Compreender eventos e alertas de desempenho

OnCommand Unified Manager 9.5

NetApp
October 23, 2024

Índice

Compreender eventos e alertas de desempenho

Os eventos de desempenho são notificações que o Unified Manager gera automaticamente quando ocorre uma condição predefinida ou quando um valor do contador de desempenho cruza um limite. Os eventos ajudam a identificar problemas de desempenho nos clusters monitorados.

Você pode configurar alertas para enviar notificações por e-mail automaticamente quando ocorrerem eventos de desempenho de determinados tipos de gravidade.

Fontes de eventos de desempenho

Eventos de performance são problemas relacionados à performance de workload em um cluster. Eles ajudam a identificar objetos de storage com tempos de resposta lentos, também conhecidos como alta latência. Juntamente com outros eventos de saúde que ocorreram ao mesmo tempo, você pode determinar os problemas que podem ter causado ou contribuído para os tempos de resposta lentos.

O Unified Manager recebe eventos de desempenho das seguintes fontes:

- **Eventos de política de limite de desempenho definidos pelo usuário**

  Problemas de desempenho baseados em valores de limite personalizados definidos por você. Você configura políticas de limite de performance para objetos de storage, por exemplo, agregados e volumes, para que eventos sejam gerados quando um valor de limite para um contador de performance for violado.

  Você deve definir uma política de limite de desempenho e atribuí-la a um objeto de storage para receber esses eventos.

- **Eventos de política de limite de desempenho definidos pelo sistema**

  Problemas de performance com base em valores de limite definidos pelo sistema. Essas políticas de limite são incluídas na instalação do Unified Manager para cobrir problemas comuns de desempenho.

  Essas políticas de limite são ativadas por padrão e você pode ver eventos pouco depois de adicionar um cluster.

- **Eventos de limite de desempenho dinâmico**

  Problemas de performance resultantes de falhas ou erros em uma INFRAESTRUTURA DE TI ou de workloads que sobreutilizam recursos de cluster. A causa desses eventos pode ser um problema simples que se corrige ao longo de um período de tempo ou que pode ser resolvido com um reparo ou alteração de configuração. Um evento de limite dinâmico indica que os workloads de volume em um sistema ONTAP estão lentos devido a outros workloads com alta utilização de componentes de cluster compartilhados.

  Esses limites são ativados por padrão e você pode ver eventos após três dias de coleta de dados de um novo cluster.

Tipos de gravidade de eventos de performance

Cada evento de performance está associado a um tipo de gravidade para ajudar você a priorizar os eventos que exigem ação corretiva imediata.

- **Crítica**

  Ocorreu um evento de desempenho que pode levar a interrupção do serviço se uma ação corretiva não for tomada imediatamente.

  Eventos críticos são enviados apenas a partir de limites definidos pelo usuário.

- **Aviso**

  Um contador de desempenho para um objeto de cluster está fora do intervalo normal e deve ser monitorado para garantir que ele não atinja a gravidade crítica. Os eventos desta gravidade não causam interrupções no serviço e podem não ser necessárias ações corretivas imediatas.

  Os eventos de aviso são enviados a partir de limites definidos pelo usuário, definidos pelo sistema ou dinâmicos.

- **Informação**

  O evento ocorre quando um novo objeto é descoberto ou quando uma ação do usuário é executada. Por exemplo, quando qualquer objeto de armazenamento é excluído ou quando há alterações de configuração, o evento com informações de tipo de gravidade é gerado.

  Os eventos de informação são enviados diretamente do ONTAP quando deteta uma alteração de configuração.

Alterações de configuração detetadas pelo Unified Manager

O Unified Manager monitora seus clusters para ver se há alterações de configuração para ajudar você a determinar se uma alteração pode ter causado ou contribuído para um evento de performance. As páginas do Explorador de desempenho apresentam um ícone de alteração de evento (●) para indicar a data e a hora em que a alteração foi detetada.

Você pode revisar os gráficos de desempenho nas páginas do Performance Explorer e na página Detalhes de desempenho/volume para ver se o evento de alteração impactou o desempenho do objeto de cluster selecionado. Se a alteração tiver sido detetada ao mesmo tempo ou em torno de um evento de desempenho, a alteração pode ter contribuído para o problema, o que fez com que o alerta de evento fosse acionado.

O Unified Manager pode detetar os seguintes eventos de mudança, que são categorizados como eventos informativos:

- Um volume se move entre agregados.

  O Unified Manager pode detetar quando a movimentação está em andamento, concluída ou com falha. Se o Unified Manager estiver inativo durante uma movimentação de volume, quando estiver fazendo backup, ele detetará a movimentação de volume e exibirá um evento de mudança para ele.

- O limite de taxa de transferência (Mbps ou IOPS) de um grupo de políticas de QoS que contém uma ou mais alterações de workloads monitorados.

  A alteração do limite de um grupo de políticas pode causar picos intermitentes na latência (tempo de resposta), o que também pode acionar eventos para o grupo de políticas. A latência volta gradualmente ao normal e quaisquer eventos causados pelos picos se tornam obsoletos.

- Um nó em um par de HA assume ou devolve o storage de seu nó de parceiro.

  O Unified Manager pode detetar quando a operação de takeover, takeover parcial ou giveback foi concluída. Se o takeover for causado por um nó em pânico, o Unified Manager não detetará o evento.

- Uma operação de atualização ou reversão do ONTAP foi concluída com êxito.

  São apresentadas a versão anterior e a nova versão.

O que acontece quando um evento é recebido

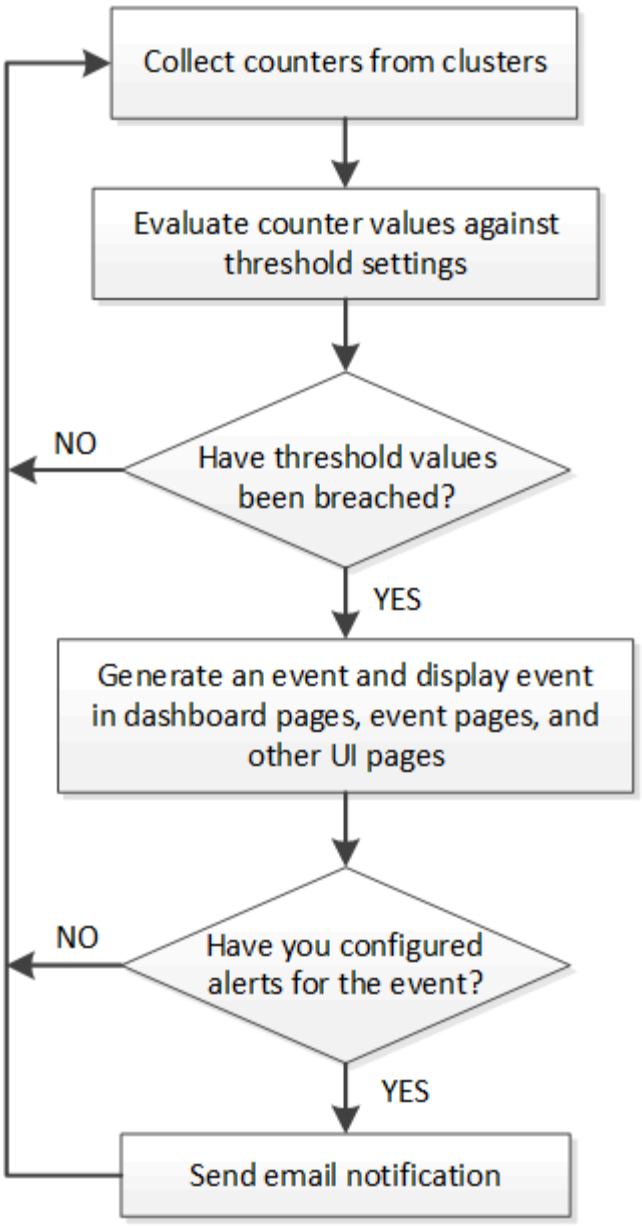
Quando o Unified Manager recebe um evento, ele é exibido na página Dashboards/Overview, nas guias Summary e Explorer da página Performance/Cluster, na página inventário Eventos e na página inventário específico do objeto (por exemplo, a página de inventário de integridade/volumes).

Quando o Unified Manager deteta várias ocorrências contínuas da mesma condição de evento para o mesmo componente do cluster, ele trata todas as ocorrências como um único evento, não como eventos separados. A duração do evento é incrementada para indicar que o evento ainda está ativo.

Dependendo de como você configura as configurações na página Configuração/alertas, você pode notificar outros usuários sobre esses eventos. O alerta faz com que as seguintes ações sejam iniciadas:

- Um e-mail sobre o evento pode ser enviado a todos os usuários do Unified Manager Administrator.
- O evento pode ser enviado para destinatários de e-mail adicionais.
- Um trap SNMP pode ser enviado para o recetor de trap.
- Um script personalizado pode ser executado para executar uma ação.

Este fluxo de trabalho é mostrado no diagrama a seguir.



Quais informações estão contidas em um e-mail de alerta

Os e-mails de alerta do Unified Manager fornecem o tipo de evento, a gravidade do evento, o nome da política violada para causar o evento e uma descrição do evento. A mensagem de e-mail também fornece um hiperlink para cada evento que permite exibir a página de detalhes do evento na IU.

Os e-mails de alerta são enviados a todos os usuários que se inscreveram para receber alertas.

Se um contador de desempenho ou valor de capacidade tiver uma grande alteração durante um período de coleta, isso pode fazer com que um evento crítico e um evento de aviso sejam acionados ao mesmo tempo para a mesma política de limite. Neste caso, você pode receber um e-mail para o evento de aviso e um para o evento crítico. Isso ocorre porque o Unified Manager permite que você se inscreva separadamente para receber alertas de aviso e violações de limites críticos.

Após a atualização para o Unified Manager 7,2 ou superior, os links para eventos e alertas de e-mails enviados de versões mais antigas do Unified Manager não funcionarão mais devido a uma alteração nos URLs de eventos e alertas.

Um exemplo de e-mail de alerta é mostrado abaixo:

From: 10.11.12.13@company.com
Sent: Tuesday, May 1, 2018 7:45 PM
To: sclaus@company.com; user1@company.com
Subject: Alert from OnCommand Unified Manager: Thin-Provisioned Volume Space At Risk (State: New)

A risk was generated by 10.11.12.13 that requires your attention.

Risk - Thin-Provisioned Volume Space At Risk
Impact Area - Capacity
Severity - Warning
State - New
Source - svm_n1:/sm_vol_23
Cluster Name - fas3250-39-33-37
Cluster FQDN - fas3250-39-33-37-cm.company.com
Trigger Condition - The thinly provisioned capacity of the volume is 45.73% of the available space on the host aggregate. The capacity of the volume is at risk because of aggregate capacity issues.

Event details:
https://10.11.12.13:443/events/94

Source details:
https://10.11.12.13:443/health/volumes/106

Alert details:
https://10.11.12.13:443/alerting/1

Adicionar alertas

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

Antes de começar

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

- Você deve ter a função Administrador do OnCommand ou Administrador do armazenamento.

Sobre esta tarefa

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

Passos

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

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

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

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

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

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

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

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

7. Clique em **Salvar**.

Exemplo de adição de um alerta

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

- Nome do alerta: HealthTest
- Recursos: Inclui todos os volumes cujo nome contém "abc" e exclui todos os volumes cujo nome contém "xyz"

- Eventos: Inclui todos os eventos críticos de saúde
- Ações: Inclui "ample@domain.com", um script "Teste", e o usuário deve ser notificado a cada 15 minutos

Execute as seguintes etapas na caixa de diálogo Adicionar alerta:

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

   Você pode configurar um alerta para enviar repetidamente notificações aos destinatários por um tempo especificado. Você deve determinar a hora a partir da qual a notificação de evento está ativa para o alerta.
7. No menu Selecionar Script para execução, selecione **Test** script .
8. Clique em **Salvar**.

Adição de alertas para eventos de desempenho

Você pode configurar alertas para eventos de desempenho individuais, como qualquer outro evento recebido pelo Unified Manager. Além disso, se você quiser tratar todos os eventos de desempenho e mandar e-mails para a mesma pessoa, você pode criar um único alerta para notificá-lo quando quaisquer eventos críticos ou de desempenho de aviso forem acionados.

Antes de começar

Você deve ter a função Administrador do OnCommand ou Administrador do armazenamento.

Sobre esta tarefa

O exemplo abaixo mostra como criar um evento para todos os eventos críticos de latência, IOPS e Mbps. Você pode usar essa mesma metodologia para selecionar eventos de todos os contadores de desempenho e para todos os eventos de aviso.

Passos

1. No painel de navegação esquerdo, clique em **Configuration** > **Alerting**.
2. Na página **Configuração/alertas**, clique em **Adicionar**.
3. Na caixa de diálogo **Adicionar alerta**, clique em **Nome** e insira um nome e uma descrição para o alerta.

4. Não selecione nenhum recurso na página **recursos**.

   Como não há recursos selecionados, o alerta é aplicado a todos os clusters, agregados, volumes e assim por diante, para os quais esses eventos são recebidos.

5. Clique em **Eventos** e execute as seguintes ações:
   a. Na lista gravidade do evento, selecione **Crítica**.
   b. No campo Nome do evento contém, digite `latency` e clique na seta para selecionar todos os eventos correspondentes.
   c. No campo Nome do evento contém, digite `iops` e clique na seta para selecionar todos os eventos correspondentes.
   d. No campo Nome do evento contém, digite `mbps` e clique na seta para selecionar todos os eventos correspondentes.
6. Clique em **ações** e selecione o nome do usuário que receberá o e-mail de alerta no campo **alertar esses usuários**.
7. Configure quaisquer outras opções nesta página para emitir toques SNMP e executar um script.
8. Clique em **Salvar**.

Tipos de políticas de limite de performance definidas pelo sistema

O Unified Manager fornece algumas políticas de limite padrão que monitoram o desempenho do cluster e geram eventos automaticamente. Essas políticas são habilitadas por padrão e geram eventos de aviso ou informações quando os limites de desempenho monitorados são violados.

> As políticas de limite de performance definidas pelo sistema não estão habilitadas em sistemas Cloud Volumes ONTAP, ONTAP Edge ou ONTAP Select.

Se estiver a receber eventos desnecessários de quaisquer políticas de limite de desempenho definidas pelo sistema, pode desativar políticas individuais a partir da página Configuração/gerir Eventos.

Políticas de limite de nó

As políticas de limite de performance de nós definidos pelo sistema são atribuídas, por padrão, a todos os nós dos clusters que estão sendo monitorados pelo Unified Manager:

- **Recursos do nó sobreutilizados**

  Identifica situações em que um único nó está operando acima dos limites de sua eficiência operacional e, portanto, potencialmente afetando as latências de workload. Este é um evento de aviso.

  Para nós instalados com o ONTAP 8,3.x e software anterior, ele faz isso procurando nós que estejam usando mais de 85% de seus recursos de CPU e RAM (utilização de nós) por mais de 30 minutos.

  Para nós instalados com o ONTAP 9.0 e o software posterior, ele faz isso procurando nós que estejam usando mais de 100% da capacidade de performance por mais de 30 minutos.

- **Par de HA de nós sobreutilizado**

  Identifica situações em que os nós de um par de HA estão operando acima dos limites da eficiência operacional do par de HA. Este é um evento informativo.

  Para nós instalados com o ONTAP 8,3.x e o software anterior, ele faz isso analisando o uso da CPU e da RAM para os dois nós no par de HA. Se a utilização combinada de nós dos dois nós exceder 140% por mais de uma hora, o failover de controladora afetará as latências de workload.

  Para nós instalados com o ONTAP 9.0 e o software posterior, ele faz isso analisando o valor da capacidade de performance usada para os dois nós no par de HA. Se a capacidade de performance combinada usada nos dois nós exceder 200% por mais de uma hora, um failover de controladora afetará as latências de workload.

- **Fragmentação de disco do nó**

  Identifica situações em que um disco ou discos em um agregado são fragmentados, retardando os principais serviços do sistema e potencialmente afetando as latências de workload em um nó.

  Ele faz isso observando certas taxas de operação de leitura e gravação em todos os agregados em um nó. Essa política também pode ser acionada durante a ressincronização do SyncMirror ou quando erros são encontrados durante operações de limpeza de disco. Este é um evento de aviso.

  A política ""fragmentação de disco de nós"" analisa agregados somente HDD; agregados Flash Pool, SSD e FabricPool não são analisados.

Políticas de limite de agregado

A política de limite de desempenho agregado definido pelo sistema é atribuída por padrão a todos os agregados nos clusters que estão sendo monitorados pelo Unified Manager.

- **Agregar discos sobreutilizados**

  Identifica situações em que um agregado está operando acima dos limites de sua eficiência operacional, afetando potencialmente as latências de workload. Ele identifica essas situações procurando agregados onde os discos no agregado são mais de 95% utilizados por mais de 30 minutos. Essa política de multicondição então executa a seguinte análise para ajudar a determinar a causa do problema:

  - Um disco no agregado está atualmente em atividade de manutenção em segundo plano?

    Algumas das atividades de manutenção em segundo plano que um disco pode estar passando são a reconstrução de disco, a limpeza de disco, a ressincronização de SyncMirror e a reparidade.

  - Existe um gargalo de comunicação na interconexão Fibre Channel do compartimento de disco?
  - Há muito pouco espaço livre no agregado? Um evento de aviso é emitido para esta política apenas se uma (ou mais) das três políticas subordinadas também forem consideradas violadas. Um evento de desempenho não é acionado se apenas os discos no agregado forem mais de 95% utilizados.

A política de "discos agregados sobre-utilizados" analisa agregados somente HDD e agregados Flash Pool (híbridos); agregados SSD e FabricPool não são analisados.

Políticas de limite de QoS

As políticas de limite de performance de QoS definidas pelo sistema são atribuídas a qualquer workload que tenha uma política de taxa de transferência máxima de QoS ONTAP configurada (IOPS, IOPS/TB ou Mbps). O Unified Manager aciona um evento quando o valor da taxa de transferência de workload é 15% menor do que o valor de QoS configurado.

- * Limite máximo de IOPS ou Mbps de QoS*

  Identifica volumes e LUNs que excederam o limite máximo de IOPS ou taxa de transferência em Mbps de QoS e que estão afetando a latência de workload. Este é um evento de aviso.

  Quando um único workload é atribuído a um grupo de políticas, ele faz isso procurando cargas de trabalho que tenham excedido o limite máximo de taxa de transferência definido no grupo de políticas QoS atribuídas durante cada período de coleta da hora anterior.

  Quando vários workloads compartilham uma única política de QoS, isso acontece adicionando o IOPS ou Mbps de todos os workloads na política e verificando esse total em relação ao limite.

- **IOPS/TB de pico de QoS ou IOPS/TB com limite de tamanho de bloco**

  Identifica volumes que excederam o limite de taxa de transferência de IOPS/TB de pico de QoS adaptável (ou IOPS/TB com limite de tamanho de bloco) e que estão afetando a latência de workload. Este é um evento de aviso.

  Ele faz isso convertendo o limite máximo de IOPS/TB definido na política de QoS adaptável em um valor máximo de IOPS de QoS com base no tamanho de cada volume e, em seguida, busca volumes que excederam o IOPS máximo de QoS durante cada período de coleta de desempenho da hora anterior.

  > Essa política é aplicada a volumes somente quando o cluster é instalado com o ONTAP 9.3 e o software posterior.

  Quando o elemento ""tamanho do bloco"" foi definido na política de QoS adaptável, o limite é convertido em um valor de Mbps máximo de QoS com base no tamanho de cada volume. Em seguida, ele procura volumes que excederam o QoS máximo Mbps durante cada período de coleta de desempenho para a hora anterior.

  > Essa política é aplicada a volumes somente quando o cluster é instalado com o software ONTAP 9.5 e posterior.

Informações sobre direitos autorais

Informações sobre marcas comerciais