperação de desastres do MetroCluster se o cluster com peering estiver inativo. 3) para o Fabric MetroCluster, verifique se os ISLs de malha back-end estão funcionando. Repare as ISLs de tecido back-end se estiverem inoperantes. 4) para configurações MetroCluster que não sejam de malha, verifique se o cabeamento está correto entre os adaptadores de interconexão RDMA. Reconfigure o cabeamento se os links estiverem inativos.

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
Parceiros MetroCluster não alcançáveis através da rede de peering	CRÍTICO	A conetividade com o cluster de pares está quebrada.	1) Certifique-se de que a porta está conetada à rede/switch correto. 2) garantir que o LIF entre clusters esteja conetado com o cluster de peered. 3) Certifique-se de que o cluster de peered está ativo e em execução usando o comando "cluster peer ping". Consulte o Guia de recuperação de desastres do MetroCluster se o cluster com peering estiver inativo.
Todos os links para baixo são MetroCluster Inter	CRÍTICO	Todos os ISLs (Inter-Switch Links) no comutador de armazenamento estão inativos.	1) reparar os ISLs de tecido back-end no interrutor de armazenamento. 2) Certifique-se de que o switch do parceiro está ativo e seus ISLs estão operacionais. 3) garantir que os equipamentos intermediários, como os dispositivos xWDM, estejam operacionais.
Nó MetroCluster para a ligação SAS da pilha de armazenamento para baixo	AVISO	O adaptador SAS ou seu cabo conetado podem estar com falha.	1. Verifique se o adaptador SAS está on-line e em execução. 2. Verifique se a conexão do cabo físico está segura e funcionando e substitua o cabo, se necessário. 3. Se o adaptador SAS estiver conetado às gavetas de disco, verifique se os IOMs e os discos estão corretamente assentados.
O iniciador do MetroClusterFC liga para baixo	CRÍTICO	O adaptador do iniciador FC está com falha.	1. Certifique-se de que o link do iniciador FC não foi adulterado. 2. Verifique o status operacional do adaptador do iniciador FC usando o comando "system node run -node local -command storage show adapter".

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
Ligação de interligação FC-VI descendente	CRÍTICO	O link físico na porta FC-VI está offline.	1. Certifique-se de que a ligação FC-VI não foi adulterada. 2. Verifique se o status físico do adaptador FC-VI é "Up" usando o comando "MetroCluster interconnect adapter show". 3. Se a configuração incluir switches de malha, verifique se eles estão cabeados e configurados corretamente.
Discos de reserva MetroCluster deixados para trás	AVISO	O disco sobressalente foi deixado para trás durante o switchback.	Se o disco não falhar, devolva-o ao proprietário original usando o comando "MetroCluster switchback".
Porta de ponte de armazenamento MetroCluster para baixo	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 conetividade lógica e física à porta.
Falha nas ventoinhas do interrutor de armazenamento do MetroCluster	CRÍTICO	A ventoinha no interrutor de armazenamento falhou.	1) assegurar-se de que os ventiladores do contactor estão a funcionar corretamente, utilizando o comando "interrutor de memorização show -refrigeração". 2) Certifique-se de que as FRUs do ventilador estão inseridas corretamente e operacionais.

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
Comutador de armazenamento MetroCluster inalcançável	CRÍTICO	O comutador de armazenamento não é acessível através da rede de gestão.	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 está ativo usando o comando "network ping". 3) Certifique-se de que o switch está acessível através de SNMP, verificando suas configurações SNMP depois de fazer login no switch.
As fontes de alimentação do interrutor MetroCluster falharam	CRÍTICO	Uma unidade de fonte de alimentação no interrutor de armazenamento não está operacional.	1) Verifique os detalhes do erro usando o comando "storage switch show -error -switch-name <swtich name>". 2) identificar a unidade de fonte de alimentação defeituosa usando o comando "interrutor de armazenamento show -POWER -switch-name <switch name>". 3) assegurar que o unite da fonte de alimentação inserido corretamente no chassi do interrutor de armazenamento e totalmente operacional.
Sensores de temperatura do interrutor MetroCluster falharam	CRÍTICO	O sensor no interrutor Fibre Channel falhou.	1) verificar o estado de funcionamento dos sensores de temperatura no contactor de memorização, utilizando o comando "interrutor de memorização indicar -refrigeração". 2) Verifique se o interrutor está operando sob condições de temperatura recomendadas.

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
Temperatura do interrutor do MetroCluster anormal	CRÍTICO	O sensor de temperatura no interrutor do canal de fibra comunicou uma temperatura anormal.	1) verificar o estado de funcionamento dos sensores de temperatura no contactor de memorização, utilizando o comando "interrutor de memorização indicar -refrigeração". 2) Verifique se o interrutor está operando sob condições de temperatura recomendadas.
Falha no Heartbeat do processador de serviço	INFORMATIVO	Esta mensagem ocorre quando o ONTAP não recebe um sinal de "heartbeat" esperado do processador de serviço (SP). Junto com esta mensagem, os arquivos de log do SP serão enviados para depuração. O ONTAP repõe o SP para tentar restaurar a comunicação. O SP estará indisponível por até dois minutos enquanto ele for reinicializado.	Entre em Contato com o suporte técnico da NetApp.

Nome do monitor	Gravidade	Descrição do monitor	Ação corretiva
O Heartbeat do processador de serviço parou	AVISO	Esta mensagem ocorre quando o ONTAP não está mais recebendo batimentos cardíacos do processador de Serviço (SP). Dependendo do design do hardware, o sistema pode continuar fornecendo dados ou pode determinar o desligamento 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) de firmware aberto. Se o seu sistema estiver configurado para o fazer, ele gera e transmite uma mensagem AutoSupport (ou "Call Home") para o suporte técnico da NetApp e para os destinos configurados. A entrega bem-sucedida de uma mensagem AutoSupport melhora significativamente a determinação e resolução de problemas.	Se o sistema tiver desligado, tente um ciclo de alimentação rígido: Puxe o controlador para fora do chassis, empurre-o de volta e, em seguida, ligue o sistema. Entre em Contato com o suporte técnico da NetApp se o problema persistir após o ciclo de energia ou para qualquer outra condição que possa justificar atenção.

Voltar ao topo

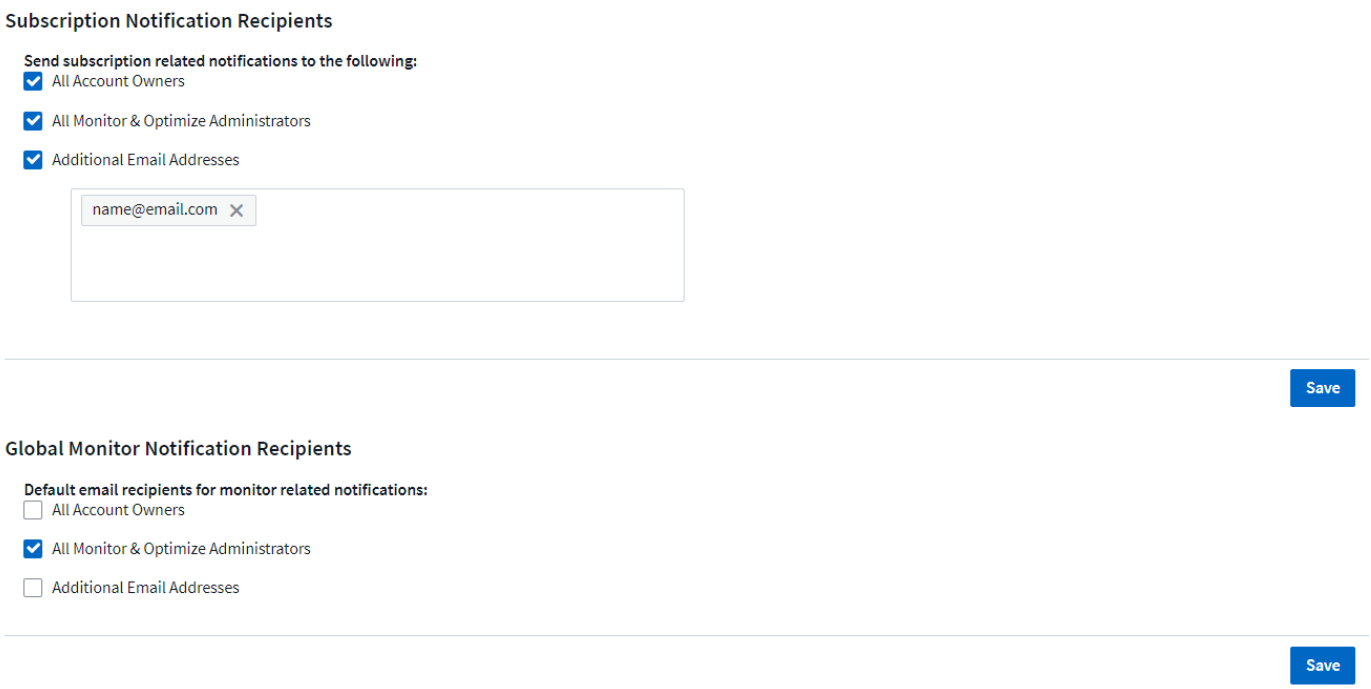
Mais informações

- "Visualização e ausência de alertas"

Configurar notificações por e-mail

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

Para configurar as configurações do destinatário de e-mail de notificação, vá para a página **Admin > notificações** e selecione a guia *e-mail*.



Destinatários da notificação de assinatura

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

- Todos os proprietários de contas
- Todos os administradores *Monitor & Otimize*
- Endereços de e-mail adicionais que você especificar

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

Notificação:	**Ação do Usuário:**
A versão de avaliação ou subscrição foi atualizada	Reveja os detalhes da subscrição "Subscrição"na página
A assinatura expirará em 90 dias. A assinatura expirará em 30 dias	Nenhuma ação necessária se a "renovação automática" estiver ativada entre em Contato com as vendas da NetApp para renovar a assinatura
O teste termina em 2 dias	Renove o teste a partir "Subscrição"da página. Você pode renovar um teste uma vez. Entre em Contato com a NetApp Sales para comprar uma assinatura
A conta de teste ou assinatura expirou deixará de coletar dados em 48 horas a conta será excluída após 48 horas	Entre em Contato com a NetApp Sales para comprar uma assinatura

Para garantir que seus destinatários recebam notificações do Data Infrastructure Insights, adicione os seguintes endereços de e-mail a qualquer lista de "permitir":

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

Lista de destinatários globais para alertas

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

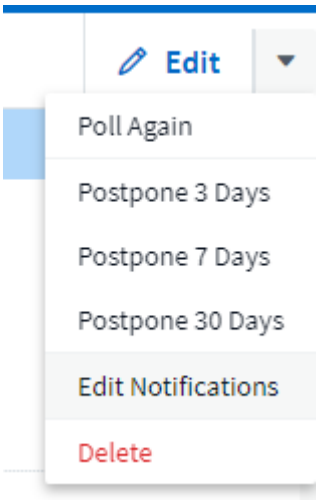
Para configurar destinatários de alerta global, escolha os destinatários desejados na seção **destinatários de notificação do Monitor Global**.

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

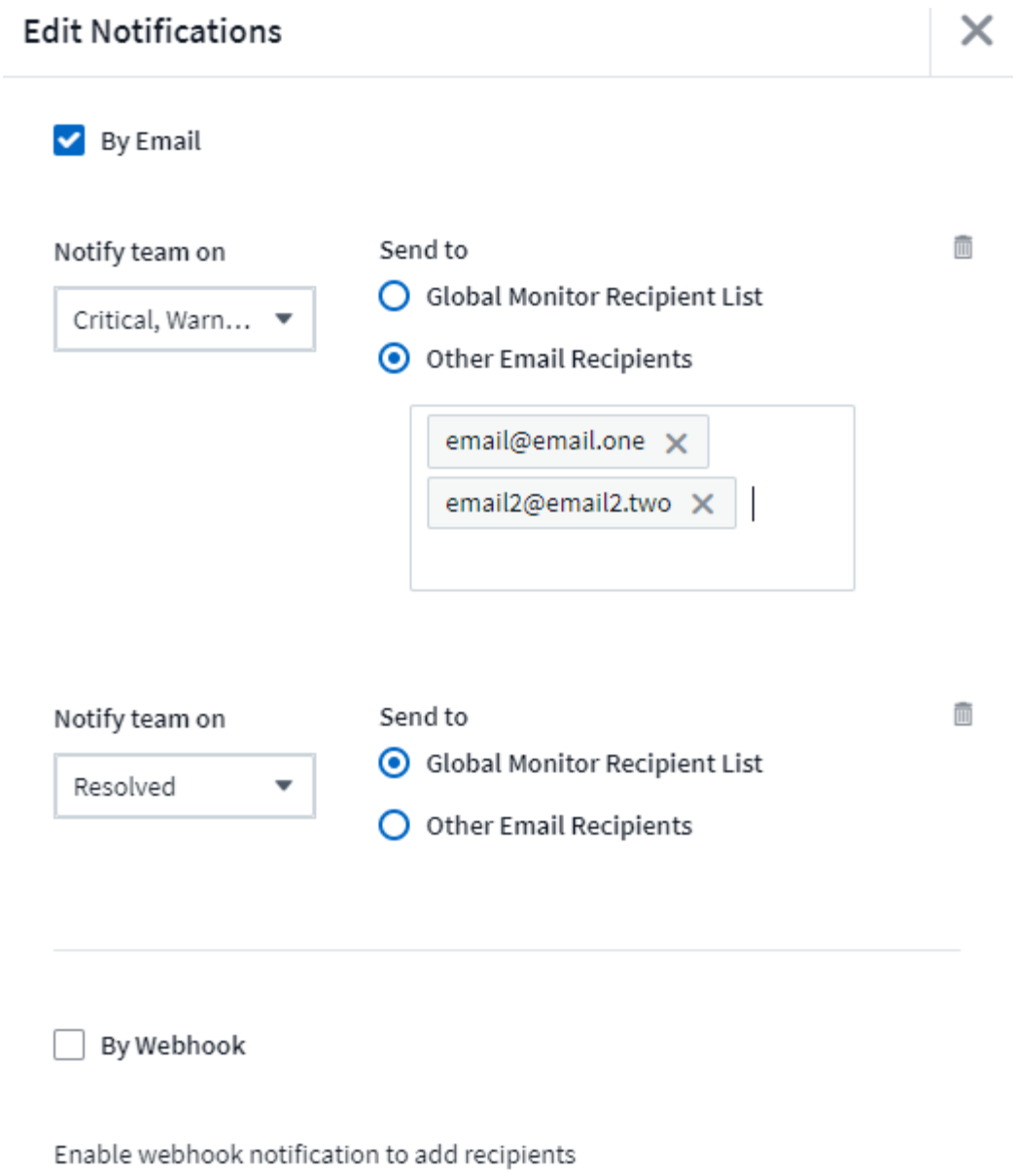
As notificações do ONTAP Data Collector têm precedência sobre quaisquer notificações específicas do Monitor que sejam relevantes para o cluster/coletor de dados. A lista de destinatários definida para o coletor de dados receberá os alertas do coletor de dados. Se não houver alertas ativos do coletor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

Editando notificações para ONTAP

Você pode modificar notificações para clusters do ONTAP selecionando *Editar notificações* na lista suspensa superior direita em uma página inicial do 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.



Notificações do webhook

Notificação usando Webhooks

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

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

Você pode criar vários canais de webhook, cada canal direcionado para um propósito diferente; aplicativos separados, destinatários diferentes, etc.

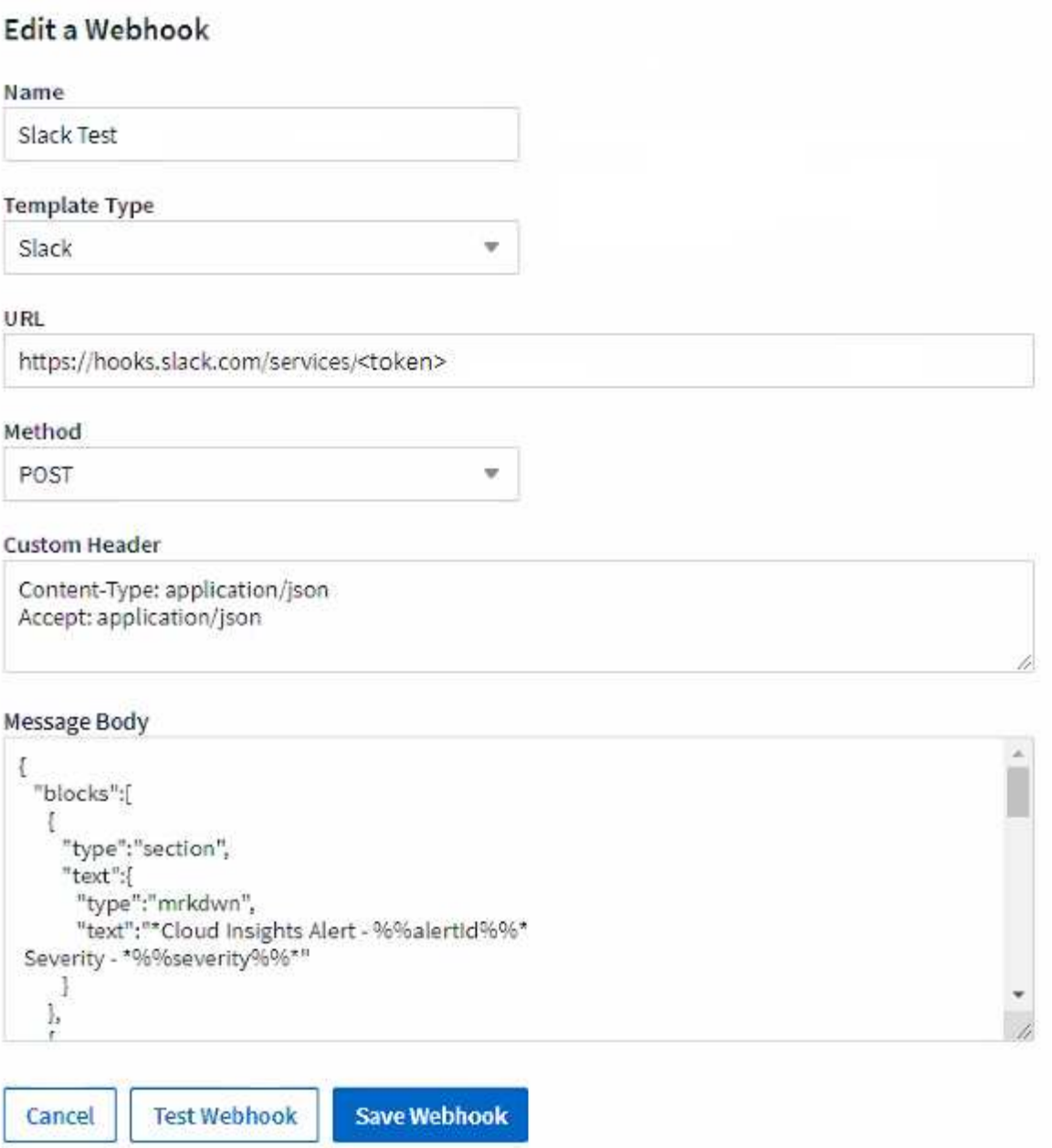
A instância do canal webhook é composta pelos seguintes elementos:

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 aqui quaisquer linhas de cabeçalho personalizadas
Corpo da mensagem	Coloque o corpo da sua mensagem aqui
Parâmetros de alerta predefinidos	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, vá para **Admin > notificações** e selecione a guia **Webhooks**.

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



Introduza as informações adequadas para cada um dos campos e clique em "Guardar" 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 incluem vários parâmetros padrão. Além disso, você pode criar seus próprios parâmetros personalizados ou segredos.

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 os utilizo?

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

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

Note que nesta seção, as substituições são *não* executadas 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

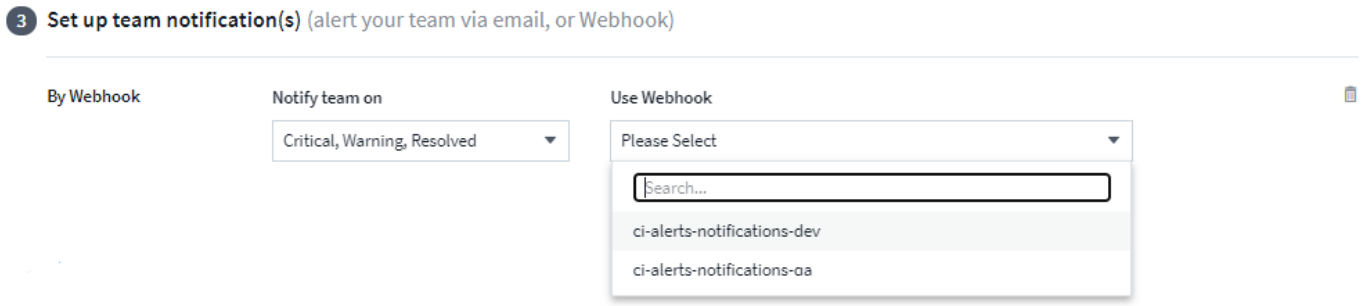
Nesta seção, você pode adicionar quaisquer parâmetros personalizados e / ou segredos que desejar. Por razões de segurança, se um segredo é definido, apenas o criador do webhook pode modificar este canal do webhook. É somente leitura para os outros. Você pode usar segredos em URL/cabeçalhos como *%%<secret_name>%%*.

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 a notificação do Webhook em um monitor

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



Exemplos de webhook:

Webhooks "Folga"para Webhooks para Webhooks "PagerDuty" "Equipas" para "Discórdia"

Webhook exemplo para discord

Webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado. Esta página fornece um exemplo para configurar webhooks para o discord.

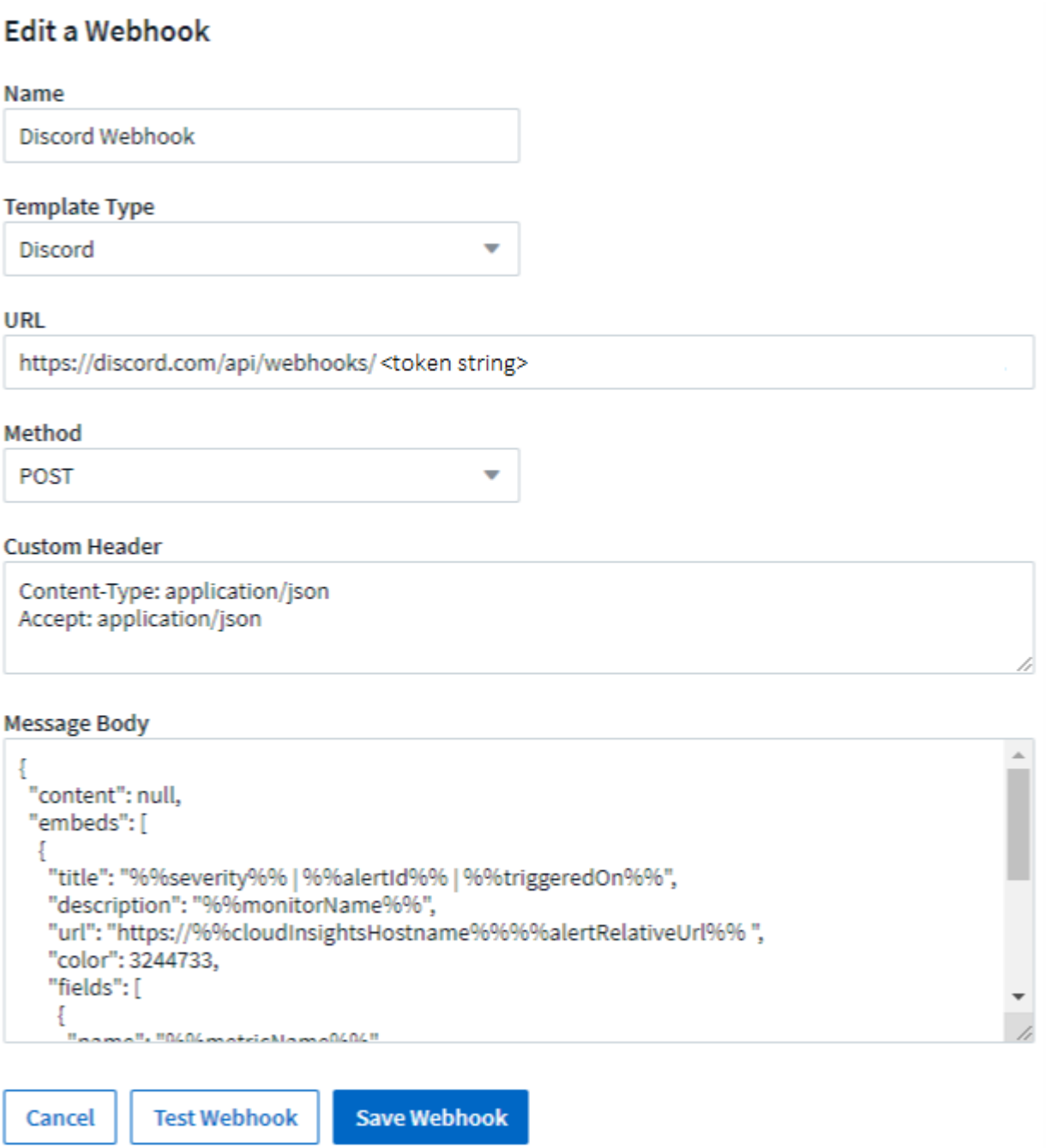
Esta página refere-se a instruções de terceiros, que podem estar sujeitas a alterações. Consulte a "Documentação do discord"para obter as informações mais atualizadas.

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 **New Webhook**
- Copie o URL do Webhook. Você precisará colar isso na configuração do webhook do Data Infrastructure Insights.

Crie o Webhook do Data Infrastructure Insights:

1. Em 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. Na lista suspensa *Template Type*, selecione **discord**.
4. Cole o URL de cima no campo *URL*.

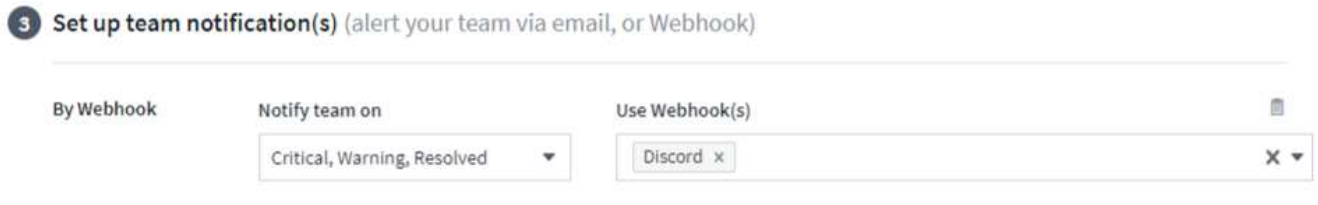


Para testar o webhook, substitua temporariamente o valor do url no corpo da mensagem por qualquer URL válido (como *https://NetApp.com*) e clique no botão *testar Webhook*. Certifique-se de que volta o corpo da mensagem assim que o teste for concluído.

Notificações via Webhook

Para notificar eventos via webhook, em Data Infrastructure Insights navegue até **Alertas > monitores** e clique em * Monitor* para criar um novo "monitorar".

- Selecione uma métrica e defina as condições do monitor.
- Em _Configurar notificação(s) da equipe, escolha o método **Webhook** Delivery.
- Escolha o webhook "discord" para os eventos desejados (crítico, Aviso, resolvido)



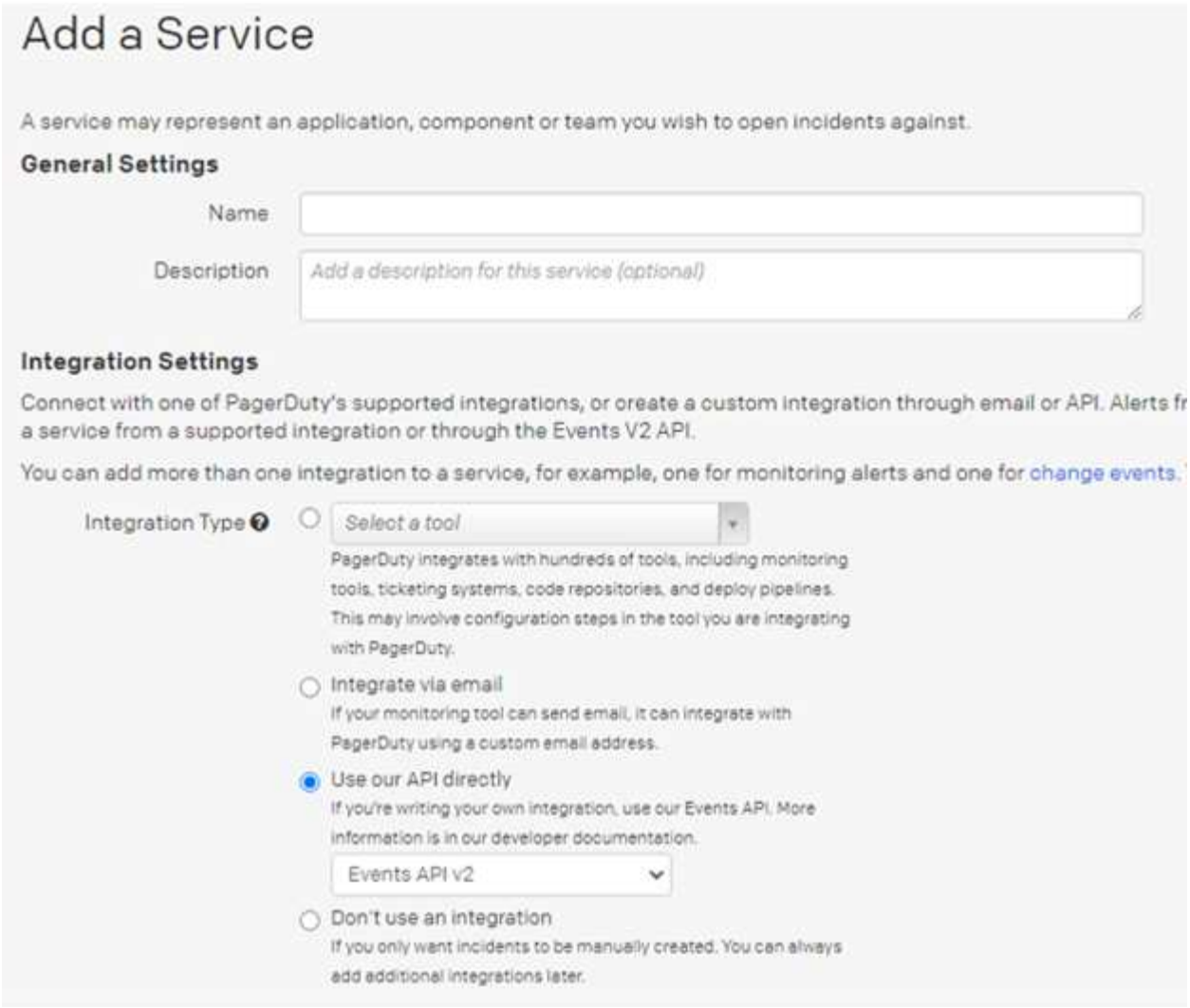
Exemplo de webhook para PagerDuty

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

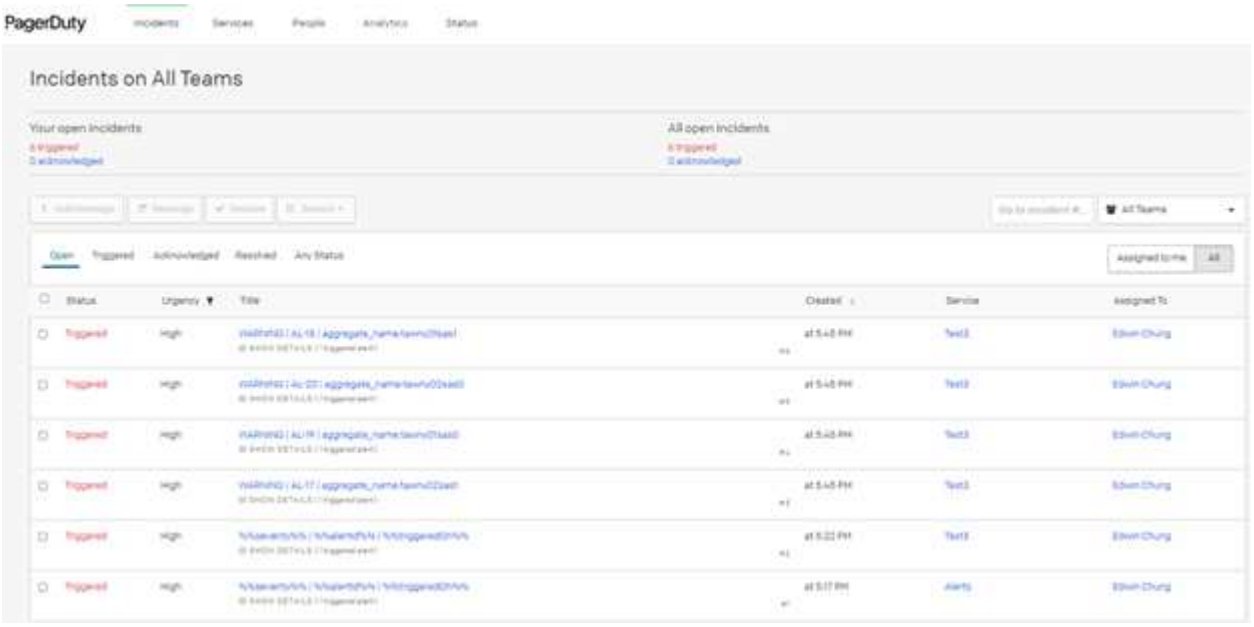
Esta página refere-se a instruções de terceiros, que podem estar sujeitas a alterações. Consulte a "PagerDuty documentação"para obter as informações mais atualizadas.

Configuração PagerDuty:

1. No PagerDuty, navegue até **Serviços > diretório de Serviços** e clique no button novo Serviço*
2. Digite um *Name* e selecione *Use nossa API diretamente*. Clique em *Adicionar serviço*.

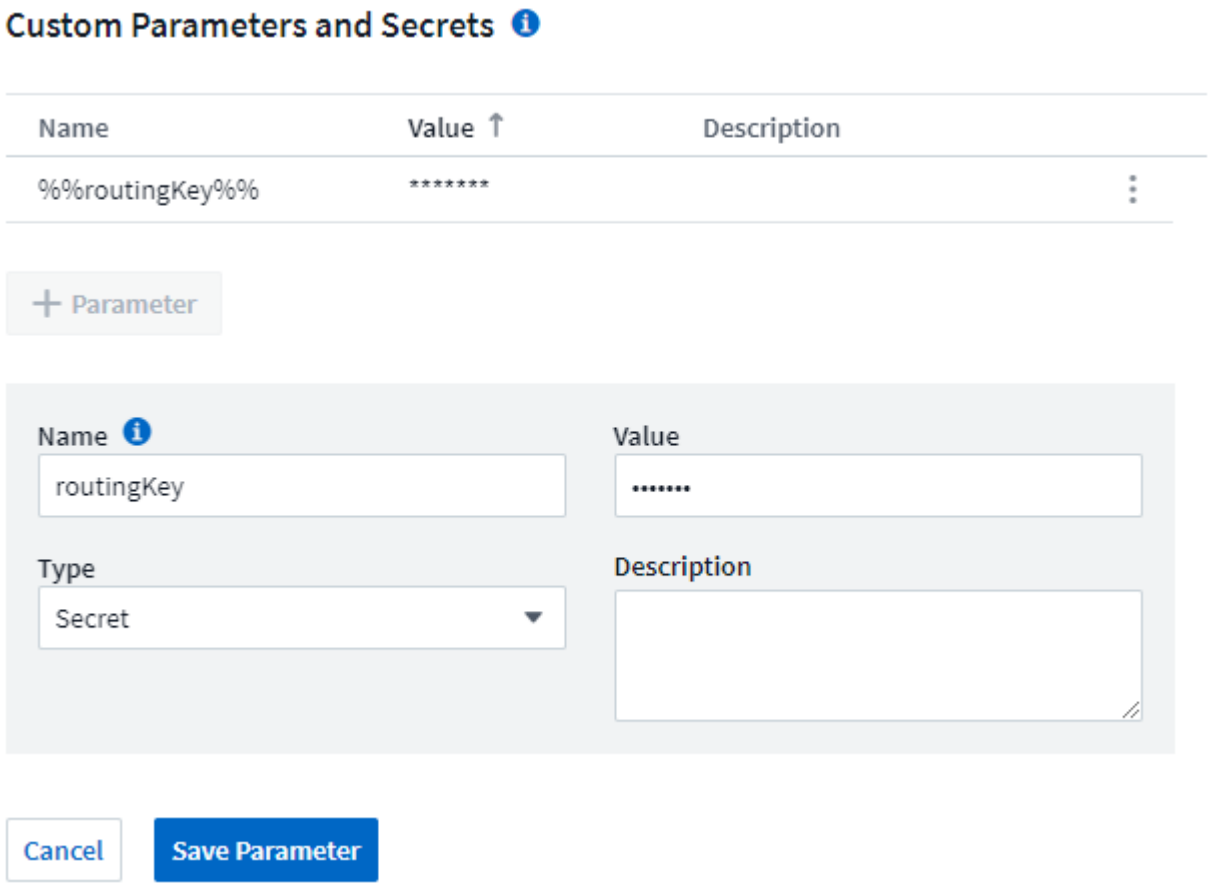


3. Clique na guia *integrações* para ver a **chave de integração**. Você precisará dessa chave quando criar o webhook do Data Infrastructure Insights abaixo.
4. Vá para **incidents** ou **Services** para ver Alertas.



Crie o Webhook do Data Infrastructure Insights:

1. Em 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 críticos e de nível de aviso.
3. Na lista suspensa *Template Type*, selecione **PagerDuty**.
4. Crie um segredo de parâmetro personalizado chamado *routingKey* e defina o valor para o valor PagerDuty *Integration Key* de cima.



Repita estas etapas para criar um webhook "PagerDuty resolve" para eventos resolvidos.

PagerDuty to Data Infrastructure Insights Field Mapping

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

PagerDuty	Insights da infraestrutura de dados
Tecla de alerta	ID de alerta
Fonte	Ativado
Componente	Nome da métrica
Grupo	Tipo Objeto

PagerDuty	Insights da infraestrutura de dados
Classe	Nome do monitor

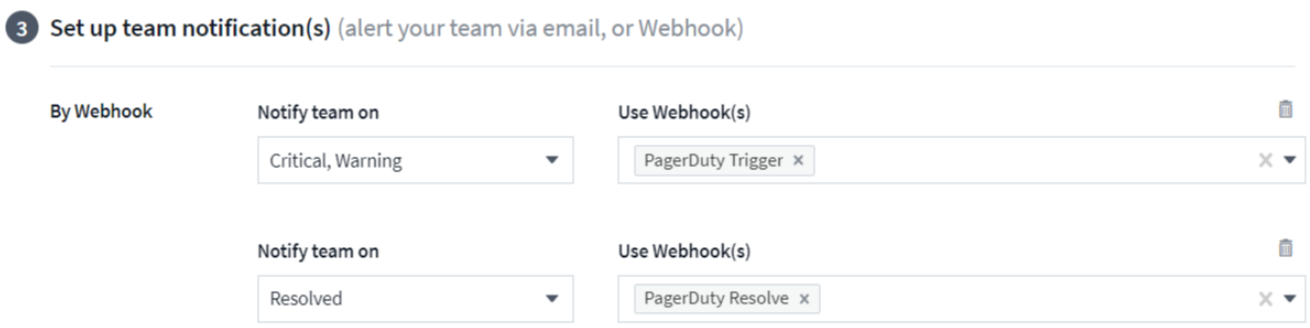
Message Body

```
{
 "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, em Data Infrastructure Insights navegue até **Alertas > monitores** e clique em * Monitor* para criar um novo "monitorar".

- Selecione uma métrica e defina as condições do monitor.
- Em _Configurar notificação(s) da equipe, escolha o método **Webhook** Delivery.
- Escolha o webhook "PagerDuty Trigger" para eventos de nível crítico e de Aviso.
- Escolha "PagerDuty resolve" para eventos resolvidos.



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

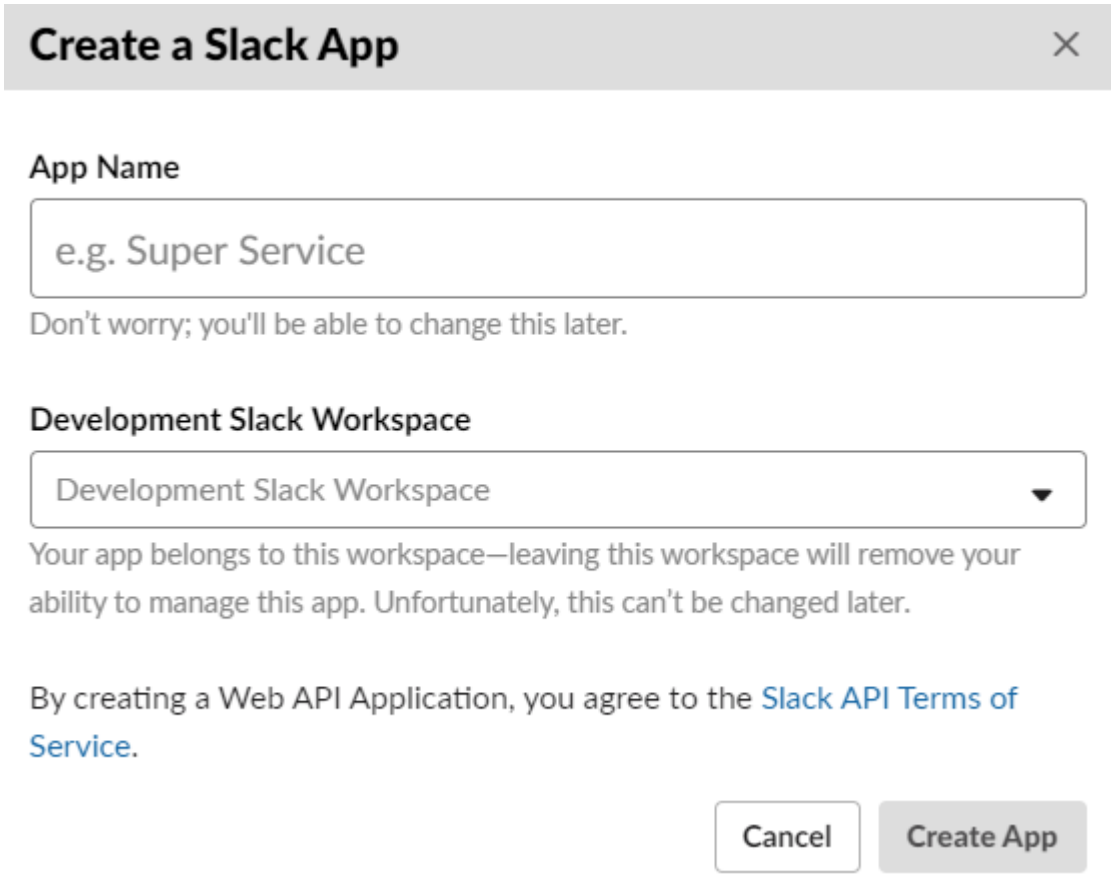
Exemplo de webhook para Slack

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

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

Exemplo do Slack:

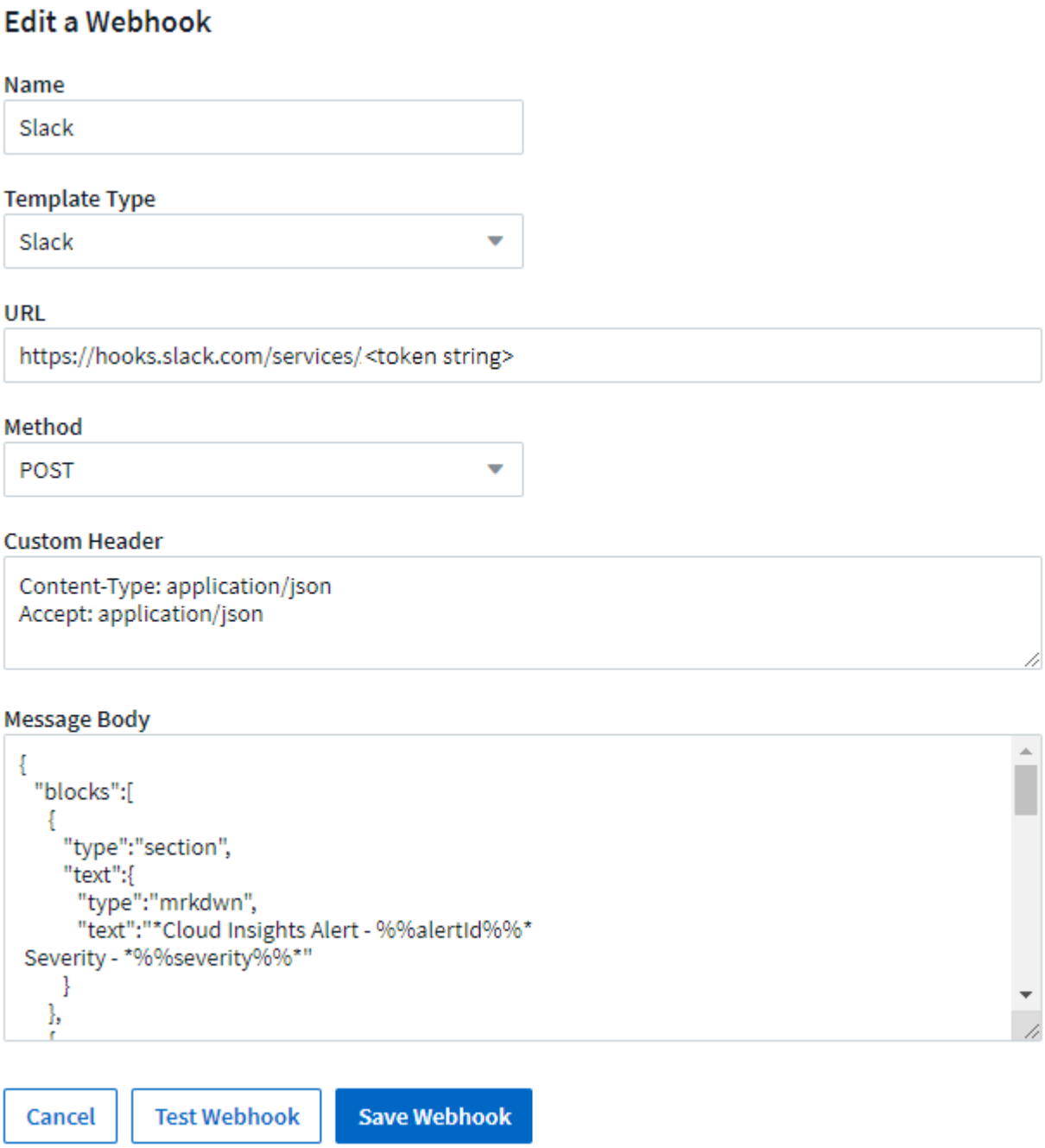
- Vá para https://api.slack.com/apps e crie um novo App Dê a ele um nome significativo e selecione o espaço de trabalho do Slack.



- Vá para Incoming Webhooks, clique em *Activate Incoming Webhooks*, solicite a *Add New Webhook* e selecione o Canal no qual postar.
- Copie o URL do Webhook. Você precisará colar isso na configuração do webhook do Data Infrastructure Insights.

Crie o Webhook do Data Infrastructure Insights:

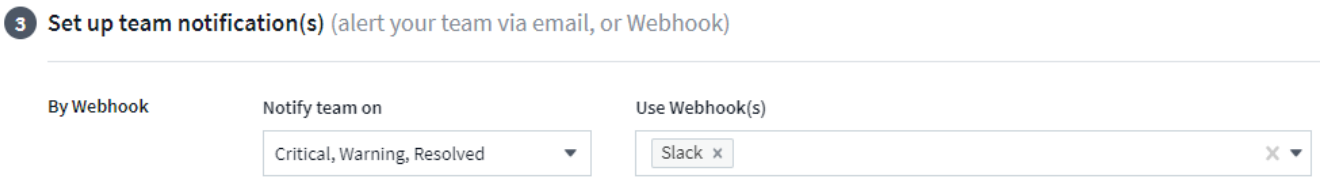
1. Em Data Infrastructure Insights, navegue até **Admin > notificações** e selecione a guia **Webhooks**. Clique em * Webhook* para criar um novo webhook.
2. Dê ao webhook um Nome significativo, como "Slack Webhook".
3. Na lista suspensa *Template Type*, selecione **Slack**.
4. Cole o URL de cima no campo *URL*.



Notificações via Webhook

Para notificar eventos via webhook, em Data Infrastructure Insights navegue até **Alertas > monitores** e clique em * Monitor* para criar um novo "monitorar".

- Selecione uma métrica e defina as condições do monitor.
- Em _Configurar notificação(s) da equipe, escolha o método **Webhook** Delivery.
- Escolha 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

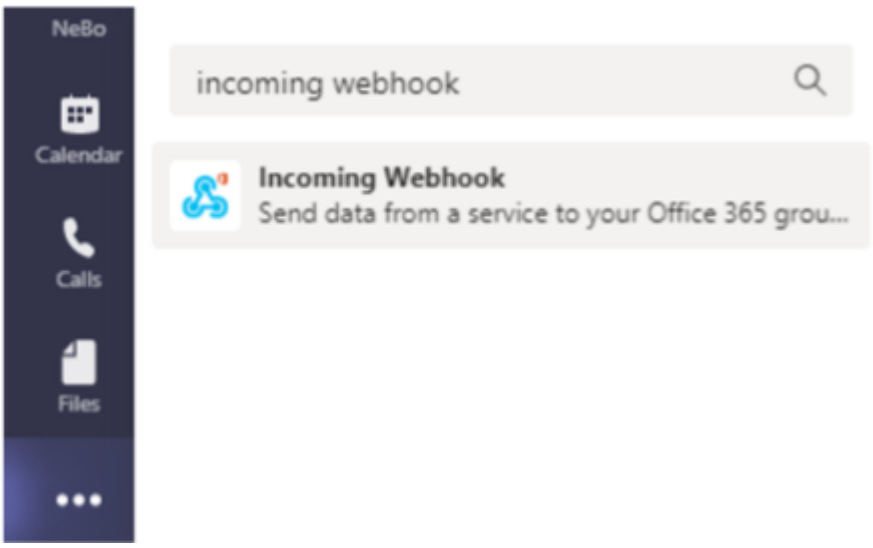
Exemplo de webhook para Microsoft Teams

Webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado. Esta página fornece um exemplo para configurar webhooks para equipes.

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

Configuração equipas:

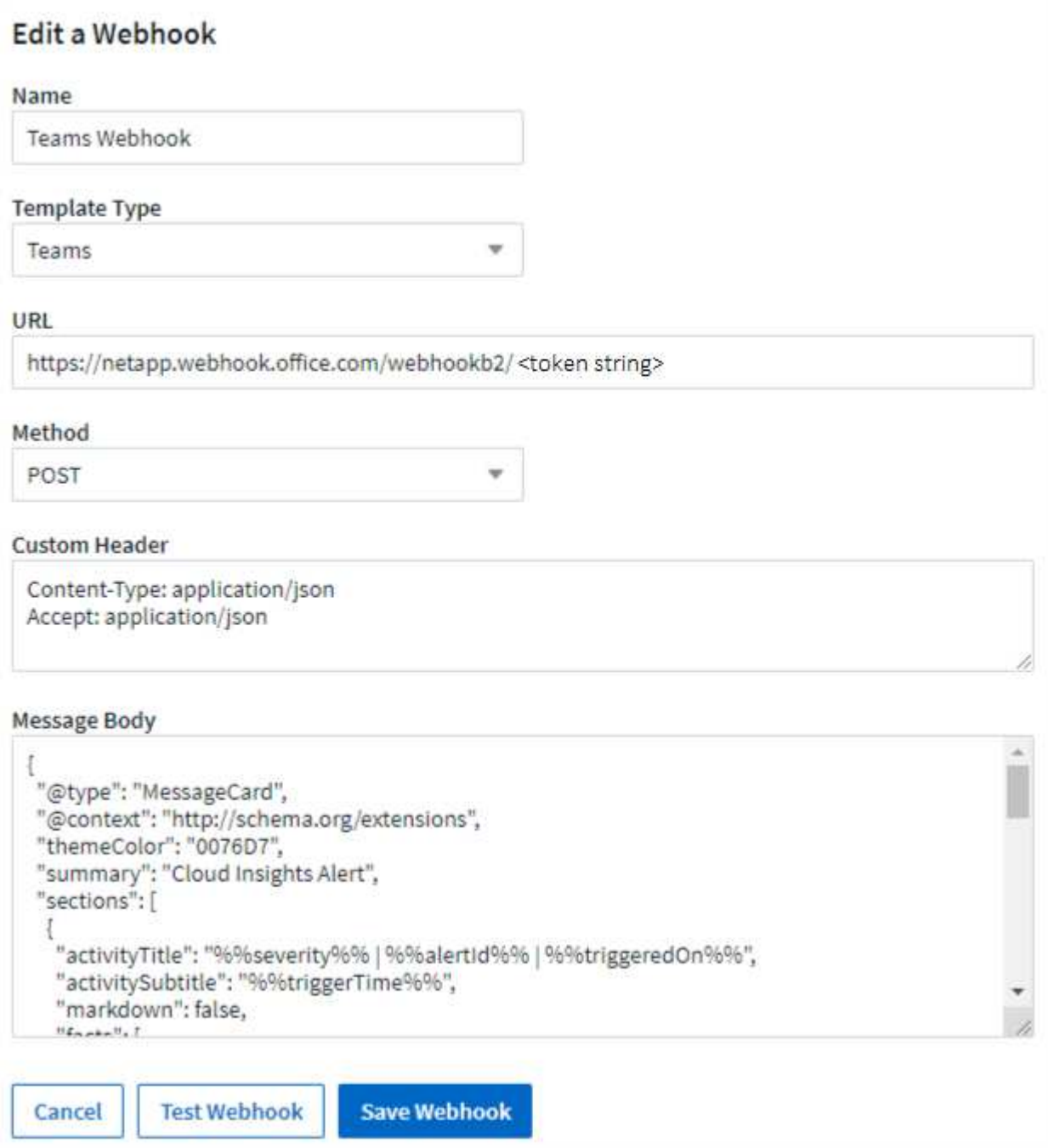
1. Em equipes, selecione o kebab e procure por webhook de entrada.



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

Crie o Webhook do Data Infrastructure Insights:

1. Em 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. Na lista suspensa *Template Type*, selecione **Teams**.

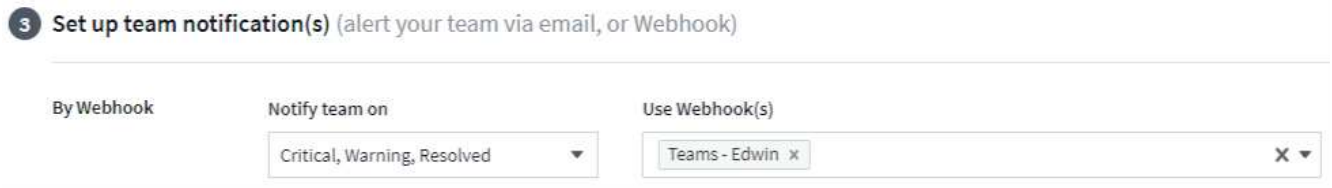


1. Cole o URL de cima no campo *URL*.

Notificações via Webhook

Para notificar eventos via webhook, em Data Infrastructure Insights navegue até **Alertas > monitores** e clique em * Monitor* para criar um novo "monitorar".

- Selecione uma métrica e defina as condições do monitor.
- Em _Configurar notificação(s) da equipe, escolha o método **Webhook** Delivery.
- Escolha o webhook "Teams" para os eventos desejados (crítico, Aviso, resolvido)



Informações sobre direitos autorais

Informações sobre marcas comerciais